

Lighting the way to...
Charleston

2017 Winter Meeting

March 6 - 10, 2017

Charleston, South Carolina



Lighting the way to...

Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10



Table of Contents

EDUCATIONAL SESSIONS

EMPLOYMENT PRACTICES AND WORKPLACE LIABILITY

Employers, “You can’t have any pudding if you don’t eat your alphabet soup!” The regulatory agencies are filling your plate with rules to digest.....	4

CLASS ACTION AND MULTIDISTRICT LITIGATION AND TRIAL TACTICS, PRACTICE AND PROCEDURE SECTIONS

Amended Rules of Civil Procedure - How They are Being Implemented.....	21

ENERGY AND UTILITIES LAW

When Everything Goes Black: The Cyber-Threat to Our Energy Infrastructure.....	44

EXTRA CONTRACTUAL LIABILITY

Defending Against Attorney’s Fee Requests.....	74

INTERNATIONAL PRACTICE AND LAW

Window on Europe - Brexit.....	84

TRANSPORTATION AND PRODUCTS LIABILITY SECTIONS

Follow-Up on Autonomous Vehicles.....	96

PLENARY PROGRAM

Best Practices When Dealing with Reptiles.....	147

PLENARY PROGRAM

What is your Tech Strategy?.....	175

PLENARY PROGRAM

Closing Remarks - Leaving the Best Impression.....	199

Trial Technology Learning Laboratory.....	209

CIVIL RIGHTS AND PUBLIC ENTITY LIABILITY

Balancing Interests in an Armed Society.....	233

CONSTRUCTION LAW and PROFESSIONAL LIABILITY SECTIONS

What lies beneath - Beware the Meaning and Implications of “Incorporation by Reference”.....	281

HEALTHCARE PRACTICE and LIFE, HEALTH & DISABILITY SECTIONS

Telemedicine Liability and Compliance.....	287

DRUG, DEVICE & BIOTECHNOLOGY

Promotional Claims: Off-Label Promotion and Debunking the Theory and Defending the Claim.....	299

PREMISES AND SECURITY LIABILITY

Current Trends in Negligent Security Defense.....	316

Table of Contents

INTELLECTUAL PROPERTY, COMMERCIAL LITIGATION and ALTERNATIVE DISPUTE RESOLUTION SECTIONS	
“Can You Keep a Secret?” The Federal Courts Can Help.....	327
Trial Technology Learning Laboratory.....	356
LAW PRACTICE MANAGEMENT	
Succession Planning: Protecting Your Firm and Your Clients’ Legal Interests in Times of Transition.....	380
INSURANCE COVERAGE	
When a Disaster Turns the Insured’s Address into the Boulevard of Broken Dreams, Does Business Interruption Coverage Become Contentious?.....	392
TOXIC TORTS AND ENVIRONMENTAL LAW	
A Tsunami of Rising Water Litigation.....	442
APPELLATE LAW	
Legal Writing in the Electronic Age.....	479
DATA BREACH, PRIVACY AND CYBER INSURANCE LAW	
What’s Hot and the Impact of Technology Competence Comment 8 to the ABA Model Rules.....	514
PLENARY PROGRAM	
Part I - Cool Kids Go International.....	565



WEDNESDAY, MARCH 8, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

EMPLOYMENT PRACTICES AND WORKPLACE LIABILITY

Employers, “You can’t have any pudding if you don’t eat your alphabet soup!” The regulatory agencies are filling your plate with rules to digest.

Colleton

Moderator:

Paul M. Finamore

Speakers:

Jeff Kelsey

Helen R. Holden

Caroline J. Berdzik

William E. Vita

Committee: Employment Practices and Workplace Liability Section

Title: “Employers, you can’t have any pudding if you don’t eat your alphabet soup!” The Regulatory Agencies are filling your plate with rules to digest.

The panel will review the new regulations from the federal agencies that seem to be published daily. From the DOL to OSHA, the agencies are affecting the manner in which businesses handle issues from pay to safety and drug testing. The panel will discuss what businesses need to know to stay compliant, how to update handbooks, and areas of growing scrutiny.

Format: 60 minute roundtable discussion led by moderator

Moderator: Paul M. Finamore
Niles, Barton, & Wilmer, LLP
111 South Calvert St., Suite 1400
Baltimore, MD 21202
410 783-6349
pmfinamore@nilesbarton.com

AV: Projector and Screen for PowerPoint presentation

Presenters: Jeff Kelsey
Federal Express Corp.
Managing Director – Employment Law
3620 Hacks Cross Rd., Building B
Memphis, TN 38125
jkelsey@fedex.com

Helen R. Holden
Sacks Tierney P.A.
4250 N. Drinkwater Blvd., Fourth Floor
Scottsdale, AZ 85251
Telephone 480.425.2611
Helen.Holden@sackstierney.com

Caroline J. Berdzik, Esq.
Goldberg Segalla
902 Carnegie Center, Suite 100
Princeton, NJ 08540-6530
cberdzik@goldbergsegalla.com

William E. Vita, Esq.
Westerman Ball Ederer Miller Zucker & Sharfstein, LLP
1201 RXR Plaza
Uniondale, New York 11556
wvita@westermanllp.com

Written Materials: Paper to be prepared by panel

***“Employers, you can’t have any pudding if you don’t eat your alphabet soup!”
The Regulatory Agencies are filling your plate with rules to digest.***

Employment Practices and Workplace Liability Section

Paul M. Finamore
Niles, Barton, & Wilmer, LLP
111 South Calvert St., Suite 1400
Baltimore, MD 21202

Jeff Kelsey
Federal Express Corp.
Managing Director – Employment Law
3620 Hacks Cross Rd., Building B
Memphis, TN 38125

Helen R. Holden
Sacks Tierney P.A.
4250 N. Drinkwater Blvd., Fourth Floor
Scottsdale, AZ 85251

Caroline J. Berdzik
Goldberg Segalla
902 Carnegie Center, Suite 100
Princeton, NJ 08540-6530

William E. Vita, Esq.
Westerman Ball Ederer Miller Zucker
& Sharfstein, LLP
1201 RXR Plaza
Uniondale, New York 11556

Introduction and Caveat

Under the Obama Administration, the regulatory agencies have been very active, issuing new regulations that have sought to accomplish the priorities set by President Obama. Many of the regulations have directly affected employers, requiring employers to revise practices, publish updated policies, review employment classification, and update pay policies. Free of the Congressional gridlock due to partisan politics, the agencies have been moving forward with the regulatory process without having to wait on Congress to amend or create law.

This paper starts with a caveat that some or most of it could be obsolete by the time that it goes to print. On Inauguration Day, January 20, 2017, much like has been on many inauguration days before it, the White House issued a memorandum, this time by Chief of Staff Reince Priebus, which he directed each department head and federal agency to freeze the regulatory process pending review by an appointee of President Trump. The memorandum applies to proposed or pending regulations in the following manner:

1. For regulations that have not been sent to the Office of the Federal Register, departments and agencies are to send no regulation to it, subject to certain exceptions by the Director of the Office of Management and Budget;

2. Subject to the same exceptions, for regulations that have been sent to the Federal Register but not published, the regulations are to be withdrawn immediately; and,
3. For regulations that have been published in the Federal Register, departments and agencies are to temporarily postpone their effective dates, consistent with law, for a sixty-day period.

The memorandum does not affect regulations that are already in effect. To make changes to existing regulations will require an Act of Congress or further actions by the appropriate department or agency to initiate the regulatory process to effect changes to the existing regulations.

Employers will need to wait to see what priorities are established by President Trump, who runs the different federal departments and agencies, and how and whether new, proposed and existing regulations will be affected. Stay tuned to stay compliant.

www.worker.gov and Its Implications

Employers who question the myriad of government agencies regulating them, they need only look to www.worker.gov, which promises: “You have rights. We’ll help you exercise them. This site is dedicated to the needs of workers and is designed to improve based on your input,” published by the Department of Labor, National Labor Relations Board, Department of Justice and the Equal Employment Opportunity Commission. After indicating their employment status, a viewer is led to another screen where they are offered to answer questions regarding various employment issues, after which they are offered the opportunity to click on a link that takes them to the appropriate agency with which to file a complaint. It is one-stop shopping for an employee, supported by federal agencies, to get the claim process started. To avoid choking on the alphabet soup, Employers need to become educated on their areas of risk. To enjoy their pudding, Employers need to put processes in place to ensure compliance and to protect them from unknown risks and claims.

Independent Contractor V. Employee

The issue of misclassification of workers as independent contractor as opposed to employee has been a topic of increasing interest since the recession when many unemployment divisions faced financial challenges arising out of unfunded claims, some of which relate to this misclassification. Many state and federal agencies, from the Department of Labor to the Internal Revenue Service, focused on the issue. Last summer, the Department of Labor added a section to its website along with a publication entitled, “Misclassification Mythbusters.” The General Counsel of the National Labor Relations Board issued an Advice Memorandum in late summer that set forth his opinion that misclassification could be an unfair labor practice to the extent that it affected an employee’s Section 7 rights. The focus on this issue is only seemingly increasing. In the Fair Pay and Safe Workplace Safety Rule, which will be discussed below, government contractors are required to include whether a worker is an independent contractor or employee. Similarly, the EEOC included discussion of independent contractors in its Strategic Enforcement Plan, which will be discussed below.

As noted by the 3rd Circuit recently, the issue of the appropriate classification of workers as employees or independent contractors is “a classic and reoccurring issue in American law.” *Williams v. Jani-King of Philadelphia Inc.*, 837 F.3d 314, 316 (3d Cir. 2016). And, in recent years, federal regulators have embarked upon a number of strategic initiatives to address what the Department of Labor viewed as a serious issue. In July, 2015, for example, the U.S. Wage and Hour Administrator issued an Administrator's Interpretation addressing the issue of misclassification of workers as independent contractors, noting that “most workers are employees under the [Fair Labor Standards Act],” and discussing the economic realities test at length. U.S. Department of Labor, Wage and Hour Division, Administrator's Interpretation No. 2015-1, July 15, 2015, “The Application of the Fair Labor Standards Act's ‘Suffer or Permit’ Standard in the Identification of Employees Who Are Misclassified as Independent Contractors,” (the “Misclassification AI”), available at: <http://www.dol.gov/WHD/opinion/adminIntrprtnFLSA.htm> at 2. It should be noted that the Supreme Court has recently held that the Administrator's Interpretations applying the FLSA have, in effect, the force of law. See *Perez v. Mortgage Bankers Ass’n*, ___ U.S. ___, 135 S. Ct. 1199 (2015).

Employers have questioned whether the enforcement initiatives under which independent contractor classification will continue under the Trump Administration, as most employers view the enforcement efforts of recent years as very aggressive. Experience shows that Department of Labor investigations into independent contractor misclassification are difficult to manage, as companies utilizing independent contractors frequently do not maintain the records for these workers that they would routinely maintain if the workers were classified as employees.

The issues with aggressive enforcement and compliance challenges in recent years aside, it should be noted that the Fair Labor Standards Act (“FLSA”) was originally enacted in the late 1930s, and contains a very broad definition of employment: to “suffer or permit to work.” 29 U.S.C. § 203(g). Moreover, the economic realities test discussed in the 2015 Misclassification AI has been utilized since at least 1961. *Goldberg v. Whitaker House Coop., Inc.*, 366 U.S. 28 (1961). Thus, the statute itself is unlikely to change, although recently promulgated regulations under the statute have been enjoined. *Nevada v. United States Dep’t of Labor*, 4:16-CV-00731, 2016 WL 6879615, at *6 (E.D. Tex. Nov. 22, 2016) (holding that “With the Final Rule, the Department exceeds its delegated authority and ignores Congress's intent by raising the minimum salary level such that it supplants the duties test.”) (appeal pending).

What, then, to expect under the Trump Administration? As one former Administrator of the Wage and Hour Division recently quipped, “Republicans do enforce; after all, we are the law-and-order party.” “Shift in Wage and Hour Enforcement may not be Radical,” by Martin Berman Gorvine, found at <https://www.bna.com/shift-wageandhour-enforcement-n73014449930/> (January 18, 2017) (quoting Tammy McCutchen). As many experts are predicting, the new Wage and Hour Division is likely to change its enforcement emphasis, returning to pursuit of employee complaints, limitations on strategic initiatives, and a willingness to negotiate over findings of willfulness, so that liquidated damages and three year limitations periods may not be insisted upon in every case. Employers would do well to remember, however, that FLSA litigation—particularly collective action litigation—continues to increase. According to one report, more than sixty

percent of in-house legal departments are currently defending at least one class action lawsuit.¹ Nearly a quarter of these class or collective actions are labor and employment related. As a result, employers must continue to be proactive in ensuring that they classify employees appropriately.

Employee Safety

The regulations issued under the Occupational Safety and Health Act have required employers to maintain records of workplace injuries for many years. In 2016, a new rule made explicit what the Occupational Safety and Health Administration contends was always implicit in its rules: a requirement that employers “have a reasonable procedure for employees to report work-related injuries and illnesses.” October 19, 2016 Memorandum to Regional Administrators from Dorothy Dougherty, Deputy Assistant Secretary of Labor, found at https://www.osha.gov/recordkeeping/finalrule/interp_recordkeeping_101816.html. Another new provision prohibits discrimination or retaliation against employees who report workplace injuries. Initially scheduled to go into effect in August, OSHA delayed implementation of these rules until December, 2016.

The regulation at 29 C.F.R. § 1904.35 was amended to add two new provisions: section 1904.35(b)(1)(i), and section (b)(1)(iv). These regulations require employers to:

- ensure that the procedure for reporting illnesses and injuries is reasonable such that it not deter employees from reporting;
- refrain from retaliating against employees for reporting; and
- tell employees that they will not be retaliated against if they report an injury or illness.

While the anti-retaliation requirement is not new, OSHA also established a new mechanism to enforce it. Previously, OSHA could pursue these issues only upon employee complaint; now, OSHA can pursue an employer for discrimination or retaliation *even if the employee does not complain*. Upon finding that an employer did discriminate or retaliate, OSHA may issue steep penalties of up to \$12,471 per violation or, for willful violations, up to \$124,712.

In its interpretive guidance, OSHA cited concerns with three employer policy areas that it contended could discourage reporting: disciplinary policies, post-accident drug testing policies, and employee incentive programs. In its guidance on the subject of disciplinary policies, OSHA stressed that its rule does not prohibit employers from disciplining employees who “violate legitimate safety rules or reasonable reporting procedures.” https://www.osha.gov/recordkeeping/finalrule/interp_recordkeeping_101816.html. Instead, the agency explains, employers may not discipline employees “simply because they report a work-related injury or illness.” *Id.*

Another source of potential employer liability under this rule is post-injury drug testing. In its comments to this regulation, OSHA stated that a policy or practice of automatic testing after

¹ <http://classactionsurvey.com/pdf/2016-class-action-survey.pdf>.

every accident is *per se* retaliatory. An exception exists if the drug testing is done in compliance with other regulations, such as testing required for drivers' subject to Department of Transportation regulation. It is OSHA's position that blanket post-injury drug-testing policies deter proper reporting by employees and can be a form of adverse action against employees, and that drug testing, which is designed in a way that may be perceived as punitive or embarrassing to the employee, is likely to deter injury reporting. In order to address this concern, drug testing policies should be reviewed to ensure that no *automatic* post-injury testing occurs. Rather, testing should be based upon all of the circumstances present, and there should be a reasonable possibility that drug or alcohol use by the reporting employee was a contributing factor to the reported injury or illness if the employer will be testing.

Finally, OSHA noted concerns over safety incentive programs. The agency states that:

Withholding a benefit—such as a cash prize drawing or other substantial award—simply because of a reported injury or illness would likely violate section 1904.35(b)(1)(iv) regardless of whether such an adverse action is taken pursuant to an incentive program. Penalizing an employee simply because the employee reported a work-related injury or illness without regard to the circumstances surrounding the injury or illness is not objectively reasonable and therefore not a legitimate business reason for taking adverse action against the employee.

Id. The example in the interpretive guidance notes that the rule “does not prohibit safety incentive programs. Rather, it prohibits taking adverse action against employees simply because they report work-related injuries or illness.” The interpretive guidance can be found at https://www.osha.gov/recordkeeping/finalrule/interp_recordkeeping_101816.html.

Employer Takeaways

1. Ensure Employers understand that they may not discipline employees solely for reporting workplace accidents.
2. Review any drug testing policy and ensure that it indicates that the employer “may” (not “must”) test post-accident, unless a state worker’s compensation or other regulation requires post-accident testing.
3. Advise employees that they have the right to report work-related injuries and illnesses.
4. Advise employees that they may report injuries without retaliation.
5. Advise employees that the Company will not discharge or in any manner discriminate against them for reporting work-related injuries or illnesses.
6. When a workplace accident occurs, before testing, determine whether there is a reasonable basis to believe that impairment could have contributed to the incident.
7. When reasonable basis exists, require that two supervisors be present observe the basis and that the supervisors document their observations in writing.
8. Review accident reporting requirements; if they are overly burdensome, revise them to avoid the appearance of retaliation, be very cautious in disciplining employees for late reporting of an accident.
9. Ensure that implementation of safety incentive programs is consistent with the intention of the rule.

Fair Pay and Safe Workplaces (“Blacklisting”) Executive Order

On August 25, 2016, the Federal Acquisition Regulatory Council (FAR Council) and the U.S. Department of Labor (DOL) published the final rule and guidance implementing President Barack Obama’s Executive Order 13673 addressing “Fair Pay and Safe Workplaces,” often referred to as the “blacklisting” Executive Order.

Blacklisting

The blacklisting rule requires self-disclosure by contractors and subcontractors pre-award, which becomes part of the government’s review of responsible bidders. Once fully implemented, the final rule will require contractors and subcontractors to disclose any violations of 14 enumerated federal labor laws, Executive Orders, and their state law equivalents, in the previous three years. Contractors need only disclose violations for the legal entity that holds the specific government contract or subcontract. Contractors that are awarded contracts must update their violation information every six months for the duration of the contract. Depending upon the self-disclosures, the government agency is authorized to enter into agreements that could involve remedial measures, compliance assistance, and resolution of issues to assist in avoidance of further violations. The rule also provides for certain remedies such as decisions not to exercise an option on a contract, contract termination, or potentially debarment.

For all relevant laws, three specific types of violations requiring self-disclosure include arbitral awards or decisions, civil judgments, and “administrative merits determinations.” The applicable laws and orders include:

- Fair Labor Standards Act (FLSA)
- Occupational Safety and Health Act (OSHA)
- National Labor Relations Act (NLRA)
- Migrant and Seasonal Agricultural Worker Protection Act (MSPA)
- Davis-Bacon Act (DBA)
- Service Contract Act (SCA)
- Executive Order 13658 (establishing a minimum wage for contractors)
- Executive Order 11246 (establishing nondiscriminatory hiring and employment practices for contractors)
- Section 503 of the Rehabilitation Act
- Vietnam Era Veterans’ Readjustment Assistance Act (VEVRAA)
- Family Medical Leave Act (FMLA)
- Title VII of the Civil Rights Act of 1964
- American’s with Disabilities Act (ADA)
- Age Discrimination in Employment Act (ADEA)

At this time, the only state law for which violations must be disclosed is the state law equivalents of OSHA.

Implementation

The final rule was originally intended to take effect October 25, 2016, and its key requirements would have been phased in over the course of the next year:

- For the first year the rule is in effect, (originally October 25, 2016, through October 24, 2017), only prime contractors are required to disclose their violations. Subcontractors do not begin reporting until October 25, 2017.
- For the first six months the rule is in effect, (through April 24, 2017), disclosure is required only for contracts of \$50 million or more. The disclosure threshold drops to \$500,000 on April 25, 2017.
- When the final rule takes effect, the “look-back” period for which violations must be reported is only one year. The look-back period gradually increases until it reaches a full three years on October 25, 2018.

Violation Reporting Process

Contractors will use an existing online system, the General Services Administration’s System for Award Management (SAM), to report violations. The violation information will be publicly viewable. For each violation, contractors are required to disclose the following:

- The law violated;
- The case number or other unique identification number;
- The date of determination, judgment, award, decision;
- The name of the court, arbitrator, agency, board, or commission that rendered the decision;
- Mitigating information is optional.

Agency Review

The violation information will be reviewed by an agency contracting officer who will make a determination about whether the contractor is responsible and therefore eligible to contract with the government. The final rule requires each contracting agency to designate an agency labor compliance advisor (ALCA) to implement the reporting framework. ALCA’s will analyze the violation and mitigation information submitted by contractors, categorize violations as serious, repeated, willful, or pervasive, and write a report and recommendation that helps the contracting officer in making a responsibility determination.

ALCAs will also help contractors take steps to come into compliance, recommend the establishment of remedial labor compliance agreements (LCAs), and serve as contract points for third parties who wish to share information about a contractor’s labor violations.

For its part, the Department of Labor is required to issue guidance to contracting agencies to assist them in determining whether violations of the labor laws were "serious, repeated, willful or pervasive."

Preliminary Injunction Precludes Implementation of the Blacklisting Rule

On October 24, 2016, the U.S. District Court for the Eastern District of Texas issued a [nationwide preliminary injunction](#) that prevents the FAR Council from implementing the final blacklisting rule. Specifically, the court's decision blocks the federal government from implementing any provision of the [FAR Rule](#) or the [DOL's guidance](#) relating to the new reporting and disclosure requirements. As a result, these provisions of the final blacklisting rule did not go into effect on October 25. However, the preliminary injunction does not block implementation of the paycheck transparency provisions of the final rule.

Employer Takeaways

Notwithstanding the injunction, Employers should consider whether they should be undertaking steps to prepare themselves for future self-disclosures. The steps include both short- and long-term efforts.

- Implement training such as harassment prevention and workplace safety
- Review employment handbooks and policies to ensure compliance with the laws that are the subject of self-disclosure
- Publish policies for early resolution of employee claims, including procedures for reporting of employee complaints, correction of wage complaints, accommodation of disabilities and leave issues
- Review recordkeeping systems and record retention policies
- Audit complaints within the last 3 years to identify trends, problem areas and implement targeted policies to improve identified deficiencies

Paycheck Transparency

Effective January 1, 2017, prime contractors and subcontractors must provide detailed wage statements each pay period to all workers for whom the contractor is required to maintain wage records. The wage statement must contain hours worked, overtime hours, pay, and any additions to or deductions from pay, including notice of any independent contractor relationship and overtime exemptions to their covered workers. The wage statement requirements are substantially similar to what is already required in New York and California.

Paid Sick Leave for Federal Contractors

President Obama signed Executive Order 13706 on September 7, 2015. The Order requires federal contractors to provide their employees with up to seven days of paid sick leave annually. This is precisely the type of Executive Order that President Trump may vacate, as it is burdensome to businesses. On the other hand, President Trump is in favor of requiring employers to provide

six weeks of paid maternity leave, so perhaps he will not be so fast to overturn this Executive Order.

The Order applies to contracts awarded or solicited after January 1, 2017. The Order identifies four main categories of contracts: construction contracts; service contracts; concession contracts; and contracts in connection with federal property or lands. There are a few minor exemptions, for example, construction contracts worth less than \$2,000. But for the most part, any business entity doing business with the federal government will have to comply.

The Department of Labor has decreed that this Executive Order applies to any employee “engaged in performing work on or in connection with the contract covered by the Executive Order...” Thus, in theory, a corporation with Federal Contracts awarded to one department would not, necessarily, have to provide seven days of paid sick leave to employees working in other departments, not engaged in government work. It also exempts employees who spend less than 20% of their work week performing government work. However, although these exemptions may exist in theory, any employer would be faced with practical difficulties in providing seven days of paid sick leave to the group of employees who work on government contracts while excluding other employees. Such a discrepancy in treatment is not likely to improve employee morale for those employees who are not eligible. For these reasons, many expect that contractors performing both government and non-government work will implement policies providing paid sick leave to all employees. Undoubtedly, this is the outcome sought by the government and, indeed, the Department of Labor estimates that the Executive Order will provide paid sick leave to nearly 437,000 employees of federal contractors who currently receive no paid sick leave, whatsoever.

The sick leave would be accrued at the rate of one hour per every 30 hours worked. The contractors would be permitted to limit the sick leave of their employees to 56 hours each year when that amount was accrued.

The Executive Order specifies that the paid sick leave may be used for absences resulting from: (1) physical or mental illness, injury or medical condition; (2) obtaining a diagnosis or care from a healthcare provider; (3) caring for the employee’s child, parent, spouse, domestic partners, or other person who is “the equivalent of a family relationship;” or (4) the victim of domestic violence, sexual assault or stalking (such injuries would already seem to be encompassed in subparagraph (1) but they are specified anyway).

The Executive Order addresses when the employee needs to document that the leave qualifies as sick leave. For example, a certification is required when the employee is absent for three or more consecutive days. The employer can deny the paid sick leave request, but any denial must be made in writing and include the reason for the denial. There is no mention of an appeal process if a request is denied, nor are any suggested reasons for denial provided. Given that an employer may not request documentation for absences less than three days, it is difficult to imagine how an employer could deny a request for leave of less than three days. When the request for sick leave involves domestic violence, sexual assault or stalking, the employer is only entitled to the minimum information necessary to establish the need for the sick leave.

Obviously, this Executive Order affects the myriad of American companies that contract, in some way, with the federal government. The Order, however, may be even broader than that. Even for employers who have no federal contracts, recruitment and retentions standards may require that they match competing companies that do. For valued employees or those in competing industries, seven days of annual paid sick leave may become the accepted standard in the American economy.

An Overview of the EEOC's 2017-2021 Strategic Enforcement Plan (SEP) and What It Means for Employers

In Fall 2016, the U.S. Equal Employment Opportunity Commission (EEOC) released an updated Strategic Enforcement Plan (SEP) for Fiscal Years 2017-2021. The EEOC initially provided a SEP in 2012 for the years covering 2013-2016, which attempted to provide more transparency in terms of the EEOC's targeted focus areas and tried to reconcile some of the inconsistencies in process and case handling from the various district offices. It goes without saying that the last four years of activity at the EEOC can be characterized as unprecedented and exceedingly aggressive. Not surprisingly, the new SEP does not back down from some of these controversial priorities. However, the SEP was released prior to the outcome of the U.S. Presidential election, and it will be interesting to see how much deviation will occur from the SEP based on Trump Administration appointees and priorities.

The purported goal of the SEP is to sharpen the agency's areas of focus and update the plan to recognize additional areas that require attention. While developing the SEP, the EEOC was guided by three principles: 1) a targeted approach focused on priorities where government efforts can have a strategic impact; 2) an integrated approach that has collaboration, coordination and consistency; and 3) a sense of accountability that takes ownership to achieve results given existing resources.

The EEOC SEP for Fiscal Years 2017-2021 continues to prioritize the substantive areas identified in its previous SEP, with some modifications. These substantive areas of focus were developed through the considerations of the following criteria: 1) issues that have a broad impact because of the number of individuals, employers or employment practices affected; 2) issues affecting workers who may lack an awareness of their legal protections or who may be reluctant or unable to exercise their rights; 3) issues involving developing areas of the law, where the expertise of the EEOC is particularly salient; 4) issues involving discriminatory practices that impede or impair full enforcement of employment anti-discrimination laws; and 5) issues that may be best addressed by government enforcement, based on the EEOC's access to information, data and research. The EEOC's focus on systemic litigation is even further emphasized in the updated SEP. However, there does appear to be some recognition that individual cases in and of themselves may be meritorious and advance the greater goals of the agency and a more balanced approach should be taken.

This new SEP does not change the six priorities initially identified in the 2013-2016 SEP. Namely, these priorities are: 1) Eliminating barriers in recruitment and hiring; 2) Protecting vulnerable workers, including immigrant and migrant workers, and underserved communities from

discrimination; 3) Addressing selected emerging and developing issues; 4) Ensuring equal pay protections for all workers; 5) Preserving access to the legal system; and 6) Preventing systemic harassment. With respect to the prevention of systemic harassment, the EEOC issued on June 20, 2016, a final report on its Study of Harassment in the Workplace. Some themes which emerged from this report were addressing anti-harassment training in the workplace to emphasize the importance of bystanders to report harassment of others they may observe, as well as consideration of different mechanisms for employees to report harassment. Additionally, the report emphasized the need of the NLRB and EEOC to work together to harmonize EEO law and decisions coming out of the NLRB, which at times have been in conflict, particularly in the areas of confidentiality of harassment investigations and social media policies.

In the SEP, the EEOC reemphasizes some of the emerging and developing issues such as pregnancy accommodations under the Americans with Disabilities Act as well as LGBT issues in the workplace. This should come as no surprise to employers as some of the higher profile litigation coming out of the EEOC in the last few years involved these precise areas.

However, the most notable updates made by this SEP are the addition of two areas to the emerging issues priority that warrant close attention by employers: 1) issues related to complex employment relationships in the 21st century workplace (e.g. temporary workers, staffing agencies, independent contractor relationships, and the on-demand economy); and 2) “backlash discrimination” against those who are Muslim or Sikh, or persons of Arab, Middle Eastern or South Asian descent, as well as persons perceived to be members of these groups. In short, employers can expect that joint employment relationships will be closely scrutinized and workplaces that rely on staffing companies and other similar entities will have those interactions more closely examined. Further, closer attention will be focused on discrimination of certain minority groups.

Eliminating Barriers In Recruitment and Hiring

The EEOC will focus on class-based discriminatory recruitment and hiring practices. These include exclusionary policies and practices, the channeling/steering of individuals into specific jobs, job segregation, restrictive application processes, and screening tools that disproportionately impact workers based on their protective status. The lack of diversity in technology and the increasing use of data-driven screening tools are also recognized as priorities within this area.

Protecting vulnerable workers, including immigrant and migrant workers, and underserved communities from discrimination

The EEOC will focus on job segregation, harassment, trafficking, pay, retaliation and other policies and practices against vulnerable workers, including immigrant and migrant workers, as well as persons perceived to be members of these groups, and against members of underserved communities. According to the EEOC, these workers are often unaware of their rights under the equal employment laws or reluctant or unable to exercise them. For instance, employment discrimination against members of Native American tribes might be a focus for some offices as part of this priority. In addition, the EEOC has and will continue to protect vulnerable workers, such as migrant workers, and those with intellectual disabilities

Addressing selected emerging and developing issues

In addition to the areas previously mentioned as emerging and developing for the EEOC, the agency is also focusing on:

1. Qualification standards and inflexible leave policies that discriminate against individuals with disabilities; and
2. Clarifying the employment relationship and the application of workplace civil rights protections.

Ensuring equal pay protections for all workers

The SEP reinforces the EEOC's efforts to address pay discrimination based on sex, but also now includes focus on combatting pay discrimination that persists based on race, ethnicity, age, and for individuals with disabilities. The SEP also emphasizes coordinated strategies across the EEOC to leverage the agency's resources. Employers should keep a close eye at the state and local level for equal pay laws as some of the more progressive states and cities tend to take EEOC policy and turn it into law. The recent laws being passed banning employers from inquiring into the wage history of applicants is yet another indication of an increased focus on equal pay. Additionally, Ban the Box laws are continuing to garner increased attention on the proper evaluation of criminal history.

Preserving access to the legal system

The EEOC will focus on policies and practices that limit substantive rights, discourage or prohibit individuals from exercising their rights under employment discrimination statutes, or impede the EEOC's investigative or enforcement efforts. Specifically, the EEOC will focus on: 1) overly broad waivers, releases, and mandatory arbitration provisions; 2) employers' failure to maintain and retain applicant and employee data and records required by EEOC regulations; and 3) significant retaliatory practices that effectively dissuade others in the workplace from exercising their rights. Severance agreements are increasingly under attack by the EEOC and employers would be well served to review their current agreements, if they have not done so already. Recent years have also seen EEOC investigators becoming increasingly bold with contacting employees. Employers should expect this trend to continue.

Preventing systemic harassment

The EEOC believes it has an obligation to ensure meaningful legal protections for individuals while also effectively using its resources to have the greatest impact. Accordingly, the EEOC will continue to improve the coordination across all of its offices and improve efficiencies of its processes.

It remains to be seen how these priorities may shift with a new General Counsel of the EEOC and the Trump Administration. Recent Cabinet picks would seem to suggest a potential retrenchment of the EEOC's proactive approach over the last few years under President Obama.

Further, President Trump will be able to appoint a new Chair of the EEOC. Jenny Yang was named chair in 2014 and has been credited with advancing a very forward-thinking agenda on the part of the EEOC. Further, it is likely that funding to the EEOC will drop under the Trump administration, which will mean less resources for the agency to carry out its initiatives.

White House Policy on Non-Compete Agreements

On May 5, 2016, President Obama issued a policy paper entitled: *Non-Compete Agreements: Analysis of the Usage, Potential Issues, and State Responses*. This policy paper does not carry the force of regulation, so it may be soon forgotten when President Obama departs. However, the evolving law on non-competes is an interesting and dynamic topic and is worth reviewing at this time.

President Obama pronounced himself concerned, despite “a historic turnaround since the depths of the Great Recession,” by “institutional changes in labor markets, such as greater restrictions on a worker’s ability to move between jobs.” For this reason, he “directed executive departments and agencies to propose new ways of promoting competition... in an effort to improve competitive markets and empower consumers and workers voices across the country.”

The Paper acknowledges that non-compete agreements “encourage innovation by preventing workers with ‘trade secrets’ from transferring technical and intellectual property of companies to rival firms even when there are trade secrets laws to protect companies.” However, the Paper goes on to opine that non-competes “can reduce worker’s ability to use job-switching or the threat of job-switching to negotiate for better conditions and higher wages.” Such non-competes can also result in higher unemployment, if departed employees are unable to find employment that does not conflict with their non-compete contract.

The Paper states that “research suggests that 18%, or 30 million, American workers are currently covered by non-compete agreements.” Significantly, the Paper does not provide any citation to what research makes this suggestion. The Paper also contends that “approximately 15% of workers without a college degree are currently subject to non-compete agreements, and 14% of individuals earning less than \$40,000 are subject to that.” Again, no citation is provided.

The Paper notes approvingly, that some states, such as California have, by statute, “rendered non-compete contracts generally unenforceable in their state.” The Paper also suggests that worker “bargaining power is reduced after a non-compete is signed, possibly leading to lower wages.”

Some economists aligned with the Obama White House claimed that employers exercise “Monopsony” power over employees. As explained by Jason Furman the Chairman of President Obama’s Council of Economic Advisors and Alan Krueger, a former Chairman of the Council, in the *Wall Street Journal*, on November 4, 2016, “a monopsony is the flip side of a monopoly: it occurs when a buyer, rather than a seller, has sufficient market power to set its own price.” It is alleged that, by requiring employees to sign non-compete agreements, it suppresses wages as part of a monopsony.

The poster child for the harmful effects of non-competes is Jimmy John's Gourmet Sandwiches. Prior to reaching an agreement with the New York Attorney General, it required its sandwich makers and delivery drivers to sign non-compete agreements. The agreements prevented such employees from taking another job with a different restaurant that sold sandwiches within a three-mile range of their employer. This situation reminds us of the maxim that bad facts lead to bad law. Why a minimum wage employee engaged in placing meat and condiments on a sandwich needs to sign a non-compete agreement is somewhat baffling. It is impossible to discern how Jimmy John's would be harmed if one of its employees takes his/her skills wielding the condiments to a Subway Store. Jimmy John's settled with the New York A.G. in June of 2016, perhaps because its management came to see that the non-competes were generating too much bad publicity.

As anyone who has practiced in the area of non-competes will acknowledge, it is relatively easy to get a respectful hearing from a judge when one is trying to enforce a non-compete agreement against a commissioned sales person earning \$1 million per year in commissions who has taken his/her employer's customer lists, and knowledge of customer buying cycles, procurement needs and pricing expectations. On the other hand, it is very difficult to get a judge to enforce a non-compete agreement against a support staff employee without customer contract or access to a customer list, when the employee has a family to support. That comparison brings us to the following point: non-compete agreements have traditionally been litigated in court. Judges traditionally look to the overall effect of the contract, including an employer's legitimate business interests, including the temporal and geographical limitations that the employer attempts to impose, against the employee's need and ability to make a living. A vast number of courts have long understood that citizens need to earn a living for themselves and their families and therefore the courts already look at the enforcement of non-compete agreements with a very critical eye.

The Obama White House's interest in non-compete agreements was a not very subtle attempt to take decisions regarding the enforceability of non-competes out of the hands of individual state court judges and to "federalize" enforcement of non-compete agreements. It is important to understand that the White House Paper is not an executive order and has no "teeth" in the sense that it does not provide regulations or prohibitions. Nonetheless, to quote the recent Nobel Laureate, Bob Dylan: "you don't need a weatherman to know which way the wind blows."



WEDNESDAY, MARCH 8, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

**CLASS ACTION AND MULTIDISTRICT LITIGATION AND TRIAL TACTICS,
PRACTICE AND PROCEDURE SECTIONS**

Amended Rules of Civil Procedure - How They are Being Implemented

Dogwood

Moderators:

Christopher P. DePhillips

Marc A. Young

Speakers:

Gray T. Culbreath

Edward B. Ruff, III

Paul C. Kuhnel

***"AMENDED RULES OF CIVIL PROCEDURE –
HOW THEY ARE BEING IMPLEMENTED"***

**Christopher P. DePhillips, Esq.
Chair, FDCC Class Actions Section
March 8, 2017**

RULE 26(b)(1) & PROPORTIONALITY FACTORS

THE RULE:

The change that was made to Rule 26(b)(1) is included in the following underlined language (with the omitted language indicated by strikethrough):

(b) Discovery Scope and Limits.

(1) Scope in General. Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any non-privileged matter that is relevant to any party's claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable. ~~including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admission at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C).~~

PROPORTIONALITY OVERVIEW:

The initial August 2013 Preliminary Draft of the proposed rule amendments report (<http://www.ediscoverylaw.com/files/2013/11/Published-Rules-Package-Civil-Rules-Only.pdf>), stated that the old Rule 26(b)(1) was subject to Rule 26(b)(2)(C). In that report the committee says: “Although the rule now directs that the court “must” limit

discovery, on its own and without motion, it cannot be said to have realized the hopes of its authors. Surveys produced in connection with the Duke Conference by various groups, including the Federal Judicial Center, the ABA Section of Litigation, the National Employment Lawyer's Association, and Lawyers for Civil Justice, indicate that excessive discovery occurs in a worrisome number of cases, particularly those that are complex, involve high stakes, and generate contentious adversary behavior. The number of these cases and the burdens they impose present serious problems. These problems have not yet been solved."

The committee noted that the "problem is not with the rule text [as it then currently existed] but with its implementation -- it is not invoked often enough to dampen excessive discovery demands." Accordingly, the committee stated that they are essentially transferring the analysis required under Rule 26(b)(2)(C)(iii) to become a "limit on the scope of discovery," and proposed the following text:

proportional to the needs of the case considering the amount in controversy, the importance of the issues at stake in the action, the parties's [sic] resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit

The April 2014 committee minutes give a history of how proportionality has been a focus of the rules since 1983, with amendments made in 1993 and 2000 to help reinforce this point. (<http://www.uscourts.gov/rules-policies/archives/meeting-minutes/advisory-committee-rules-civil-procedure-april-2014>).

A change was made to place the "importance of the issues at stake in the action" first and "the amount in controversy" second because of the following:

Many claims may seek relatively low amounts of money damages, or seek only specific relief without any damages at all. Focus on the importance of the issues at stake was included in the 1983 rule as an explicit recognition that many actions that seek minimal or no damages involve matters of personal or public importance beyond, and perhaps far beyond, money alone. Often an individual plaintiff may be functioning in part as a private attorney general. Proportionality cannot be measured by the money alone. Although this principle has been embodied by the rules from the beginning, there is a fear that placing the amount in controversy first in the list may cause courts to impose inappropriate limits on discovery. At the other end of the line, other comments expressed a fear that focus on the money involved might lead some courts to allow

absolutely unlimited discovery in actions involving huge sums of money.

The committee also noted the need to add a new proportionality consideration: “the parties’ relative access to relevant information.” The committee stated the following with respect to adding this change:

This language, along with an explanation proposed for the Committee Note, is meant to address circumstances commonly described as involving “asymmetric information.” Some categories of litigation are characterized by an uneven distribution of discoverable information. Civil rights actions in general, and most particularly individual employment claims, are examples identified by many comments and much testimony. An individual plaintiff claiming adverse employment action, for example, may have very little information that the defendant employer needs to discover. The employer, on the other hand, may have relatively large amounts of information that the employee can obtain only through formal discovery, particularly when it is necessary to present evidence of the treatment of other employees in similar circumstances. An asymmetric distribution of discoverable information often means an asymmetric incidence of discovery burdens. This factor recognizes that proportionality may allow one party to request more extensive discovery than its adversary requests.

In September 2014, the committee submitted the revisions with the June 2014 Rules Committee Report. (located here as Appendix B beginning on page 78, <http://www.uscourts.gov/rules-policies/archives/committee-reports/reports-judicial-conference-september-2014>). The report states that proportionality as a topic in the rules is not new, and these factors are not new. “The Committee’s purpose in returning the proportionality factors to Rule 26(b)(1) is to make them an explicit component of the scope of discovery, requiring parties and courts alike to consider them when pursuing discovery and resolving discovery disputes.” The Committee wanted to allay fears expressed during the comment period about these changes:

The Committee considered carefully the concerns expressed in public comments: that the move will shift the burden of proving proportionality to the party seeking discovery, that it will provide a new basis for refusing to provide discovery, and that it will increase litigation costs. None of these predicted outcomes is intended, and the proposed Committee Note has been revised to address them. The Note now explains that the change does not

place a burden of proving proportionality on the party seeking discovery and explains how courts should apply the proportionality factors. The Note also states that the change does not authorize boilerplate refusals to provide discovery on the ground that it is not proportional, but should instead prompt a dialogue among the parties and, if necessary, the court, concerning the amount of discovery reasonably needed to resolve the case. The Committee remains convinced that the proportionality considerations will not increase the costs of litigation. To the contrary, the Committee believes that more proportional discovery will decrease the cost of resolving disputes without sacrificing fairness.

Commentators have stated that the overall goal of adding the factors to Rule 269b0(1) is to reduce over-discovery, and each factor should be viewed in that light. (<http://defensecounseljournal.org/doi/full/10.12690/0895-0016-82.4.411>).

The official Notes of the Advisory Committee on the 2015 Amendments are clear that the Rule 26(b)(1) amendments are designed to “restore[] the proportionality factors to their original place in defining the scope of discovery. This change reinforces the Rule 26(g) obligation of the parties to consider these factors in making discovery requests, responses, or objections.” However, “the change does not place on the party seeking discovery the burden of addressing all proportionality considerations.” On the other hand, the change is not intended “to permit the opposing party to refuse discovery simply by making a boilerplate objection that it is not proportional.”

THE FACTORS FOR PROPORTIONALITY:

Factor 1. “importance of the issues at stake in the action”

- Background: Originally this factor was second, but the Committee put it first to add “prominence to the importance of the issues.” (<http://www.uscourts.gov/rules-policies/archives/committee-reports/reports-judicial-conference-september-2014>).
- Committee Note: “A party claiming that a request is important to resolve the issues should be able to explain the ways in which the underlying information bears on the issues as that party understands them.”
- Duke Guidelines: “This factor recognizes that many cases raise issues that are important for reasons beyond any money the parties may stand to gain or lose in a particular case.” As an example, Duke provides the following commentary: “A case seeking to enforce constitutional, statutory, or common-law rights, including a case filed under a statute using attorney fee-shifting provisions to encourage enforcement, can serve public and private interests that have an importance

beyond any damages sought or other monetary amounts the case may involve.” (<http://www.ned.uscourts.gov/internetDocs/cle/2015-09/Guidelines-and-Practices-Sept.19.pdf>)

Factor 2. “amount in controversy”

- Background: Originally this factor was the first factor, but changed in the 2014 revision to the second factor “to avoid any implication that the amount in controversy is the most important concern.” (<http://www.uscourts.gov/rules-policies/archives/committee-reports/reports-judicial-conference-september-2014>)
- Committee Note: “It also is important to repeat the caution that the monetary stakes are only one factor, to be balanced against other factors. The 1983 Committee Note recognized ‘the significance of the substantive issues, as measured in philosophic, social, or institutional terms. Thus the rule recognizes that many cases in public policy spheres, such as employment practices, free speech, and other matters, may have importance far beyond the monetary amount involved.’ Many other substantive areas also may involve litigation that seeks relatively small amounts of money, or no money at all, but that seeks to vindicate vitally important personal or public values.”
- Duke Guidelines: “This factor examines what the parties stand to gain or lose financially in a particular case as part of deciding what discovery burdens and expenses are reasonable for that case. The amount in controversy is usually the amount the plaintiff claims or could claim in good faith.” As an example, Duke offers the following commentary on this factor: “If a specific amount in controversy is alleged in the pleadings and challenged, or no specific amount is alleged and the pleading is limited to asserting that the amount exceeds the jurisdictional minimum, the issue is how much the plaintiff could recover based on the claims asserted and allegations made. When an injunction or declaratory judgment is sought, the amount in controversy includes the pecuniary value of that relief. The amount in controversy calculation can change as the case progresses, the claims and defenses evolve, and the parties and judge learn more about the damages or the value of the equitable relief.” (<http://www.ned.uscourts.gov/internetDocs/cle/2015-09/Guidelines-and-Practices-Sept.19.pdf>)

Factor 3. “parties’ relative access to relevant information”

- Background: This factor was not originally in the proposed change, but was added to address “the reality that some cases involve asymmetric distribution of information” and that “Courts should recognize that proportionality in asymmetric cases will often mean that one party must bear greater burdens in responding to discovery than the other party bears.” (<http://www.uscourts.gov/rules-policies/archives/committee-reports/reports-judicial-conference-september-2014>).

- Committee Note: “The direction to consider the parties' relative access to relevant information adds new text to provide explicit focus on considerations already implicit in present Rule 26(b)(2)(C)(iii). Some cases involve what often is called ‘information asymmetry.’ One party--often an individual plaintiff--may have very little discoverable information. The other party may have vast amounts of information, including information that can be readily retrieved and information that is more difficult to retrieve. In practice these circumstances often mean that the burden of responding to discovery lies heavier on the party who has more information, and properly so.”
- Duke Guidelines: “The issues to be examined include the extent to which a party needs formal discovery because relevant information is not otherwise available to that party.” As an example, Duke offers the following commentary: (<http://www.ned.uscourts.gov/internetDocs/cle/2015-09/Guidelines-and-Practices-Sept.19.pdf>)
 - Issue 1: Information Asymmetry - “In a case involving ‘information asymmetry’ or inequality, in which one party has or controls significantly more of the relevant information than other parties, the parties with less information or access to it depend on discovery to obtain relevant information. Parties who have more information or who control the access to it are often asked to produce significantly more information than they seek or are able to obtain from a party with less.”
 - Issue 2: Recognizing Unequal Discovery Burdens - “The fact that a party has little discoverable information to provide others does not create a cap on the amount of discovery it can obtain. A party’s ability to take discovery is not limited by the amount of relevant information it possesses or controls, by the amount of information other parties seek from it, or by the amount of information it must provide in return. Discovery costs and burdens may be heavier for the party that has or can easily get the bulk of the essential proof in a case.
 - Issue 3: Limiting Unfairness - “When a case involves information asymmetry or inequality, proportionality requires permitting all parties access to necessary information, but without the unfairness that can result if the asymmetries are leveraged by any party for tactical advantage. Unfairness can occur when a party with significantly less information imposes unreasonable demands on the party who has voluminous information. Unfairness can also occur when a party with significantly more information takes unreasonably restrictive or dilatory positions in response to the other party’s requests.”
- Commentator: “The parties' ‘relative access to relevant information’ – added to the rule as part of the 2015 amendments – is not meant to open the floodgates in cases where one party holds most of the information. It does not provide an

independent reason to allow needless discovery, nor does it add any new considerations to the scope of discovery that were not present prior to the amendments.” (<http://defensecounseljournal.org/doi/full/10.12690/0895-0016-82.4.411>). The commentator goes on to say: “Requests for ‘all’ of certain types of information are often overbroad and burdensome, triggering a court’s duty to limit their scope as appropriate. In *Holloway v. Dollar Tree Distribution*, for example, the court limited a series of such requests because the ‘breadth of this request is not sufficiently justified in light of the amount in controversy and the significance of the discovery to the current issues.’” (<http://defensecounseljournal.org/doi/full/10.12690/0895-0016-82.4.411>).

Factor 4. “parties’ resources”

- Committee Note: “So too, consideration of the parties’ resources does not foreclose discovery requests addressed to an impecunious party, nor justify unlimited discovery requests addressed to a wealthy party. The 1983 Committee Note cautioned that ‘[t]he court must apply the standards in an even-handed manner that will prevent use of discovery to wage a war of attrition or as a device to coerce a party, whether financially weak or affluent.’”
- Duke Guidelines: “This factor examines what resources are available to the parties for gathering, reviewing, and producing information and for requesting, receiving, and reviewing information in discovery. ‘Resources’ means more than a party’s financial resources. It includes the technological, administrative, and human resources needed to perform the discovery tasks.” As an example, Duke provides the following commentary: (<http://www.ned.uscourts.gov/internetDocs/cle/2015-09/Guidelines-and-Practices-Sept.19.pdf>)
 - o Issue 1: Likely Heavier Demand on Party with Greater Resources - “In general, more can be expected of parties with greater resources and less of parties with scant resources, but the impact of the parties’ reasonably available resources on the extent or timing of discovery must be specifically determined for each case.”
 - o Issue 2: Ability to Take/Give Discovery Not Determined Solely by Resources - “As with all of the factors, this factor is only one consideration. Even if one party has significantly greater resources, this factor does not require that party to provide all or most of the discovery proposed simply because it is able to do so. Nor does it mean that parties with limited resources can refuse to provide relevant information simply because doing so would be difficult for financial or other reasons. A party’s ability to take discovery is not limited by the resources it has available to provide discovery in return.”

- o Issue 3: Reasonable Resources Available for Discovery When Needed - “The basic point is what resources a party reasonably has available for discovery, when it is needed. Evaluating the resources a party can reasonably be expected to expend on discovery may require considering that party’s competing demands for those resources.”
- Commentator: One commentator stated that this is a “pragmatic check on disproportionate discovery; it would be a topsy-turvy reading to interpret this factor to justify needless discovery from a rich party or insufficient discovery from a poor one.” That commentator goes on to say “As the Committee pointed out in 1983 when it inserted this phrase into the Rules, ‘consideration of the parties’ resources does not foreclose discovery requests addressed to an impecunious party, nor justify unlimited discovery requests addressed to a wealthy party.’ The 1983 Committee Note explains that ‘[t]he court must apply the standards in an even-handed manner that will prevent use of discovery to wage a war of attrition or as a device to coerce a party, whether financially weak or affluent.’” (<http://defensecounseljournal.org/doi/full/10.12690/0895-0016-82.4.411>)

Factor 5. “importance of the discovery in resolving the issues”

- Duke Guidelines: “This factor examines the importance of the discovery to resolving the issues in the case.” By way of commentary, Duke offers the following: (<http://www.ned.uscourts.gov/internetDocs/cle/2015-09/Guidelines-and-Practices-Sept.19.pdf>)
 - o Issue 1: Ranking Issues - “One aspect of this factor is to identify what issues or topics are the subject of the proposed discovery and how important those issues and topics are to resolving the case. Discovery relating to a central issue is more important than discovery relating to a peripheral issue.”
 - o Issue 2: How Discovery Resolves Issues - “Another aspect is the role of the proposed discovery in resolving the issue to which that discovery is directed. If the information sought is important to resolving an issue, discovery to obtain that information can be expected to yield a greater benefit and justifies a heavier burden, especially if the issue is important to resolving the case or materially advances resolution. If the information sought is of marginal or speculative usefulness in resolving the issue, the burden is harder to justify, especially if the issue is not central to resolving the case or is unlikely to materially advance case resolution.”
 - o Issue 3: Hypothesis of the Requesting Party - “Understanding the importance of proposed discovery may involve assessing what the requesting party is realistically able to predict about what added

information the proposed discovery will yield and how beneficial it will be. “

Factor 6. “whether the burden or expense of the proposed discovery outweighs its likely benefit”

- Committee Note: “A party claiming undue burden or expense ordinarily has far better information--perhaps the only information--with respect to that part of the determination.”
- Committee Note: “The burden or expense of proposed discovery should be determined in a realistic way. This includes the burden or expense of producing electronically stored information. Computer-based methods of searching such information continue to develop, particularly for cases involving large volumes of electronically stored information. Courts and parties should be willing to consider the opportunities for reducing the burden or expense of discovery as reliable means of searching electronically stored information become available.”
- Duke Guidelines: “There is no fixed burden-to-benefit ratio that defines what is or is not proportional. When proportionality disputes arise, the party in the best position to provide information about the burdens, expense, or benefits of the proposed discovery ordinarily will bear the responsibility for doing so. Which party that is depends on the circumstances. In general, the party from whom proposed discovery is sought ordinarily is in a better position to specify and support the burdens and expense of responding, while the party seeking proposed discovery ordinarily is in a better position to specify the likely benefits by explaining why it is seeking and needs the discovery.” By way of commentary, Duke states the following: (<http://www.ned.uscourts.gov/internetDocs/cle/2015-09/Guidelines-and-Practices-Sept.19.pdf>)
 - o Issue 1: Factors to Consider in the Balancing Assessment - “In general, proposed discovery that is likely to return important information on issues that must be resolved will justify expending more resources than proposed discovery seeking information that is unlikely to exist, that may be hard to find or retrieve, or that is on issues that may be of secondary importance to the case, that may be deferred until other threshold or more significant issues are resolved, or that may not need to be resolved at all.”
 - o Issue 2: Objecting to Time with Specificity - “If a party objects that it would take too many hours, consume unreasonable amounts of other resources, or impose other burdens to respond to the proposed discovery, the party should specify what it is about the search, retrieval, review, or production process that requires the work or time or that imposes other burdens.”

- o Issue 3: Objecting to Cost with Specificity - “If a party objects to the expense of responding to proposed discovery, the party should be prepared to support the objection with an informed estimate of what the expenses would be and how they were determined, specifying what it is about the source, search, retrieval, review, or production process that requires the expense estimated.”
- o Issue 4: Objecting as Overly Broad with Specificity - “If a party requests discovery and it is objected to as overly burdensome or expensive, the requesting party should be prepared to specify why it requested the information and why it expects the proposed discovery to yield that information. Assessing whether the requesting party has adequately specified the likely benefits of the proposed discovery may involve assessing the information the requesting party already has, whether through its own knowledge, through publicly available sources, or through discovery already taken.”
- o Issue 5: Requesting Party without Resources to Assess Discovery Benefit - “A party with inferior access to discoverable information relevant to the claims or defenses may also have inferior access to the information needed to evaluate the benefit, cost, and burden of the discovery sought. Assessing the benefits of proposed discovery may also involve assessing how well the requesting party is able to predict what added information the proposed discovery will yield and how beneficial it will be.”
- o Issue 6: Cooperation Between Parties - “Party cooperation is particularly important in understanding the burdens or benefits of proposed discovery and in resolving disputes. The parties should be prepared to discuss with the judge whether and how they communicated with each other about those burdens or benefits. The parties should also be prepared to suggest ways to modify the requests or the responses to reduce the burdens and expense or to increase the likelihood that the proposed discovery will be beneficial to the case.”
- o Issue 7: How (b)(1) Applies to (b)(2)(B) - “Rule 26(b)(2)(B) addresses a specific type of burden argument—that discovery should not proceed with respect to a particular source of electronically stored information because accessing information from that source is unduly burdensome or costly. Examples might include information stored using outdated or ‘legacy’ technology or information stored for disaster recovery rather than archival purposes that would not be searchable or even usable without significant effort. Rule 26(b)(2)(B) has specific provisions for discovery from such sources. Those provisions do not apply to discovery from accessible sources, even if that discovery imposes significant burden or cost.”

RELEVANT CASELAW

CASE: State Farm v. Fayda, No. 14 Civ. 9792, 2015 U.S. Dist. LEXIS 162164 (S.D.N.Y. Dec. 3, 2015) (Memorandum and Order)

JUDGE: James C. Francis, IV (Magistrate)

OVERVIEW: State Farm filed a motion to compel defendant health care providers (including acupuncture services) to produce financial records and other documents based upon the theory that defendants had filed fraudulent insurance claims for services that were not medically necessary. State Farm alleged that defendants gained access to the patients by paying kickbacks to non-physicians through paying extremely high rent on properties to the non-physicians. Additionally, discovery produced prior to the motion showed that defendants made payments at the direction of a particular non-physician (who had been tied to multiple indictments for money laundering and healthcare fraud) to certain businesses. Further, discovery showed that one defendant paid an interest-free loan to a co-defendant in the amount of \$30,000, which was not repaid.

According, State Farm requested bank records and tax returns, as well as the following: (a) agreements, including leases regarding activities at these other practices; (b) documents reflecting or relating to payments relating to such agreements; and (c) transcripts of testimony from examinations under oath. The bank records and tax returns were the only documents subject to a proportionality assessment. Defendants objected to production of the bank records and tax returns on relevance and privacy grounds.

Judge Francis granted the motion.

PROPORTIONALITY ANALYSIS:

Judge Francis dedicated a fair amount of analysis on proportionality. With respect to bank records and tax returns, he noted that the burden of demonstrating relevance remains on the party seeking discovery, and the party resisting discovery has the burden of showing undue burden or expense. After finding the documents sought as relevant, Judge Francis focused on proportionality. Out of the proportionality factors, the Court focused on the following: “Rule 26(b)(1) instructs parties and courts to evaluate whether the benefit of the discovery sought is proportional to the burden of producing it, taking into account issues like access, importance, and available resources.” Id. at *13 (emphasis added). The Court noted that the defendants did not rebut relevance and materiality, and failed to establish an alternative to obtaining the information, or that producing the documents would be particularly burdensome. Accordingly, the Court ordered defendants to produce the requested bank records and tax returns to State Farm.

NOTE: The Court also rejected defendants’ argument based on privacy.

CASE: Gilead Sciences, Inc. v. Merck & Co., Inc., No. 5:13-cv-04057-BLF, 2016 U.S. Dist. LEXIS 5616 (N. Dist. Ca. Jan. 13, 2016) (Order denying motion to compel)

JUDGE: Paul S. Grewal (Magistrate)

OVERVIEW: This is a patent case. As the Court states: “Merck asserts that Gilead infringes two of its patents to a certain kind of nucleoside analog. Among other things, Gilead says it was the one to conceive and reduce to practice the inventions, in 2003, in a compound named PSI-6130.3 And so a key issue in this case is what did Gilead synthesize and when did it know it.” As part of a related litigation record in Canada, Gilead’s expert produced a photograph showing a tube that listed the same molecular weight as the compound in question. Accordingly, Merck demanded further production of the contents of that tube and related information.

Judge Grewal noted that Merck has been in possession of records showing that many different compounds share the same molecular weight, and that the tubes in question contained different compounds, not the one in question.

Judge Grewal denied Merck’s motion to compel on proportionality grounds.

PROPORTIONALITY ANALYSIS:

Judge Grewal notes that nothing is new as it relates to proportionality under the federal rules. The Court places a primary emphasis on proportionality as a result of the rules amendment:

What will change--hopefully--is mindset. No longer is it good enough to hope that the information sought might lead to the discovery of admissible evidence. In fact, the old language to that effect is gone. Instead, a party seeking discovery of relevant, non-privileged information must show, before anything else, that the discovery sought is proportional to the needs of the case.

The Court was clear that Merck’s request was not proportional to the case. The Court stated the following in denying Merck’s motion:

Merck's demands are exactly the type of disproportionate demands that Rule 26(b)(1) proscribes. Sure, it's possible that Gilead's evidence confirming the compounds are not PSI-6130 is false and even concocted. But Merck offers no real evidence that this is the case, and as the court recently explained in denying a motion to compel by Gilead, "[w]ithout more specific information triggering some reason for doubt, the Court must take the producing party . . . at its word."

And so that leaves Gilead in the position of having to produce discovery on all sorts of compounds that bear no indication of any nexus to the disputes in this case. This is untenable. It would be like requiring GM to produce discovery on Buicks and Chevys in a patent case about Cadillacs simply because all three happen to be cars. In the absence of any reason to doubt the proof Gilead has tendered about the identity of the disputed compounds, and given the cost and potential delay introduced by the requested production, Merck's request is precisely the kind of disproportionate discovery that Rule 26--old or new--was intended to preclude.

[Citation omitted.]

CASE: Bagley v. Yale, No. 3:13-cv-01890, 2015 U.S. Dist. LEXIS 166759 (D. Conn. Dec. 14, 2015) (Ruling granting in part and denying in part Bagley's motion to compel)

JUDGE: Charles S. Haight, Jr. (Senior U.S. District Judge)

OVERVIEW: This is a case alleging that Yale violated federal anti-discrimination statutes, including Title VII, in failing to reappoint Bagley as a professor in the practice (PiP) at Yale's School of Management (SOM). Bagley sought discovery related to other non-tenured professors at the Yale School of Management who were appointed or reappointed to the faculty (Bagley was not appointed to the faculty). Underlying this demand, is identifying "comparators" of Bagley—people who similarly situated in all material respects—and thus subject to significant discovery. It was Yale's position that Bagley did not have a comparator, and Bagley's position is that she had eleven comparators. Alternatively, Yale argues that, even if Bagley has comparators, her discovery demands are excessive.

Judge Haight found that Bagley is entitled to full discovery with respect to specific PiPs in the SOM at the time she sought reappointment (meaning those individuals were her comparators).

Specifically, Bagley sought discovery as it related to several individuals, some who were PiPs, and some who were not. Bagley also sought discovery as it related to the events precipitating the appointment of several individuals.

The Court was clear that the issue to be decided in this case is the following:

[T]he pertinent issue in the case at bar arises from Bagley's claim that whatever reasons Yale gave for refusing to

reappoint her, those reasons were pretextual, fashioned to conceal Yale's true (and illicit) discriminatory reason. Further analysis of this issue, in response to Bagley's motion to compel discovery, is hindered by the fact that the present record does not sufficiently reveal the reason or reasons Yale gave and presumably still gives for its decision not to reappoint Bagley.

[Id. at *23-24.]

PROPORTIONALITY ANALYSIS:

The Court reiterated Judge Francis' legal recitation of the rules amendments. Interestingly, the Court did not focus on proportionality, as much as the Court focused on relevance (which is encompassed within the proportionality factors). The Court stated that it "cannot decide whether information is relevant to Bagley's claim that Yale's reason was pretextual without first knowing what that reason was." Id. at *26. Although stating that the new rules were applicable to the motion at bar, the Court gave no recitation regarding the proportionality of the discovery, despite giving credence to Judge Francis' thoughtful opinion issued a week prior.

NOTE: The Court ordered that Yale file an Offer of Proof for its nondiscriminatory reason for declining to reappoint Bagley to faculty. More specifically, the Court granted Bagley's motion compel and directed Yale to produce discovery on the certain comparators. The Court otherwise denied the motion to compel without prejudice for any additional discovery.

As an aside, it is important to read this case in the context of a Senior District Court Judge approving of the reasoning of a Magistrate Judge.

CASE: Siriano v. Goodman Manufacturing Co., No. 2:14-cv-1131, 2015 U.S. Dist. LEXIS 165040 (S.D. Ohio Dec. 9, 2015) (Opinion and Order granting in part Plaintiffs' motion to compel with respect to condenser coils)

JUDGE: Elizabeth Preston Deavers (Magistrate Judge)

OVERVIEW: This is a breach of warranty, products liability, and consumer fraud action, "alleging that the evaporator coils and condenser coils found in Defendants' air conditioners, air handlers and heat pumps have defects that cause 'premature corrosion and holes or cracks in the coils.'" Id. at *1-2. Specifically, Plaintiffs contend that

Defendant Goodman Products' copper coils, as the result of a design or manufacturing defect, are too thin and prematurely corrode or crack causing refrigerant to leak

through the fissures. The defects are widespread, affecting as much as 80% of the products sold. Defendants knew about, but failed to disclose, the defects. Defendants deny these allegations.

[Id. at *2 (internal citations omitted).]

Plaintiffs argued that Defendants must be compelled to respond fully to twenty separate discovery demands, and use Plaintiffs' suggest ESI search terms in doing so. Here, the defendants directly argued that producing the requested information would be unduly burdensome, stating that it would take roughly 4,000 hours of lawyer time to review the requested documents.

PROPORTIONALITY ANALYSIS:

In its legal recitation, the Court cited Rule 26(b)(1), and noted that in “considering the scope of discovery, the Court may balance Plaintiffs' ‘right to discovery with the need to prevent ‘fishing expeditions.’” Id. at *12 (quoting *Conti v. Am. Axle & Mfg., Inc.*, 326 F. App'x 900, 907 (6th Cir. 2009)).

The Court cites ample authority that existed prior to the rules amendments for the proposition that there is a balancing test to determine whether the scope of discovery demanded must be produced. The Court adds that “[r]estoring proportionality is the touchstone of revised Rule 26(b)(1)'s scope of discovery provisions.” Id. at 16 (citations and internal quotation marks omitted). The Court conducts an analysis of the proportionality factors, focusing on the availability of the information, the resources of a corporate defendant over plaintiffs, and the amount in controversy:

In the instant case, the discovery sought by Plaintiffs is directly related to their claims, which include assertions of defects in the design and manufacture of Defendants' condenser coils. It is highly unlikely that Plaintiffs could discover similar information from another source or in another manner. Defendants are, therefore, in a unique position with respect to these documents. Similarly, Plaintiffs assert several breach of warranty claims. Documents related to warranty complaints filed by other customers, who are not parties to this litigation, would be easily accessible to Defendants but almost completely inaccessible to Plaintiffs. Additionally, it is much more efficient for Plaintiffs to seek information related to Defendants' dealings with their distributors from Defendants themselves, who have access to all of those records, rather than assemble it piecemeal from the distributors themselves. Furthermore, Defendants' corporate resources vastly exceed Plaintiffs', and, to date,

Defendants have expended relatively little in complying with discovery in this matter. Defendants' production thus far consists of the electronic disclosure of documents previously collected and reviewed pursuant to discovery in other, related cases. Lastly, because Plaintiffs in their Complaint present a putative class action that could include a significant number of class members who each purchased costly products from Defendants, the amount in controversy in this matter is potentially very large.

[Id. at *16-17.]

The Court recognized that the cost of compliance with plaintiffs' discovery demands could be costly, but that it did not believe compliance to be unduly burdensome. Further, the Court noted that Defendants did not provide an alternative to limit the discovery.

Interestingly, instead of granting all of plaintiffs' discovery demands, the Court takes a pragmatic approach, engaging in active judicial case management. To facilitate the spirit of the amendments, including Rule 26 and Rule 1, the Court stated it would do the following:

[T]he Court will schedule a discovery conference with the parties to discuss whether and to what extent discovery should proceed in phases. For instance, it appears to the Court that Plaintiffs may first want to discover whether Defendants received any complaints or warranty claims regarding the condenser coils before discovering documents related to investigations, schematics and the all-encompassing "[a]ll records summarizing, categorizing, and/or documenting evaporator and/or condenser coil failures. . . ." In the interim, the parties are directed to engage in further cooperative dialogue in an effort to come to an agreement regarding proportional discovery.

[Id. at *19-20 (internal citations omitted).]

CASE: In re: Blue Cross Blue Shield Antitrust Litigation, No. 2:13-CV-20000-RDP, 2015 U.S. Dist. LEXIS 174768 (N.D. Alab. Dec. 9, 2015) (

JUDGE: T. Michael Putnam (Magistrate Judge)

OVERVIEW: This is a motion for clarification of a discovery order, specifically expressing opposition to the production of expert reports and depositions in a separate case.

PROPORTIONALITY ANALYSIS:

The Court listed the proportionality factors as one part in its analysis to determine whether the expert reports in question were discoverable. Judge Putnam undertook a thorough analysis of the proportionality factors.

The Court found that the expert reports are only tangentially related to the issues in the case:

[I]t appears that the expert reports and depositions from the Aetna litigation are only tangentially "important to the issues at stake" in this action. While plaintiffs claim that "Most Favored Nation" clauses has been used by the Blues, including BCBS-MI, as a barrier to competition in the health-insurance market, their principal claim is that the Blues have conspired to divide up the market geographically to avoid competing among themselves. Given the nature of the issues alleged in Aetna, it would appear that the expert reports and depositions in that case would address only a small, secondary issue in this case, and then only in the geographically limited area of Michigan.

[Id. at *21.]

The Court also spent time analyzing the amount in controversy, the parties' relative access to the information sought, the parties' resources, and the importance of the discovery in resolving the issues.

Next, the amount at stake in this case is great, involving perhaps billions of dollars, as well as the continued viability of the Blue Cross-Blue Shield business model. Also, as to this particular information, the plaintiffs have no access (or perhaps very little access provided by some cooperation from Aetna Inc.) to the expert reports and depositions in the Aetna litigation; if they are to see the information, it must be obtained from BCBS-MI. The parties' resources are not entirely equivalent, but the plaintiffs seem to be able to meet the man-power and financial demands of such high-stake litigation.

It is not clear that this discovery of the expert reports and depositions from the Aetna litigation is important in resolving the issue whether of the most-favored-nation clauses are an illegal restraint on trade. Here, a distinction must be made between the expert reports

and depositions of experts retained by BCBS-MI and those retained by Aetna. Subject to the limitations imposed by the protective orders entered in the Aetna litigation, the factual information and data underlying the expert reports and depositions are being produced by BCBS-MI. Although having the opinions and conclusions of BCBS-MI's experts might be helpful to plaintiffs, none of these experts has been identified as a retained expert in the instant case. Allowing the plaintiffs to obtain BCBS-MI's experts' reports and testimony sheds little or no light on this case while effectively prejudicing BCBS-MI. The reports and the testimony of the experts were never used in the Aetna litigation and should not be treated as binding on BCBS-MI in this case. In the event any of BCBS-MI's experts in Aetna is later identified by any defendant in this case as an expert witness, the expert's previous report and testimony may become discoverable. Until that occurs, plaintiffs' own experts should be capable of analyzing the underlying information and forming their own opinions and conclusions in this case.

[Id. at *21-23.]

The Court concluded by finding the last factor--whether the burden or expense of the proposed discovery outweighs its likely benefit--to be the most persuasive in this case:

The question remains whether the reports and testimony of the experts retained and disclosed by Aetna in the other litigation should be produced by BCBS-MI. The defendant can hardly complain that the opinions and conclusions of those experts, who presumably were adverse to BCBS-MI in the Aetna case, are in any way binding on it. Perhaps the most persuasive factor in the proportionality analysis for these experts is "whether the burden or expense of the proposed discovery outweighs its likely benefit." In this case, at issue are eleven expert reports and eight expert depositions. They are readily identifiable and available; there is no undue expense associated with producing them. The "burden or expense" of production is very light, so much so that the court cannot say that they outweigh the likely benefits of the discovery sought by plaintiffs.

[Id. at *23-24.]

Even though it appeared that the volume of factors weighed against the discoverability of the expert reports and depositions in question, Judge Putnam found that the expert reports

and depositions are discoverable under Rule 26(b)(1), that they are relevant and proportional to the needs of the case, and that their production would not unfairly prejudice Blue Cross Blue Shield.

NOTE:

In light of the advisory committee's emphasis on the first factor--the importance of the issues at stake in the action--it is surprising and interesting that Judge Putnam found the last factor to be the most persuasive. This case illustrates a great example of a judge taking thoughtful consideration of each factor, and exercising judicial discretion in determining how to fairly weigh the factors.

CASE: LightSquared Inc. v. Deere & Co., No. 13 Civ. 8157, 2015 U.S. Dist. LEXIS 166403 (S.D.N.Y. Dec. 10, 2015) (Memorandum and Order granting in part Plaintiffs' motion to compel to produce documents and use specific search terms)

JUDGE: James C. Francis, IV (Magistrate Judge)

OVERVIEW: LightSquared planned to build and deploy a wireless broadband network through satellite and terrestrial transmitters and receivers. Defendants objected to this on the grounds that the network could interfere with GPS devices. LightSquared thought those issues were allayed after negotiations, but defendants raised new concern (that LightSquared's network made GPS devices susceptible to overload and malfunction). The Federal Communications Commission agreed, and indefinitely blocked LightSquared's network from operating. In an earlier decision, Judge Richard Berman found that the defendants knew about this issue earlier, and failed to disclose it in violation of a legal obligation to do so. Accordingly, all of LightSquared's counts had been dismissed, except negligent misrepresentation and constructive fraud claims.

The Court then ordered initial, targeted discovery concerning defendants' duty to disclose the above information. The parties were unable to agree to discovery on several issues, and were directed to submit their discovery disputes to the Court.

PROPORTIONALITY ANALYSIS:

This case is interesting. Judge Francis had issued the State Farm opinion six days earlier and clearly explored the impact of the rules amendments, but here simply cited the new rule including proportionality, and moved on to address only relevance. The Court did not take the opportunity to address proportionality in any additional measure, even though it had found some of the discovery demands relevant and ordered production. This case is a cautionary tale that even a judge who is acutely aware of the new rules and has analyzed their impact requires, at minimum, a simple proportionality objection.

RULE 26(c) & COST ALLOCATION

THE RULE:

All that was added to Rule 26(c)(1)(B) was the following underlined language:

(c) Protective Orders.

(1) In General. A party or any person from whom discovery is sought may move for a protective order in the court where the action is pending--or as an alternative on matters relating to a deposition, in the court for the district where the deposition will be taken. The motion must include a certification that the movant has in good faith conferred or attempted to confer with other affected parties in an effort to resolve the dispute without court action. The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following:

....

(B) specifying terms, including time and place or the allocation of expenses, for the disclosure or discovery;

BACKGROUND

With respect to allocation of expenses, the August 2013 report by the committee stated that they were adding to Rule 26(c)(1)(B) as “an explicit recognition of the authority to enter a protective order that allocates the expenses of discovery.” They go on:

This power is implicit in present Rule 26(c), and is being exercised with increasing frequency. The amendment will make the power explicit, avoiding arguments that it is not conferred by the present rule text. The Committee soon will begin to focus on proposals advanced by some groups that greater changes should be made in the general presumption that the responding party should bear the costs imposed by discovery requests. It will be some time, however, before the Committee determines whether any broader recommendations might be made.

(<http://www.ediscoverylaw.com/files/2013/11/Published-Rules-Package-Civil-Rules-Only.pdf>)

The April 2014 committee minutes give further color to the rule change. The minutes state that the reference to a protective order for the allocation of expenses “simply confirms authority that is already established by the rule provisions for protecting against undue burden or expense.” (<http://www.uscourts.gov/rules-policies/archives/meeting-minutes/advisory-committee-rules-civil-procedure-april-2014>). Specifically, the committee states that the new rule “should not change current practice by making cost-shifting a common event.”

In September 2014, the committee submitted the revisions with the June 2014 Rules Committee Report. (located here as Appendix B beginning on page 78, <http://www.uscourts.gov/rules-policies/archives/committee-reports/reports-judicial-conference-september-2014>). The report gives limited comment on the rule change, and states the following:

Rule 26(c)(1)(B) would be amended to include “the allocation of expenses” among the terms that may be included in a protective order. Rule 26(c)(1) already authorizes an order to protect against “undue burden or expense,” and this includes authority to allow discovery only on condition that the requesting party bear part or all of the costs of responding. The Supreme Court has acknowledged that courts have that authority now, *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358 (1978), and it is useful to make the authority explicit on the face of the rule to ensure that courts and the parties will consider this choice as an alternative to either denying requested discovery or ordering it despite the risk of imposing undue burdens and expense on the party who responds to the request.

The Committee Note explains that this clarification does not mean that cost-shifting should become a common practice. The assumption remains that the responding party ordinarily bears the costs of responding.

Committee Note: “Rule 26(c)(1)(B) is amended to include an express recognition of protective orders that allocate expenses for disclosure or discovery. Authority to enter such orders is included in the present rule, and courts already exercise this authority. Explicit recognition will forestall the temptation some parties may feel to contest this authority. Recognizing the authority does not imply that cost-shifting should become a common practice. Courts and parties should continue to assume that a responding party ordinarily bears the costs of responding.”

Commentator: (<http://defensecounseljournal.org/doi/full/10.12690/0895-0016-82.4.411>)

- This rule change further reaffirms the courts' ability to shift costs.
- “Clarifying courts' power in this regard is important because allocation of costs is a key mechanism by which courts and lawyers can focus discovery on information that is most important to the parties' claims and defenses – in other words, proportionality. It also confirms that ‘requester pays’ rulings are likely to become more common as courts enforce ‘proportional discovery.’”
 - o NOTE: The Chair of the subcommittee on this rule stated that no prejudging of “requester pays” proposals has happened and that work on cost issues would continue, but “it will not be easy.” (<http://www.uscourts.gov/rules-policies/archives/meeting-minutes/advisory-committee-rules-civil-procedure-april-2014>)
- “A key motivation behind the 2015 Amendments was to encourage courts and parties to manage discovery more actively so that cases may be determined on the merits at the lowest cost and in the least burdensome manner possible.”
- “Requiring requesting parties to share the costs of discovery is a common sense and self-executing management mechanism that incentivizes efficient discovery.”
- “It encourages each party to tailor its discovery requests by placing the cost-benefit decision on the party fashioning the request, and it provides an automatic disincentive to request overbroad discovery. A party making a claim or raising a defense is in the best position to decide if information is worth the cost of obtaining it.”
- “The newly amended rule affirms courts' ability to customize cost allocation for each individual case.”
- “A rule requiring a requester to pay some or all of the expenses resulting from its requests would also encourage practical cooperation among the parties.”
- → May 2, 2015 Report of the Rules Committee, 27 (noting that “[t]he Discovery Subcommittee continues to have the ‘requester pays’ topic on its agenda” and outlining questions involved in further information gathering efforts), available at pp. 171-175, available at <http://www.uscourts.gov/rules-policies/archives/agenda-books/committee-rules-practice-and-procedure-may-2015>.



WEDNESDAY, MARCH 8, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS
ENERGY AND UTILITIES LAW

When Everything Goes Black: The Cyber-Threat to Our Energy Infrastructure
Hampton

Speakers:

Bryony B. Hodges

Miles Keogh

James L. Kelly, Jr.



NARUC

**The National
Association
of Regulatory
Utility
Commissioner**

Cybersecurity for State Regulators

With Sample Questions for Regulators to Ask Utilities

**Miles Keogh
Christina Cody
NARUC Grants & Research**

June 2012

Funded by the U.S. Department of Energy

Acknowledgements and Disclaimers

The report you are reading was created under the State Electricity Regulators Capacity Assistance and Training (SERCAT) program, a project of the National Association of Regulatory Utility Commissioners (NARUC) Grants & Research Department. This material is based upon work supported by the Department of Energy under Award Number DE-OE0000123.

This report was authored by the Grants and Research Department. Throughout the preparation process, the members of NARUC provided the authors with editorial comments and suggestions. However, the views and opinions expressed herein are strictly those of the author(s) and may not necessarily agree with positions of NARUC or those of the U.S. Department of Energy.

Special thanks to:

Denis Bergeron, *Maine Public Utilities Commission*

Edison Electric Institute

Commissioner Terry Jarrett, *Missouri Public Service Commission*

Annabelle Lee, *Electric Power Research Institute*

Patrick Miller, *EnergySec & National Electric Sector Cybersecurity Organization*

NARUC Staff

Thomas Pearce, *Public Utility Commission of Ohio*

Jeffrey Pillon, *National Association of State Energy Officials*

Bridgette Remington, *Vermont Public Service Board*

Alan Rivaldo, *Public Utility Commission of Texas*

Daniel Searfoorce, *Pennsylvania Public Utility Commission*

Christopher Villarreal, *California Public Utilities Commission*

In addition, thanks to Patricia Hoffman and Larry Mansueti of the U.S. Department of Energy for their support of the SERCAT program.

Please direct questions regarding this report to Miles Keogh, NARUC's Director of Grants & Research, mkeogh@naruc.org; (202) 898-2200 and Christina Cody, Program Officer, Grants & Research, ccody@naruc.org; (202) 898-9374.

Disclaimer: This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

Introduction

We often hear reports of cyber attacks in the news, but how serious are the threats to our country's essential utility infrastructure, such as electricity, gas, water and telecommunications?¹ Many State utility regulators have begun asking how to best protect the services, information and data that are valuable to customers, companies, as well as the country. These regulators are charged with assuring that utility companies provide reliable and affordable service to their customers, and putting cybersecurity into the field of view of State regulators. Cybersecurity threats challenge the reliability, resiliency and safety of the electric grid, and utility spending to address cyber vulnerabilities can impact the bills that customers pay.

This primer addresses cybersecurity – particularly for the electric grid – for State utility regulators, though we hope that it will be useful for a wide audience of policymakers in this field. The primer provides some conceptual cybersecurity basics for the electric grid and provides links to how regulators can:

- Develop internal cybersecurity expertise;
- Ask good questions of their utilities;
- Engage in partnerships with the public and private sector to develop and implement cost-effective cybersecurity; and
- Begin to explore the integrity of their internal cybersecurity practices.

We find ourselves at a critical juncture for infrastructure protection as the grid transitions from a previously isolated environment to a complexly interconnected one. Today's electrical grid interconnects components of our traditional physical electrical infrastructure with less tangible information technology (IT) components such as networks, software and data. For the purposes of this primer (in which our primary concerns are areas pertinent to State regulators' jurisdiction) when we talk about cybersecurity and infrastructure, we are referring to the cybersecurity of not only the physical distribution and transmission grids, substations and offices, but also equipment and systems that communicate, store and act on data. Cybersecurity must encompass not only utility-owned systems, but some aspects of customer and third party components that interact with the grid, such as advanced meters and devices behind the meter. And more than simply being a function of hardware, cybersecurity is critically important as a function of software, data and the networks that use data to keep the system operating. Finally, there are human elements to cybersecurity, including system operators, customers and "bad guys" interacting at all levels of a system. With such a dynamic and broad landscape to consider, cybersecurity cannot be a stagnant prescription handed down from experts. It should evolve as technology, threats and vulnerabilities evolve, introducing the building blocks that stand the test of time while still being flexible enough to meet changing cybersecurity requirements.

Why Cybersecurity?

Cyber attacks that cripple the power grid or shut down other infrastructures may be rampant in Hollywood, but to date there have been no reports of a cyber attack successfully crippling critical utility

¹ DHS Critical Infrastructure Sectors are the following: Food and Agriculture; Banking and Finance; Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Government Facilities; Healthcare and Public Health; Information Technology; National Monuments and Icons; Nuclear Reactors, Materials and Waste; Postal and Shipping; Transportation Systems; Water (http://www.dhs.gov/files/programs/gc_1189168948944.shtm)

infrastructures in the United States – it is harder to do in the real world than in the movies. With all the attention given to impossible fictional attacks, it might be helpful to imagine an improbable but realistic scenario.

Imagine that one Sunday afternoon you turn on the TV to find major news reporting a troublesome, though not devastating blackout affecting a number of areas in your region. In the subsequent days, police and the system operator report that the information about load and generation the grid's regional transmission operator receives had been snuck out – exfiltrated – by parties unknown, and replaced with erroneous data. Dispatchers had to rely on conservative operations in dispatching power plants because they could not trust the data they were receiving without careful review. A few days later, a similar exploit occurs in a vertically-integrated utility's service territory, and soon it is occurring widely and regularly enough, regionally, that careful data review, cross-checking and expensive conservative dispatch become standard practices while the perpetrators are tracked down. Soon thereafter, utility officials report massive denial of service attacks directing tens of thousands of emails an hour to the mobile email systems of their experts and executives, clogging up the flow of information to coordinate response. The situation worsens when substations in the region begin experiencing equipment malfunctions, creating load management problems at the very time that system operators are addressing the system operations data integrity and denial of service problems. Checks of the substations reveal that the firmware in the programmable logic controllers of key sensor devices has been rewritten. It will take ongoing digital forensics to determine what the rewritten firmware even contains, much less how it was overwritten, or by whom.

Internal utility emails forwarded to the Public Service Commission warn their staff that malevolent programs are spreading on a peer-to-peer basis within the utility's business process systems looking to exfiltrate customer data, and the utility alerts the regulator that their system may be at risk as well because of the frequency of communications. The Public Service Commission orders an audit of its own internal data systems and IT staff reports that the State system has been successfully penetrated by intruders, but the vendor cannot be certain whether legally protected, commercially sensitive or even detailed utility infrastructure data has been taken. Market-driven system operations are on the shelf for the time being, distribution level reliability is regionally affected and customers are wondering if they can rely on their electric service. Companies and citizens alike are asking hard questions about whether their data is safe. Experts believe they have determined a remedy for breach, but as of now, they cannot be sure who perpetrated the attack and whether more attacks are planned. Service interruptions continue over the next few months, customers' information is still at large and the GDP has contracted significantly after months of stunted power provision across the interconnection.

This is a pretty bad scenario, but far from the worst case. A dedicated hacker group could accomplish the situation above. A nation-state or well-funded criminal syndicate could theoretically accomplish worse. The more likely scenario is a smaller attack that compromises data without necessarily affecting the operation of the grid. While the above scenario is realistic, the likelier reality may be much easier to address and mitigate. If regulators (and utilities) can imagine the more drastic possibility, it might be easier to imagine – and be prepared for – scenarios of lesser consequence.

Responding to Threats and Vulnerabilities

State governments are already hard at work implementing energy assurance plans across the country that help respond to vulnerabilities, as well as preventing and protecting against threats. There is an important distinction to understand between threats and vulnerabilities. A threat is the potential for an actor, circumstance or event to adversely affect assets, people or organizational operations of the system. A vulnerability is a specific weakness at any point in the system that can be exploited by a threat source. A good example is the difference between leaving a door to your house unlocked (creating a vulnerability) and doing so when there are burglars on your street (who pose a threat). Providing true energy assurance in cybersecurity includes addressing vulnerabilities and responding to threats in a way that is timely and assures normal conditions for the near future. The responsibility of prevention, protection, detection and responding is multi-pronged and shared between industry, local, state and federal actors.

Where Cybersecurity Fits

Cybersecurity vulnerabilities exist wherever computer systems and data exist. With the advent of smart grid technologies, which layer software on top of utility operations and computer systems, threats become increasingly likely and relevant. While a smarter grid is generally more reliable, new vulnerabilities appear that must be managed as grids become two-way exchanges of kilowatts, as well as network and customer-usage data that may be valuable and desirable to bad actors.²

Increase in Documented IT Vulnerabilities, Per Year

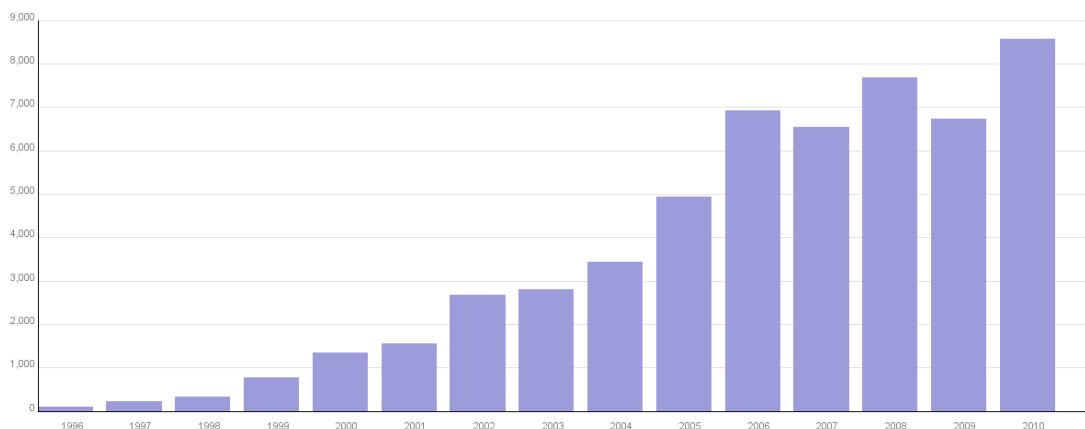


Figure 1 Data source: IBM X-Force 2010 Trend and Risk Report (for the IT and Telecom sectors).
<http://www-958.ibm.com/software/data/cognos/manyeyes/visualizations/vulnerabilities-per-year>

Threat Sources

While cybersecurity breaches can be caused by people, they are not always who we think of as “bad guys.” Criminal threats to the bulk power system can range from those of minimal impact to those of great consequence. For the purpose of this primer, we will focus on cyber attacks from intentionally malicious actors and how to protect against them, although the steps taken to create cybersecure systems are only one part of an all-hazards approach.³ Cybersecurity must protect against inadvertent sources – user errors (including accidents), hardware failure, software bugs, operator errors or plain negligence – as well as intentional attacks. Natural disasters can also play a role: a flooded server room

² NERC, “High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,” June 2010: 39.

³ All-hazards approach takes into account any threat to security, including unintentional or naturally-occurring ones

"On the low-impact end of the spectrum are common events, such as copper theft and the types of routine cyber attack common to all business networks in the Information Age. In the intermediate-impact range are events that may involve damage to a single system component in an unsophisticated, unstructured attack. On the high-impact end of the scale are highly-coordinated, well-planned attacks against multiple assets designed to disable the system."

High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," North American Electric Reliability Corporation (NERC), June 2010

cannot provide service any better than one flooded with data traffic from a denial of service attack. Other resources⁴ may be helpful in establishing an all-hazards approach that addresses risks other than intentional cyber attacks.

The aims and implications of cybersecurity violations vary widely. Gaining system control – the ability to remotely modify and operate the system as a vehicle for attack – is often the most difficult and least probable outcome. Data theft (or "exfiltration") is a known and ongoing problem. The scope of a cyber attack is

also an important consideration. Attacks that affect one person's data or that cripple one meter will generally have less impact than attacks that exploit larger amounts of data or that attack not one component, but multiple components or the network that connects them.

What Are We Protecting? Three Flavors

While natural disasters, human error, software bugs or equipment breakdowns can be the origins of a system failure, deliberate attacks involve the element of intent – a person at the other end of the operation with the capability to bring down a system specifically outside its existing protective barriers.⁵ Malicious attacks threaten utilities on multiple levels in ways that sometimes overlap and compound each other. It may be helpful to visualize the application of cybersecurity in three areas: IT, supervisory control and data acquisition (SCADA) systems, and smart grid. We'll explain each of these components of the data-connected grid and how cybersecurity relates to each.

Information Technology Systems

This is the arena where cybersecurity has historically focused: business process systems such as those found on your laptop computer, as well as in more sophisticated systems and networks that connect data and perform intelligent tasks with that data. It includes both components, like individual workstations, and network components that allow interoperability between components. If IT is all about connectivity – how systems talk to each other – then IT security begins by protecting the network that enables the flow of data through the system, as well as by protecting the data itself. This data can be financial information, a customer's street address, phone number, or information about their power usage, to name a few. IT connects all systems, from simple to complex, including communications between systems like the hub or the switch ("dumb") all the way to the firewall and the server ("smart"). Considering how valuable the data of utilities' systems are, the communication, transferences

Figure 2 Spectrum of Device Intelligence

⁴ Such as the NARUC/National Association of State Energy Officials (NASEO)/DOE Energy Assurance Guidelines: http://www.naruc.org/Publications/State_Energy_Assurance_Guidelines_Version_3.1.pdf

⁵ NERC, High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," 29.

and actions based on this data compound its intelligence value. For IT, cybersecurity not only includes software and hardware strategies – passwords, antivirus systems, firewalls, logical and physical separation of servers, for example – but also training personnel and creating policies so that their interaction with the IT system enhances, rather than erodes, cybersecurity. Because of this human element, simply upgrading or making hardware more obscure does not equal improved cybersecurity.⁶

Control Systems

SCADA encompasses systems that monitor and control industrial, infrastructure or facility-based processes, such as utility operations. They include simple functions such as “on/off,” sensor capability, communications capability and human-machine interface (HMI) that connects them to people operating the system. In other words, they are automatic (and often remote) control devices. SCADA security means the machine does what it is supposed to do and does it accurately. With a secure SCADA system, you can trust what your machine is telling you. However, according to executives with SCADA responsibilities, these systems more and more often have connections to Internet Protocol (IP) networks, including the internet in some cases.⁷ Even those physically and logically disconnected from other systems may be locally or remotely accessible and have vulnerabilities to be exploited. SCADA access and control points are also frequently located in remote and unmanned areas of the utility system, and therefore may require either increased physical security or the ability to isolate those points from the overall system if they become compromised.

Security for SCADA systems requires a system-wide understanding of how each of the components fit together so that vulnerabilities can be prioritized and addressed at each point.⁸ Depending on the situation, some devices may need to be remotely upgradeable, in which case these devices may need capability to use encryption, certificates and authentication. For other devices this may be impractical and access might be required in order to adjust to updated technology. When systems are remotely monitored and maintained, calibration and auditing can be important ways to ensure that they continue giving accurate information and perform functions in a trusted manner.

Crossing Over from Data Attacks to Physical Impacts: Aurora and Stuxnet

The most common target of cyber attack is sensitive data, but some examples are emerging that highlight the possibility of a successful physical attack that originates in the cyber arena.

In 2006, the Idaho National Laboratory (INL) staged a cyber attack nicknamed “Aurora” that crippled an electric power generator. The attack involved controlled hacking into a replica of a power plant's control system and misusing safety systems to change the operating cycle of the generator, sending it out of control and physically damaging and disabling it.

Emerging in 2009, “Stuxnet” was a self-replicating and –propagating software worm that also had the capacity to physically attack the grid. When an infected USB stick was inserted into a computer, malicious code awakened and surreptitiously dropped a large, partially encrypted file onto the computer, re-writing the programmable logic controller and changing the frequency of spinning drives that it controlled. By 2011, reports were circulating that it had been designed to attack specific centrifuges in Iran; it remains an example of software that can cause physical damage to the grid.

⁶ Miles Keogh, “The Smart Grid: Frequently Asked Questions for State Commissions,” *National Association of Regulatory Utility Commissioners*, May 2009: 6.

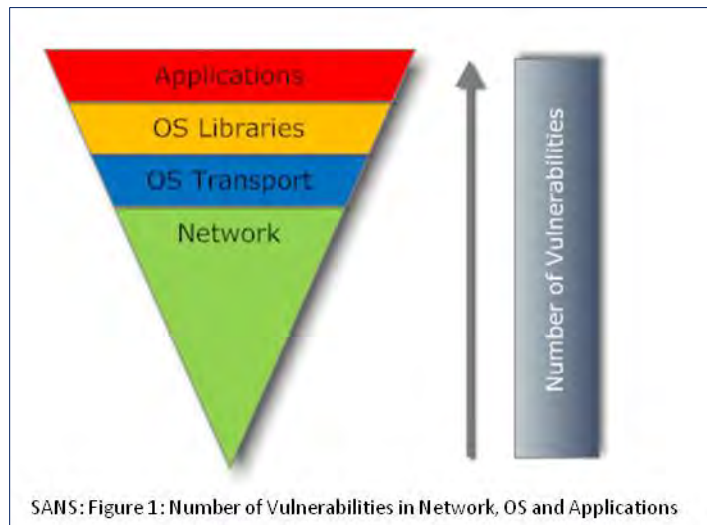
⁷ NERC, “High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,” 31.

⁸ Asset owners should be encouraged to do a risk assessment to determine which vulnerabilities to mitigate. Addressing all vulnerabilities may be cost and performance prohibitive.

Smart Grid

The smart grid is defined differently depending on who you ask, but for this primer it represents the modernization of electricity infrastructure through added technology, allowing the grid to gather and store data, to create a “dialogue” between all components of the grid, and allowing for automatic command and response within the function of the grid. In concept, smart grid provides so many improvements in situational awareness, prevention, management and restoration that, in spite of the new vulnerabilities it introduces, it fundamentally makes the electric system more secure.⁹ However, the smart grid enhances the need for cybersecurity because it adds a layer of computer systems and

software – all with additional doors to be hacked – to existing utility infrastructure. It may increase the portals through which a cyber threat could enter the system. Keep in mind that the more systems communicate with each other and their human operators, the more channels across which data is shared and, therefore, the more the systems require an assessment of their cybersecurity.



components that are compromised do not threaten the network, and that infiltrators are only able to access data in such a way that the attack is unproductive, undesirable, not valuable and detectable by operators.¹⁰

Compliance-Based and Risk-Based Approaches to Cybersecurity

Using Compliance as a Basis for Cybersecurity

The owners and operators of critical infrastructure have not been sitting idly by while cyber threats mount. NERC have developed standards- and compliance-based structures that require the operators of the bulk power system to take steps to conform to specific cybersecurity practices. These standards include assessing the systems you have, determining if there are specific vulnerabilities, and then taking action to address these as part of a compliance regime. In practice, these standards appear to be effective for motivating compliance, although some critics note that responding to a compliance regime does not necessarily overlap entirely with responding to a risk-assessed landscape of potential vulnerabilities and threats.

⁹ Keogh, “The Smart Grid: Frequently Asked Questions for State Commissions,” 6.

¹⁰ *Ibid.*

Any regulator interested in cybersecurity will be well-served by becoming familiar with what the NERC Critical Infrastructure Protection (CIP) standards require for the bulk power system. The NERC CIP Standards are enumerated below:

NERC CIP Standards

Number	Title/Summary	Date	Link
CIP-001-2a	Sabotage Reporting	02.16.2011	pdf
CIP-002-3	Cyber Security - Critical Cyber Asset Identification	12.16.2009	pdf
CIP-002-3a	Cyber Security - Critical Cyber Asset Identification	05.09.2012	pdf
CIP-002-4	Cyber Security - Critical Cyber Asset Identification	01.24.2011	pdf
CIP-002-4a	Cyber Security - Critical Cyber Asset Identification	05.09.2012	pdf
CIP-003-3	Cyber Security - Security Management Controls	12.16.2009	pdf
CIP-003-4	Cyber Security - Security Management Controls	01.24.2011	pdf
CIP-004-3	Cyber Security - Personnel & Training	12.16.2009	pdf
CIP-004-4	Cyber Security - Personnel & Training	01.24.2011	pdf
CIP-005-3a	Cyber Security - Electronic Security Perimeter(s)	02.16.2010	pdf
CIP-005-4a	Cyber Security - Electronic Security Perimeter(s)	01.24.2011	pdf
CIP-006-3c	Cyber Security - Physical Security of Critical Cyber Assets	02.16.2010	pdf
CIP-006-3d	Cyber Security - Physical Security of Critical Cyber Assets	02.09.2012	pdf
CIP-006-4c	Cyber Security - Physical Security of Critical Cyber Assets	01.24.2011	pdf
CIP-006-4d	Cyber Security - Physical Security of Critical Cyber Assets	02.09.2012	pdf
CIP-007-3	Cyber Security - Systems Security Management	12.16.2009	pdf
CIP-007-4	Cyber Security - Systems Security Management	01.24.2011	pdf
CIP-008-3	Cyber Security - Incident Reporting and Response Planning	12.16.2009	pdf
CIP-008-4	Cyber Security - Incident Reporting and Response Planning	01.24.2011	pdf
CIP-009-3	Cyber Security - Recovery Plans for Critical Cyber Assets	12.16.2009	pdf
CIP-009-4	Cyber Security - Recovery Plans for Critical Cyber Assets	01.24.2011	pdf

Figure 3 <http://www.nerc.com/page.php?cid=2%7C20>

While these standards are robust and a strong improvement over what existed before, State regulators should bear in mind that the NERC CIP Standards are still evolving as they relate to the bulk electric system. Those interested in improving upon these standards argue that distribution systems and other key areas where cybersecurity remain a concern to State regulators may not be entirely covered by the existing standards. Additionally, those who argue that the CIP standards are incomplete point out that compliance only proves *compliance*; utilities' cybersecurity should be based in *risk assessment*. Risk management includes assessment, mitigation and continuous improvement, whereas compliance offers a view of cybersecurity at a fixed point in time, not a dynamic picture of it. Utilities may be compliant to the CIP standards and still not be secure. Utilities may also be secure but not be compliant to the CIP standards. One is not the guarantee of the other.

Using Risk as a Basis for Cybersecurity

Understanding risk means understanding the relationship between vulnerability (such as a system with a known but unaddressed weakness), threat (such as a bad actor propagating viruses or worms) and consequence (such as physical damage and loss of public safety).¹¹ Simply understanding risks is just the first step: a risk-based approach prioritizes components for protection, as well as the threats and vulnerabilities that require attention. A risk-based approach starts with the assumption that an unauthorized user can and will gain access to data or the system, and thus designs responses based on the value of the data or system that could be compromised by the inevitable access. This calls for prioritizing data and systems based on their value to the organization or other useful criteria such as reliability and privacy. The utility or other organization can then decide which systems and programs should have the highest level of cybersecurity, best personnel resources, the right tools, and of course the right budget. Basing a cybersecurity strategy on risk augments traditional “outer wall” approaches to cybersecurity that seek to protect and deny access to the entire system with activities that focus on identifying and addressing the most significant cybersecurity issues. This includes understanding risks, prioritizing them by likelihood, consequence and potential interactions with other risks, and allocating resources accordingly.¹²

A Few Helpful Cybersecurity Concepts

State regulators are not responsible for building a strong cybersecurity capacity for critical infrastructure – utilities are responsible for this – but it is increasingly important that regulators be able to recognize underlying concepts of robust cybersecurity when it comes before them in a proceeding. A few of the concepts that should inform a regulator’s assessment of a utility’s cybersecurity proposal should include the following:

- Prioritizing systems and networks over components
- Ensuring that human factors are considered
- Deploying defense-in-depth
- Promoting system resilience

Securing Systems and Networks vs. Devices on the Network

Cybersecurity may call for securing entire networks, in addition to devices on that network. For example, the meters within a smart grid system can be fortified against attack, but in order to ensure the entire network of the smart grid system is secure, the components *linking* those meters, as well as every other component in between, must be secured as well. That way, if an attack occurs at one meter, the rest of the

system linked to that meter is not also at risk because the components linking them have been protected.¹³ This concept was explored in each of the three “flavors” of risk: IT, SCADA and smart grid.

Figure 4 Networks vs. Devices

¹¹ U.S. Department of Energy, “Electricity Subsector Cybersecurity Risk Management Process,” May 2012.

¹² Rich Baich and Ted DeZabala, “Cyber crime: a clear and present danger; Combating the fastest growing cyber security threat,” *Deloitte Center for Security & Privacy Solutions* (2010), http://www.deloitte.com/assets/Dcom-UnitedStates/Local%20Assets/Documents/AERS/us_aers_Deloitte%20Cyber%20Crime%20POV%20Jan252010.pdf.

¹³ It is worth mentioning that specific cybersecurity mechanisms will likely vary among devices and protection may be stronger or weaker across the devices in the system, depending on their importance and functionality.

Personnel Surety: Securing People As Well As Systems

A system is only as secure as the people who run and operate it. Training is essential to ensure that in the event of a cyber attack, personnel are skilled in identifying and responding to the impacts. Personnel can also be “insiders” involved in a deliberate or accidental cybersecurity breach. Identifying key personnel and using background checks is a potential strategy to mitigate this, but once they have been hired, policies that limit an individual’s ability to inflict harm may also be important. These policies, such as the Principle of Least Privilege and “Need to Know,”¹⁴ segregate duties. Securing personnel may also include conducting background checks, ensuring expertise through education,¹⁵ safe and supportive working conditions and finally, continual training to keep expertise up-to-date.¹⁶ Lastly, effective separation policies for employees, regardless of the reason for separation, should ensure that separated employees’ access to facilities, networks and SCADA systems are terminated as soon as it is appropriate.

Defense-In-Depth

Achieving defense-in-depth requires placing multiple, diverse barriers in front of a potential attacker. Imagine not only locking the outermost doors of an apartment building, but also hiring a guard who checks identification, locking the doors to each apartment, and monitoring loading docks and other points of access that are otherwise unwatched. Likewise, defense-in-depth starts with an overall cybersecurity policy that calls for multiple measures and employs cybersecurity strategies such as identifying authentication and authorization, admission control, encryption, integrity checking, detections of policy violations, data logging and data auditing. For more sophisticated equipment, these strategies may be a straightforward element bundled within the existing software. For older, “dumber” equipment, such as simple control systems, enabling this capacity may be difficult or impossible, necessitating other cybersecurity strategies. Effective cybersecurity often encompasses physical as well as technological measures – restricted access to server rooms, locks on smart meters, security fencing and cameras at key substations, for example.

Resilience and Recovery

The electric industry is an incredibly resilient industry. In the event of extreme storms in the past, power lines have been restored much sooner than homes are rebuilt. Resilience of the electric sector to cyber attack should be no less resilient than to a tornado. While defense-in-depth plans for the unexpected, resilience ensures that the unexpected will not persist indefinitely. A resilient system will not only be prepared for deterring, defending against and mitigating attacks, but also for ensuring quick and efficient restoration in the event that an attack compromises the system, through disaster recovery planning. Plans should be stored in a way that a cyber attack does not affect access to them, such as a backup hard copy in an accessible, but physically secured, location that is water- and fireproof.

What Regulators Can Do

The regulatory role in this arena is increasing. More cyber attacks to business processes and NERC CIP Standards compliance are driving new cybersecurity expenditures by utilities that may be featured in future rate cases. The deployment of smart grid adds new cost and reliability elements to this puzzle. Regulators are already hard at work to address cybersecurity risks to the American power grid and the

¹⁴ Principle of least privilege is defined as having access to the least information or fewest resources necessary to complete a legitimate purpose; “Need to know” is a practice that restricts information or resources in the execution of a task outside of what is critical in order to complete that task, despite clearance level.

¹⁵ A good example is available from the State of Michigan’s personnel protocol: www.michigan.gov/cybersecurity.

¹⁶ NERC, “High-Impact, Low-Frequency Event Risk to the North American Bulk Power System,” 15.

greater infrastructure of utilities. But there's more to be done and, in the face of shrinking budgets, fluctuating workforce and the absence of comprehensive legislation, regulators need a dynamic strategy to strike the right balance of security and resources.

Although regulators will not need to be experts at implementing utility cybersecurity, they will be well-served by asking smart cybersecurity questions of utilities, the entities responsible for conducting risk assessment. These questions are the basis of evaluating prudence, which we will discuss in the next section. Staff specializing in cybersecurity at commissions are an invaluable resource for drafting the relevant cybersecurity questions for Commissioners to ask utilities during cases. It is very important that questions posed to utilities, however, do not reveal information that could be valuable to a cyber attacker, because answers submitted by utilities during a proceeding are subject to the Freedom of Information Act (FOIA) and can therefore be accessed by the public – potentially including people with malicious intent. Some States have a Critical Infrastructure Confidentiality Statute or other authority that protects against this vulnerability. Please see the Appendix for NARUC's *Sample Cyber Questions to Ask Your Utilities*. It is intended that you will customize these questions to each relevant scenario, while maintaining the phrasing of the questions, which avoids potential cybersecurity risk in the utility's response.

The NARUC Resolution Regarding Cybersecurity, adopted on February 17, 2010, calls for "continued vigilance against all potential sources of cyber threat to be both prepared to prevent cyber attacks capable of disrupting utility services and to mitigate the harmful consequences of such attacks in order to protect public health, public safety and the economy."¹⁷ Key tenets of the resolution encourage Commissioners to prioritize the consistent monitoring and evaluating of cybersecurity in collaboration with agencies having expertise in cyber threat management and mitigation in order to remain effective in meeting evolving cyber challenges. Commissioners should regularly revisit their own cybersecurity policies and procedures "to ensure that they are in compliance with applicable standards and best practices."¹⁸ Keep in mind that ensuring new investments in technologies that are designed with cybersecurity in mind at the front end will create cybersecurity more effectively than adding it to systems later.

The resolution encourages regulators to initiate a dialogue with their utilities to ensure that the utilities are also in compliance with standards. In order to properly review filings to this end, regulators may wish to develop and maintain staff expertise on cybersecurity as it relates to the following topics suggested by NASEO¹⁹:

1. What is the insider threat and what policies and procedures are in place to prevent intrusion and manipulation?
2. Technical solutions to cybersecurity should account for human behavior, which can be driven by both cultural and psychological factors
3. Nature of the threat from employees, contractors, consultants or anyone with short or long term access to IT systems and knowledge about system vulnerabilities
4. Effect of new systems on consumer behavior – will it strengthen cybersecurity or incite actions to attack the system?

¹⁷ NARUC Committee on Critical Infrastructure, "Resolution Regarding Cybersecurity," adopted at the NARUC Winter Meeting of 2010, February 17, 2010.

¹⁸ *Ibid.*

¹⁹ NASEO, "Smart Grid and Cyber Security for Energy Assurance," November 2011: 16.

Training Resources

Regulators may wish to invest in training staff on cybersecurity standards and to provide regular updates to training as information changes and technology advances. Internal staff should also be responsible for understanding the cybersecurity of their agency. It may be valuable to have staff members fluent in the concepts of cybersecurity available to serve as a point person for the rest of the staff on all issues relating to cybersecurity. In this way, not only those with an information technology workload familiar with cybersecurity, but those involved with rate cases, siting cases, reliability oversight and planning will have access to cybersecurity concepts and principles so that this becomes a regular part of the content of a regulatory process when appropriate.

NARUC provides cybersecurity training free of charge through grant-funded programs once or twice per year and convenes cybersecurity expertise at its meetings. In partnership with the National Electricity Sector Cybersecurity Organization (NESCO), NARUC also hosts regular threat assessment teleconferences. It may also be worthwhile to explore what training options may be available through your State's homeland security department, or other in-state sources.

Other resources include:

- U. S. Computer Emergency Readiness Team's (U.S. Computer Emergency Readiness Team (CERT) and U.S. Department of Homeland Security (DHS) Control Systems Security Program training: http://www.us-cert.gov/control_systems/cstraining.html
- Pacific Northwest Control System training: <http://eioc.pnnl.gov/training.stm>
- INL "Red Team / Blue Team" training: http://www.inl.gov/scada/training/advanced_scada.shtml
- Multi-State Information Sharing and Analysis Center (MS-ISAC) <http://msisac.cisecurity.org/>
- FBI's InfraGard Program: <http://www.infragard.net/>

Ask Questions

Standards, such as the NERC CIP Standards described later in this document, are important but should not be considered to be exhaustive. For example, specific technology standards will not address all the aspects of cybersecurity that are critical, such as high level policies and procedures, that are commonly excluded from standards. Furthermore, existing processes may cover many bulk generation and smart grid aspects of the system, but guidance, standards and other regulations may not currently suffice for elements of the distribution system. It may fall to regulators to ask questions of utilities to determine if there are gaps and facilitate action.

This may be the key role for commissions in cybersecurity. Commissions do not need to become cyber industry authorities or enforcers, but asking a utility a question may motivate the development of a well-founded answer. NARUC has been developing a series of sample questions that originate with some of the interrogatories developed by States with their utilities. These may prove a helpful starting point and are included in *Appendix A* of this primer.

Asking questions isn't enough – once the right questions have been asked of utilities, regulators bear the responsibility of understanding the answers to determine whether they represent prudent activities and investments. Regulators have to determine whether the amount being invested is insufficient or excessive and whether it is allocated appropriately. Regulators must then help prioritize these investments along with all the other proposed spending that a utility proposes in a rate case. Regulators must keep the cost of electricity affordable for customers while asking utilities to spend more on cybersecurity in the face of increasing media attention on stories of cybersecurity threats and vulnerabilities.

Information Protection

The line between knowing enough to determine that a utility's actions are prudent and knowing so much that the information held by the Commission can pose a cybersecurity risk is a line that commissions should walk carefully. In cybersecurity, the information itself is sometimes the asset worth stealing. To address this issue, States may wish to consider establishing a critical infrastructure information policy. This policy would govern not only the type of information the commission could take possession of (or refuse to take possession of), but also under what circumstances, as well as which access, handling and storage protocols would govern that data. For example, Pennsylvania's Public Utility Confidential Security Information Disclosure Protection Act allows public utilities to restrict certain information from public disclosure and Right-to-Know requests. The Act also puts the onus on State agencies to protect any confidential cybersecurity information belonging to the utility that the State has in its possession, including sensitive parts of emergency or cybersecurity plans.

Commissions should become familiar with their State's information access and transparency laws – such as the FOIA and Sunshine laws – and ensure that sensitive information is not gathered in a context which would enable it to be publicly accessible. Many States have good cybersecurity exemption rules that properly address utility sectors and associated processes while providing automatic protection of information related to cybersecurity. State agencies can develop and communicate their non-disclosure procedures and, where appropriate, may want to consider stronger protections for cybersecurity and information than for commercially sensitive information.

Finally, just because it is legally and procedurally protected does not mean that it's actually cybersecure. Commissions should carefully consider whether they need information before asking for it, because even if they can keep it out of the public record and exclude it from FOIA, it may still be vulnerable to theft via cyber attack.

Prudence

Ordinarily, a regulator could examine the likelihood and consequence of a potential incident to determine whether the cost of a mitigation strategy was prudent, but with no history of cyber attack and a wide range of potential consequences, there is little guidance that a regulator can turn to. What is a regulator to do?

The below formula is one potential to start from in evaluating prudence by trying to keep the cost of protection lower than the value of what is being protected.

$$P \leq V \leq A$$

Where

V = the value of the components or service provided by the system or data

P = the cost to protect the system/data, and

A = the cost, or risk to an attacker, of the attack.

The value of the service should be greater than the cost of protecting it. These variables can be highly dynamic. For example, the value of keeping electricity flowing to Fenway Park is higher during a Red Sox

game than it is in the dead of night after the game is over.²⁰ Strategies such as loss containment (protecting the overall system, even if some individual components can be compromised) and deterrence (making the attack unprofitable, limited in scope and easily traceable) may be effective alternatives to complete protection. The values assigned to P and V should be based on a risk assessment that utilities have the ability and responsibility to perform with regulatory oversight and auditing. Understanding the cost or risk of attack is an additional tool in assessing the quality of cybersecurity. If expensive protection can be cheaply defeated, regulators may want to explore an alternative investment.

Developing Expertise: Resources for Regulators to Become Familiar With

Cybersecurity remains an area where a lot of work needs to be done, but it is worth noting that many institutions and frameworks have been set up that have already made an enormous amount of progress. Some of these are listed below. Many of these groups are open to State personnel to monitor, join and participate in, and this may be an important way to become appropriately engaged with companies and other stakeholders working on these issues before they emerge in the context of a hearing room. Particularly if a State has multiple regulated utilities, information sharing between utilities, and potentially PUCs, may be a very important step towards coordinated cyber defense.

Drivers for Cybersecurity Expenditures

Aside from good business practices by the utilities that dictate that they should prevent attacks on their systems, State regulators should understand three key additional areas that motivate and inform smart utility investments in cybersecurity: laws, enforceable standards and voluntary best-practice guidance.

Industry standards enforce legislation that utilities must meet, and these standards do not come cheaply. Standards require additional resources in the form of employees, hours and technology, all of which increases the cost of providing reliable electricity to the customer. Therefore, the standards of cybersecurity that protect the customer are then ultimately paid by the customer. So what are these standards and who sets them? Some of the most important sets of standards are described in this section.

NERC CIP

<http://www.nerc.com/page.php?cid=6|69>

The first step for developing cyber expertise is to understand, and where possible engage with, the NERC CIP Standards. These standards already drive a good deal of cybersecurity investments and, as greater coverage is applied to protection of the electric grid, this process will only become more important. NERC's CIP efforts include standards development, compliance enforcement, and supporting and providing technical subject matter expertise to the program. The committee consists of industry experts and reports to NERC's board of trustees in the areas of cybersecurity, physical and operational security. The U.S. Department of Energy (DOE) designated NERC as electricity sector coordinator for critical infrastructure protection.

NIST National Cybersecurity Center of Excellence

<http://www.nist.gov/itl/csd/nccoe-022112.cfm>

The National Institute of Standards and Technology (NIST) recently announced the establishment, in partnership with the state of Maryland and Montgomery County, Maryland, a National Cybersecurity

²⁰ The authors concede this example may be debatable depending on the visiting team and the score.

Center of Excellence. The center will assume \$12 million of NIST's 2012 budget and will bring together researchers, user and vendors in targeted tests to address cybersecurity issues.

NIST Smart Grid Interoperability Panel and Cyber Security Working Group

<http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG>

NIST works collaboratively with industry and government agencies. A wide range of stakeholders and working groups make up the NIST Smart Grid Interoperability Panel (SGIP), responsible, through an open consensus-based process, for interoperable standards aimed at enhancing economic security and quality of life. The SGIP's Cyber Security Working Group (CSWG) works to develop an overall cybersecurity strategy for the smart grid that includes a risk mitigation strategy to ensure interoperability of solutions across different parts of the infrastructure. The CSWG has developed the NIST Interagency Report (NISTIR) 7628, Guidelines for Smart Grid Cyber Security, available here: <http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628>.

The NARUC/NASEO Energy Assurance Guidelines

Along with organizations like NARUC and the NASEO, which runs an energy assurance program to address state-level coordination on critical infrastructure protection, other national organizations are doing their part to address cybersecurity needs for the energy sector and to serve as resources to government decision makers. Those efforts are detailed in the following. You can learn more about NASEO's Energy Assurance Program here: <http://naseo.org/energyassurance/>.

Securities and Exchange Commission Corporation Finance Disclosure Guidance: Cybersecurity

<http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>

In October 2011, the SEC released this guidance to clarify the cybersecurity responsibility of publicly traded companies. Federal securities law requires that publicly traded companies report "material" risk – something that was not clearly defined or followed for cybersecurity risks before this document was released.²¹ This is a vital moment because now a publicly traded company can consider cybersecurity as a business investment.

DHS Cross Sector Working Group – CIPAC

http://www.dhs.gov/files/committees/gc_1277402017258.shtm

The DHS Cross-Sector Security Working Groups include the Critical Infrastructure Partnership Advisory Council (CIPAC), which facilitates coordination between federal IP programs and the equivalent programs of private sector, State, local, territorial and travel entities. It also operates a forum in which government and critical infrastructure – key resource owners can coordinate critical infrastructure protection.

EI Principles for Cybersecurity and Critical Infrastructure Protection

The Edison Electric Institute (EEI) released the principles in 2010 to address the electric utility industry's mandate to provide reliable power. EEI prioritizes collaboration between the State and federal level, as well as distinguishing between the priorities of responses to threats and vulnerabilities. The *EEI Principles for Cybersecurity and Critical Infrastructure Protection* can be found here: http://www.eei.org/ourissues/ElectricityTransmission/Documents/cyber_security_principles.pdf.

²¹ Jay Rockefeller and Michael Chertoff, "A new line of defense in cybersecurity, with help from the SEC," *The Washington Post*, November 17, 2011, http://www.washingtonpost.com/opinions/a-new-line-of-defense-in-cybersecurity-with-help-from-the-sec/2011/11/15/gIQAjBX8VN_story.html.

NESCO/NESCOR

To meet the “exponential increase in complexity in securing an ever growing electric grid with an increasing number of stakeholders,” NESCO creates a “comprehensive public private partnership to coordinate the efforts in the industry to meet the growing challenge of securing the electric sector.” The Energy and Water Development and Related Agencies Appropriations Act of 2010 enabled DOE to establish “an independent national energy sector cybersecurity organization.” EnergySec and Electric Power Research Institute (EPRI) received fund awards to form NESCO and NESCOR (National Electric Sector Cybersecurity Organization Resource). The two organizations bring together experts to strengthen the cybersecurity posture of the electric sector by working with the DOE Electricity Sector Information Sharing and Analysis Center and industry. More information can be found here: http://www.energysec.org/Websites/energysec/files/Content/840313/2011.02.22_WhatIsNESCO_Webinar.pdf.

Smart Grid Investment Grant Cybersecurity Requirements

The American Recovery and Reinvestment Act of 2009 (Recovery Act) authorized funding for the DOE to modernize the electric power grid, including accelerating smart grid development through competitive selection of investment projects in a number of areas, one of which was cybersecurity.²² This program, called the Smart Grid Investment Grant (SGIG) program, currently supports initiatives like Critical Intelligence Inc.’s Intelligence Training for Targeted Cyber Attacks based in Idaho to train energy sector information security employees to detect and respond to cyber threats (http://www.smartgrid.gov/project/critical_intelligence_inc), and broader programs such as Pepco’s “Smart Grid Workforce Training Project” in Washington, D.C., which includes a cybersecurity component through compliance training as part of their overall implementation program (<http://www.smartgrid.gov/project/pepco>). The SGIG program is just one example of the hardening of the US smart grid currently in place.

NRECA Guide to Developing a Cybersecurity and Risk Mitigation Plan

The National Rural Electric Cooperative Association (NRECA) cybersecurity plan addresses general business operations for cooperatives addressing critical infrastructure needs in their systems. The plan is based on the NISTIR 7628, a survey of standards and security concepts specifically for the smart grid, found: <http://www.smartgrid.gov/sites/default/files/doc/files/CyberSecurityGuideforanElectricCooperativeV11-2%5B1%5D.pdf>.

DOE/NIST/NERC RMP

The Risk Management Process (RMP), resulting from a collaboration between DOE, NIST and NERC, is a resource geared toward strategic long-term risk management mapped specifically to the electric sector. Authorship of the document, which is still in the works, includes industry and utility-specific trade groups. More information can be found here: <http://energy.gov/oe/articles/departement-energy-releases-draft-cybersecurity-risk-management-process-rmp-guideline>

Electric Sector Cybersecurity Risk Management Maturity Initiative

This initiative will serve as a tool for the electric sector to assess their security posture at a given point in time. Driven by the highest levels of the US government the resulting resource should be relevant and important, though as of this writing it remains a work in progress.

²² www.smartgrid.gov

Developing Legislation

Congress has been working on comprehensive legislation for the past four years. Regardless of federal actions in this arena, however, State commissions should be tackling this issue within their jurisdictions to ensure a secure cyber future. The Congressional Research Service (CRS) provides good information on relevant legislation in their latest report, *Cybersecurity: Authoritative Reports and Resources*, which can be found here: <http://www.fas.org/sgp/crs/misc/R42507.pdf>.²³

Conclusion

Absolute cybersecurity is neither attainable, nor is it the end goal. What's more, according to NERC, addressing high-impact, low-frequency risk like cybersecurity requires the re-allocation of "already strained human and financial resources available to the sector."²⁴ Therefore, cybersecurity is best approached through a nimble and complex balance of functionality, security and cost. The reality of a "perfect" defense against cyber attack has a cost that may, and often does, outweigh the value of the information it protects. Simply put, the energy sector cannot expect to "gold plate" the grid. Planning for, protecting against, detecting and responding to cyber attack must take into account a dynamic relationship of systems, physical components, people and their function.

State utility regulators can and should:

- Create expertise within their own organizations
- Ask the right questions of utilities
- Assess their own cybersecurity and information protection capabilities
- Engage with other efforts: led by the private sector, State agencies or federal officials, as well as engaging with processes that link these sectors

Regulators are already doing significant work to protect the grid, but the key to successful cybersecurity may prove to be the development of a partnership between public and private actors to create a cybersecurity structure and culture that can meet current needs while also being flexible enough to meet the ever-evolving threat.

²³ Rita Tehan, "Cybersecurity: Authoritative Reports and Resources," *Congressional Research Service*, April 26, 2012.

²⁴ NERC, "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," pg. 23

Appendix A:

National Association of Regulatory Utility Commissioner

Sample Cyber Questions to Modify and Ask Your Utilities

The following questions grew out of several PUCs efforts to ask critical cybersecurity questions of utilities in an effort to ensure reliable electricity for their rate payers. NARUC has built the following list from those original questions, editing where necessary for sensitivities, clarity and general usage so that these questions could be used in commissions across the country. These are general questions, they are not exhaustive, nor are they all appropriate for every scenario or region. You must adapt the questions to your own taste, but when you do so, make sure the answers will not create vulnerabilities. These questions not only generate answers from utilities, but inspire their action to meet any gaps in current operations. Your utilities may not be particularly forthcoming with some of their answers, but their answers create a dialogue of understanding and responsibility in the event of a cyber attack.

Your needs for your PUC will vary – please modify these questions before using them in order to suit your needs. For example, drop the questions that are too difficult or are unnecessary! You do not need to use questions below which you think will yield answers that contain unnecessary or overly complex information. Where questions below reference a process or a plan that the utility probably has in hard copy, you may want to ask to see a copy of it.

You may want to describe to the utility how you will handle and safeguard the responses to these questions. Lastly, and most importantly, *do not ask questions whose answers can create vulnerabilities.*

Planning

Having a plan indicates that the response isn't piece-meal, reactive or fragmented. Asking planning questions aims to encourage proactive and strategic action on the part of the utilities, rather than a patchwork response.

1. Does your company have a cybersecurity policy, strategy or governing document?
2. Is the cybersecurity policy reviewed or audited? Internally or by an outside party? What qualifications does the company consider relevant to this type of review?
3. Does your cybersecurity plan contain both cyber *and* physical security components, or does your physical security plan identify critical cyber assets? (See the *Glossary, Appendix 2*, for helpful definitions).
4. Does your cybersecurity plan include recognition of critical facilities and/or cyber assets that are dependent upon IT or automated processing?
5. Are interdependent service providers (for example, fuel suppliers, telecommunications providers, meter data processors) included in risk assessments?

6. Does your cybersecurity plan include alternative methods for meeting critical functional responsibilities in the absence of IT or communication technology?
7. Has your organization conducted a cyber risk or vulnerability assessment of its information systems, control systems and other networked systems?
8. Has your company conducted a cybersecurity evaluation of key assets in concert with the National Cyber Security Division of the Department of Homeland Security? Has your company had contact with the National Cyber Security Division of DHS or other elements of DHS that may be helpful in this arena?
9. Has your cybersecurity plan been reviewed in the last year and updated as needed?
10. Is your cybersecurity plan tested regularly? Is it tested internally or by or with a third party?
11. What is your process/plan for managing risk? (Example: DOE/NIST/NERC Risk RMP)
12. Has your company undergone a whole-system, comprehensive cybersecurity audit or assessment? When and by whom?

Standards

Standards are an important driver of enforceable action with which regulators can attempt to ensure utilities' compliance.

13. Describe the company's compliance status with NERC CIP-002 through CIP-009. *(Note: Be aware that this may create double-reporting).*
14. What collaborative organizations or efforts has your company interacted with or become involved with to improve its cybersecurity posture (such as NESCO, NESCOR, Fusion centers, Infragard, US-CERT, ICS-CERT, ES-ISAC, SANS, the Cross-Sector Cyber Security Working Group of the National Sector Partnership, etc.)?
15. Can your company identify any other mandatory cybersecurity standards that apply to its systems? What is your company's plan for certifying its compliance or identifying that it has a timetable for compliance? *(Note: PUCs might also need to first establish standards for compliance they find suitable)*
16. Compliance as a floor, not a ceiling: are there beyond-compliance activities? Given that there are very little or no cybersecurity standards specified at this point by State regulatory authorities in regard to the distribution portion of the electrical grid, what are you doing to get in front of this?
17. How do you determine which systems, components and functions get priority in regard to implementation of new cybersecurity measures?

18. Is cybersecurity addressed differently for each major electrical component: distribution, transmission, generation, retail customers?

Procurement Practices

While the information of procurement seen upstream to vendors may only be proprietary to the utility, the decisions the vendor makes around procurement may contain key elements for cybersecurity. The questions below cover these aspects of procurement.

19. Has your organization conducted an evaluation of the cybersecurity risks for major systems at each stage of the system deployment lifecycle? What has been done with the results?
20. Are cybersecurity criteria used for vendor and device selection?
21. Have vendors documented & independently verified their cybersecurity controls? Who is the verifier and how are they qualified?
22. Does your organization perform vulnerability assessment activities as part of the acquisition cycle for products in each of the following areas: cybersecurity, SCADA, smart grid, internet connectivity and Web site hosting?
23. Has the company managed cybersecurity in the replacement and upgrade cycle of its networked equipment? Does this include smart meters?
24. What kind of guidance do you follow to ensure that your procurement language is both specific and comprehensive enough to result in acquiring secure components and systems? (Note: Does your company include Cyber Security Procurement Language for Control Systems within its Procurement Language? Available at http://www.us-cert.gov/control_systems/pdf/FINAL-Procurement_Language_Rev4_100809.pdf IEC 62443)
25. Would the company be willing to provide a presentation to Staff (as a closed, *in-camera* and non-disclosable setting with no documentation or materials coming into possession of the PUC)?

Personnel and Policies

Personnel, the people who run the systems we aim to protect, are key to ensuring cybersecurity. The way employees are hired, trained and separated from operations can make or break cybersecurity.

26. Is cybersecurity budgeted for? What is the current budget for cybersecurity activities relative to the overall security spending?
27. Are individuals specifically assigned cybersecurity responsibility? Do you have a Chief Security Officer and do they have explicit cybersecurity responsibilities?

28. Does your company employ IT personnel directly, use outsourcing or employ both approaches to address IT issues? For companies that lack a full IT department, explain if one individual in your company is held responsible for IT security. (You may want to ask same questions in regard to Operations Technology (OT) (i.e. energy operations) security; larger companies may have separate staffs.)
29. What training is provided to personnel that are involved with cybersecurity control, implementation and policies?
30. What personnel surety / background checking is performed for those with access to key cyber components? Are vendors and other third parties that have access to key cyber systems screened?
31. For the most critical systems, are multiple operators required to implement changes that risk consequential events? Is a Change Management process in place, especially in regard to systems which could present a risk to electrical reliability?
32. Has business process cybersecurity has been included in continuity of operations plans for areas like customer data, billing, etc.?
33. Describe the company's current practices that are employed to protect proprietary information and customer privacy and personal information. Does the company have an information classification and handling policy?
34. Does the company collect personally identifiable information electronically? What type of information (name, address, social security number etc.) is collected? Is there a policy for the protection of this information? How is your company ensuring that any third parties you deal with are also keeping this information secure?
35. Identify whether the company has identified points of contact for cybersecurity:
 - a. Emergency management / law enforcement?
 - b. National security? DHS, including protective and cybersecurity advisors?
 - c. Fellow utilities, ISO/RTO, NERC CIPC, others?
 - d. NESCO, VirtualUSA, Einstein, Fusion centers, Infragard, US-CERT, ICS-CERT, ES-ISAC?
 - e. Interdependent system service providers?

Systems and Operations

Be aware that as the questioning agency, you want to consider carefully whether answers to the below questions are needed and, if so, whether the answers to them could create vulnerabilities to the system. Modify them to your needs accordingly.

36. Is cybersecurity integrated between business systems and control systems? For the existing grid and for the smart grid?
37. Have logical and physical connections to key systems been evaluated and addressed?
38. Does the company maintain standards and expectations for downtime during the upgrade and replacement cycle?
39. Does the company have equipment dependant on remote upgrades to firmware or software, or have plans to implement such systems? Does the company have a plan in place to maintain system cybersecurity during statistically probable upgrade failures? Is there a schedule for required password updates from default vendor or manufacturer passwords?
40. Has cybersecurity been identified in the physical security plans for the assets, reflecting planning for a blended cyber / physical attack?
41. Discuss what the PUC can do to assist your company in the area of cybersecurity.
42. What network protocols (IP, proprietary, etc.) are used in remote communications? Is the potential vulnerability of each protocol considered in deployment?
43. Does the company have a log monitoring capability with analytics and alerting – also known as “continuous monitoring”?
44. Are records kept of cybersecurity access to key systems?
45. Are systems audited to detect cybersecurity intrusions?
46. Are records kept of successful cybersecurity intrusions?
47. What reporting occurs in the event of an attempted cybersecurity breach, successful or not? To whom is this report provided (internal and external)? What reporting is required and what is courtesy reporting?

Appendix B

Glossary	
All-Hazards Approach	Comprehensive approach to security that includes intentional, unintentional, man-made and naturally-occurring threats to the electric grid
Attestation ²⁵	The validation of all aspects of a component that relate to its safe, secure and correct operation
Authentication ²⁶	Verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources
Authorization ²⁷	Verifying a user's permissions (after the user had been authenticated) for accessing certain resources or functionality
Bandwidth ²⁸	A communication channel the amount of information that can be passed through a communication channel in a given amount of time, usually expressed in bits per second
Boundary protection ²⁹	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels)
Bulk Electric System (BES) Cyber Asset ³⁰	A cyber asset that if rendered unavailable, degraded or misused would, within 15 minutes of its required operation, mis-operation or non-operation, adversely impact facilities, systems or equipment, which, if destroyed, degraded or otherwise rendered unavailable when needed, would affect the reliable operation of the bulk electric system
Connectivity ³¹	the minimum number of nodes or links whose removal results in losing all paths that can be used to transfer information from a source to a sink
Confidentiality ³²	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information
Contingency ³³	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch or other electrical element
Control Center ³⁴	Facilities hosting operating personnel that monitor and control the Bulk Electric System (BES) in real-time to perform the reliability functional tasks of: 1) a Reliability Coordinator, 2) a Balancing Authority, 3) a Transmission Operator for Transmission Facilities at two or more locations, or 4) a

²⁵ Evgeny Lebanidze and Craig Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," *National Rural Electric Cooperative Association Cooperative Research Network* (2011): 113.

²⁶ *Ibid.*

²⁷ *Ibid.*

²⁸ ATIS Telecom Glossary 2012, <http://www.atis.org/glossary/definition.aspx?id=5692>

²⁹ Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.

³⁰ NERC, "Glossary of Terms Used in NERC Reliability Standards," May 25, 2012: 9.

³¹ ATIS Telecom Glossary 2012, <http://www.atis.org/glossary/definition.aspx?id=6637>

³² Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.

³³ *Ibid.*

³⁴ NERC, "Glossary of Terms Used in NERC Reliability Standards," 13.

	Generation Operator for generation Facilities at two or more locations
Credential ³⁵	Information passed from one entity to another to establish the sender's access rights or to establish the claimed identity of a security subjective relative to a given security domain
Critical Assets ³⁶	Facilities, systems and equipment which, if destroyed, degraded or otherwise rendered unavailable, would affect the reliability or operability of the bulk electric system
Critical Infrastructure ³⁷	The assets, systems and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety or any combination thereof
Cyber Asset ³⁸	Programmable electronic devices, including the hardware, software and data in those devices
Cybersecurity Incident ³⁹	A malicious act or suspicious event that: 1) Compromises, or was an attempt to compromise, the ESP or PSP, or 2) disrupts, or was an attempt to disrupt, the operation of a BES cyber system
Denial of Service (DoS) ⁴⁰	Unauthorized prevention or (for time-critical operations) delay of any part of an information system (IS) from legitimate access or functioning
Deterrence	Designing a system to that an attack would be unprofitable, limited in scope and easily traceable
Electronic Security Perimeter (ESP) ⁴¹	The logical border surrounding a network to which systems are connected
Energy Assurance	Infrastructure that is robust, secure, provides reliable energy and is able to restore services rapidly in the event of any disaster
Encryption (also encipherment) ⁴²	The cryptographic transformation of data that produces coded text
Firmware	Embedded software that cannot be modified, but allows reading and executing software
Header ⁴³	The portion of a message that contains information used to guide the message to the correct destination. <i>Note:</i> Examples of items that may be in a header are the addresses of the sender and receiver, precedence level, routing instructions and synchronizing bits
Identity-Based Access Control ⁴⁴	Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of

³⁵ ATIS Telecom Glossary 2012, <http://www.atis.org/glossary/definition.aspx?id=6764>

³⁶ Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.

³⁷ U.S. Department of Homeland Security, "Critical Infrastructure," (May 23, 2012):

http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

³⁸ Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.

³⁹ NERC, "Glossary of Terms Used in NERC Reliability Standards," 14.

⁴⁰ Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.

⁴¹ NERC, "Glossary of Terms Used in NERC Reliability Standards," 18.

⁴² ATIS Telecom Glossary 2012, <http://www.atis.org/glossary/definition.aspx?id=8119>

⁴³ ATIS Telecom Glossary 2012, <http://www.atis.org/glossary/definition.aspx?id=4731>

⁴⁴ Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 113.

	that user) where access authorizations to specific objects are assigned based on user identity
Impacta ⁴⁵	Damage to an organization's mission and goals due to the loss of confidentiality, integrity or availability of system information or operations
Incident ⁴⁶	An occurrence that actually or potentially jeopardizes the confidentiality, integrity or availability of a system or the information the system processes, stores or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures or acceptable use policies
Information Security ⁴⁷	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability
Information System ⁴⁸	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information (Note: information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems and environmental control systems.)
Information Technology	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information
Integrity ⁴⁹	Guarding against improper information modification or destruction; includes ensuring the non-repudiation and authenticity of information
Internet protocol	A formal set of conventions (both semantic and syntactic) governing the format and control of interaction among parts of the system that communicate with each other
Interoperability ⁵⁰	Ability of diverse systems and their components to work together; enables integration, effective cooperation and two-way communication among the many interconnected elements of the electric power grid
Least Privilege	Principle of having access to the least information or fewest resources necessary to complete a legitimate purpose
Latency ⁵¹	Refers to the speed with which network data is transmitted or processed. A system with low latency communicates more quickly, while a high latency connection generally communicates less frequently and has longer delays
Loss Containment	Protecting the overall system, even if some individual components can be compromised

⁴⁵ *Ibid.*

⁴⁶ *Ibid.*

⁴⁷ Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.

⁴⁸ *Ibid.*

⁴⁹ *Ibid.*

⁵⁰ NIST, "NIST & the Smart Grid," (May 23, 2012): <http://www.nist.gov/smartgrid/nistandsmartgrid.cfm>.

⁵¹ Keogh, "The Smart Grid: Frequently Asked Questions for State Commissions," 5.

Management controls ⁵²	The security controls (i.e., safeguards or countermeasures) of an information system that focus on the management of risk and of information system security
Need to Know	A practice that restricts information or resources in the execution of a task outside of what is critical in order to complete that task, despite clearance level
Network (Computer Network) ⁵³	collection of hardware components and computers interconnected by communication channels that allow sharing of resources and information
Non-repudiation	Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information or receiving a message
Operational controls	The security controls (i.e., safeguards or countermeasures) of an information system that are primarily implemented and executed by people (as opposed to systems)
Packet ⁵⁴	The sequence of binary digits transmitted and switched as a composite whole
Physical Security Perimeter (PSP) ⁵⁵	The physical border surrounding locations in which cyber assets, systems or electronic access control systems reside and for which access is controlled
Potential impact ⁵⁶	The loss of confidentiality, integrity or availability that might be expected to have: (i) a limited adverse effect (FIPS 199 low); (ii) a serious adverse effect (FIPS 199 moderate); or (iii) a severe or catastrophic adverse effect (FIPS 199 high) on organizational operations, organizational assets or individuals
Privileged user ⁵⁷	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform
Programmable logic controller (PLC) ⁵⁸	A digital computer used for the automation of electromechanical processes
Resilience	The ability to restore services rapidly in the event of any disaster
Right-to-Know	Legal principle that a citizen has the right to know a piece of information about a potential hazard
Risk ⁵⁹	Measure of the extent to which an entity is threatened, typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Security risks related to information security arise from the loss of confidentiality, integrity or availability of information or information systems with potential adverse impacts on operations

⁵² Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.

⁵³ ATIS Telecom Glossary 2012, <http://www.atis.org/glossary/definition.aspx?id=6555>

⁵⁴ ATIS Telecom Glossary 2012, <http://www.atis.org/glossary/definition.aspx?id=30770>

⁵⁵ NERC, "Glossary of Terms Used in NERC Reliability Standards," May 25, 2012:36.

⁵⁶ Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 114.

⁵⁷ *Ibid.*

⁵⁸ Lebanidze and Miller, "Guide to Developing a Cyber Security and Risk Mitigation Plan," 115.

⁵⁹ *Ibid.*

Risk management	The process conducting a risk assessment, implementing a risk mitigation strategy and employing of techniques and procedures for the continuous monitoring of the security state of the information system. Risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place – synonymous with risk analysis
Risk severity ⁶⁰	A combination of the likelihood of a damaging event actually occurring and the assessed potential impact on the organization’s mission and goals if it does occur
Role-based access control ⁶¹	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals
Sensitive information ⁶²	Information of which the loss, misuse, unauthorized access or modification could adversely affect the organization, its employees or its customers
Smart Grid	Modernization of electricity infrastructure through added technology, allowing the grid to gather and store data, to create a “dialogue” between all components of the grid, and allowing for automatic command and response within the function of the grid
Supervisory Control and Data Acquisition (SCADA)	Systems that monitor and control industrial, infrastructure or facility-based processes, such as automatic (and often remote) control devices. They include simple functions such as “on/off” and sensor capability, communications capability and the human-machine interface (HMI) that connects them to people operating the system
Threat	The potential for an actor, circumstance or event to adversely affect assets, people or organizational operations of the system
Traffic ⁶³	The information moved over a communication channel, including the quantitative measurement of the total messages and their length, expressed in CCS or other units, during a specified period of time
Virus	An unwanted computer program that replicates itself and spread from one computer to another. “Virus” is often incorrectly used to refer to malware, including adware and spyware programs, which do not have a reproductive ability
Vulnerability	A specific weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source

⁶⁰ Lebanidze and Miller, “Guide to Developing a Cyber Security and Risk Mitigation Plan,” 115.

⁶¹ *Ibid.*

⁶² Lebanidze and Miller, “Guide to Developing a Cyber Security and Risk Mitigation Plan,” 116.

⁶³ ATIS Telecom Glossary 2012, <http://www.atis.org/glossary/definition.aspx?id=649>

Lighting the way to...



Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10



WEDNESDAY, MARCH 8, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

EXTRA CONTRACTUAL LIABILITY

Defending Against Attorney's Fee Requests

Cypress

Speakers:

Robert L. Kaufman

Donald L. Miller

W. Neil Rambin

Jennifer D. Eubanks

RECENT TRENDS IN ATTORNEY FEE AWARDS CONCERNING CONSUMER PROTECTION AND BAD FAITH LAW

GENERAL RULES AND BACKGROUND

- **American Rule:** Recognized in all states and federal appellate districts: “Unless otherwise specified by contract, rule, or statute, each party is responsible for its own attorney fees.”

Alyeska Pipeline Serv. Co. v. Wilderness Soc'y, 421 U.S. 240, 247, 257, 95 S.Ct. 1612, 44 L.Ed.2d 141 (1975); *Fox v. Vice*, 563 U.S. 826, 131 S.Ct. 2205, 2213, 180 L.Ed.2d 45 (2011). See also, *Merit Const. Alliance v. City of Quincey*, 759 Fed.3d 122 (1st Cir. 2014); *ReliaStar Life Ins. Co. of N.Y. v. EMC Nat. Life Co.*, 564 F.3d 81 (2d Cir. 2009); *Polonski v. Trump Taj Mahal Assoc.*, 137 F.3d 139 (3d Cir. 1998); *Andrews v. America’s Living Centers, LLC*, 827 F.3d 306 (4th Cir. 2016); *Moench v. Marquette Transp. Co. Gulf-Inland, L.L.C.*, 838 F.3d 586, 595 (5th Cir. 2016); *McQueary v. Conway*, 614 F.3d 591 (6th Cir. 2010); *Fednav Intern. Ltd. V. Continental Ins. Co.*, 624 F.3d 834 (7th Cir. 2010); *Lamb Engineering and Const. Co. v. Nebraska Public Power Dist.*, 103 F.3d 1422 (8th Cir. 1997); *Riordan v. State Farm Mutual Auto. Ins. Co.*, 589 F.3d 999 (9th Cir. 2009); *United States v. McCall*, 235 F.3d 1211, 1216 (10th Cir.2000); *Misener Marine Const., Inc. v. Norfolk Dredging Co.*, 594 F.3d 832 (11th Cir. 2010); *Nepera Chem., Inc. v. Sea-Land Serv., Inc.*, 794 F.2d 688 (D.D.C. 1986); *Bywaters v. U.S.*, 670 F.3d 1221 (Fed. Cir. 2012).

- **Exceptions:**

(1) Equitable Grounds (conduct-based)

-Federal Courts

- Federal courts have inherent authority to award attorney fees against losing party based upon proof of “bad faith” conduct. See *Alyeska Pipeline Serv. Co. v. Wilderness Soc'y*, 421 U.S. 240, 247, 257, 95 S.Ct. 1612, 44 L.Ed.2d 141 (1975); *F.D. Rich Co. v. United States ex rel. Indus. Lumber Co.*, 417 U.S. 116, 129 (1974) (court may assess attorney fees upon proof losing party "acted in bad faith, vexatiously, wantonly, or for oppressive reasons.")

- State courts – some recognize as exception, but not all

a) West Virginia recognizes a court’s authority in equity to award to the prevailing litigant his or her reasonable attorney's fees as ‘costs,’ without express statutory authorization, “when the losing party has acted in bad faith, vexatiously, wantonly or for oppressive reasons.” *Thomas v. Houck*, 2016 WL 6780095, at *5 (W.Va. Nov. 16, 2016)

b) Idaho courts do not possess a general equitable authority to order a party to pay an opponent’s attorney fees. *Fournier v. Fournier*, 874 P.2d 600, 602, 125 Idaho 789, 791 (Idaho Ct. App. 1994).

(2) Contract Provision (substance of action)

Contracting parties can establish the right to attorney fees by contract and, when done so, “the contract controls, so that attorney fees are awarded under such contracts with no difficulty”)

James G. Davis Constr. Corp. v. HRGM Corp., 147 A.3d 332, 339 (D.C. 2016) (citing *Dobbs, Law of Remedies* § 3.10 (3), at 402–03; § 3.11 (3), at 483))

(3) Statutory Provision (substance of action)

- Where an award of attorney fees is allowed by statute, a trial court retains the authority to determine what claims for attorneys’ fees are reasonable. *Capitol Cadillac Olds, Inc. v. Roberts*, 813 S.W.2d 287 (Ky. 1991).

- *Alexander v. S & M Motors, Inc.*, 28 S.W.3d 303 (Ky. 2000). Kentucky Consumer Protection Act permits (but does **not** mandate) award of attorney fees and costs. This is intended to compensate litigants for pursuing rights under the statute in cases where recovery often “does not provide a reasonable return.” *Id.* at 305. Also provides attorneys with incentive to represent litigants asserting claims serving a public purpose, traditionally “low-value” claims. A court’s guiding “polar star” when considering a motion for attorney fees under the KCPA should be to “[keep] the courthouse door open for those aggrieved by violations of the act.” *Id.* at 306.

- **“Prevailing Party” defined:** either plaintiff or defendant; not necessarily required to obtain final judgment. Rather, plaintiff can prevail upon settlement (*Maher v. Gagne*, 448 U.S. 122, 129 (1980); *Williams v. Alioto*, 625 F.2d 845, 848 (9th Cir. 1980) (per curiam), *cert. denied*, 101 S. Ct. 1723 (1981)). However, prevailing defendant standard different, as often requires proof of bad faith conduct on part of plaintiff. *See, e.g., Arcese v. Daniel Schmitt & Company*, – S.W.3d --- 2016 WL 4598539 (Mo.App. Sept. 6, 2016) (see Section II, below).

- **Disparate Financial Positions No Exception**

Savannah College of Art and Design, Inc. v. Houeix, 2005 WL 1073608 (S.D. Ohio 2005); courts should not recognize the disparate financial positions of the parties to be a factor making an “exceptional” case for attorney fees. *See also, Kellogg Co. v. Toucan Golf, Inc.*, 337 F.3d 616, 629 (6th Cir.2003), and *Eagles Ltd. v. American Eagle Foundation*, 356 F.3d 724 (6th Cir. 2004).

- **Fee Must Meet “Reasonableness” Standard**

- *Reed v. Rhodes*, 179 F.3d 453 (6th Cir.1999). Primary concern is that fee awarded be reasonable. Prevailing market rates, not the attorney’s normal hourly rate, qualifies the “reasonableness” of fees. Hourly rates should not exceed market rates or prevailing market rates in community necessary to encourage lawyers to undertake representation in question.

- *Blum v. Stenson*, 465 U.S. 886, 897, 104 S. Ct. 1541, 79 L. Ed. 2d 891 (1984). Reasonable fee is adequate to attract competent counsel, but not produce windfalls to attorneys.

- *Johnson v. Georgia Highway Express, Inc.*, 488 F.2d 714 (5th Cir.1974), adopted by *Hensley v. Eckerhart*, 461 U.S. 424, 103 S. Ct. 1933, 76 L. Ed. 2d 40 (1983): court must first determine the lodestar amount by multiplying the reasonable number of hours billed by a reasonable billing rate. *Johnson* court expressly noted that “courts must remember that they do not have a mandate ... to make the prevailing counsel rich.” 488 F.2d at 719.

- *Brown v. Fulton, Hubbard & Hubbard*, 817 S.W.2d 899 (Ky. App. 1991): factors to be considered in determining reasonableness:

- (1) time and labor required, novelty and difficulty of the questions involved, and skill requisite to perform the legal service properly;
- (2) likelihood that the acceptance of the particular employment will preclude other employment by lawyer;
- (3) fee customarily charged in locality for similar legal services;
- (4) amount involved and results obtained;
- (5) time limitations imposed by client or circumstances;
- (6) nature and length of professional relationship with client;
- (7) experience, reputation, and ability of lawyer or lawyers performing services;
- and
- (8) whether fee is fixed or contingent.

• Use of Survey Data to Determine Reasonableness: Courts frequently consider survey data to resolve fees disputes and contested fee issues. In consumer protection cases, many courts use US Consumer Law Attorney Fee Survey Report. See, e.g., *Decker v. Transworld Systems, Inc.*, 2009 WL 2916819 (N.D. Ill. 2009); *Suleski v. Bryant Lafayette & Assoc.*, 2010 WL 1904968 (E.D.Wis. 2010); and *Wamsley v. Kemp*, 2010 WL 1610734 (S.D. OH 2010).

Standard of Review on Appeal

Awards of attorneys' fees are reviewed for an abuse of discretion. *Indihar v. State Farm Mut. Auto. Ins. Co.*, No. 2015 WL 9033348, at *6 (Ariz. Ct. App. Dec. 15, 2015) (citing *Co hen v. Frey*, 215 Ariz. 62, 68, ¶ 18, 157 P.3d 482, 488 (App.2007))

II. RECENT CONSUMER PROTECTION / BAD FAITH CASES CONSIDERING ATTORNEY FEE AWARDS.

E.D.N.Y. 2016: (National Flood Insurance Program preempts state law extra-contractual requests for attorneys' fees and penalties)

Melanson v. U.S. Forensic, LLC, 183 F. Supp. 3d 376 (E.D.N.Y. 2016)

Claims by insureds, other than for breach of contract, arising from conduct falling within the scope of the NFIP, are preempted (*citing Ravasio v. Fid. Nat'l Prop. & Cas. Ins. Co.*, 81 F.Supp.3d 274 (E.D.N.Y.2015) (Spatt, J.) (expressly rejecting the plaintiffs "extra-contractual requests for interest, costs, and attorneys' fees" because the NFIP "preempts state law claims for penalties and attorneys' fees brought against WYO insurance carriers participating in the" Program); and *Wing Bldg. Holding Co. LLC v. Std. Fire Ins. Co.*, 2015 WL 631956, at *4, (N.D.N.Y. Feb. 13, 2015) (rejecting proposed claims based on fraud and unfair claims settlement practices because, under Article IX, "the SFIP preempts all state-law claims"); *Southbridge 21 LLC v. Std Fire Ins. Co.*, No. 3:14-cv-374, 2014 WL 4637083, at *3, 2014 U.S. Dist. LEXIS 128960, at *6-*12 (N.D.N.Y. Sept. 16, 2014) (dismissing claim based on an insurer's alleged "willful and negligent refusal to bargain in good faith"; noting that "[a]lthough the Second Circuit has not spoken on this issue," the weight of authority from other circuits holds that "absent authorization by the NFIA and/or the SFIP, an insured may not assert extra-contractual claims against a private insurance company authorized to "write their own" federally-underwritten Standard Flood Insurance Policy).

• Missouri Court of Appeals, 2016: (prevailing defendant not entitled to attorneys' fee award under statute permitting fees to "prevailing party," under facts presented)

Arcese v. Daniel Schmitt & Company, – S.W.3d --- 2016 WL 4598539 (Mo.App. Sept. 6, 2016): Missouri Court of Appeals reversed sizeable attorney fees awarded to prevailing **defendant** under Missouri Merchandising Practices Act, Section 407.010, *et seq.*, which permitted award to "prevailing party." Court acknowledged legislature's employ of "prevailing party" in the fee-shifting clause of the MMPA was not unique. However, fundamental purpose of MMPA is to protect customers and consumers, citing *Berry v. Volkswagen Grp. of Am., Inc.*, 397 S.W.3d 425, 433 (Mo. banc 2013).

"The MMPA is paternalistic legislation designed to protect those that could not otherwise protect themselves." *Id.* (citations omitted). To promote this laudable purpose, the MMPA broadly prohibits false, fraudulent or deceptive merchandising practices and affords our trial courts remedial measures (i.e., damages, injunctions, equitable relief, and attorney's fees), "designed not only to remedy violations of the MMPA, but also prospectively to deter prohibited conduct and protect Missouri citizens." *Id.*

Arcese, 2016 WL 4598539, at *15 (Mo. Ct. App. Sept. 6, 2016). *Arcese* concluded an award of attorney fees to prevailing defendant should occur only rarely, and only upon proof that plaintiff pursued vexatious and frivolous claims.

• **E.D. Kentucky 2016** (*attorneys' fees did not constitute "ascertainable loss" for KCPA*)

Foster v. Am. Fire & Cas. Co., 2016 WL 6662695, at *6 (E.D. Ky. Nov. 10, 2016)

The district court rejected plaintiff's argument that his attorneys fees incurred in litigation he initiated constituted an "ascertainable loss" for purposes of KRS § 367.220(1) and KY Consumer Protection Act. *Foster* court distinguished *Indiana Insurance Company v. Demetre*, 2015 WL 393041 (Ky Ct. App., Jan. 30, 2015, *Opinion ordered not to be published*), which held "attorney fees incurred due to unfair, fraudulent or tortious conduct by an insurer is an ascertainable loss [for purposes of Act]." See 2015 WL 393041 (currently pending on discretionary review to KY Supreme Court). However, *Foster* court held plaintiff sufficiently pointed to additional "evidence from which a factfinder could find or infer that [he] suffered an actual loss." A jury could reasonably determine that a UIM benefits policy under which it would take plaintiff almost seven years to recover would constitute "an item that is different from or inferior to" that for which Mr. Foster bargained. See *Capps*, 2015 WL 2445911, at *5. In this light, the court refused to grant defendant insurer's motion for summary judgment.

• **W.D. Kentucky 2016**: (*attorneys' fees provided by statute or contract could be considered in determining amount in controversy for diversity jurisdiction, 28 U.S.C. § 1332*).

Everett v. Am. Gen. Life Ins. Co., 2016 WL 4746214, at *1 (W.D. Ky. Sept. 12, 2016)

Plaintiff Everett sought judgment against Defendant Am. Gen Life Ins. Co. for policy benefit of \$50,000 allegedly owed to her, plus a claim under the Kentucky Unfair Claims Settlement Practices Act ("UCSPA"), KRS 304.12-230. This action was originally filed in KY state court and removed to federal district court by Am. Gen Life under 28 U.S.C. § 1332. Plaintiff moved to remand on grounds of timeliness and amount in controversy. In determining whether it had jurisdiction, Court considered all of Plaintiff's damages claims under the UCSPA—including the request for punitive damages and **attorneys' fees** (citing *Hayes v. Equitable Energy Res. Co.*, 266 F.3d 560, 572 (6th Cir. 2001) (citation omitted); *Pendergrass v. Time Ins. Co.*, No. 5:09-CV-00215-R, 2010 WL 989154, at *2 (W.D. Ky. Mar. 12, 2010)). The Court reached conclusion that when claims for compensatory and punitive damages and **attorneys' fees** under the UCSPA are coupled with Plaintiffs breach of contract claim for \$50,000, it is "more likely than not" that Defendant has established by a preponderance of the evidence that the amount in controversy exceeds \$75,000. Motion to remand denied. See also, *Brady v. Safeco Ins. Co.*, 2015 WL 4720242, at *1 (W.D. Ky. Aug. 7, 2015) (Plaintiffs asserted claims under the Unfair Claims Settlement Practices Act and the Consumer Protection Act, and also sought to recover reasonable attorneys' fees, which provided basis for the court to find by a preponderance of the evidence that the amount in controversy requirement has been met.)

• **S.D.N.Y. 2016** (*no cause of action for third-party claimant under Alaska's UCSPA*)

Barba v. Allianz Glob. Risks US Ins. Co., 2016 WL 6236324, at *9 (S.D.N.Y. Oct. 25, 2016).

Plaintiff, survivor of helicopter crash on Arizona lake in December 2012, sued defendant Allianz Global Risks US Insurance Company ("Allianz") for (1) breach of contract/wrongful denial of coverage; and (2) breach of the duty of good faith and fair dealing. She sought declaratory relief; damages; and attorneys' fees and costs. Plaintiff was the assignee of an aviation insurance policy provided by Allianz to the owners of the helicopter that crashed. Court dismissed Plaintiff's

claims against Allianz for breach of contract and bad faith. In particular, court dismissed alleged violations under the Alaska UCSPA, AS 21.36.125, for failure to state claim because “no private right of action lies under that statute,” (citing *O.K. Lumber Co. v. Providence Washington Ins. Co.*, 759 P.2d 523, 527 (Alaska 1988) (“We therefore conclude that a third party claimant has no cause of action against an insurer under AS 21.36.125.”)).

- **E.D. Kentucky 2015:** (*Kentucky’s UCSPA limiting attorneys’ fees award to 1st party claimants only does not apply to limit 3d party award for costs and expenses*)

Ellis v. Arrowood Indem. Co., 2015 WL 2061936, at *11 (E.D. Ky. Apr. 30, 2015)

Court agreed plain text of provision in Kentucky’s UCSPA, KRS § 304.12–235(3), permitting attorney’s fees for “insured person[s]” and “health care provider[s]” does not extend to third-party claimants. However, the limited authorization of “attorneys’ fees” to first-party claimants did not bar third-party claimants from seeking their costs and expenses, exclusive of attorneys’ fees.

- **District of Maine 2015:** (*Maine fee-shifting statute and common law permits award of attorneys’ fees where insured prevails in duty-to-defend action*)

Metro. Prop. & Cas. Ins. Co. v. McCarthy, 2015 WL 5440793 (D. Me. Sept. 15, 2015)

Maine fee-shifting statute for duty-to-defend declaratory judgment actions involving insurance policies, Title 24–A M.R.S. § 2436–B(2), instructs “[i]n an action... to determine an insurer’s contractual duty to defend an insured under an insurance policy, if the insured prevails in such action, the insurer shall pay court costs and reasonable attorney’s fees.” This right to fees is personal to the insured and cannot be construed to permit assignment of rights by insured to any other person or create or extend any right or cause of action for a 3rd-party claimant). Court held insured entitled to fees under statute.

Maine common law also establishes a fee-shifting regime in duty-to-defend cases. Unlike the statute, this right is available to 3rd party assignees. Its purpose is to “place the insured in a position equally as good as the insured would have occupied had the insurance contract been fully and properly performed from the beginning.” (citing *Gibson v. Farm Family Mut. Ins. Co.*, 673 A.2d 1350, 1355 (Me.1996)). Under Maine common law, attorney fees are available to the insured only when the insurer resists a duty to defend that is clear from the policy and the pleadings filed against the insured. Court held 3rd party assignee entitled to be made whole for the full amount of attorneys’ fees incurred defending insurance company’s declaratory judgment action.

- **New Jersey 2015:** (*NJ Rule of Court permitting attorneys’ fees award in insurance liability action not extended to first-party claimant*)

Wadeer v. New Jersey Mfrs. Ins. Co., 220 N.J. 591, 612, 110 A.3d 19, 31 (2015), court noted “New Jersey Court Rules allow for counsel fees to be awarded “in an action upon a liability or indemnity policy of insurance, in favor of a successful claimant.” R. 4:42–9(a)(6). However, with respect to first-party insurance, such as UM/UIM coverage, the statutory prescription for attorney’s fees is inapplicable. Rule 4:42–9(a)(6) has not been extended to authorize a fee award

to an insured who brings direct suit against his insurer to enforce any direct coverage, including UM/UIM coverage. We refer this issue to the Civil Practice Committee for comments and recommendations addressing the issue.”

• **New York 2014:** *(recovery of attorneys' fees may not be had in an affirmative action by insured to settle its rights)*

Kings Infiniti Inc. v. Zurich Am. Ins. Co., 43 Misc. 3d 1207(A), 990 N.Y.S.2d 437 (N.Y. Sup. 2014). Court dismissed plaintiffs' demand for attorneys' fees and costs in unfair claims settlement case. “Attorneys' fees and disbursements are incidents of litigation which the prevailing party may not collect from the loser unless such an award is authorized by agreement between the parties, by statute, or by court rule” [citations omitted]. Although it is true that an insured is allowed to recover its legal fees in an action brought against it by an insurer “in an effort to free itself from its policy obligations,” the recovery of attorneys' fees “may not be had in an affirmative action by [the insured] to settle its rights” (*Mighty Midgets*, 47 N.Y.2d at 21; see also *New York Univ.*, 87 N.Y.2d at 324; *Stein, LLC v. Lawyers Title Ins. Corp.*, 100 AD3d 622, 623 [2d Dept 2012]). Thus, even where an insurer improperly disclaims coverage, it is not liable for attorneys' fees expended in suing the insurer to establish coverage (see *Mighty Midgets*, 47 N.Y.2d at 21; *Kramarik v. Travelers*, 25 AD3d 960, 963 [3d Dept 2006]; *Chase Manhattan Bank v. Each Individual Underwriter Bound to Lloyd's Policy No. 790/004A89005*, 258 A.D.2d 1, 4 [1st Dept 1999]).”

• **Washington Court of Appeals 2014:** *(defendants entitled to attorneys' fees award for successful defense of contract action, where contract provided for attorneys' fees to “prevailing party”)*

Kloster v. Roberts, 179 Wash. App. 1025 (2014). Where land sale contract provided “If the Buyer, Seller, or any real estate licensee or broker involved in this transaction is *involved in any dispute relating to this transaction*, any prevailing party shall recover reasonable attorneys' fees and costs,” Washington Court of Appeals held trial court properly awarded reasonable attorney fees and costs to defendants, real estate broker and land seller, who successfully defended action which also included claims for violations of UCSPA and Consumer Protection Act, because parties sale agreement provided for same. Plaintiffs argued the trial court erred when awarding defendants' fees because their claim was not for a breach of *contract* but for misrepresentation and concealment. The appellate court disagreed and upheld fees award.

Washington Court of Appeals 2013: *(Where offer of judgment silent on attorneys' fees, it did not preclude award of same)*

Washington Greensview Apartment Assocs. v. Travelers Prop. Cas. Co. of Am., 295 P.3d 284 (Wash. App. 2013). Owner of apartment complex asserted various claims against his property insurer, including breach of insurance contract and violations of Washington's Unfair Claims Settlement Practices Regulation and Consumer Protection Act. Owner then accepted offer of judgment from insurer, and moved for entry of judgment and for an award of attorney fees against insurer. Trial court entered judgment against insurer and awarded costs to owner but denied owner's request for attorney fees. Owner appealed. Appellate court held the offer was

silent on the issue of attorney fees and, thus, did not preclude an award of attorney fees to owner in addition to the judgment amount set forth in the offer; any misapprehension of law by insurer as to the requirement that the offer unambiguously indicate whether it included attorney fees did not equate to an absence of a meeting of the minds of insurer and owner; authority on which owner relied for an award of attorney fees that it incurred as a result of its insurance-coverage claim did not define attorney fees as costs, and thus owner was entitled to those fees as well as the judgment amount set forth in the offer; and owner was entitled to an award of attorney fees on appeal.

- **West Virginia 2013:** *(plaintiffs entitled to attorneys' fees for successful defense of coverage claim but not entitled to attorneys' fees for successful litigation of bad faith claim)*

Lemasters v. Nationwide Mut. Ins. Co., 232 W. Va. 215, 224, 751 S.E.2d 735, 744 (2013)

Majority opinion affirmed trial court's conclusion that plaintiff who prevailed in action against an insurer for coverage was permitted attorneys' fees award, but was not entitled to attorneys' fees incurred in litigating alleged violation of the Unfair Trade Practices Act ("UTPA"). Dissent contended the conclusion was based upon flawed reasoning and overruled precedent established by the Court in *Jenkins v. J.C. Penney Casualty Insurance Co.*, 167 W.Va. 597, 280 S.E.2d 252 (1981), *overruled on other grounds by State ex rel. State Farm Fire & Casualty Co. v. Madden*, 192 W.Va. 155, 451 S.E.2d 721 (1994), and its progeny.

- **Idaho, 2013/2010:** *(party's successful invocation of Idaho's Consumer Protection Act entitled to attorneys' fees)*

Duspiva v. Filmlmore, 293 P.3d 651, 661 (Idaho 2013). The Idaho Supreme Court stated "Under I.C. § 48-08(5), a party who invokes the protection of the ICPA [Idaho Consumer Protection Act] and prevails is entitled to reasonable attorney fees based on an application of the prevailing party analysis from I.R.C.P. 54(d)(1)(B)."

See also, Taylor v. McNichols, 243 P.3d 642, 665 (Idaho 2010). Idaho's is one of several consumer protection statutes providing for attorney fees to a prevailing defendant when the plaintiff's action is found to be for harassment or is spurious in nature. *See*, IDAHO CODE § 48-608(5) (2015). In *Taylor*, defendant awarded attorney fees because plaintiff appealed his consumer protection claim despite fact that it failed as a matter of law, evidence the claim brought spuriously and for harassment purposes.

- **Elderly or Disabled Victim – Additional Penalty**

Idaho statute I.C. § 48-608 (2) provides for **extra \$15,000 penalty** or treble damages, whichever is greater, assessed for unfair trade practices where the victim is elderly or disabled. *See* I.C. § 48-608 (2).

Nevada's Deceptive Trade Practices Act. *See* Nev. Rev. Stat. §§ 598.0903–598.0999. A private civil action may be commenced under the NDTPA **only by** "an elderly person or a person with a disability." *In re Chocolate Confectionary Antitrust Litig.*, 749 F. Supp. 2d 224, 234 (M.D. Pa. 2010).

Kansas Consumer Protection Act, Kansas Statute Annotated 1999 Supp. 50–677, provides: If any person is found to have violated any provision of the Kansas consumer protection act, and such violation is committed against elder or disabled persons, in addition to any civil penalty otherwise provided by law, the court may impose an ***additional civil penalty not to exceed \$10,000*** for such violation. *Caputo v. Prof'l Recovery Servs., Inc.*, 261 F. Supp. 2d 1249, 1262 (D. Kan. 2003).

Delaware and New Jersey Consumer Fraud Acts: DE and NJ state statutes provide civil penalties of \$10,000 for violations of the Delaware and New Jersey Consumer Fraud Acts that may have affected elderly or disabled persons in violation of 6 Del. C. §§ 2580 *et seq.* and N.J. Stat. Ann. § 56:8–14.3. *Harnish v. Widener Univ. Sch. of Law*, 931 F. Supp. 2d 641, 646 (D.N.J. 2013)



WEDNESDAY, MARCH 8, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS
INTERNATIONAL PRACTICE AND LAW

Window on Europe - Brexit
Drayton

Speakers:

Stephen L. Carter (UK)
Jorge Angell (Spain)
Christophe Adrien (France)
Pelin Baysal (Turkey)

BREXIT

Stephen Carter – Partner (Carter Perry Bailey LLP, London, England)

FDCC INTERNATIONAL SECTION

WINTER MEETING – 7 MARCH 2017

About 6,000 years ago, a small piece of land (a little smaller than Oregon) was separated from the rest of Europe by about 20 miles of water as a result of rising seas and the Storegga Slides. For the next 6,000 years we pretty much kept ourselves to ourselves (save for a little trade with Gaul) – until in 55BC we were invaded by a Roman, Julius Caesar. He actually only stayed about a year. The Emperor Claudius led the Romans back to Britain in 43AD, and this time they stayed as occupiers for some 350 years. During that time, they never did manage to control the Picts and Scots, so the Emperor Hadrian built a wall from coast to coast to keep them out.

The Romans called this country “Britannia”. After they left, there were a series of invasions, none of which really took the whole country over. There were the Angles and Saxons, whose legacy was the name “Angeland”, the Norsemen and the Danes. However, for about 650 years, we remained fairly isolated from Europe – until 1066, when following the childless death of Edward the Confessor, the right to succession was disputed by Harold (who actually was crowned), Harald Hadrada, a Norseman, and one William the Bastard, a Norman. Harold defeated the Norse claimant, at Stamford Bridge, near York, but then had to march immediately to Hastings to deal with William the Bastard. Harold was defeated and the crown devolved upon William, thenceforth known as “William the Conqueror”. The island has never been invaded since and thereafter developed its own common law system (rather than adopting the codified Roman law system) and also its system whereby the King was subject to the law.

Thereafter, we became embroiled in a number of spats in Europe and beyond, largely maintaining a policy of ensuring that no one country became so powerful that it would invade us again. This in turn involved the building of a large fleet and trading relations worldwide. By the end of the 19th Century, the British Empire, the largest the world has ever seen, had also been built.

All empires, of course, rise and fall. Largely in the first half of the 20th Century, the UK gave independence to most of its empire. Fourteen outposts remain, now called “British Overseas Territories” – including parts of the Caribbean (Bahamas, Anguilla etc), Pitcairn Island (where the mutineers of HS Bounty famously set up), Gibraltar (now the home to major financial services and internet betting industries) and, famously, the Falkland Islands. The former colonies, with one notably rather large exception, remained in a loose confederation known as the “the Commonwealth”, of which the Queen is Head, now comprising 52 countries. Britain had a policy of preferential trading with Commonwealth countries.

In 1958, six European countries set up a trading block called the European Economic Community (commonly known in England as the “Common Market”). The UK sought to join it twice, in 1963 and 1967 – but on both occasions were vetoed by the French, led by President de Gaulle, who stated that:

“England in effect is insular, she is maritime, she is linked through her interactions, her markets and her supply lines to the most diverse and often the most distant countries; she pursues essentially

industrial and commercial activities, and only slight agricultural ones. She has, in all her doings, very marked and very original habits and traditions.”

(<http://www.spectator.co.uk/2016/04/de-gaulle-knew-it-britain-does-not-belong-in-the-eu/>)

In 1973, with de Gaulle no longer in power, we joined the EEC. However, there was no referendum. Joining involved signing a treaty. International treaties can be entered into by the government using the Royal Prerogative.

This caused some controversy, particularly among those that considered it a betrayal of our policy of Commonwealth preference. In 1974, the then Prime Minister, Harold Wilson, having been elected on a manifesto that a referendum would be called to resolve the issue, did just that. The result was a substantial majority in favour of remaining in the EEC – 67.2% to 32.8% (on a 64.6% turnout). This in the face of warnings by those who wanted to leave, that the EEC was the precursor to a European super-state – warnings that have been repeated regularly to this day.

Over the years, the European Economic Community morphed into the “European Union”, something much more pervasive than just a common trading market. It included:

- A single market
- A common currency (to which the UK never subscribed)
- Freedom of movement between member states (including freedom to live and work)
- A common passport
- Its own European Parliament
- Its own President
- EU Regulations which have direct force in members’ law.
- EU Directives, which oblige member states to achieve a particular result without dictating the means of achieving it (like the Solvency II Directive).
- The common “passport” system for financial services companies (including insurers and brokers) allowing them to operate in each other’s countries subject only to their home regulator
- Subjugation of member countries’ Courts to European Courts in relation to European matters
- Very substantial contributions to the European budget
- Substantial payments from the European budget by way of subsidies, as decided by the EU (e.g to farmers)
- Mutual enforcement of judgments throughout the EU

- Common jurisdictional rules
- European arrest warrants and criminal anti-terrorist cooperation

Membership also gave trade and diplomatic negotiating weight for deals with other trading blocks, but at the cost of greater centralisation. That growing centralisation became increasingly viewed as rule from Brussels, a derogation of national sovereignty and an inability to control one's own borders. The size of the net EU budget contribution also gave rise to increasing concern and debate (notwithstanding Margaret Thatcher's negotiation of some rebate). All were reflected in the growth of popular support for UKIP (although it never had more than one MP due to the "first past the post" system). All this culminated in the current Conservative government winning the last General Election (against the predictions of opinion polls), in significant part because of a manifesto commitment to call a referendum on the EU.

The referendum took place on 23 June 2016. The vote was close, and like so many recent elections, confounded the pollsters:

- 33,551,983 votes cast representing a 72.2% turnout
- 51.9% leave
- 48.1% remain

Had the vote been counted by constituencies, rather than one vote per person, the result would have been a more resounding vote in favour of leave.

Gibraltar, the overseas dependency caught up in the middle of all this and whose citizens were therefore entitled to vote, came out strongly in favour of remain – unsurprising because of the large proportion of its economy that relies on passported financial services business and its difficult relationship with Spain. The Scots and Northern Irish also voted strongly to remain. London, again reliant heavily on financial services, voted strongly to remain. Most of the rest of the English and Welsh disagreed.

Meanwhile, in 2014, there had been a referendum in Scotland on independence, following the electoral successes of the Scottish Nationalist Party. Scotland voted to remain part of the UK, in part because if it left the UK it would be leaving the EU with no guarantee of getting in back in – Spain in particular was concerned not to encourage its own secessionists. The Scottish Nationalists are now pointing to this anomaly to reinvigorate a campaign for another referendum, which they believe could result in Scotland becoming independent and then, in these changed circumstances, joining the EU.

Those of you with long memories may recall that this is not the first time a territory has left the EU. In 1982, Greenland decided by 53% to 47% to leave the then European Communities (EC). However, that process does not really shed any light on the process involved here. This is because Greenland was not actually a sovereign state, but was, and is, a part of the then EC (now EU) member Denmark. Hence, the withdrawal of Greenland was not actually the withdrawal of a sovereign state member, as Denmark remains a member, but a reduction of the territorial jurisdiction of the treaties within Denmark. This constituted a treaty change and was therefore ratified by all Member States. An arrangement was entered into whereby Greenland became an "associated overseas territory" under Article 204 TFEU, with special

arrangements with the EU, particularly with regard to fisheries – it is given access to the single market for fisheries' production in return for EU fishermen's access to Greenland waters.

Could this be a precedent for Scotland to remain an EU member, notwithstanding UK withdrawal? Almost certainly not, for two reasons: First, it would have to become an independent state before being able to negotiate its own membership deal. This, of course, is the route that the Scottish Nationalist Party may opt for – requiring another Scottish referendum. Second, Article 50 is a black and white provision, so treaty revision would be needed for part of a sovereign state to remain when the sovereign state itself exits (i.e. the opposite of what happened in the Greenland case). This is the view put forward by the European parliament in the Briefing.

Returning to the position of the UK as a whole, although the UK EU referendum was technically advisory, and so not binding on parliament, it is considered unthinkable by the vast majority of people and MPs (most of the latter of which voted remain) that the referendum should not be put into practice. However, the fact that it was not binding on parliament gave rise to a question as to what the mechanism would be in the UK for triggering Brexit.

The Exit Process

It is clear under Article 50 of the Treaty of Lisbon that a country leaving has to give notice and that the notice period is 2 years, to allow time for negotiation of a withdrawal agreement. If those negotiations do not result in a withdrawal agreement, then the country giving notice simply ceases to be a member from that two year date.

At this point, I should make clear that the UK parliament and the UK government are not the same thing. Parliament means both houses of parliament, the House of Commons and the House of Lords – in US terms, that would be the House of Representatives and the Senate. The question was whether the government could, as it argued, give notice by virtue of its operation of the Royal Prerogative or whether an Act of Parliament, which has to be passed both the House of Commons and the House of Lords, was required to authorise government to trigger notice under Article 50. There were impassioned views on all sides.

In *R, on the application of Miller v Secretary of State for Exiting the European Union* [2016 EWHC 2768], the Court found that government could not simply implement the result of the referendum without the authority of an Act of Parliament. Certain elements of the press reacted in an extreme way. In one headline, the Judges were branded "Enemies of the People".

By the time the Supreme Court (a unique sitting of all 11 Supreme Court Law Lords together), upheld the decision in a 96 page judgment, by 8 to 3, the press had calmed down a little. (*R, on the application of Miller v Secretary of State for Exiting the European Union* [2017] UKSC5). It was, of course, not an anti-Brexit judgment, but one that upheld the UK Constitution in ensuring that due process of law and democratic principles were followed in giving notice under Article 50. Had the action not been brought now, but later, and had the Court then found that notice, having been given, was not authorised, there probably would have been a constitutional crisis!

As it is, the government has introduced a simple 2 clause Bill which passed the Commons with a huge majority and is now going to the House of Lords. The bill does nothing more than give the government

power to give notice under Article 50, so as to start the Brexit process rolling. Lots of amendments were tabled, both by those who wanted to frustrate Brexit and by those who felt that the Act should, for example, enshrine the rights of European workers already resident here who could lose their right to remain, just as English workers in the EU could lose theirs. At the time of writing, the focus moved to the House of Lords, where similar amending attempts are threatened. Ultimately, the House of Lords can only delay the Bill if the Commons repeatedly refuse to pass its amendments, but a constitutional crisis is being predicted (as to the future existence of the House of Lords, at least in its current form) were it to try to frustrate a Bill passed with such a large Commons majority backed by a referendum.

It is probably fair to predict that the Act will pass and government will be authorised to trigger Article 50. But what happens then?

Article 50 says:

“... the Union shall negotiate and conclude an agreement with that State, setting out the arrangements for its withdrawal, taking account of the framework for its future relationship with the Union. That agreement shall be negotiated in accordance Article 218(3) of the treaty on The Functioning of the European Union. It shall be concluded on behalf of the Union by the Council, acting by a qualified majority, after obtaining the consent of the European Parliament”.

Article 218(3) of the treaty on The Functioning of the European Union (“TFEU”) provides essentially that the Commission must submit recommendations to the Council which shall adopt a decision authorising the opening of negotiations and nominating the Union negotiator or head of the Union’s negotiating team.

Following negotiations during the two year notice period, it is envisaged that an agreement will be entered into. Indeed the wording of Article 50 is mandatory in this respect – *“shall negotiate and conclude an agreement ...”* – However, Article 50 does also provide for the possibility of failure to enter into such an agreement. In those circumstances, the EU treaties cease to apply to the State in question (the UK in this case) from two years after the notification. As notification has been promised by the end of March, this would mean some time at the end of March 2019.

Article 50 provides that the negotiations must be concluded on behalf of the Union by the Council acting by a *“qualified majority”* after obtaining the consent of the European Parliament. A qualified majority is defined in Article 283(3)(b) of TFEU, as at least 72% of the members of the Council comprising at least 65% of the population of the Members States (without the withdrawing State). However, it seems that the vote of the European Parliament consenting to this does not exclude the withdrawing State’s MEPs. Accordingly, although the procedure is complex, the leaving agreement of itself does not require consent of all 27 remaining States.

As to the negotiating process in between these procedural requirements, there is really no precedent. The European Parliament itself, in a briefing published by the European Parliamentary Research Service in February 2016 (“the Briefing”) (EPRS/European Parliamentary Research Service: author Eva-Maria Poptcheva: Members Research Service PE 577.971) acknowledges that:

“The role of the European Commission in the withdrawal procedure is not entirely clear in the treaties. According to Article 218(3) TFEU, the European Commission would make recommendations to the council to open negotiations with the withdrawing state. As a general

rule, the Commission negotiates agreements with third party countries on behalf of the EU, but Article 218(3) leaves it open for the Council to nominate a different Union negotiator”.

Although there is no requirement for ratification of the withdrawal of a Member State by the remaining members (unlike accession of a new member), any treaty changes or international agreements necessitated by the withdrawal agreement (such as free trade provisions) would need to be ratified by all remaining Member States (Article 48 TEU). Hence, it is highly likely, assuming that a withdrawal agreement is reached with the EU negotiators, that its implementation will involve a number of matters that will require the separate agreement of all remaining 27 States.

What Does the Future Hold for the UK's International Relationships?

However one looks at it, it will be a brave man who predicts exactly what form the relationship between the UK and the EU will take following expiry of the two year period or under a withdrawal agreement negotiated during it.

The government has published a White Paper setting out in broad terms what it would hope to achieve by way of a withdrawal agreement (“The United Kingdom’s exit from and new partnership with the European Union”; February 2017; pub HMSO). It would be surprising were this to represent the government’s bottom line, as you would not expect the bottom line to be set out ahead of the commencement of any negotiations. Subject to that, the paper seems to expect a hard Brexit, perhaps acknowledging that trading off concessions for a softer Brexit will, insofar as it may require treaty change, be subject to the agreement of all 27 remaining States and hence be a difficult process.

The White Paper says *“no deal for the UK is better than a bad deal for the UK”*. It signposts that the government will prepare legislation *“to ensure our economic and other functions can continue”*. It pledges to make the UK a *“champion of free trade”* with bilateral agreements and multilateral agreements worldwide through the World Trade Organisation. Trading arrangements with the USA and Canada appear already to have been discussed on a bilateral basis. There has been talk of the USA becoming closer to the 52 nations of the Commonwealth as a whole. It is understood that there have been discussions with Australia and India. There has been a noticeable improvement in relations with China and a promoting of mutual trade.

The White Paper also emphasises that the government aims to secure *“the freest and most frictionless trade possible in goods and services”* with the EU outside the single market via *“an ambitious and comprehensive free trade agreement”*. The *“single market”* differs from the EU as it includes Norway and Switzerland in the European Economic Area (the *“EEA”*) on terms involving budget contributions and freedom of movement. The UK is a member of the EEA by virtue of its membership of the EU, so it is difficult to set out one’s stall on the basis that somehow we will remain in the EEA. Furthermore, the UK needs to be outside the Customs Union, so that it can negotiate its own trade deals, but the White Paper says it would nevertheless like a *“new customs agreement”*. It says that the UK will not seek to adopt an existing model used by other countries (a reference to Norway and Switzerland in particular).

The extent to which the aims set out in the White Paper, which some may consider incompatible, are achievable will be the subject of the negotiations, the outcome of which I am certainly not brave enough to predict. In essence, if a withdrawal agreement is reached it will have to sit somewhere in the spectrum of

what is described as “soft Brexit” (i.e with a deal done on trading relations, budgeting contributions, freedom of trade etc) and a “hard Brexit”, where no such deals are done.

However, one thing that can be predicted with some confidence is that whatever the political and trading outcomes of the negotiations with the EU, there are a number of changes that will have to be made to UK law in order to facilitate Brexit.

1. The Great Repeal Bill:

The European Communities Act 1972, the Act of Parliament which subjugated UK law to EU law, will have to be repealed. The Institute for Government explains the need for this Act;

“What will it do?”

- 1. The bill will bring all EU laws onto the UK books. This means that when we trigger Article 50 of the Lisbon Treaty, laws and regulations made over the past 40 years while the UK was part of the EU will continue to apply. Specifically the bill will*
- 2. repeal the European Communities Act 1972, which provides legal authority for EU law to have effect as national law in the UK, and transfer all EU laws currently in force onto the UK statute book”*

(<https://www.instituteforgovernment.org.uk/brexit-explained/brexit-explained-great-repeal-bill>).

At first sight it may appear anomalous that having voted to leave the EU in large part because of the centralised legislation imposed on the UK, we now choose to adopt it all into domestic legislation for after we leave. Again, the Institute for Government explains:

“These laws cover numerous areas such as environmental regulation, workers’ rights, and the regulation of financial services. Without the Great Repeal Bill, when the UK leaves the EU all these rules and regulations would no longer have legal standing in the UK, but there would be nothing to replace them - creating a ‘black hole’ in the UK statute book and leading to uncertainty and confusion.”

Hence, by carrying EU laws over into UK law, the Government gives itself time to review, amend or scrap these laws in future. This is important because there is a vast amount of detailed law and regulation to be considered. For example, there is a UK law on licences for the use of different plant varieties which, in turn, references an EU regulation (which may, of course, itself change). It gives powers to an EU community plant variety office, but when we leave, we would probably want those functions to go to a UK version of the same thing.

2. Immigration

The control of borders was a key argument in the Brexit campaign. It will be very difficult, probably impossible, for the government to agree a withdrawal agreement with the EU by which all EU citizens and UK citizens will in future continue to enjoy the full freedom of movement, including freedom to work,

between the countries. The price for that will inevitably be that the UK will not be able to enjoy a full single market membership – a position that the White Paper appears to accept. There have been negotiations around this problem recently between the EU and Switzerland, which, being neither an EEA nor an EU country, has a bilateral arrangement with the EU. The UK's relationship with the EU is, by virtue of having withdrawn from full membership, a rather more complex one – not least because the UK cannot be seen by EU members to be better off in its arrangements with the EU than when it was a member, for obvious reasons.

However, there are serious issues that concern British citizens currently living and working in the EU and the many EU citizens currently living and working in the UK. In 2015 there were 1.2 million UK born people living in member states. There are about 3.2 million EU citizens living in the UK. What will their respective rights be on withdrawal?

The government White Paper says that securing their status is *“one of the government's early priorities”*, but the UK Prime Minister has refused to confirm that EU citizens in England will have the right to remain until the EU confirms reciprocity, which it has not done. It is, of course, to be hoped that reciprocity will be agreed, as it would be unseemly for the people who in good faith have established themselves throughout the EU to be political pawns. In this respect, it may be significant that the Briefing pointed out that some scholars argue that standalone rights derive from EU citizenship, detached from the nationality of a Member State, so that the nationals of the State in question would keep their EU citizenship even after its withdrawal from the EU. (CM Reider, *“The withdrawal clause of the Lisbon Treaty in the light of EU citizenship”*, Fordham International Law Journal, Vol 147, 2013).

However, the Briefing also points out that this is a minority view, the majority viewing EU citizenship as *“additional”* to a Member State's nationality under Article 20(1) TFEU, and without any freestanding character. Ominously, the Briefing opines:

“Moreover it should be noted that the decision to withdraw from the EU is taken according to the constitutional requirements of the state concerned and thus taking into account all possible consequences, including for the individual citizens of the withdrawing state”.

This position, by focusing only on the position of UK citizens in the EU, rather ignores the fact that it is a two-way street, so perhaps one can reasonably hope that it will be modified.

One way or another, the issue of rights of movement, both of those already in another member state and for the future, between the countries concerned – and especially the Republic of Ireland and Northern Ireland – will have to be resolved. If it isn't and there is no agreement when the EU treaties cease to apply to the UK, the rights that they give will cease to exist in the UK. Domestic administrative law will have to take over. As regards UK citizens in the EU, they may have to rely on EU general principles of EU fundamental rights insofar as their legal situation falls within the scope of the EU third country immigration laws. At the very least, it is therefore to be hoped that acquired rights of residence and work will be retained by all concerned as part of the withdrawal agreement.

3. Implications for the Insurance Industry

The prudential requirements of Solvency II regime will not automatically be applicable in the UK, but essentially have already been adopted as UK insurance regulation. Moreover, the UK was at the helm of

Solvency II and generally has a reputation for gold-plating mandatory EU provisions relating to insurance prudential requirements. Although the UK after withdrawal will be able to legislate for different requirements, it is unlikely that they will change significantly, as “equivalence” to Solvency II will be important to facilitate business with EU insurers and reinsurers. Accordingly, whilst Solvency II may evolve at the edges, the core is likely to remain unchanged.

The real problem is the potential removal of passporting rights. This is the rights of insurance entities and intermediaries based in the EU countries to conduct insurance business throughout the EU and be regulated only by their home regulator (all of which are, of course, subject to Solvency II). If withdrawal arrangements do not maintain this, there may be a move by UK based companies to establish in the EU in order to obtain the benefit of the passporting rights; and by EU companies to establish in the UK in order to facilitate operations in the London market.

It is apparent from the White Paper that the UK government believes it has a strong hand in relation to financial services. It says that the EU has a clear interest in “*mutual cooperation arrangements*”, describing the City of London as Europe’s only global hub for money, trading and investment on which the EU will continue to rely.

The current “passporting” system essentially relies upon the insurer, intermediary or other regulated institution concerned applying to its home regulator for a passport to carry out a particular type of financial service throughout the EU. One company may have a number of passports. At present, there are a total of 359,953 passports in existence, of which 23,532 are inbound to London and 336,421 are outbound from London to Europe. The differential is less surprising when one takes into account that there are separate passports for conducting business in each of the separate EU countries. Hence, a firm conducting one type of activity under one directive in 25 countries, would require 25 passports. If one reduces the statistics to firms with passports, there are 8,008 regulated EU financial services firms passported into London and 5,476 passported from London into Europe. The insurance element of this is:

<u>Directive</u>	<u>Inbound to London</u>	<u>Outbound to Europe</u>
Insurance mediation	5,727	2,758
Solvency II (insurers/reinsurers)	726	220

(Figures taken from a letter dated 17 August 2016 from the Financial Conduct Authority (the UK Regulator) to the Chairman of the Treasury Committee at the House of Commons.)

Although the government clearly hopes that a mutually beneficial accommodation on the passporting of financial services will be achieved within the next two years, Lloyd’s has nevertheless said that it will in any event establish a presence in the EU. Others may follow and Ireland in particular may expect to benefit from UK companies wishing to have an EU establishment.

With respect to Lloyd’s, Malta was much touted as the potential jurisdiction for its EU establishment. However, Inga Beale has said that Malta has now been ruled out (see, e.g, Malta Today 20 January 2017 – www.maltatoday.com.mt/business/business_news/73618/loyds_ceo_inga_beale_rules_out_malta_for_eu_subsidiary#WKXWJm-LS70). Although Lloyd’s have given no indication as to which jurisdiction they will choose, the rumour-mill suggests that it may be Luxembourg (see e.g “*Lloyd’s leaning towards Luxembourg for post-Brexit base – report*”: Insurance Business 8 February 2017). Watch this space.

4. Continuing Status of EU Law

Where EU law is preserved in the domestic context, the status of European Court of Justice (“ECJ”) case law in relation to it needs to be considered. The position could perhaps be likened to that of former British territories that on succession from the Empire, retained English law as a basis from which they then developed their own law. In those circumstances, I understand that Canada, for example, treats English precedent as persuasive but not binding. This is not unusual. It is therefore possible, perhaps likely, that the English Courts will construe laws imported from EU law taking into account ECJ decisions, but nevertheless in a way different from constructions that continue to be applied by the ECJ.

5. Jurisdiction and Enforcement of Judgments – a Boost to Arbitration?

The Brussels regulation on the automatic recognition of judgments within the EU will cease to be effective in respect of UK judgments two years from the invocation of Article 50. Bearing in mind the length of time that some cases take to be decided, particularly after appeals, this is therefore already a consideration. Accordingly, amongst the treaties which will have to be renegotiated (even if only by seeking to put back in place the treaties that preceded them – although one would hope these could be improved) will be necessary in respect of the 27 remaining Member States.

Professor Burkhard Hess and Professor Marta Requejo-Isidro have observed:

“The main interest of the Union won’t be to maintain or strengthen London’s dominant position in the European judicial market ... [and] ... there is a genuine interest to the Union to see mandatory EU law applied in disputes relating to the internal market by courts operating within its regulatory framework”.

This is an area in which the EU enjoys exclusive competence to enter into international treaties with third countries, so bilateral arrangements with individual EU members will not be possible. It may be that it is considered in the interests of justice generally that the judgments should continue to be enforceable on a cross border basis. However, this certainly cannot be taken for granted. There is therefore uncertainty as to the extent and manner of enforceability of judgments between the UK and EU countries. As a consequence, at least until the picture of the relationship between the UK and the EU is clearer, one should perhaps expect an increase in arbitration clauses, as all EU Member States and the UK are parties to the 1958 New York Convention, which grants the recognition of arbitration awards in all countries and will not change following Brexit.

-:-

This paper merely scratches the surface of the many and complex issues of trade, commerce, politics and law that arise from the withdrawal of the UK from the European Union. It raises many questions and unfortunately, whilst this paper identifies some of them and some of the requirements that will have to be met, it can make few predictions. Negotiations will be difficult and drawn out. The situation is further complicated by forthcoming elections in some of the EU’s most powerful members – Germany, France,

Netherlands and Italy. Accordingly, for next several months it will be difficult to know what is being said for the purposes of internal consumption, and whether the person saying it will be in power after the elections. The results of these elections have the potential to change the EU political climate. In France, for example one of the flagship policies of Marine La Pen (the French National Front's presidential candidate) is taking France out of the EU. Her party has been growing in strength and she is considered by some to have a genuine chance of election. I understand that pollsters consider that she will not succeed, but pollsters have been having a pretty torrid time lately. If she is elected, the subject of the next "Window to the World" may well be "Frexit"!

In any event, it will probably be another two years before I am able to revert with answers to the issues raised in this paper, and indeed many that aren't raised in it.



WEDNESDAY, MARCH 8, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

TRANSPORTATION AND PRODUCTS LIABILITY SECTIONS

Follow-Up on Autonomous Vehicles

Jenkins

Speakers:

Matthew R. Cairns

Terrence L. Graves

PRODUCTS LIABILITY AND AUTONOMOUS VEHICLES

INTRODUCTION

The advent of autonomous vehicles creates many new legal questions. A growing area of concern for both consumers and manufacturers of autonomous vehicles is the issue of liability. When an autonomous vehicle causes an accident, who is ultimately responsible? Is it the person who was sitting in the car, not paying attention because he or she believed the car could navigate safely, or is it the manufacturer who claimed that the car was safe? This question is not easily answered, and will likely be highly debated as new legislation and regulations are formulated over the coming years, and insurers, consumers, and manufacturers find their place in this new paradigm. This article will focus on new issues in products liability in the context of autonomous vehicles.

PRODUCTS LIABILITY OVERVIEW

Products liability holds a manufacturer or distributor who sells or distributes a defective product liable for any harm caused by the defect.¹ The main theories of products liability include negligence, strict liability, tortious misrepresentation, and breach of warranty.² Strict liability allows a plaintiff to hold a manufacturer liable even when the manufacturer exercised reasonable care. There are three actionable categories of product defects in strict liability: manufacturing defects, design defects, defective warnings.³ While automobile accident plaintiffs often bring claims for crashworthiness as well, these claims will remain largely unchanged in autonomous vehicles because they have to do with the structure of the vehicle rather than any autonomous features.⁴

A manufacturing defect occurs when the product was not produced according to its specifications⁵, or under the malfunction doctrine, which arises when there is an inexplicable accident.⁶ A design is defective when there was a foreseeable risk of harm that could have been reduced or avoided by a reasonable alternative design, and failure to implement the alternative design rendered the product "not reasonably safe."⁷ There are two tests for design defect: the consumer expectations test, and the risk-utility test.⁸ The risk-utility test is more widely accepted,⁹ and both will be discussed in more detail in the following section. A failure to warn claim implicates the manufacturer's dual duty to provide instruction on how to safely use the product and to warn of hidden dangers.¹⁰ This duty is limited to

¹ RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 (1998); Kevin Funkhouser, *Paving the Road Ahead: Autonomous Vehicles, Products Liability, and the Need for A New Approach*, 2013 UTAH L. REV. 437 (2013).

² JOHN VILLASENOR, BROOKINGS INST., PRODUCTS LIABILITY AND DRIVERLESS CARS: ISSUES AND GUIDING PRINCIPLES FOR LEGISLATION, at 7-8 (2014), http://www.brookings.edu/~media/research/files/papers/2014/04/products-liability-driverless-cars-villasenor/products_liability_and_driverless_cars.pdf; Funkhouser, *supra* note 1, at 444-45.

³ RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (1998); Jeffrey K. Gurney, *Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles*, U. ILL. J.L. TECH. & POL'Y, Fall 2013, at 257.

⁴ Gurney, *supra* note 3, at 257; Funkhouser, *supra* note 1, at 445.

⁵ RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (1998).

⁶ Gurney, *supra* note 3, at 258 (citing David G. Owen, *Manufacturing Defects*, 53 S.C. L. REV. 851, 871-72 (2002))

⁷ RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (1998).

⁸ Gurney, *supra* note 3, at 258, 260-64.

⁹ *Id.*

¹⁰ *Id.* at 264.

risks reasonably foreseeable at the time of sale.¹¹ Possible defenses the manufacturer may assert include assumption of the risk, waiver, misuse, state of the art, and comparative negligence.

PRODUCTS LIABILITY AND AUTONOMOUS VEHICLES

While products liability has long existed and has adapted to many new technologies over the years,¹² the application to autonomous vehicles will likely present new challenges. In a traditional car accident, the two (or more) drivers, with the help of their insurance companies, apportion fault between them. However, in an accident involving an autonomous vehicle, many more parties could potentially be implicated. They include the driver of the car, the vehicle manufacturer, the manufacturer of a particular component of the vehicle, the software engineer, the designer or programmer of the navigational system, or in the case of an intelligent road system, the road designer. Any or all of these parties could be sued by a driver or passenger in any or all of the vehicles involved in the accident. Although the realm of possibilities is broad, it is most likely that the vehicle manufacturer will be the principal liable party because it will have the deepest pockets.¹³ The question then becomes, what new issues arise when the manufacturer of the autonomous vehicle is the liable party in a car accident?

Manufacturing Defects

As mentioned above, a manufacturing defect exists when a product was not produced as intended, or under the malfunction doctrine, when there is an inexplicable accident. In autonomous vehicles, the most likely part to malfunction significantly is the software that tells the car how to maneuver without human input. Any other malfunction would have the same liability analysis as malfunctions in non-autonomous vehicles. For example, a plaintiff could claim that a defective sensor caused the car to collide with something it should otherwise have avoided.¹⁴ However, courts have not yet applied the manufacturing defect doctrine to software as software is not generally considered a product.¹⁵ The plaintiff could attempt to argue that the autonomous technology did not meet the manufacturing specifications, but it would be difficult to disentangle the "autonomous technology" as a whole from the software that enables the car to be autonomous.¹⁶ Therefore a manufacturing defect claim would likely be unsuccessful in the context of autonomous vehicles.

The malfunction doctrine allows a plaintiff to recover even if he cannot demonstrate how the product was defective, similar to the tort theory of *res ipsa loquitur*.¹⁷ The plaintiff must prove that "(1) the product malfunctioned, (2) the malfunction occurred during proper use, and (3) the product had not been altered or misused in a manner that probably caused the malfunction."¹⁸ While the first two

¹¹ Gary E. Marchant & Rachel A. Lindor, The Coming Collision Between Autonomous Vehicles and the Liability System, 52 SANTA CLARA L. REV. 1321 (2012).

¹² VILLASENOR, *supra* note 2, at 15.

¹³ Jessica S. Brodsky, Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit the Brakes on Self-Driving Cars, 31 Berkeley Tech. L.J. 851, 862 (2016).

¹⁴ Gurney, *supra* note 3, at 259.

¹⁵ Gurney, *supra* note 3, at 259; Brodsky, *supra* note 13, at 863. See also 68 AM. JUR. 3D PROOF OF FACTS 333 § 8 (last updated Dec. 2016) ("[N]o cases have been found applying strict liability to software.").

¹⁶ See Gurney, *supra* note 3, at 259.

¹⁷ See Andrew P. Garza, "Look Ma, No Hands!": Wrinkles and Wrecks in the Age of Autonomous Vehicles, 46 NEW ENG. L. REV. 581 (2012).

¹⁸ Gurney, *supra* note 3, at 259.

elements are easily satisfied by the fact of the accident, the third may be harder to prove.¹⁹ Additionally, the malfunction doctrine has not been recognized in all jurisdictions.²⁰ Even courts that recognize it may be hesitant to apply it, and often require an expert to show that nothing else could have caused the accident.²¹ These limitations impede the usefulness of the malfunction doctrine in the context of autonomous vehicles.

Design Defects

Design defect will likely be the most common product liability claim in cases of autonomous vehicle accidents. There are two tests for design defects: the consumer expectations test and the risk-utility test.²²

The consumer expectations test examines whether the design is unreasonably dangerous beyond the expectation of the average consumer.²³ This test was rejected by the Restatement (Third) of Torts: Products Liability, but many states still accept it.²⁴ In the context of autonomous vehicles, manufacturers will likely argue that the vehicles and systems are too complex for the average consumer to form appropriate and realistic expectations about their safety.²⁵ Some courts already hesitate to apply the consumer expectations test to traditional automobiles because they are highly complex even without autonomous driving.²⁶ However, other courts take the position that consumer can form reasonable expectations about a complex product with which they are familiar, or where the mechanics may be complex but the concept is not.²⁷

Design defects:²⁸

- Consumer expectations test (rejected by the Restatement (third) of Torts – acceptance depends on the state).
 - o Design is unreasonably dangerous if beyond contemplation of the consumer
 - o Vehicles are complex, but consumer expectations of them aren't usually
- Risk-utility test (majority rule)
 - o “when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller” and not adopting the alternative made the product “not reasonably safe” AND the safety benefits from the alternative design would have outweighed the costs of alternation²⁹

¹⁹ Gurney, *supra* note 3, at 259-60.

²⁰ *Id.* at 560.

²¹ *Id.*

²² Garza, *supra* note 17, at 599.

²³ RESTATEMENT (SECOND) OF TORTS § 402A cmt. g (1965).

²⁴ Gurney, *supra* note 3 at 261.

²⁵ Garza, *supra* note 17, at 599.

²⁶ Garza, *supra* note 17, at 601-02; Gurney, *supra* note 3 at 261.

²⁷ See, e.g., Jackson v. Gen. Motors Corp., 60 S.W.3d 800, 806 (Tenn. 2001) (citing Cunningham v. Mitsubishi Motors Corp., No. C-3-88-582, 1993 WL 1367436, at *6 (S.D. Ohio June 16, 1993)) (“This Court is simply not willing to . . . preclud[e] the use of the consumer expectation test in a situation involving a familiar consumer product which is technically complex or uses a new process to accomplish a familiar function. Many familiar consumer products involve complex technology.”).

²⁸ Gurney, *supra* note 1 at 260-66

²⁹ Restatement (Third) of Torts § 2(b)

- Easier to prove with design elements like sensors than software because experts are easier to produce – most defects will likely concern software
- Difficult to use in a widespread manner because the suit will be so expensive, and difficult to prove software caused issue³⁰

Failure to warn³¹

- Two duties: inform buyers of hidden dangers, instruct buyers how to safely use product
- Example: if vehicle has certain map areas that it struggles with (remote locations)
- Biggest issue will be safe operation
- Safe operation concerns differ with the level of autonomy of the vehicle – see Tesla example
 - Tesla:³²
 - Level 3 autonomy that requires driver's attention – autopilot for highways
 - Provides warnings every time the system is turned on
 - Tesla buyers agree with purchase contract to keep hands on wheel

Contract law - warranties:³³

- Express warranties – advertising, sale, description, sample
- Implied warranty of merchantability
- Implied warranty for fitness for particular purpose under contract law UCC § 2-314. Can be disclaimed by the manufacturer³⁴
 - Manufacturer still liable for “software flaws that are foreseeable as a class but neither preventable nor reasonably discoverable in their individual instance”

Misrepresentation³⁵

- Communication of false or misleading information
- Fraudulent, negligence, strict liability
- Ex. Car requires human intervention more often than advertised

Defenses³⁶

- Comparative negligence
 - Level 3 vehicles³⁷
 - Driver negligently turns on autopilot or some other autonomous feature

³⁰ See, e.g., *In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Prod. Liab. Litig.*, 978 F. Supp. 2d 1053, 1081 (C.D. Cal. 2013) (excluding causation opinion of expert because causal connection between software defect and collision “too tenuous to be admissible”);

³¹ Gurney, *supra* note 1 at 264.

³² <https://www.theguardian.com/technology/2016/jul/06/tesla-autopilot-crash-joshua-brown-family-potential-lawsuit>; <http://money.cnn.com/2016/07/07/technology/tesla-liability-risk/>

³³ John Villasenor, Brookings Inst., Products liability and driverless cars: Issues and guiding principles for legislation (2014), http://www.brookings.edu/~media/research/files/papers/2014/04/products-liability-driverless-cars-villasenor/products_liability_and_driverless_cars.pdf

³⁴ <http://cohen-lawyers.com/wp-content/uploads/2016/08/WestLaw-Automotive-Cohen-Commentary.pdf>

³⁵ Villasenor, *supra* note 12.

³⁶ Gurney, *supra* note 1 at 265

³⁷ Marchant & Lindor, *supra* note 2 at ____.

- Example: instructions say not to use in certain weather or road conditions and driver does anyway
 - driver fails to regain control when he should have
- any vehicle that can still be controlled whether fully autonomous or not – driver's decision not to intervene when vehicle malfunctioned
 - but what is the standard of care in a fully autonomous vehicle?
 - Requiring "drivers" to pay attention defeats the productivity purpose of having driverless cars to begin with – not a good policy
 - focus instead on ability of person to prevent accident, not what they were doing
- Misuse – manufacturer has a duty to protect against foreseeable misuse
 - Distraction or other activities won't count as misuse because it's foreseeable
 - Driver altering the vehicle could be a defense
- State of the art
 - Warning defects: what could the manufacturer reasonably foresee
 - Design defect: "feasibility of adopting curative design measures to reduce or eliminate a risk of which the manufacturer is aware" – technological limits may make it impossible to reduce or eliminate a risk
- Assumption of the risk
 - 1. P knows and understands risk, 2 p voluntarily encounters the risk
 - Manufacturers would have had to disclose risks
 - This likely wouldn't apply to general use of an autonomous vehicle, but rather situations that increase the risk like snowy conditions where manufacturer has warned that car is not as good in snow and shouldn't be driven or should be driven manually
- Waiver³⁸ – ask consumers to sign waivers accepting risks and taking personal responsibility for accidents – but risks must be fully disclosed, which is likely difficult because the whole point is that the risks are hard to predict

Additional issues:

- In multiple-vehicle crashes, both/all drivers can sue the same manufacturer
- Juror perception is a huge factor in liability – if juries believe in autonomous vehicles' safety, less liability is likely
- Too much liability could deter innovation, increase costs, but decrease consumer insurance costs, increase consumer confidence
- Create a shift in accident liability from driver to manufacturer
- Evidentiary issues:³⁹
 - Expert testimony
 - Prohibitively expensive because tech is so complicated – cost will likely outweigh value of suit
 - Evidence of reasonable alternative design

³⁸ Brodsky, *supra* note 5 at 864.

³⁹ Gurney, *supra* note 1 at 265

- Computer scientist for algorithm, mathematician to rewrite equation, economist to weigh costs and benefits, autonomous vehicle expert to show feasibility
- Subsequent remedial measures - Later update in software could be evidence, but need to get around FRE 407
- Insurance⁴⁰
 - Will insurance still be totally necessary
 - Will insurance companies incentivize autonomous vehicles, or certain types of autonomous technology
 - Will insurance companies require access to vehicle data
 - Lower risk of accident could mean lower premiums, but severity of accidents could increase – insurers can most accurately predict the costs and risks, and charge a premium on less safe cars, pushing consumers away from them – incentive cycle
- Upswing in lawsuits likely as autonomous vehicles are introduced – trend that when new tech is introduced, products liability suits increase – analogous to vaccine introduction between 1980 and 1988⁴¹

Analogous situations:⁴²

- Industrial robots in manufacturing – usually injuries are attributed to employees' failure to take safety precautions or disabling safety features of the machines
- Autopilot failures – unexpected acceleration or deceleration
- Airplane autopilot – one case – court found error was pilot's because "[t]he obligation of those in charge of a plane under robot control to keep a proper and constant lookout is unavoidable"⁴³
- Safety benefit overall may outweigh risks such that it's necessary to pass regulation to protect manufacturers. However, there will always be a situation where the benefit turns into a risk⁴⁴
 - Failure of airbags to deploy resulted in liability even though airbags are not required
 - Vaccines – statutory protections for manufacturers because there are risks but the public benefit is too great to leave the manufacturers completely liable and discourage production of vaccines.

REGULATIONS/LAWS AND THEIR IMPACT ON LIABILITY

Variations in state law⁴⁵

- Current vehicle legislation is largely state specific, although NHTSA has federal safety standards

⁴⁰ Villasenor, *supra* note 11 at 13

⁴¹ Brodsky, *supra* note 5 at 864.

⁴² Gary E. Marchant & Rachel A. Lindor, The Coming Collision Between Autonomous Vehicles and the Liability System, 52 SANTA CLARA L. REV. 1321 (2012).

⁴³ *Brouse v. United States*, 83 F. Supp. 373, 374 (N.D. Ohio 1949).

⁴⁴ Orly Ravid, Don't Sue Me, I Was Just Lawfully Texting & Drunk When My Autonomous Car Crashed into You, 44 SW. L. REV. 175 (2014)

⁴⁵ Brodsky, *supra* note 5 at 867-71.

- States have varying specific laws (one hand on steering wheel, no honking at bicycles, always honk at bicycles) that could create issues for autonomous vehicle development⁴⁶
- Eight states have enacted laws regulating autonomous vehicles, and 19 more have bills under consideration, which different definitions of driver, control, autonomous, etc.
- How do existing laws apply to autonomous vehicles?
- DC, Florida, Michigan statutes have protective language decreasing manufacture liability for defects introduced on aftermarket by third party that converts non-autonomous to autonomous⁴⁷

Potential solutions:

some car manufacturers support strict liability⁴⁸

- Volvo, Google, Mercedes-Benz all pledged to accept liability if their vehicles cause an accident.
- This pretty much only works for fully autonomous vehicles, and would not work for level 3 autonomous vehicles because they rely on human intervention.
- Google's cars have been in accidents, but have never caused accidents. They've all been rear-ended. Google isn't worried about assuming the liability because they are confident that their cars won't cause accidents
- Google skipped level 3 and went straight to fully autonomous vehicles

Consider regulations that don't have the effect of putting the manufacturers out of business

- Liability caps
- No-fault auto insurance system – like vaccines
- Federal preemption⁴⁹ - not unprecedented for developing or new tech
- Insurance act⁵⁰ - 1957 Price-Anderson Act as an example – nuclear accident compensation and liability limitation – required insurance, spread risk across manufacturers
- Create an entirely new regulatory body⁵¹ – in the past new agencies have been created for new technologies (radio, trains)
- Chattel tort law⁵² – strict liability for owners

Existing regulations:

NHSTA has recognized that in Google's car, the software is the driver⁵³

⁴⁶ See Brodsky, *supra* note 5 at 867-68 for examples of varying state laws that may hinder or challenge autonomous vehicle development.

⁴⁷ Villasenor, *supra* note 11 at 14

⁴⁸ <http://cohen-lawyers.com/wp-content/uploads/2016/08/WestLaw-Automotive-Cohen-Commentary.pdf>

⁴⁹ Brodsky, *supra* note 5 at 871.

⁵⁰ Brodsky, *supra* note 5 at 867-68

⁵¹ *Id.*

⁵² *Id.*

⁵³ <https://isearch.nhtsa.gov/files/Google%20--%20compiled%20response%20to%2012%20Nov%20%2015%20interp%20request%20--%204%20Feb%2016%20final.htm>

NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies⁵⁴

- NHTSA retains enforcement authority of automating vehicles – recall power
- Considers software motor vehicle equipment within the meaning of the Safety Act
- Software defect, including vulnerability to hacking, constitutes a defect compelling recall if it poses an unreasonable safety risk

Federal motor vehicle safety standards; V2V communications⁵⁵

- Liability:
 - o V2V safety warning tech is similar enough to currently existing warning tech that there isn't any new or unbounded liability risk, although industry still advocates liability limitations
 - o Liability is a hotly debated topic that doesn't have a resolution yet
 - o V2V systems are necessarily cooperative, communication with other manufacturers' vehicles muddies the liability waters – which manufacturer is responsible?

⁵⁴ https://www.transportation.gov/sites/dot.gov/files/docs/12507-AV_site_FedReg_Final-Defects-Authority-Enforcement-Bulletin_2016.0....pdf

⁵⁵ Notice of proposed rulemaking: 82 CFR 3854, Published 1/12/17, comments due 4/12/17

Liability basics

Products liability basics:¹

- Can sue for manufacturing defects, design defects, failure to warn, and crashworthiness.
- Crashworthiness issues wouldn't change with autonomous vehicles
- Manufacturing defect: good not produced according to specifications or under malfunction doctrine (inexplicable accident)
- Design defect: foreseeable risk of harm could have been reduced or avoided by reasonable alternative design
 - o Consumer expectations test, risk-utility test
- Failure to warn: manufacturer's duty to provide instruction on how to use safely and warn of hidden dangers. Limited to risks reasonably known at time of sale.²
- Defenses: comparative negligence, misuse, state of the art, assumption of the risk

Liability and autonomous vehicles

Potential liable parties:³

- Vehicle manufacturer
- Manufacturer of a component
- Software engineer
- Road designer of intelligent road system

Vehicle manufacturer is most likely liable party

Manufacturing defects:⁴

- Courts have not yet applied the manufacturing defect doctrine to software because "nothing tangible is manufactured" – therefore P cannot allege that software erred but only that "autonomous technology did not meet manufacturing specifications" – have to use malfunction doctrine instead
 - o Software is "not a product"⁵
- Malfunction doctrine - P must prove: "(1) the product malfunctioned, (2) the malfunction occurred during proper use, and (3) the product had not been altered or misused in a manner that probably caused the malfunction."
 - o Not all courts recognize it, are hesitant to apply it broadly, may require unique circumstances to apply it. Expert to show nothing else could have caused the accident

¹ Jeffrey K. Gurney, *Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles*, U. Ill. J.L. Tech. & Pol'y, Fall 2013, at 257

² Gary E. Marchant & Rachel A. Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, 52 SANTA CLARA L. REV. 1321 (2012).

³ <http://cohen-lawyers.com/wp-content/uploads/2016/08/WestLaw-Automotive-Cohen-Commentary.pdf>

⁴ Gurney, *supra* note 1 at 259.

⁵ Jessica S. Brodsky, *Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit the Brakes on Self-Driving Cars*, 31 Berkeley Tech. L.J. 851, 863 (2016)

Design defects:⁶

- Consumer expectations test (rejected by the Restatement (third) of Torts – acceptance depends on the state).
 - o Design is unreasonably dangerous if beyond contemplation of the consumer
 - o Vehicles are complex, but consumer expectations of them aren't usually
- Risk-utility test (majority rule)
 - o “when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller” and not adopting the alternative made the product “not reasonably safe” AND the safety benefits from the alternative design would have outweighed the costs of alternation⁷
 - o Easier to prove with design elements like sensors than software because experts are easier to produce – most defects will likely concern software
 - o Difficult to use in a widespread manner because the suit will be so expensive, and difficult to prove software caused issue⁸

Failure to warn⁹

- Two duties: inform buyers of hidden dangers, instruct buyers how to safely use product
- Example: if vehicle has certain map areas that it struggles with (remote locations)
- Biggest issue will be safe operation
- Safe operation concerns differ with the level of autonomy of the vehicle – see Tesla example
 - o Tesla:¹⁰
 - Level 3 autonomy that requires driver's attention – autopilot for highways
 - Provides warnings every time the system is turned on
 - Tesla buyers agree with purchase contract to keep hands on wheel

Contract law - warranties:¹¹

- Express warranties – advertising, sale, description, sample
- Implied warranty of merchantability
- Implied warranty for fitness for particular purpose under contract law UCC § 2-314. Can be disclaimed by the manufacturer¹²

⁶ Gurney, *supra* note 1 at 260-66

⁷ Restatement (Third) of Torts § 2(b)

⁸ See, e.g., *In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Prod. Liab. Litig.*, 978 F. Supp. 2d 1053, 1081 (C.D. Cal. 2013) (excluding causation opinion of expert because causal connection between software defect and collision “too tenuous to be admissible”);

⁹ Gurney, *supra* note 1 at 264.

¹⁰ <https://www.theguardian.com/technology/2016/jul/06/tesla-autopilot-crash-joshua-brown-family-potential-lawsuit>; <http://money.cnn.com/2016/07/07/technology/tesla-liability-risk/>

¹¹ JOHN VILLASENOR, BROOKINGS INST., PRODUCTS LIABILITY AND DRIVERLESS CARS: ISSUES AND GUIDING PRINCIPLES FOR LEGISLATION (2014), http://www.brookings.edu/~media/research/files/papers/2014/04/products-liability-driverless-cars-villasenor/products_liability_and_driverless_cars.pdf [<https://perma.cc/UNZ3-GDE2>].

¹² <http://cohen-lawyers.com/wp-content/uploads/2016/08/WestLaw-Automotive-Cohen-Commentary.pdf>

- Manufacturer still liable for “software flaws that are foreseeable as a class but neither preventable nor reasonably discoverable in their individual instance”

Misrepresentation¹³

- Communication of false or misleading information
- Fraudulent, negligence, strict liability
- Ex. Car requires human intervention more often than advertised

Defenses¹⁴

- Comparative negligence
 - Level 3 vehicles¹⁵
 - Driver negligently turns on autopilot or some other autonomous feature
 - Example: instructions say not to use in certain weather or road conditions and driver does anyway
 - driver fails to regain control when he should have
 - any vehicle that can still be controlled whether fully autonomous or not – driver’s decision not to intervene when vehicle malfunctioned
 - but what is the standard of care in a fully autonomous vehicle?
 - Requiring “drivers” to pay attention defeats the productivity purpose of having driverless cars to begin with – not a good policy
 - focus instead on ability of person to prevent accident, not what they were doing
- Misuse – manufacturer has a duty to protect against foreseeable misuse
 - Distraction or other activities won’t count as misuse because it’s foreseeable
 - Driver altering the vehicle could be a defense
- State of the art
 - Warning defects: what could the manufacturer reasonably foresee
 - Design defect: “feasibility of adopting curative design measures to reduce or eliminate a risk of which the manufacturer is aware” – technological limits may make it impossible to reduce or eliminate a risk
- Assumption of the risk
 - 1. P knows and understands risk, 2 p voluntarily encounters the risk
 - Manufacturers would have had to disclose risks
 - This likely wouldn’t apply to general use of an autonomous vehicle, but rather situations that increase the risk like snowy conditions where manufacturer has warned that car is not as good in snow and shouldn’t be driven or should be driven manually

¹³ JOHN VILLASENOR, BROOKINGS INST., PRODUCTS LIABILITY AND DRIVERLESS CARS: ISSUES AND GUIDING PRINCIPLES FOR LEGISLATION (2014), http://www.brookings.edu/~media/research/files/papers/2014/04/products-liability-driverless-cars-villasenor/products_liability_and_driverless_cars.pdf [<https://perma.cc/UNZ3-GDE2>].

¹⁴ Gurney, *supra* note 1 at 265

¹⁵ Marchant & Lindor, *supra* note 2 at ____.

- Waiver¹⁶ – ask consumers to sign waivers accepting risks and taking personal responsibility for accidents – but risks must be fully disclosed, which is likely difficult because the whole point is that the risks are hard to predict

Additional issues:

- In multiple-vehicle crashes, both/all drivers can sue the same manufacturer
- Juror perception is a huge factor in liability – if juries believe in autonomous vehicles' safety, less liability is likely
- Too much liability could deter innovation, increase costs, but decrease consumer insurance costs, increase consumer confidence
- Create a shift in accident liability from driver to manufacturer
- Evidentiary issues:¹⁷
 - o Expert testimony
 - Prohibitively expensive because tech is so complicated – cost will likely outweigh value of suit
 - Evidence of reasonable alternative design
 - Computer scientist for algorithm, mathematician to rewrite equation, economist to weigh costs and benefits, autonomous vehicle expert to show feasibility
 - o Subsequent remedial measures - Later update in software could be evidence, but need to get around FRE 407
- Insurance¹⁸
 - o Will insurance still be totally necessary
 - o Will insurance companies incentivize autonomous vehicles, or certain types of autonomous technology
 - o Will insurance companies require access to vehicle data
 - o Lower risk of accident could mean lower premiums, but severity of accidents could increase – insurers can most accurately predict the costs and risks, and charge a premium on less safe cars, pushing consumers away from them – incentive cycle
- Upswing in lawsuits likely as autonomous vehicles are introduced – trend that when new tech is introduced, products liability suits increase – analogous to vaccine introduction between 1980 and 1988¹⁹

Analogous situations:²⁰

- Industrial robots in manufacturing – usually injuries are attributed to employees' failure to take safety precautions or disabling safety features of the machines
- Autopilot failures – unexpected acceleration or deceleration

¹⁶ Brodsky, *supra* note 5 at 864.

¹⁷ Gurney, *supra* note 1 at 265

¹⁸ Villasenor, *supra* note 11 at 13

¹⁹ Brodsky, *supra* note 5 at 864.

²⁰ Gary E. Marchant & Rachel A. Lindor, The Coming Collision Between Autonomous Vehicles and the Liability System, 52 SANTA CLARA L. REV. 1321 (2012).

- Airplane autopilot – one case – court found error was pilot’s because “[t]he obligation of those in charge of a plane under robot control to keep a proper and constant lookout is unavoidable”²¹
- Safety benefit overall may outweigh risks such that it’s necessary to pass regulation to protect manufacturers. However, there will always be a situation where the benefit turns into a risk²²
 - o Failure of airbags to deploy resulted in liability even though airbags are not required
 - o Vaccines – statutory protections for manufacturers because there are risks but the public benefit is too great to leave the manufacturers completely liable and discourage production of vaccines.

Regulations/laws and their impact on liability

Variations in state law²³

- Current vehicle legislation is largely state specific, although NHTSA has federal safety standards
- States have varying specific laws (one hand on steering wheel, no honking at bicycles, always honk at bicycles) that could create issues for autonomous vehicle development²⁴
- Eight states have enacted laws regulating autonomous vehicles, and 19 more have bills under consideration, which different definitions of driver, control, autonomous, etc.
- How do existing laws apply to autonomous vehicles?
- DC, Florida, Michigan statutes have protective language decreasing manufacture liability for defects introduced on aftermarket by third party that converts non-autonomous to autonomous²⁵

Potential solutions:

some car manufacturers support strict liability²⁶

- Volvo, Google, Mercedes-Benz all pledged to accept liability if their vehicles cause an accident.
- This pretty much only works for fully autonomous vehicles, and would not work for level 3 autonomous vehicles because they rely on human intervention.
- Google’s cars have been in accidents, but have never caused accidents. They’ve all been rear-ended. Google isn’t worried about assuming the liability because they are confident that their cars won’t cause accidents
- Google skipped level 3 and went straight to fully autonomous vehicles

Consider regulations that don’t have the effect of putting the manufacturers out of business

- Liability caps
- No-fault auto insurance system – like vaccines

²¹ *Brouse v. United States*, 83 F. Supp. 373, 374 (N.D. Ohio 1949).

²² Orly Ravid, Don’t Sue Me, I Was Just Lawfully Texting & Drunk When My Autonomous Car Crashed into You, 44 Sw. L. Rev. 175 (2014)

²³ Brodsky, *supra* note 5 at 867-71.

²⁴ See Brodsky, *supra* note 5 at 867-68 for examples of varying state laws that may hinder or challenge autonomous vehicle development.

²⁵ Villasenor, *supra* note 11 at 14

²⁶ <http://cohen-lawyers.com/wp-content/uploads/2016/08/WestLaw-Automotive-Cohen-Commentary.pdf>

- Federal preemption²⁷ - not unprecedented for developing or new tech
- Insurance act²⁸ - 1957 Price-Anderson Act as an example – nuclear accident compensation and liability limitation – required insurance, spread risk across manufacturers
- Create an entirely new regulatory body²⁹ – in the past new agencies have been created for new technologies (radio, trains)
- Chattel tort law³⁰ – strict liability for owners

Existing regulations:

NHTSA has recognized that in Google's car, the software is the driver³¹

NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies³²

- NHTSA retains enforcement authority of automating vehicles – recall power
- Considers software motor vehicle equipment within the meaning of the Safety Act
- Software defect, including vulnerability to hacking, constitutes a defect compelling recall if it poses an unreasonable safety risk

Federal motor vehicle safety standards; V2V communications³³

- Liability:
 - o V2V safety warning tech is similar enough to currently existing warning tech that there isn't any new or unbounded liability risk, although industry still advocates liability limitations
 - o Liability is a hotly debated topic that doesn't have a resolution yet
 - o V2V systems are necessarily cooperative, communication with other manufacturers' vehicles muddies the liability waters – which manufacturer is responsible?

Gary E. Marchant & Rachel A. Lindor, The Coming Collision Between Autonomous Vehicles and the Liability System, 52 SANTA CLARA L. REV. 1321 (2012).

Orly Ravid, Don't Sue Me, I Was Just Lawfully Texting & Drunk When My Autonomous Car Crashed into You, 44 Sw. L. Rev. 175 (2014)

²⁷ Brodsky, *supra* note 5 at 871.

²⁸ Brodsky, *supra* note 5 at 867-68

²⁹ *Id.*

³⁰ *Id.*

³¹ <https://isearch.nhtsa.gov/files/Google%20--%20compiled%20response%20to%2012%20Nov%20%2015%20interp%20request%20--%204%20Feb%2016%20final.htm>

³² https://www.transportation.gov/sites/dot.gov/files/docs/12507-AV_site_FedReg_Final-Defects-Authority-Enforcement-Bulletin_2016.0....pdf

³³ Notice of proposed rulemaking: 82 CFR 3854, Published 1/12/17, comments due 4/12/17

Dorothy J. Glancy, Autonomous and Automated and Connected Cars-Oh My! First Generation Autonomous Cars in the Legal Ecosystem, 16 Minn. J.L. Sci. & Tech. 619 (2015)

Jeffrey K. Gurney, Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles, U. Ill. J.L. Tech. & Pol'y, Fall 2013, at 247

Jessica S. Brodsky, Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit the Brakes on Self-Driving Cars, 31 Berkeley Tech. L.J. 851 (2016)

Kevin Funkhouser, Paving the Road Ahead: Autonomous Vehicles, Products Liability, and the Need for A New Approach, 2013 Utah L. Rev. 437 (2013)

Andrew P. Garza, "Look Ma, No Hands!": Wrinkles and Wrecks in the Age of Autonomous Vehicles, 46 New Eng. L. Rev. 581 (2012)

<https://one.nhtsa.gov/nhtsa/av/av-policy.html#>

<https://perma.cc/UNZ3-GDE2>

Automated Vehicles—Regulatory and Other Considerations

**By: Terrence L. Graves, Esq. and
Christopher K. Jones, Esq.**

Terrence L. Graves is a shareholder in the firm of Sands Anderson PC in Richmond, Virginia where he heads the firm's Coverage & Casualty Litigation Group and its Commercial Transportation and Premises/Landlord Liability Teams. His practice focuses on the defense of transportation, toxic tort, and general insurance defense matters involving catastrophic injury and property damages. Mr. Graves is an active member of the DRI, FDCC, VADA, and TLA, and is listed in America's Best Lawyers in Transportation Law and Personal Injury Defense. He is also a Fellow of the American College of Trial Lawyers.

Christopher K. Jones is counsel with the firm of Sands Anderson PC in Richmond, Virginia where he is a member of the firm's Coverage & Casualty Litigation Group and its Commercial Transportation, Premises/Landlord Liability, and CyberSecurity Teams. His practice focuses on the defense of transportation and general liability matters. He also provides counseling and litigation support in Cybersecurity matters. Mr. Jones is an active member of DRI and VADA.

I. Introduction

In an election year in which general consensus seemed a thing of the past, there was one thing about which everyone did seem to agree: our transportation infrastructure is overtaxed and crumbling. The most recent report card of the American Society of Civil Engineers gives the four million miles of U.S. public roads an overall grade of "D."ⁱ This poor mark reflects the reality that many of our roads are badly maintained and overly congested, leading to wasted fuel and costing motorists time and money. The impacts of this are felt especially severely by the U.S. trucking industry. Another problem faced by the industry — a shortfall of up to 85,000 drivers — may also be related to frustration with these road conditions.ⁱⁱ Making matters even worse, U.S. highways are becoming more dangerous. Deaths from accidents, which had been edging down for years, jumped 10.4% in the first six months of 2016, compared to the same period in 2015.ⁱⁱⁱ

Automated vehicles (AVs) have the potential to alleviate many of these problems. 94% of auto accidents are caused by human error, so there is an enormous potential safety benefit to be realized from removing humans from the wheel.^{iv} The quicker reaction time of an AV may also permit these vehicles to be driven closer together at higher speeds, turning congestion from a problem into an asset and eliminating fuel wastage from stop and go traffic. Additionally, while the logical endpoint of AV technology is the ability to take over completely from human drivers, the technology must first be developed and adapted through a period where it complements drivers, rather than replacing them. This enhanced driving experience may make truck driving more desirable, and help ease the driver shortage.

The rapid development of every new industry poses novel challenges for policymakers. The AV industry is no different. If it is to succeed, lawmakers must strike the right balance of regulations to ensure that we realize the benefits of AV technology, before smothering it under red tape.

This past October, a Volvo tractor outfitted with an after-market AV kit produced by a subsidiary of Uber drove 2,000 cases of beer from Budweiser's brewery in Fort Collins, CO, to Colorado Springs.^v While a human driver was present in the tractor, he spent much of the 120 mile trip in the sleeper cab, and never touched the wheel.^{vi} As a proof of concept exercise, this was an unmitigated success. It demonstrated the incredible leaps that AV technology has already made, and offered a glimpse of the possible future. At the same time, it also offered a stark reminder of the potential dangers of AV technology, and the many challenges it faces to its widespread adoption: the beer truck had a dedicated police escort for its entire journey.

II. The Technology

It is impossible to assess how best to regulate AV technology without first understanding what it is, and how it is commonly described. There is a common misconception that vehicles are either automated or they are not- that some hard line exists between the two concepts. In reality, owing to the many different driving tasks that technology can take over, the distinction is much more fluid. SAE, formerly the Society of Automotive Engineers, has created a six level scheme for describing AVs. This scheme, which was recently adopted by the National Highway Transportation Safety Administration (NHTSA) is as follows:^{vii}

- Level 0: A vehicle with no automated features whatsoever. The human driver is responsible for all driving tasks. Think Model T.
- Level 1: A vehicle that has one or more automated features, but each automated feature relates exclusively to acceleration/deceleration or to steering. An example is a vehicle that has both antilock brakes and cruise control.
- Level 2: A vehicle that has an automated feature capable of changing both the steering and acceleration/deceleration of the vehicle, though a human driver must constantly monitor the driving environment. An example is a vehicle with collision avoidance.
- Level 3: A vehicle with automated features capable of controlling all aspects of acceleration/deceleration and steering. Under certain conditions, it can monitor and decide how to move through the driving environment without human intervention. A human driver must be present and able to take control at a moment's notice, however, in case driving conditions develop that the vehicle is unable to deal with (such as inclement weather or poor road markings).
- Level 4: This vehicle is completely automated and able to operate without human intervention within a specified operational design domain (ODD), such as highways, or a city. A human driver does not need to respond immediately to a request to assume the driving task. If the vehicle exceeds its ODD and a human does not take over, it will pull over to the side of the road.
- Level 5: A Level 5 vehicle is capable of fully operating the vehicle at all times, under all conditions, without human intervention or monitoring. Think Knight Rider.

NHTSA classifies vehicles at levels 3, 4, and 5 as Highly Automated Vehicles (HAVs).^{viii}

Automated vehicles achieve their varying levels of autonomy by combining a number of familiar systems.

Sensors: sensors enable a vehicle to gather data about the environment around it. Examples of sensors include: radar, which detects objects by bouncing radio waves off of them; Lidar, which does the same using lasers, and can provide a 3-D picture of a vehicle's surrounding; ultrasonic sensors, which utilize sound waves; and video.

Navigation: navigation technology is how a HAV knows where it is in space relative to where it wants to go. An example of this are the GPS systems that many of us have now been using for many years in our cars and phones. A navigation system allows an HAV to know when it needs to make a turn, its sensors prevent it from hitting something as it makes that turn.

Actuators and other system controls: these are the devices that actually apply the gas or direct the tires. They are the muscles of the AV, and in the case of higher level HAVs they eliminate the need for physical interaction between a vehicle and its human operator.

Central Processor: the central processor is the brain of any automated system. It uses information from the sensors to tell the actuators what to do.

As effective as these systems can be when integrated, they can also benefit a great deal from improvements to existing infrastructure. This includes taking such basic steps as providing better-maintained road signs and markings which, for example, create a better environment for optical recognition technology, optimizing performance in areas such as lane changing. Roads could be further improved by "smartening" them- embedding them with sensors enabling vehicles to communicate with them about weather, road and traffic conditions, a system known as road-to-vehicle (R2V) communication.

In addition to talking to the roads, HAVs will acquire an enormous amount of information from communicating with other vehicles driving on the roads- vehicles at various stages of the automation spectrum. This vehicle-to-vehicle (V2V) communication permits other vehicles on the road to serve as sensory extensions of each other, sharing helpful information concerning such things as the occurrence of sudden stops ahead, and changing traffic conditions.

A contemporaneous example of how the latter will work is the popular navigational app Waze. For those that have not yet used it, Waze provides GPS-based directions to its users, but also selects the fastest route based on current traffic conditions. For that information, Waze relies on data from other app users, who report traffic conditions on the roads on which they are driving. The aggregate of this data provides fairly nuanced real-time data on the nations highly traveled roadways. The advantages of a HAV taking over this process are obvious: not only will the amount of data — and therefore its usefulness — increase exponentially, but there will be fewer accidents and slowdowns caused by people helpfully inputting data into their phones as they drive.

III. Problems Facing HAV Technology

Despite its obvious potential as a time-, cost- and life- saver, HAV technology faces a number of hurdles to its adoption. Perhaps the one we hear most about is the fairly widespread perception that people will simply be unwilling to entrust their safety to a HAV. The argument goes that America is a nation of car lovers, who are used to controlling their vehicles and are simply unwilling to surrender that control. We are unconvinced. Very simply, this argument ignores history, both of the recent and older variety.

When elevators were first introduced, their users were ushered from floor to floor by elevator operators. Eventually, of course, the elevators were automated, the operators were phased out, and elevator users were expected to tell the device where to go themselves. When this process first began around 1900, elevator users balked.^{ix} Now, of course, it has been some time since someone insisted on taking the stairs when an elevator door opened to reveal the

absence of a livery-clad operator. For a more modern example, there is the growing number of people who are committing their investments to an algorithm that makes automatic trades based on relatively simple inputs from the account holder. And if financial security does not seem a vital enough concern, there is the fact that most airline travelers understand that their plane is on autopilot for much of its flight. The point is that automation already exists in various aspects of our lives, and in fact is often essentially unnoticed, due both to its ubiquity and its seamless integration. There will be people who refuse to use HAV tech due to basic concerns about a loss of control. But there will also undoubtedly be early adopters, and if HAV technology delivers on its promises, then the number of users will continue to grow.

A corollary to the above argument is that there is something of a Catch-22 to the adoption of HAV technology. This argument holds that HAV technology cannot be slowly phased in, because HAVs cannot share the roads with unpredictable human drivers and their less-automated vehicles. Because it is impractical to simultaneously replace every vehicle on the road with an HAV, this technology will never see widespread use.

This argument misunderstands HAV technology, and ignores the facts on the ground. AV technology is already deployed. The roads are already filled with vehicles possessed of different degrees of automation, and these vehicles coexist peaceably. A collision avoidance system, for example, does not work only if the vehicle being avoided is also equipped with that feature. Similarly, HAV technology is predicated on the assumption that it will not be deployed until it is capable of reacting to any vehicle on the road- whether it is operated by a person or otherwise. A more fully automated vehicle may be more predictable and easier for an HAV to react to, but HAV technology is being developed with other human drivers very much in mind.

There are more serious problems facing the widespread adoption of HAVs, however. One of these is an intrinsic flaw with Level 3 vehicles. Recall that, at Level 3, a HAV may be moving through the driving environment without any human intervention, but that a human driver must be present and able to take control at a moment's notice. The problem this creates is that a car that is driving itself will be an extreme challenge to the attention span of the average driver. It may be unrealistic to expect any driver operating a Level 3 vehicle in autonomous mode to maintain the degree of alertness required to assume control at a moment's notice. Level 3 vehicles — the first rung in the HAV ladder — may therefore actually present a serious safety concern that hinders the widespread adoption of HAV tech. For this reason, Google and Ford have opted to skip Level 3 and proceed directly to the development of Level 4 vehicles.^x

Cybersecurity is another critical problem for HAV developers to address. The ability to receive software updates remotely and to engage in R2V and V2V communication means these vehicles will be networked, and anything on a network is vulnerable to hacking. This creates a number of dire potential problems, from the theft of consumer data to the remote thievery of a vehicle and its cargo. A special concern for commercial operators, particularly given recent events in Europe, is that one or more vehicles in their fleet could be controlled and effectively weaponized as an agent of terror.

Liability and insurance are additional issues that must be puzzled through before HAVs are deployed. The traditional liability scheme in many states holds the actions of human driver to the standard of a reasonable man, and requires manufacturers to produce a reasonably safe product. Accidents involving HAVs at Levels 3 and 4, however, will beg the question of who was in control and who should have been in control at the time of the accident- the human or the operating system (OS) of the HAV. Not only does this create difficulties for the apportionment

of fault in an accident, but it raises questions concerning insurance. For instance, should a Level 4 vehicle have two policies of insurance, one carried by the driver which provides coverage when the driver is in control, and another by the manufacturer, which provides coverage when the OS is driving?

Commercial trucking companies can also expect some blowback in the courtroom when one of their HAVs is involved in an accident. Juries, of course, are already famously hostile to trucking companies and their drivers. Pointing the finger at the manufacturer — that is, arguing that the accident was the fault of the truck — is unlikely to improve this situation, especially in the early days of HAV technology, before most people are familiar with it.

Another issue faced by HAV technology is testing. Multiple research and manufacturing facilities throughout the country have developed rigorous testing schemes for HAVs. Some, like Virginia Tech's "Smart Road," are incredibly complex and go to extraordinary lengths to mimic the conditions that HAVs will confront on public highways.^{xi} Mimicry, though, however elaborate, is no substitute for the real thing. Testing on public roads accomplishes the dual purpose of presenting HAVs with the actual conditions they will face, and, if the HAVs perform well, increasing public confidence in the technology.

In this respect, Uber's recent testing of HAVs on public roads in California may have done HAVs a disservice. In late 2016, Uber deployed a fleet of 16 Level 3 vehicles to San Francisco, where they were integrated into its ride-hailing service. The vehicles may not have been road-ready, however, as there were multiple reports that they failed to recognize or stop for red lights, including at least one instance that was caught on camera.^{xii} Because these were Level 3 vehicles with a human driver in the seat, there is ambiguity over whether these infractions were caused by a human or an OS. Regardless, this bad press for HAVs was then

amplified by a public spat between California, which requested that Uber cease operations and register its fleet as "autonomous vehicles" under California law, and Uber, which argued that its vehicles did not meet the definition. California then revoked the existing registrations for Uber's vehicles, prompting the company to relocate the self-driving fleet to Arizona.^{xiii}

Around the turn of the last century, there was another technological marvel that many expected to revolutionize transportation: the Segway. It did not. Widespread adoption of the Segway was stymied by problems integrating it into existing infrastructure, and with difficulties it faced gaining public acceptance.^{xiv} Any reader who has ridden on a Segway most likely did so as part of a tour group, rather than as part of their commute to work. HAV technology faces the same hurdles. If it is to escape the fate of being relegated to novelty uses, such as fancy golf carts, and reach ubiquity, then it will be because politicians and regulators have found the proper middle ground between a concern for public safety and fostering technological development.

IV. The Current AV Regulatory Environment

AVs currently face a confused regulatory environment. One problem is that the average AV crosses over the jurisdictions of three separate federal regulatory agencies: NHTSA, the Federal Trade Commission, and the Federal Communications Commission.^{xv} Present complications from this problem are currently minimized, however, by the fact that there are so few federal regulations on the books which relate directly to AVs. There are minimal federal regulations limiting automation provided that a human driver is present and ready to assume control of the vehicle, as is the situation in all current iterations of AV technology.

Another problem lies with the traditional ways in which vehicles have been regulated. Historically, the federal government has regulated the technology and safety features of vehicles, while the states have enacted laws concerning their safe operation. HAV technology, of course,

blurs the distinction between these two areas. The safe operation of an HAV being driven by its OS depends on the quality of that HAV's technology. Vehicles being operated by an OS currently face a patchwork of different regulations depending on the state in which they are located. Most states have no laws whatsoever regarding the operation of HAVs. Those that do run from permissive laws allowing HAVs to be operated provided they comply with existing safety regulations, to more restrictive laws allowing HAVs to be operated for testing purposes only.

Clearly, this 50 state system is unsustainable. A transportation device intended to be operated across state lines cannot be expected to conform to dozens of possibly conflicting regulatory schemes. NHTSA recognizes this issue and announced its intentions to address it. This past September, Transportation Secretary Anthony Foxx declared that "when the software is operating the vehicle, that is an area that we intend to regulate."^{xvi}

This raises the question of what character NHTSA's actions will take. NHTSA provided a window into its thinking with the 2016 release of its Federal Automated Vehicles Policy. The *Policy* is advisory only, and is not a rulemaking. Among its most substantial contributions is the articulation of a model state regulatory policy. This suggests that, for the purpose of enforcing traffic laws, the states continue their traditional regulation of the safe operation of Level 1 and 2 vehicles driven by humans, but consider treating the OS of vehicles at Levels 3 and above as the "driver" of that vehicle, while being sure to identify and address any regulatory gaps this may create.^{xvii} NHTSA also suggests that states ensure there are no unnecessary impediments to the development and testing of HAVs, that states standardize road markings and other infrastructure in order to promote the safe operation of HAVs, and that states develop a framework for the testing of HAVs on their roads.^{xviii}

NHTSA's *Policy* also provides HAV performance guidance.^{xix} This section begins with the observation that current law requires a vehicle manufacturer to self-certify that its product is in compliance with all applicable Federal Motor Vehicle Safety Standards (FMVSS), and that there is no federal impediment to an HAV being offered for sale if it is compliant with existing FMVSS. It then lists and expounds on fifteen separate areas of concern for HAVs. These include such familiar concerns as the crashworthiness of a vehicle, but are mostly concerned with more novel issues, such as vehicle cybersecurity, data privacy, the ability of automated features to function properly after an accident, and the ethical considerations faced by an OS.^{xx} NHTSA urges manufacturers to consider these fifteen areas as they develop their products, and notes that while the guidance is currently just that, some of it may become mandatory in the future.

With a new presidential administration comes new leadership at DOT and an element of uncertainty regarding whether this will alter NHTSA's approach to AVs. The nomination of Elaine Chao for DOT secretary has been largely met with praise from the trucking industry, but her views on AV tech remain mostly an unknown.^{xxi} Chao's background of espousing a hands-off approach to regulation does provide some cause for optimism amongst AV developers.^{xxii} While she chaired the Department of Labor, for example, she opined that it was not necessary for the federal government to regulate certain vehicle safety standards if the industry was already meeting that standard.^{xxiii} Freedom from overregulation — particularly regulations which are hastily crafted in response to quickly evolving technology — could provide HAV developers the necessary oxygen to grow the industry. On the other hand, a lack of federal regulation and its preemptive effect permits the states to fill the vacuum, creating the potential for an industry-stifling patchwork of regulatory schemes.

IV. Conclusion: A Balanced Approach to the Future

HAV technology has the potential not only to revolutionize the average American's mode of travel, but to save thousands of lives, save money and foster a cleaner environment, and provide mobility to the old and infirm. These benefits will be accompanied by anticipated problems, such as growing unemployment among commercial drivers, and problems which are more difficult to predict, such as a possible drop in real estate values in the inner ring of suburbs as quick commuting times become less prized. In these early days of HAV technology, though, it is important to focus on what governments' proper response should be.

Given the current status of AV and HAV tech and the regulatory response thus far, it is possible to make a few straightforward recommendations as to how best to promote safety without unduly harming the health of the industry. In the short term, NHTSA should stand by its intention to regulate in those situations where an HAV is being operated by its OS. The public and consistent repetition of this intention — across administrations — should discourage states from promulgating regulations in this arena before NHTSA has a chance to do so. States may continue to regulate the human operation of vehicles.

But it is important that NHTSA regulate in the near future. These regulations will preempt those issued by the states, limiting confusion and eliminating the possibility that one state and its overly-restrictive approach could stifle HAV investment, research and development. Feedback from industry groups, safety and consumer advocates, and the public at large will be vital to assessing what form these regulations should take, and the guidance offered by NHTSA's *Policy* is a good start to promoting this conversation.

As the *Policy* points out, HAVs will be networked and generate massive amounts of data. This data presents both an asset and a liability. As to the former, the data gathered by deployed

HAVs and their many sensors could be incredibly beneficial to understanding how to improve HAV performance in all driving environments. NHTSA should require manufacturers to share anonymized data regarding the performance of their HAVs, with NHTSA acting as the collections point for this data. As to liabilities, we previously noted that because HAVs are networked, they can be hacked, creating concerns for data privacy and the safety of the vehicle and its occupants. The need to prevent malicious external interference, however, is not unique to HAVs, and extends to any networked device which is part of the growing Internet of Things (IOT). Federal regulation regarding IOT security is nonexistent, a problem that a number of industry experts recently brought before Congress last October. Their recommendation was that Congress should respond to this growing threat in much the same way as NHTSA has responded to the emergence of HAV technology- by issuing guidelines to manufacturers. While NHTSA's *Policy* briefly covered this issue,^{xxiv} if Congress continues to decline to act, then NHTSA should follow up on the *Policy* by issuing more detailed Guidelines in this area.

Most importantly, due to the pace and unpredictability of technological development, as well as the length and complexity of computer code, flexibility should be a prized asset of any regulatory scheme. Regulations that mandate the deployment of certain types of sensors, or that require an OS to incorporate certain elements of code, may quickly become anachronistic and unhelpful. The solution, advocated by Professor Hod Lipson, is to use statistics as the benchmark.^{xxv} For example, NHTSA could require that, in order for a particular model HAV to be operated by an OS on a public highway, the likelihood of that vehicle being involved in an accident must be only 50% that of a vehicle operated by a human driver. Regulating HAVs on the back end — by their results — instead of on the front end — by the ever-changing details of their technology — provides the benefits of simplicity and consistency. It is also a measure that

would be better understood by the public, leading to public confidence in HAV technology- so long as it is deserved.

ⁱ www.infrastructurereportcard.org.

ⁱⁱ Kevin O'Marah, *Truck Driver Shortage is a Shortage of Imagination*, Forbes, September 1, 2016, available at <http://www.forbes.com/sites/kevinomarah/2016/09/01/truck-driver-shortage-is-a-shortage-of-imagination/#b104a34748f2>.

ⁱⁱⁱ Daniel Victor, *U.S. Traffic Deaths Continue Alarming Climb*, Data Show, The New York Times, October 5, 2016, at A 15.

^{iv} National Highway Transportation Safety Administration, *Traffic Safety Facts*, February, 2015, available at <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115>.

^v Alan Ohnsman, *This Bud's For The Robot: Otto, Anheuser-Busch Claim First Automated Truck Shipment*, Forbes, October 25, 2016, available at <http://www.forbes.com/sites/alanohtsman/2016/10/25/this-buds-for-the-robot-otto-anheuser-busch-claim-first-automated-truck-shipment/#1d98b97865de>.

^{vi} Eric Newcomer, Alex Webb, *Uber Self-Driving Truck Packed With Budweiser Makes First Delivery in Colorado*, Bloomberg, October 25, 2016, available at <https://www.bloomberg.com/news/articles/2016-10-25/uber-self-driving-truck-packed-with-budweiser-makes-first-delivery-in-colorado>.

^{vii} NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety*, September, 2016, at 9.

^{viii} NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety*, September, 2016, at 10.

^{ix} Steve Henn, *Remembering When Driverless Elevators Drew Skepticism*, NPR Morning Edition, July 31, 2015

^x Alex Davies, *Ford's Skipping the Trickiest Thing About Self-Driving Cars*, Wired, November 10, 2015

^{xi} <http://www.vtti.vt.edu/facilities/virginia-smart-road.html>.

^{xii} <http://sanfrancisco.cbslocal.com/2016/12/14/self-driving-uber-apparently-runs-red-light-in-san-francisco/>.

^{xiii} Eric Newcomer and Ellen Huet, *Uber Ships Self-Driving Cars to Arizona After California Ban*, Bloomberg Business, December 22, 2016

^{xiv} Jordan Golson, *Well, That Didn't Work: The Segway is a Technological Marvel. Too Bad it Doesn't Make Any Sense*, Wired, January 16, 2015, available at <https://www.wired.com/2015/01/well-didnt-work-segway-technological-marvel-bad-doesnt-make-sense/>.

^{xv} Aarian Marshall, *The Hidden Task Ahead of Trump's Transport Chief*, Wired, November 30, 2016, available at <https://www.wired.com/2016/11/elaine-chao-secretary-transportation-self-driving-cars/>.

^{xvi} Melissa Nann Burke and Michael Wayland, *Feds announce unprecedented autonomous car guidelines*, The Detroit News, September 20, 2016, available at <http://www.detroitnews.com/story/business/autos/2016/09/19/feds-announce-unprecedented-autonomous-vehicle-guidelines/90716884/>.

^{xvii} NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety*, September, 2016, at 39, 43-44.

^{xviii} NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety*, September, 2016, at 39-40.

^{xix} NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety*, September, 2016, at 11 et seq.

^{xx} NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety*, September, 2016, at 15-31

^{xxi} Aarian Marshall, *The Hidden Task Ahead of Trump's Transport Chief*, Wired, November 30, 2016, available at <https://www.wired.com/2016/11/elaine-chao-secretary-transportation-self-driving-cars/>; Clarissa Hawes, *Trucking, Auto Industries Praise Elaine Chao Transportation Secretary Nomination*, Trucks.com, November 29, 2016, available at <https://www.trucks.com/2016/11/29/trucking-industry-praises-elaine-chao-us-dot-choice/>.

^{xxii} Russ Mitchell, *Why the driverless car industry is happy (so far) with Trump's pick for Transportation secretary*, Los Angeles Times, December 6, 2016, available at <http://www.latimes.com/business/autos/la-fi-hy-chao-trump-driverless-20161205-story.html>.

^{xxiii} Aarian Marshall, *The Hidden Task Ahead of Trump's Transport Chief*, Wired, November 30, 2016, available at <https://www.wired.com/2016/11/elaine-chao-secretary-transportation-self-driving-cars/>.

^{xxiv} NHTSA, *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety*, September, 2016, at 21-22.

^{xxv} Russ Mitchell, Why the driverless car industry is happy (so far) with Trump's pick for Transportation secretary, Los Angeles Times, December 6, 2016, available at <http://www.latimes.com/business/autos/la-fi-hy-chao-trump-driverless-20161205-story.html>.

The Road Ahead: How Products Liability Will Apply to Autonomous Vehicles

By Amelia Sreter*

I. INTRODUCTION

The advent of autonomous vehicles creates many new legal questions. A growing area of concern for both consumers and manufacturers of autonomous vehicles is the issue of liability. When an autonomous vehicle causes an accident, who is ultimately responsible? Is it the person who was sitting in the car, not paying attention because he or she believed the car could navigate safely, or is it the manufacturer who claimed that the car was safe? This question is not easily answered, and will likely be highly debated as new legislation and regulations are formulated over the coming years, and insurers, consumers, and manufacturers find their place in this new paradigm. This article will focus on new issues in products liability in the context of autonomous vehicles.

II. AUTONOMOUS VEHICLES OVERVIEW

To understand liability in autonomous vehicles, one needs a basic understanding of the vehicles and the different levels of autonomy being slowly developed and introduced for consumer as well as commercial use. The National Highway Traffic Safety Administration (NHTSA) released a policy statement on autonomous vehicles that adopts the SAE International definitions for levels of automation:

- At SAE Level 0, the human driver does everything;
- At SAE Level 1, an automated system on the vehicle can sometimes assist the human driver conduct some parts of the driving task;
- At SAE Level 2, an automated system on the vehicle can actually conduct some parts of the driving task, while the human continues to monitor the driving environment and performs the rest of the driving task;
- At SAE Level 3, an automated system can both actually conduct some parts of the driving task and monitor the driving environment in some instances, but the human driver must be ready to take back control when the automated system requests;
- At SAE Level 4, an automated system can conduct the driving task and monitor the driving environment, and the human need not take

* Amelia Sreter is a third year law student at the University of New Hampshire School of Law, J.D. anticipated May 2017. She is a participant in the Daniel Webster Scholar Honors Program, a Warren B. Rudman Fellow, and an Executive Editor of the UNH Law Review. Amelia received a Bachelor of Arts from Cornell University in 2014.

back control, but the automated system can operate only in certain environments and under certain conditions; and

- At SAE Level 5, the automated system can perform all driving tasks, under all conditions that a human driver could perform them.¹

Levels 0 and 1 denote the typical vehicle on the road today: cars that must be operated entirely by the human driver, or that have some features to help the driver occasionally, such as cruise control, blind spot protection, or even lane assist. Level 2 vehicles combine autonomous functions that may be present one at a time in Level 1 vehicles, such as by both steering to stay in lane and using adaptive cruise control to keep with the flow of traffic at the same time while on the highway. The Department of Transportation considers vehicles of Levels 3-5 to be “highly automated vehicles,” or HAVs, because the vehicles are responsible for monitoring the road and do not require constant vigilance from the driver.²

As of February 2017, many companies are in the process of developing autonomous vehicles for both consumer and commercial uses, and a few are already on the roadways. Tesla’s Level 2 vehicle, available to consumers, comes equipped with all hardware necessary for eventual full autonomy; Tesla will send software updates wirelessly to the vehicles to increase their functionality as it develops better autonomous technology.³ Tesla also plans to expand into electric autonomous trucks and buses.⁴ Mercedes-Benz, GM, and Nissan are introducing autonomous technology into their vehicles.⁵ Google and Ford are taking a different approach by skipping straight to Level 4 autonomy, although the vehicles are still a few years away from the consumer market.⁶ Uber is currently testing a fleet of autonomous rideshare vehicles in Pittsburgh, with human drivers who take over occasionally.⁷ Uber also acquired a startup, Otto, that successfully used an autonomous big-rig to ship a delivery of Budweiser beer 120 miles while

¹ U.S. DEPT. OF TRANSP., NAT’L HIGHWAY TRAFFIC SAFETY ADMIN., Federal Automated Vehicles Policy, September 2016, <https://one.nhtsa.gov/nhtsa/av/av-policy.html> [hereinafter, NHTSA Policy]. Note that prior to adopting the SAE levels, NHTSA used a system with five levels (Levels 0-4) instead of six (Levels 0-5), and any publications prior to September, 2016, reference the prior level system. *Id.*; see U.S. DEPT. OF TRANSP., NAT’L HIGHWAY TRAFFIC SAFETY ADMIN., Preliminary Statement of Policy Concerning Automated Vehicles, May 2013, available at <https://www.transportation.gov/briefing-room/us-department-transportation-releases-policy-automated-vehicle-development>, for a list and description of the prior automation level classifications.

² *Id.*

³ Jerry Hirsch, *Tesla Motors Will Ship Self-Driving Vehicles, Plans Ride Service*, TRUCKS.COM, October 19, 2016, <https://www.trucks.com/2016/10/19/tesla-motors-shipping-self-driving-vehicles/>; Jerry Hirsch, *Analysts: Musk’s Tesla Electric Truck Plans Takes Billions of Investment*, TRUCKS.COM, July 21, 2016, <https://www.trucks.com/2016/07/21/tesla-electric-trucks-buses/>.

⁴ *Id.*

⁵ Alex Davies, *Ford Says It’ll Have a Fleet of Fully Autonomous Cars in Just 5 Years*, WIRED, August 16, 2016, <https://www.wired.com/2016/08/ford-autonomous-vehicles-2021/>.

⁶ Alex Davies, *Google’s Self-Driving Car Company is Finally Here*, WIRED, Dec. 13, 2016, <https://www.wired.com/2016/12/google-self-driving-car-waymo/>; Davies, *supra* note 5.

⁷ Alex Davies, *We Take a Ride in the Self-Driving Uber Now Roaming Pittsburgh*, WIRED, Sept. 14, 2016, <https://www.wired.com/2016/09/self-driving-autonomous-uber-pittsburgh/>.

the human driver monitored the trip from the sleeper berth.⁸ The German company Daimler's Freightliner Inspiration Truck is licensed to make shipments in the state of Nevada, the first autonomous truck licensed to travel on US roads.⁹ Ford is also in the process of developing smaller autonomous delivery trucks to be available within five years, and FedEx is working towards introducing more autonomous technology into its fleet.¹⁰

The different levels of automation and human contribution to driving, clear from the variety of vehicles in use and development, complicate the liability landscape in interesting ways. As demonstrated throughout this article, a certain claim or defense may not apply equally to all vehicles with autonomous features, or even to all HAVs, because of the different levels of intervention and attention required.

III. PRODUCTS LIABILITY OVERVIEW

Products liability holds a manufacturer or distributor who sells or distributes a defective product liable for any harm caused by the defect.¹¹ The main theories of products liability include negligence, strict liability, tortious misrepresentation, and breach of warranty.¹² Strict liability allows a plaintiff to hold a manufacturer liable even when the manufacturer exercised reasonable care. There are three actionable categories of product defects in strict liability: manufacturing defects, design defects, and defective warnings.¹³ While automobile accident plaintiffs often bring claims for crashworthiness as well, these claims will remain largely unchanged in autonomous vehicles because they have to do with the structure of the vehicle rather than any autonomous features.¹⁴

A manufacturing defect occurs when the product was not produced according to its specifications,¹⁵ or, under the malfunction doctrine, when there is

⁸ Chris O'Brien, *Otto Hauls Budweiser in First Commercial Use of Self-Driving Truck*, TRUCKS.COM, Oct. 25, 2016, <https://www.trucks.com/2016/10/25/ubers-otto-hauls-budweiser-beer-across-colorado-first-commercial-use-self-driving-truck/>

⁹ Doug Newcomb, *Daimler Autonomous Truck Has Huge Commercial Implications*, FORBES, May 8, 2015, <http://www.forbes.com/sites/dougnewcomb/2015/05/08/daimler-autonomous-truck-has-huge-commercial-implications/#2b4c145e4978>.

¹⁰ Elizabeth Woyke, *FedEx Bets on Automation as it Prepares to Fend Off Uber and Amazon*, MIT TECHNOLOGY REVIEW, Feb. 3, 2017; Paul A. Eisenstein, *Ford Is Looking at Developing Driverless Delivery Trucks*, TRUCKS.COM, August 23, 2016, <https://www.trucks.com/2016/08/23/ford-developing-driverless-trucks/>.

¹¹ RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 (1998); Kevin Funkhouser, *Paving the Road Ahead: Autonomous Vehicles, Products Liability, and the Need for A New Approach*, 2013 UTAH L. REV. 437 (2013).

¹² JOHN VILLASENOR, BROOKINGS INST., PRODUCTS LIABILITY AND DRIVERLESS CARS: ISSUES AND GUIDING PRINCIPLES FOR LEGISLATION, at 7-8 (2014), http://www.brookings.edu/~media/research/files/papers/2014/04/products-liability-driverless-cars-villasenor/products_liability_and_driverless_cars.pdf; Funkhouser, *supra* note 11, at 444-45.

¹³ RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (1998); Jeffrey K. Gurney, *Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles*, U. ILL. J.L. TECH. & POL'Y, Fall 2013, at 257.

¹⁴ Gurney, *supra* note 13, at 257; Funkhouser, *supra* note 11, at 445.

¹⁵ RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (1998).

an inexplicable accident.¹⁶ A design is defective when there was a foreseeable risk of harm that could have been reduced or avoided by a reasonable alternative design, and failure to implement the alternative design rendered the product “not reasonably safe.”¹⁷ There are two tests for design defect: the consumer expectations test and the risk-utility test.¹⁸ The risk-utility test is more widely accepted,¹⁹ but both will be discussed in more detail in the following section. A failure to warn claim implicates the manufacturer’s dual duty to provide instruction on how to safely use the product and to warn of hidden dangers.²⁰ This duty is limited to risks reasonably foreseeable at the time of sale.²¹ Possible defenses the manufacturer may assert in any strict liability case include assumption of the risk, waiver, misuse, state of the art, and comparative negligence.

IV. PRODUCTS LIABILITY IN THE CONTEXT OF AUTONOMOUS VEHICLES

While products liability has long existed and has adapted to many new technologies over the years,²² the application to autonomous vehicles will likely present new challenges. In a traditional car accident, the two (or more) drivers, with the help of their insurance companies, apportion fault between them. However, in an accident involving an autonomous vehicle, many more parties could potentially be implicated. They include the driver of the car, the vehicle manufacturer, the manufacturer of a particular component of the vehicle, the software engineer, the designer or programmer of the navigational system, or in the case of an intelligent road system, the road designer.²³ Any or all of these parties could be sued by a driver or passenger in any or all of the vehicles involved in the accident.²⁴ Although the realm of possibilities is broad, it is most likely that the vehicle manufacturer will be the principal liable party because it will have the deepest pockets and the most control over the final product.²⁵ The question then becomes, what new issues arise when the manufacturer of the autonomous vehicle is the liable party in a car accident?

A. Manufacturing Defects

As mentioned above, a manufacturing defect exists when a product was not produced as intended, or under the malfunction doctrine, when there is an

¹⁶ Gurney, *supra* note 13, at 258 (citing David G. Owen, *Manufacturing Defects*, 53 S.C. L. REV. 851, 871–72 (2002))

¹⁷ RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (1998).

¹⁸ Gurney, *supra* note 13, at 258, 260–64.

¹⁹ *Id.*

²⁰ *Id.* at 264.

²¹ Gary E. Marchant & Rachel A. Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, 52 SANTA CLARA L. REV. 1321 (2012).

²² VILLASENOR, *supra* note 12, at 15.

²³ Marchant & Lindor, *supra* note 21, at 1326–29.

²⁴ *Id.*

²⁵ Jessica S. Brodsky, *Autonomous Vehicle Regulation: How an Uncertain Legal Landscape May Hit the Brakes on Self-Driving Cars*, 31 BERKELEY TECH. L.J. 851, 862 (2016).

inexplicable accident. In autonomous vehicles, the most likely part to malfunction significantly is the software that tells the car how to maneuver without human input. Any other malfunction would have the same liability analysis as malfunctions in non-autonomous vehicles if the malfunction occurs in a discrete part. However, courts have not yet applied the manufacturing defect doctrine to software as software is not generally considered a product.²⁶ The plaintiff could attempt to argue that the autonomous technology did not meet the manufacturing specifications, but it would be difficult to disentangle the “autonomous technology” as a whole from the software that enables the car to be autonomous.²⁷ For example, if a car collides with something it should otherwise have avoided, did the sensor fail to detect the object, or did the software fail to properly interpret the signals from the sensor?²⁸ If there is no obvious issue with the sensor, can courts rely on the vehicle’s internal memory and diagnostics, powered by software, to sort this out? Until these issues are resolved, a manufacturing defect claim would likely be unsuccessful in the context of autonomous vehicles.

The malfunction doctrine allows a plaintiff to recover even if he cannot demonstrate how the product was defective, similar to the tort theory of *res ipsa loquitor*.²⁹ The plaintiff must prove that “(1) the product malfunctioned, (2) the malfunction occurred during proper use, and (3) the product had not been altered or misused in a manner that probably caused the malfunction.”³⁰ While the first two elements are easily satisfied by the fact of the accident, the third may be harder to prove.³¹ Some courts may require that the vehicle was relatively new or that the part was never altered or repaired to satisfy the third prong.³² Additionally, the malfunction doctrine has not been recognized in all jurisdictions.³³ Even courts that recognize it may be hesitant to apply it, and often require an expert to show that nothing else could have caused the accident.³⁴ These limitations impede the usefulness of the malfunction doctrine in the context of autonomous vehicles.

B. Design Defects

Design defect will likely be the most common product liability claim in cases of autonomous vehicle accidents because of the challenges with other claims and the new and evolving nature of autonomous vehicle design. There are

²⁶ Gurney, *supra* note 13, at 259; Brodsky, *supra* note 25, at 863. *See also* 68 AM. JUR. 3D PROOF OF FACTS 333 § 8 (last updated Dec. 2016) (“[N]o cases have been found applying strict liability to software.”).

²⁷ *See* Gurney, *supra* note 13, at 259; Marchant & Lindor, *supra* note 21, at 1329 (“the various component parts and their respective roles in causing a malfunction may be hard to discern and separate”).

²⁸ Gurney, *supra* note 13, at 259.

²⁹ *See* Andrew P. Garza, “Look Ma, No Hands!”: Wrinkles and Wrecks in the Age of Autonomous Vehicles, 46 NEW ENG. L. REV. 581 (2012).

³⁰ Gurney, *supra* note 13, at 259.

³¹ *Id.* at 259-60.

³² *Id.* at 260.

³³ *Id.*

³⁴ Gurney, *supra* note 13, at 260.

two tests for design defects: the consumer expectations test and the risk-utility test.³⁵

i. Consumer Expectations Test

The consumer expectations test examines whether the design is unreasonably dangerous beyond the expectation of the average consumer.³⁶ This test was rejected by the Restatement (Third) of Torts: Products Liability, but many states still accept it.³⁷ In the context of autonomous vehicles, manufacturers will likely argue that the vehicles and systems are too complex for the average consumer to form appropriate and realistic expectations about their safety.³⁸ Some courts already hesitate to apply the consumer expectations test to traditional automobiles because they are highly complex even without autonomous driving.³⁹ However, other courts take the position that consumers can form reasonable expectations about a complex product with which they are familiar, or a product where the mechanics may be complex but the concept is not.⁴⁰ Often, the determination relies on the circumstances of the case: the consumer expectations test would apply where an airbag deploys when there is no crash, a vehicle bursts into flames in a 5-mile-per-hour collision, or a gas tank explodes at a stoplight.⁴¹ Similarly, a consumer could expect an autonomous vehicle to stop at a red light or stay within its lane.⁴² However, there will likely be accidents that go beyond a

³⁵ Garza, *supra* note 29, at 599.

³⁶ RESTATEMENT (SECOND) OF TORTS § 402A cmt. g (1965).

³⁷ RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2 cmt. g (1998) (“[C]onsumer expectations do not constitute an independent standard for judging the defectiveness of product designs.”); Gurney, *supra* note 13 at 261.

³⁸ Garza, *supra* note 29, at 599.

³⁹ Garza, *supra* note 29, at 601-02; Gurney, *supra* note 13, at 261. *See, e.g.*, *Soule v. Gen. Motors Corp.*, 882 P.2d 298, 310 (1994) (requiring use of risk-utility test to determine crashworthiness, and discussing appropriate circumstances to apply the consumer expectations test); *Bresnahan v. Chrysler Corp.*, 32 Cal. App. 4th 1559, 1567, 38 Cal. Rptr. 2d 446, 451 (1995) (“In relation to automobiles, the court observed that although ordinary consumers may legitimately form many safety expectations of their cars, providing standards for defectiveness, ‘the ordinary consumer of an automobile [also] simply has “no idea” how it should perform in all foreseeable situations, or how safe it should be made against all foreseeable hazards.’”) (quoting *Soule*, 882 P.2d at 307-08 (internal citations omitted)); *Branham v. Ford Motor Co.*, 701 S.E.2d 5, 15 (S.C. 2010) (In the context of a vehicle’s stability system, the court found “the consumer expectations test and its focus on the consumer ill-suited to determine whether a product’s design is unreasonably dangerous.”).

⁴⁰ *See, e.g.*, *Jackson v. Gen. Motors Corp.*, 60 S.W.3d 800, 806 (Tenn. 2001) (citing *Cunningham v. Mitsubishi Motors Corp.*, No. C-3-88-582, 1993 WL 1367436, at *6 (S.D. Ohio June 16, 1993)) (“This Court is simply not willing to . . . preclud[e] the use of the consumer expectation test in a situation involving a familiar consumer product which is technically complex or uses a new process to accomplish a familiar function. Many familiar consumer products involve complex technology.”).

⁴¹ *Pruitt v. Gen. Motors Corp.*, 72 Cal. App. 4th 1480, 1484, 86 Cal. Rptr. 2d 4, 6 (1999), as modified (June 23, 1999) (In *Soule*, 882 P.2d at 308 n.3, “the court gave examples of when the consumer expectations test was appropriate: automobiles that explode while idling at a stoplight or roll over and catch fire in a two-mile-per-hour collision. To this we might add air bags inflating for no apparent reason while one is cruising down the road at 65 miles per hour.”)

⁴² *See* Garza, *supra* note 29, at 601.

consumer's experience or understanding and require a more complex analysis, in which case the risk-utility test would apply.⁴³

ii. Risk-Utility Test

The risk-utility test is the majority test to prove design defects in products liability, and was put forth as the sole design defects test by the Restatement (Third) of Torts: Products Liability.⁴⁴ Under the Restatement, a design defect exists “when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller . . . , and the omission of the alternative design renders the product not reasonably safe.”⁴⁵ The risk-utility test therefore weighs the foreseeable risks of the current design with the safety benefits of an alternative design and the costs of implementing such alternative design.⁴⁶ A plaintiff must present a reasonable alternative design that would have prevented the harm caused by the current design to prevail.

Applying the risk-utility test to autonomous vehicles may present some challenges. When determining whether benefits outweigh risks, do juries and courts compare autonomous vehicles with the alternative of non-autonomous vehicles? Autonomous vehicles have already been shown to be safer than their traditional counterparts, with Google claiming traffic fatalities will be reduced by 50%⁴⁷, the NHTSA declaring that Tesla, Inc.'s Level 2 semi-autonomous vehicles reduced accidents involving their vehicles by 40%⁴⁸, and one study predicting that accidents will be reduced by 90% upon full adoption of fully-autonomous

⁴³ See *Soule*, 882 P.2d at 308 (“a complex product, even when it is being used as intended, may often cause injury in a way that does not engage its ordinary consumers' reasonable minimum assumptions about safe performance. For example, the ordinary consumer of an automobile simply has “no idea” how it should perform in all foreseeable situations, or how safe it should be made against all foreseeable hazards.”) (citing *Barker v. Lull Eng'g Co.*, 573 P.2d 443 (1978))

⁴⁴ RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(b) (1998).

⁴⁵ *Id.*

⁴⁶ Gurney, *supra* note 13, at 263.

⁴⁷ Garza, *supra* note 29, at 604.

⁴⁸ Tom Randall, *Tesla's Autopilot Vindicated with 40 Percent Drop in Crashes*, BLOOMBERGTECHNOLOGY, January 19, 2017, https://www.bloomberg.com/news/articles/2017-01-19/tesla-s-autopilot-vindicated-with-40-percent-drop-in-crashes?utm_source=ConstantContactMaster&utm_campaign=017bbd6b79-EMAIL_CAMPAIGN_2017_01_20&utm_medium=email&utm_term=0_0f8fe38cba-017bbd6b79-147894473.

vehicles.⁴⁹ In that case, even if an autonomous vehicle causes an accident,⁵⁰ it would be difficult to show that a Level 0 or Level 1 vehicle is the safer alternative. More realistically, a plaintiff would have to show that a certain aspect of the autonomous technology, whether a physical component or the software, was defective and could have been safer. A claim for a defect in the design of a physical component will not be much different from current suits, but just as with manufacturing defects, it may be challenging to determine whether the physical component or the software caused the accident, and therefore to determine which is defective.⁵¹ In either case, the technology is cutting-edge, and it may be difficult to find, or cost-prohibitive to retain, an expert with the knowledge and capacity to create a better design.⁵²

C. Failure to warn

The final category of defect in strict liability is defective warnings.⁵³ Manufacturers have a dual duty to inform buyers of the hidden dangers of a product and to instruct buyers how to safely use the product, although this duty is limited to foreseeable risks that could have been reduced by provision of reasonable warnings or instructions.⁵⁴ Failure to warn claims are most likely to come up in the context of semi-autonomous vehicles because they are not designed to handle all situations independently. For example, a manufacturer would have a duty to inform a driver that the vehicle's GPS system does not work as well in remote locations, or that it has trouble with certain road conditions, such as dirt roads or bad weather.⁵⁵ In these circumstances, a driver would need to

⁴⁹ Michele Bertoncello & Dominik Wee, *Ten Ways Autonomous Driving Could Redefine the Automotive World*, AUTO. & ASSEMBLY, MCKINSEY&COMPANY, June 2015, <http://www.mckinsey.com/industries/automotive-and-assembly/our-insights/ten-ways-autonomous-driving-could-redefine-the-automotive-world>. Tesla has also declared a goal to decrease accidents by 90%. Randall, *supra* note 48. But see Keith Naughton, *Humans Are Slamming Into Driverless Cars and Exposing a Key Flaw*, BLOOMBERGTECHNOLOGY, December 17, 2015, <https://www.bloomberg.com/news/articles/2015-12-18/humans-are-slamming-into-driverless-cars-and-exposing-a-key-flaw> (explaining that accident rates for driverless cars surrounded by human drivers are twice as high because they obey traffic laws rather than following human distracted or aggressive driving habits).

⁵⁰ Google's self-driving cars have only been the cause of one accident, although Google did not admit fault, and Tesla's semi-autonomous Level 2 car involved in a fatal crash has been absolved from responsibility by the NHTSA. Alex Davies, *Google's Self-Driving Car Caused Its First Crash*, WIRED, February 29, 2016, <https://www.wired.com/2016/02/googles-self-driving-car-may-caused-first-crash/>; Randall, *supra* note 48.

⁵¹ M. Ryan Calo, *Open Robotics*, 70 Md. L. Rev. 571, 594-600 (2011) ("It is extremely difficult to discover whether software, as opposed to hardware, is responsible for the glitch that led to an accident."). A truly autonomous vehicle would likely have learning capacity; is the manufacturer then responsible for self-taught behaviors not originally programmed that cause an accident? See Marchant & Lindor, *supra* note 21, at 1329 n.29.

⁵² Gurney, *supra* note 13, at 263-64. While autonomous vehicles will likely decrease the frequency of accidents, when an autonomous vehicle does cause an accident it is likely to be much more severe with greater consequences to the passengers. In a severe injury case, the plaintiff is likely to pursue the case regardless of increased expert costs.

⁵³ RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(c) (1998).

⁵⁴ *Id.*

⁵⁵ See Gurney, *supra* note 13, at 265-65.

be aware or be alerted by the vehicle that the driver needs to take over to ensure safe operation. The manufacturer therefore must take into consideration all foreseeable circumstances and fully inform the driver or passenger on safe operation of the vehicle, or design the vehicle to warn the driver when such circumstances arise.

Tesla's Autopilot feature provides a demonstration of the necessity of warnings. This Level 2 feature requires a driver's attention at all times, but the driver can turn on the Autopilot feature on highways and the car will stay in the lane, maintain speed appropriate to traffic conditions, and change lanes.⁵⁶ The car will also park itself, and can be summoned from a parking spot without a driver inside.⁵⁷ The Autopilot feature comes disabled and requires an explicit acknowledgement of risks before it can be enabled.⁵⁸ It also has frequent alerts to remind drivers to keep their hands on the wheel when Autopilot is engaged.⁵⁹ A Tesla car with Autopilot enabled was involved in a fatal crash in May, 2016, when the driver failed to take control in a situation the vehicle was not equipped to handle independently.⁶⁰ Despite the warnings, some believed that Tesla could be held responsible for making the feature sound more advanced and safer than it was.⁶¹ The NHTSA ultimately absolved Tesla and the Autopilot feature from any liability in the crash because it determined the driver had the opportunity to regain control and avoid the accident but did not attempt to do so.⁶² However, Tesla has since updated the software to require drivers to touch the steering wheel more frequently.⁶³ While Tesla was not liable in this instance, this accident and subsequent turmoil highlight the difficulty of providing adequate instructions and warnings, especially when the human driver retains some degree of responsibility.

Adequacy of warnings may become a more prominent issue as Level 3 and Level 4 vehicles are developed. Level 3 vehicles can alert the driver when the driver needs to reassert control, and while Level 4 vehicles do not require the driver to maintain vigilance or reassert control quickly, they only operate fully in certain driving conditions.⁶⁴ The liability analysis may then hinge on how much warning the vehicle provided the driver, whether it was clear, whether it was sufficiently loud. For example, a driver may be watching a movie with headphones on his smartphone when the vehicle warning sounds or flashes on a screen in the dashboard. If the driver does not see or hear the signal, is the driver negligent even though he was not required to remain alert, or was this a

⁵⁶ TESLA PRESS INFORMATION, AUTOPILOT, <https://www.tesla.com/presskit/autopilot#autopilot> (last visited Jan. 23, 2017)

⁵⁷ *Id.*

⁵⁸ Nicky Woolf, *Tesla fatal Autopilot Crash: Family May Have Grounds to Sue, Legal Experts Say*, THE GUARDIAN, July 6, 2016, <https://www.theguardian.com/technology/2016/jul/06/tesla-autopilot-crash-joshua-brown-family-potential-lawsuit>.

⁵⁹ *Id.*

⁶⁰ Woolf, *supra* note 58.

⁶¹ *Id.*

⁶² Randall, *supra* note 48.

⁶³ *Id.*

⁶⁴ See *supra* note 1 and accompanying text.

foreseeable circumstance that the manufacturer should have anticipated in designing an adequate warning system?⁶⁵

D. Warranties

All products involve warranties created through marketing and sales that reassure the consumer that the product is of good quality.⁶⁶ They may be express warranties, created explicitly in advertising, a product description, a contract, or even a sample of the product.⁶⁷ Warranties may also be implied, or imposed by the Uniform Commercial Code (UCC).⁶⁸ Implied warranties include the implied warranty of merchantability and the implied warranty of fitness for a particular purpose.⁶⁹ In the case of autonomous vehicles, the vehicle must be capable of performing the functions advertised, such as self-parking, and be fit for the uses reasonably anticipated by the consumer, such as allowing the driver to read while commuting. However, the manufacturer can disclaim warranties, and limit remedies for breach of warranty.⁷⁰ For example, Tesla has limited its warranties on its Autopilot feature by asserting that the driver must have his or her hands on the wheel.⁷¹ All told, the application of warranties to autonomous vehicles is likely not very different from traditional vehicles.

E. Misrepresentation

Liability arises from misrepresentation when one person makes a false or misleading representation to another, and that person is harmed by his reasonable reliance on the misrepresentation.⁷² Misrepresentation may be fraudulent, when the misrepresentation was intentional, or negligent, when the party making the representation knew or should have known it was false.⁷³ Strict liability for misrepresentation may also be imposed regardless of whether the defendant knew the information was false.⁷⁴ In the context of autonomous vehicles, similar to an express warranty, misrepresentation claims might arise where the vehicle does not live up to its advertising. For example, a semi-autonomous vehicle may advertise that it only needs human intervention rarely when in fact it requires the driver to touch the wheel every few minutes.⁷⁵ Again, the law is not likely impacted by the advent of autonomous vehicles, but novel situations and applications may arise.

⁶⁵ Wearing headphones while driving is illegal in some states. *See, e.g.*, MASS. GEN. LAWS ch. 90 § 13; VEH. & TRAF. § 375(24).

⁶⁶ VILLASENOR, *supra* note 12, at 12.

⁶⁷ UCC § 2-314; VILLASENOR, *supra* note 12, at 12.

⁶⁸ VILLASENOR, *supra* note 12, at 12.

⁶⁹ UCC §§ 2-314, 2-315; VILLASENOR, *supra* note 12, at 12.

⁷⁰ UCC § 2-316

⁷¹ Wayne Cohen & Nicole Schneider, *Potential Liability Ramifications of Self-Driving Cars*, 36 AUTOMOTIVE August 9, 2016, <http://cohen-lawyers.com/wp-content/uploads/2016/08/WestLaw-Automotive-Cohen-Commentary.pdf>.

⁷² VILLASENOR, *supra* note 12, at 11.

⁷³ *Id.*

⁷⁴ *Id.*

⁷⁵ *See id.*

F. Defenses

Manufacturers of autonomous vehicles may assert various defenses to claims brought against them for harm caused by their vehicles. These include comparative negligence, misuse, state of the art, assumption of the risk, and waiver.

i. Comparative Negligence

Comparative negligence weighs the amount of fault of the two parties, and imposes liability accordingly. Comparative negligence is most likely to arise in the context of vehicles able to be controlled by a human driver, regardless of its autonomous capabilities. Where driver control is possible, a driver could negligently enable autopilot or some other autonomous feature when it's not appropriate. For example, a driver may use the autonomous features in conditions the manufacturer advised against, such as during a snowstorm or on dirt roads. Alternatively, the driver may enable the feature appropriately, but fail to disengage it as necessary when a condition the vehicle is not equipped to handle arises. This analysis would come into play in situations similar to the Tesla example above,⁷⁶ where the manufacturer and the autonomous technology were absolved of responsibility because the driver had the opportunity to regain control of the vehicle but did not.

In the case of fully-autonomous, Level 5 vehicles, a situation may arise where the vehicle could not prevent the accident, but a human driver could have. In this situation, the manufacturer likely cannot, or should not be able to, assert comparative negligence. A fully autonomous vehicle should be able to handle all conditions, excepting any manufacturers warned against, and if one arises it isn't equipped for, the manufacturer should be responsible for any failure to adapt. The purpose of autonomous vehicles is to allow people to be more efficient and productive, and to give freedom to those who are not able to drive themselves.⁷⁷ This purpose would be defeated if the passengers in a fully-autonomous vehicle were responsible for paying attention to the road and jumping in to prevent accidents.

ii. Misuse

The misuse defense allows a manufacturer to disclaim liability for harm caused when the product was not being used as intended or designed.⁷⁸ However, a manufacturer still has a duty to protect against foreseeable misuses.⁷⁹ Therefore, a manufacturer would not be responsible for an accident that occurred because the consumer modified the vehicle, but it is required to take into account the likelihood that drivers will be distracted or take advantage of the vehicles' functionality to do other things while behind the wheel.⁸⁰

⁷⁶ See *supra* notes 58 and 62, and accompanying text.

⁷⁷ See Gurney, *supra* note 13, at 267-68 for a discussion of comparative fault across different types of drivers.

⁷⁸ See Gurney, *supra* note 13, at 267-68.

⁷⁹ *Id.*

⁸⁰ See *id.*

iii. State of the Art

The state-of-the-art defense takes into account the fact that the technology is new and not every potential consequence or accident can be foreseen. When the defense is asserted in a failure to warn claim, courts examine what the manufacturer could have reasonably foreseen based on the technology and scientific knowledge available at the time of production.⁸¹ In a design defect claim, the state-of-the-art defense highlights the feasibility aspect of an alternative design that would reduce or eliminate known risks. Even if a manufacturer is aware of a risk, it may be infeasible or impossible to reduce or eliminate it because of the limits of the scientific and technological knowledge available at the time.⁸² This defense can apply to physical aspects of the vehicle or to the software.

iv. Assumption of the Risk

The assumption of risk defense requires that the plaintiff knew and understood the risk, and voluntarily encountered the risk.⁸³ Not all jurisdictions recognize this defense, as it has merged with comparative negligence.⁸⁴ The difficulty with this defense as it applies to autonomous vehicles is that the manufacturer would have to be aware of and disclose the risk that led to the accident.⁸⁵ This defense would most likely apply to discrete conditions or circumstances the manufacturer warned against. For example, if a manufacturer warned the driver that the autopilot feature does not function well in snowy road conditions but the driver failed to disengage autopilot when it started snowing, the driver likely assumed the risk. However, this analysis becomes more complicated when considering different types of drivers in Level 4 vehicles, such as a disabled or intoxicated driver who is incapable of taking control of the car when it begins to snow.⁸⁶ Of course, the manufacturer could argue that the driver assumed the risk by even entering a car that may not function independently in all conditions. This defense is also limited to the driver and perhaps passengers of the autonomous vehicle, and does not include anyone in other vehicles involved in the accident.

v. Waiver

Finally, manufacturers could avoid liability by asking consumers to sign waivers accepting the risks and taking personally responsibility for accidents. However, risks must be fully disclosed for a consumer to appreciate them and absolve the manufacturer of liability; a waiver could not defend manufacturers against unexpected risks and unforeseeable accidents.⁸⁷

⁸¹ *Id.* at 268-69.

⁸² *Id.* at 269.

⁸³ Gurney, *supra* note 13, at 269.

⁸⁴ Marchant & Lindor, *supra* note 21, at 1336.

⁸⁵ Gurney, *supra* note 13, at 269.

⁸⁶ See *id.* at 269-70 for a discussion of the application of assumption of the risk defense to different types of drivers.

⁸⁷ Brodsky, *supra* note 25, at 865.

G. Additional issues

Clearly the largest change in the liability scheme is the shift of liability from the driver of the vehicle to the manufacturer. This change creates additional issues beyond simply the theories of liability that might apply.

i. Increased Litigation

It's likely that as autonomous vehicles are introduced on the consumer market, or become available for use by consumers in ride sharing, products liability lawsuits against manufacturers will see a sharp increase. In the past, new technologies have invited litigation as the safety of the product and the public's trust are tested. For example, there was a large increase in litigation against biotechnology companies in the 1980s, as well as an increase in jury verdicts against them.⁸⁸ This type of increased liability can severely impact a company's ability to innovate and produce new products.⁸⁹ Some argue that the large decrease in the number of biotechnology companies between the 1980s and early 2000s is attributable to the costs of insuring against products liability suits.⁹⁰ The same problem could occur in the autonomous vehicle industry if manufacturers are always held strictly liable.

Predictably, public opinion of autonomous vehicles will likely influence the legal landscape of liability for manufacturers, not only because the public will be the ones bringing the suits, but also because the public will sit on the jury and decide the outcome of these cases. Jurors could believe that autonomous vehicles are of great benefit to society, increasing traffic safety and commuter efficiency, and eventually even decreasing the number of vehicles on the road and therefore vehicle pollution.⁹¹ Alternatively, jurors could believe that self-driving cars take automation too far or displace people who drive for a living, or fear the technology simply because it is new and foreign, and therefore punish the manufacturers with unfavorable verdicts.⁹²

⁸⁸ *Id.* at 864-65.

⁸⁹ See Michael D. Stovsky, *Product Liability Barriers to the Commercialization of Biotechnology: Improving the Competitiveness of the U.S. Biotechnology Industry*, 6 BERKELEY TECH. L. J. 363, 373-76 (1991) (explaining the impact of products liability on the biotechnology industry).

⁹⁰ Kyle Colonna, *Autonomous Cars and Tort Liability*, 4 J. L., TECH. & INTERNET, 81, 110 (2012); Philip P. Boffey, *Vaccine Liability Threatens Supplies*, NEW YORK TIMES, June 24, 1984, <http://www.nytimes.com/1984/06/26/science/vaccine-liability-threatens-supplies.html?pagewanted=all>;

⁹¹ See, e.g., Katie Fehrenbacher, *Future Cities Could Run On Shared Fleets of Electric Self-Driving Cars*, FORTUNE, Oct. 11, 2016, <http://fortune.com/2016/10/11/shared-electric-self-driving-cars/> (explaining that self-driving cars will allow for increased ride sharing and fewer cars on the roads).

⁹² See Marchant & Lindor, *supra* note 21, at 1335 (explaining that jurors may be suspicious of new technology regardless of the predicted benefits or actual risk of harm); see, e.g., Matt McFarland, *The Backlash Against Self-Driving Cars Officially Begins*, CNNtech, January 10, 2017, <http://money.cnn.com/2017/01/10/technology/new-york-self-driving-cars-ridesharing/> (describing a push in New York state to ban driverless cars).

ii. Evidentiary Issues

Lawsuits involving autonomous vehicles may prove challenging to bring or follow through because of the evidentiary issues that accompany cutting-edge technology. The technology that allows vehicles to be autonomous is incredibly complicated and it would require at least one, but more likely multiple, highly specialized experts to prove liability. This is especially true for defective software, and software is the aspect of an autonomous vehicle most likely to be responsible for an accident.⁹³ To provide evidence of a reasonable alternative design, experts in computer science, mathematics, economics, and autonomous vehicles would be needed to provide an alternative algorithm and demonstrate feasibility.⁹⁴ In today's typical accident, these costs would easily outweigh any recovery. However, if the accident is more severe, as some believe all the rare autonomous vehicle accidents will be, then the costs may prove immaterial.

Depending on the jurisdiction, plaintiffs may be able to use evidence of a subsequent remedial measure, such as a software update, to prove a reasonable alternative design exists.⁹⁵ Federal Rule of Evidence 407 prohibits the use of subsequent remedial measures, but not all states' rules include the prohibition. The ability to use a later update to prove a safer alternative would greatly decrease the cost of litigation for the plaintiff. Regardless of jurisdiction, a plaintiff could also introduce evidence of an update to the software that predates the accident but wasn't installed in plaintiff's car, or of a safer algorithm used by a competitor.

iii. Insight from analogous situations

Looking to the way liability has been addressed in analogous situations may shed light on how autonomous vehicles will be treated in the future.⁹⁶ While autonomous vehicles seem new, automation is not a new concept; liability as applied to existing automated features or machines could pave the path for liability in automobiles. Clearly, current autonomous features in vehicles provide a glimpse into how juries will treat autonomous vehicles. Plaintiffs have been successful in claiming that failures in a vehicle's cruise control system caused the vehicle to accelerate unexpectedly or fail to respond to braking.⁹⁷

Commercial airplanes provide a particularly apt example because they are largely automated, with the pilot merely monitoring systems during flight.⁹⁸ However, in at least one case, a judge held the pilot liable for a crash caused by a plane with autopilot enabled because "[t]he obligation of those in charge of a plane under robot control to keep a proper and constant lookout is unavoidable."⁹⁹ This argument could easily apply to Level 1 and Level 2 vehicles, but what about HAVs, where the car is able to alert the human driver if it needs assistance?

⁹³ Gurney, *supra* note 5, at 263.

⁹⁴ *Id.*

⁹⁵ Gurney, *supra* note 13, at 266.

⁹⁶ Marchant & Lindor, *supra* note 21, at 1324-25.

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ *Brouse v. United States*, 83 F. Supp. 373, 374 (N.D. Ohio 1949).

Or Level 5 vehicles that are designed never to require human intervention? If this result were applied too broadly, it could potentially defeat the purpose of autonomous vehicles altogether because only those licensed to drive and capable of taking over could assume the obligation to oversee the “autopilot.”¹⁰⁰

Manufacturers of industrial robots used in manufacturing have been subject to litigation when their robots injure employees, indicating that manufacturers of autonomous technology of many kinds may be subject to liability for injuries caused by the technology.¹⁰¹ However, the injuries have mostly been attributed to the employees’ failing to take safety precautions or disabling safety features that would have prevented the injury.¹⁰²

iv. Insurance

One question that consumers may be particularly interested in is that of insurance. If manufacturers will be the responsible party much more frequently than consumers, will insurance continue to be necessary for owners of autonomous vehicles? While vehicles are still capable of being controlled by human drivers, there is always the risk of an accident caused by human error. However, the lower risk associated with autonomous vehicles could lead to decreased insurance premiums. For the same reason, insurance companies might incentivize autonomous vehicles by charging higher premiums for vehicles with lower levels of autonomy.¹⁰³ While accidents may be less frequent, some argue that the severity of accidents could increase. Insurers would have the best access to that type of data, and effectively steer the market towards safer vehicles or certain types of autonomous technology, thereby incentivizing manufacturers as well.

V. LAWS AND REGULATIONS AND THEIR IMPACT ON LIABILITY

The states have traditionally been responsible for regulating licensing and registration, traffic laws and enforcement, and motor vehicle insurance and liability schemes.¹⁰⁴ The Department of Transportation and the National Highway Traffic Safety Administration is in charge of ensuring the safety of motor vehicles by creating Federal Motor Vehicle Safety Standards (FMVSS), identifying safety defects, and recalling vehicles or equipment that pose an unreasonable safety risk. These divided responsibilities may make it difficult to establish a uniform approach to autonomous vehicles across the country, which could impact the development and implementation of autonomous vehicles.

¹⁰⁰ The first man to ride in an un-monitored, Level 5 autonomous car was a blind man who felt he lost his independence when he lost his sight. Riding in a self-driving car, he felt he “was given the opportunity to be the man that [he] was before,” and that it let him “be a whole person again.” Davies, *supra* note 6.

¹⁰¹ Marchant & Lindor, *supra* note 21, at 1325.

¹⁰² *Id.*

¹⁰³ VILLASENOR, *supra* note 12, at 13.

¹⁰⁴ NHTSA Policy, *supra* note 1, at 38.

A. Variations in state law

Variations in state law may provide difficulty in designing and introducing autonomous vehicles across the country. Although the NHTSA promulgates federal safety standards, current vehicle legislation is largely state specific.¹⁰⁵ Many states have laws that are incongruous or even directly contradictory to those in neighboring states.¹⁰⁶ For example, Vermont permits passing in the presence of a double yellow line, although in virtually every state a double yellow line indicates a no-passing zone. States also have different following-distance laws, and statewide maximum speed limits that may not be posted on any given road. How do manufacturers design cars that can comply with such conflicting legislation? Will they have to build vehicles designed for a specific state, or perhaps provide different software packages depending on the state in which the vehicle will be used? What if a consumer wants to move, or drive cross-country?

Some laws are simply nonsensical when applied to autonomous vehicles. Consider cell phone laws that prohibit texting while driving; many cars now have interfaces that allow voice text messaging through the vehicle. If the vehicle is the driver, is it breaking the law by texting for its passengers?¹⁰⁷ Many states also have laws that require the driver to have at least one hand on the wheel at all times; how does a self-driving car keep a hand on its own steering wheel?

In addition to the existing rules of the road, states have also begun introducing and passing legislation regulating autonomous vehicles. As of December, 2016, at least 9 states plus Washington, D.C. had enacted laws regulating autonomous vehicles, and two states governor's signed executive orders.¹⁰⁸ At least 17 other states have introduced bills regarding autonomous vehicles as well.¹⁰⁹ The statutes include varying definitions of driver, control, autonomous, and other salient terms. Some statutes ban cars without a human driver in the driver's seat, or ban cars without the capability to be manually operated. The varying levels of acceptance towards the new autonomous technologies could make it difficult for manufacturers to promulgate their autonomous vehicles, or slow down production and progress as manufacturers attempt to build cars that comply with as many states' laws as possible.

The varying state legislation could create inconsistency across states in not only the types of autonomous vehicles and degrees of autonomy allowed, but also the extent of manufacturer liability. Florida, Michigan, and the District of

¹⁰⁵ See Brodsky, *supra* note 25, at 867-68 for examples of varying state laws that may hinder or challenge autonomous vehicle development.

¹⁰⁶ *Id.*

¹⁰⁷ NHTSA has recognized that in Google's anticipated Level 5 autonomous vehicles, the software is the "driver." Nat'l Highway Traffic Safety Admin., Letter to Google Interpreting the Federal Motor Vehicle Safety Standards (Feb. 4, 2016) <https://isearch.nhtsa.gov/files/Google%20--%20compiled%20response%20to%2012%20Nov%20%2015%20interp%20request%20--%204%20Feb%2016%20final.htm>. While the letter refers to the vehicles as Level 4, the letter was written prior to the adoption of SAE levels of automation, and thus the Level 4 referenced is equivalent to SAE Level 5.

¹⁰⁸ NAT'L CONFERENCE OF STATE LEGS., *Autonomous/Self-Driving Vehicles Legislation*, Dec. 12, 2016, <http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx>.

¹⁰⁹ *Id.*

Columbia enacted statutes that include protective language decreasing manufacturer liability for accidents that occur as a result of after-market products that convert non-autonomous vehicles to include autonomous features.¹¹⁰ Other states include this language in bills currently being introduced, including a bill introduced in January in the New Hampshire House of Representatives.¹¹¹

The New Hampshire bill provides a fairly representative example. The definitions section of the New Hampshire bill appears to limit the bill's applicability to HAVs, and explicitly excludes autonomous systems that merely assist the driver in certain tasks.¹¹² However, the bill would limit the use of HAVs to testing purposes only, and requires a driver to be behind the wheel at all times.¹¹³ The company testing the vehicles must also have a five million dollar surety bond or insurance coverage, clearly indicating that the states expect the manufacturers to bear the liability burden.¹¹⁴ The New Hampshire bill is substantially similar to California's autonomous vehicle law, and to the first autonomous vehicle law in Florida, passed in 2012, although that law has since been amended.¹¹⁵ The amended Florida law, passed in 2016, is the most permissive state law relating to autonomous vehicles; it eliminates the requirement that the vehicles only be used for testing, and no longer requires an operator to be present in the vehicle while it is operating in autonomous mode.¹¹⁶

One Florida senator used the hashtag "#OpenForBusiness" when referencing the law on Twitter.¹¹⁷ Ironically, he tweeted at Uber, apparently inviting the company to test its autonomous vehicles in Florida like in Pittsburgh.¹¹⁸ However, Florida has not been welcoming to Uber, and the company only operates in a select few areas of the state.¹¹⁹ An Uber spokesman said the company would not bring its autonomous vehicles to Florida until the state passes regulations to allow it to operate throughout the state.¹²⁰ This anecdote is a telling example of the myriad conflicting regulations, across states and even within states, that will influence the development and promulgation of autonomous vehicles.

¹¹⁰ VILLASENOR, *supra* note 12, at 14.

¹¹¹ H.R. 314, 2017, Leg. 2017 Sess, (N.H. 2017).

¹¹² *Id.*

¹¹³ *Id.*

¹¹⁴ H.R. 314, 2017, Leg. 2017 Sess, (N.H. 2017).

¹¹⁵ Compare H.R. 1207, 2012 Leg. (Fla. 2012), with H.R. 314, 2017, Leg. 2017 Sess, (N.H. 2017) and Cal. Veh. C. § 38750. California's law is more restrictive in that it requires manufacturers to apply for permits before testing vehicles on public roads. Cal. Veh. C. § 38750.

¹¹⁶ H.R. 7027, 2016 Leg. (Fla. 2016); NAT'L CONFERENCE OF STATE LEGS., *supra* note 109.

¹¹⁷ Amy Sherman, *In Florida, No Permit Needed for Driverless Cars, Senator Says*, POLITIFACT.COM, December 12, 2016, <http://www.politifact.com/florida/statements/2016/dec/28/jeff-brandes/florida-no-permit-needed-driverless-cars-florida-s/>

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ *Id.*

B. Existing federal regulations

The National Highway Traffic Safety Administration issued a policy statement on autonomous vehicles in fall 2016 that outlines the NHTSA's approach to autonomous vehicles moving forward.¹²¹ The NHTSA policy statement includes a model state policy and recommendations for the states that could address the state variation issue discussed above.¹²² The policy recommends reviewing current laws to limit or eliminate unnecessary impediments to autonomous vehicle adoption, and updating references to human drivers or laws that are nonsensical when applied to autonomous vehicles.¹²³ It recommends recognizing the vehicle as the driver in HAVs to allow for the potential of unlicensed passengers in HAVs without human drivers.¹²⁴ The policy also addresses testing, and suggests a framework similar to that adopted in California, requiring permits and instituting requirements for test drivers.¹²⁵ However, in addressing the liability issue, the policy merely mentions the issues that the states need to address (which parties must carry insurance, how to allocate liability) but does not provide any guidance on how to make these determinations or how to provide consistency between states.¹²⁶

The NHTSA also issued a Guidance Bulletin on safety related defects in autonomous vehicles.¹²⁷ The guidance clarified that the NHTSA retains recall authority over autonomous vehicles regardless of the innovative nature of the technology.¹²⁸ It also asserted that it considers software to be motor vehicle equipment within the meaning of the Safety Act,¹²⁹ and therefore a software defect, including vulnerability to hacking, constitutes a defect sufficient to justify a recall if it poses an unreasonable safety risk.¹³⁰ It is unclear how this determination might influence the manufacturing defect analysis above, given that software has not previously been recognized as a product.¹³¹ However, this does make clear that software in autonomous vehicles will likely be subject to design defect claims if it causes an accident.

In January 2017, the NHTSA published a notice of proposed rulemaking that suggests a new FMVSS to mandate and standardize use of vehicle-to-vehicle (V2V) communications.¹³² The new rule would require new vehicles to be capable of V2V communication, which enables a vehicle to send and receive

¹²¹ NHTSA Policy, *supra* note 1.

¹²² *Id.* at 37-47.

¹²³ *Id.* at 39.

¹²⁴ *Id.* at 43-44.

¹²⁵ *Id.* at 41-43; see Cal. Veh. C. § 38750.

¹²⁶ NHTSA Policy, *supra* note 1, at 45.

¹²⁷ DEP'T OF TRANSP., NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., NHTSA-2016-0040, ENFORCEMENT GUIDANCE BULLETIN 2016-02: SAFETY-RELATED DEFECTS AND AUTOMATED SAFETY TECHNOLOGIES (2016) [hereinafter NHTSA Guidance Bulletin].

¹²⁸ *Id.* at 8-9.

¹²⁹ The National Traffic and Motor Vehicle Safety Act, as amended ("Safety Act"), 49 U.S.C. § 30101 *et seq.*, is the NHTSA's originating statute.

¹³⁰ NHTSA Guidance Bulletin, *supra* note 126, at 14-15.

¹³¹ See *supra* Section IV.A.

¹³² Federal Motor Vehicle Safety Standards; V2V Communications, 82 Fed. Reg. 3854 (proposed Jan. 12, 2017) (to be codified at 49 C.F.R. 571).

“Basic Safety Messages (BSM) about a vehicle’s speed, heading, brake status, and other vehicle information to surrounding vehicles, and receive the same information from them. When received in a timely manner, this information would help vehicle systems identify potential crash situations with other vehicles and warn their drivers.” The automotive industry has argued that the systems necessarily rely on information received from other vehicles over which they have no control, which inherently confuses the responsibility for any malfunction.¹³³ However, the NHTSA believes the V2V technology is similar enough to currently existing technology that the requirement does not create “new or unbounded liability exposure for the industry.”¹³⁴ Additionally, at this point, the technology is merely a warning system, and the driver retains sole responsibility for controlling the vehicle.¹³⁵ The liability debate is likely to continue over the course of the comment period for the proposed rule, which closes April 12, 2017.

VI. POTENTIAL SOLUTIONS

A. Maintain strict liability

While strict liability may be seen as harsh or stifling to technological development,¹³⁶ some car manufacturers openly support strict liability. Volvo, Google, and Mercedes-Benz have all pledged to accept liability if their vehicles cause an accident.¹³⁷ This is likely because the manufacturers are fairly confident that their vehicles will cause few, if any, accidents, especially as the technology continues to improve.¹³⁸ Google’s cars have been in multiple accidents, but all but one have involved the Google car being rear-ended.¹³⁹ The only accident in which Google “bear[s] some responsibility” is one in which the vehicle changed lanes in front of a bus that both the vehicle and the human driver saw but believed would slow down.¹⁴⁰ Strict liability realistically only applies to HAV vehicles because of the high likelihood that humans will intervene, or fail to intervene, and cause an accident if a vehicle is functioning with anything less than full autonomy. However, if HAVs prove less safe than manufacturers predict, more protections may be necessary to maintain the industry’s momentum.

B. Regulatory schemes that support autonomous vehicles

Even though some manufacturers support strict liability, the social utility of autonomous vehicles in preventing accidents is such that legislation may be

¹³³ *Id.* at 3869. 3966.

¹³⁴ *Id.*

¹³⁵ *Id.* at 3966.

¹³⁶ *See supra* Section IV.G.i.

¹³⁷ Jim Gorzelany, *Volvo Will Accept Liability for Its Self-Driving Cars*, FORBES, October 9, 2015, <http://www.forbes.com/sites/jimgorzelany/2015/10/09/volvo-will-accept-liability-for-its-self-driving-cars/#d4d44d03d80e>; Bill Whitaker & Mark Lieberman, *Hands Off the Wheel*, CBS NEWS, 60 MINUTES, October 4, 2015, <http://www.cbsnews.com/news/self-driving-cars-google-mercedes-benz-60-minutes/>.

¹³⁸ Whitaker & Lieberman, *supra* note 136.

¹³⁹ Davies, *supra* note 50.

¹⁴⁰ *Id.*

necessary to protect manufacturers and ensure the continued development of autonomous vehicles.¹⁴¹ One option would be a federal regulatory scheme for liability for autonomous vehicles that preempts state tort law.¹⁴² This would be a departure from traditional liability schemes that allow states to develop their own tort laws, but it would spare manufacturers from managing different tort laws in each state.¹⁴³

Short of complete preemption, federal liability caps could provide a method for limiting liability without infringing on states' ability to determine their own tort schemes.¹⁴⁴ In the past, Congress has limited liability for emerging industries that present unavoidable risk but high utility, including liability caps for commercial airline crashes, oil spills, and problems related to "Y2K," among others.¹⁴⁵ These caps would allow manufacturers to continue to develop autonomous vehicle technology without being crippled by litigation, while still providing some compensation to those inevitably injured by the emerging technology. Alternatively, Congress could create an insurance program similar to that created by the 1957 Price-Anderson Act, which was designed to compensate those injured in a nuclear accident.¹⁴⁶ A mandated insurance program that requires contributions from all manufacturers would distribute risks among manufacturers and limit costs to any one company.¹⁴⁷ A no-fault compensation system, like that used for vaccine-related injuries, could similarly distribute costs and risks among manufacturers.¹⁴⁸

VII. CONCLUSION

As autonomous vehicles become increasingly more available and widespread, liability issues will inevitably arise. While strict liability offers one solution, its application to autonomous vehicles may prove unique and provide new challenges to manufacturers, consumers, insurers, and law-makers alike.

¹⁴¹ See Marchant & Lindor, *supra* note 21, at 1325.

¹⁴² Brodsky, *supra* note 25, at 870.

¹⁴³ *Id.* See Villasenor, *supra* note 12, at 16 for an argument against federal preemption of state tort law.

¹⁴⁴ JAMES M. ANDERSON, ET AL., AUTONOMOUS VEHICLE TECHNOLOGY: A GUIDE FOR POLICYMAKERS 131-32 (2016) http://www.rand.org/pubs/research_reports/RR443-2.html.

¹⁴⁵ ANDERSON, *supra* note 144, at 131-32.

¹⁴⁶ Brodsky, *supra* note 25, at 872.

¹⁴⁷ *Id.*

¹⁴⁸ ANDERSON, *supra* note 144, at 131.



WEDNESDAY, MARCH 8, 2017

9:00 a.m. - 9:50 a.m.

PLENARY PROGRAM

Best Practices When Dealing with Reptiles

Magnolia Ballroom

Speakers:

Martin J. Kravtiz

Steven C. Pasarow

Robert A. Olson

Patrick E. Stockalper

Limiting Reptile Arguments, By Appeal And Otherwise

There is nothing new under the sun. Ecclesiastes 1:9. The “reptile” theory is the latest advocacy rage for the plaintiff’s bar. The appellation stems from a book (and related seminars) by David Ball (a trial consultant) and Don Keenan (a plaintiff’s lawyer) entitled *Reptile: The 2009 Manual of the Plaintiff’s Revolution* (“The Reptile”). The book’s pseudo-scientific premise is that “[w]hen the Reptile sees a survival danger, even a small one, she protects her genes by impelling the jury to protect himself and the community.” Ball & Keenan, *Reptile*, at 8. From this premise Ball & Keenan urge counsel representing plaintiffs to posture the case so as to put jurors in the position of protecting themselves, their loved ones, and their community. The premise that there is such a thing as an evolutionary “reptilian” portion of the human brain is scientifically unsupported. Ben Thomas, *Revenge of the Lizard Brain*, Guest Blog, *Scientific American* (Sept. 7, 2012), <http://blogs.scientificamerican.com/guestblog/2012/09/07/revenge-of-the-lizardbrain>.

But the theory itself is nothing new. It is a repackaging of tried and true demagoguery of appealing to the audience’s (here a jury’s) emotions, especially fear and anger. See Aristotle, *Rhetoric*, Book II, Chapter 1, <http://rhetoric.eserver.org/aristotle/rhet2-1.html> (“The Emotions are all those feelings that so change men as to affect their judgements, and that are also attended by pain or pleasure. Such are anger, pity, fear and the like, with their opposites”); A Greely, *A Brief Primer on the Reptile Theory of Trial Strategy: Plaintiff Psychology and the Defense Response*(ABA 2015 Section Annual Conference) at 1-2.

Much of what the Reptile theory advocates in presentation and argument is improper under long established legal rules. The problem is that those same rules make it exceedingly difficult to correct such inappropriate advocacy on appeal.

The Legal Landscape Limiting Improper Argument.

Demagoguery works, but for all of the wrong reasons. That’s why consistently, throughout the country, the law prohibits appeals to jurors’ passions. E.g., *Minneapolis, St. P. & S. S. M. Ry. Co. v. Moquin*, 283 U.S.

520, 521 (1931) (“In actions under the federal statute no verdict can be permitted to stand which is found to be in any degree the result of appeals to passion and prejudice. Obviously such means may be quite as effective to beget a wholly wrong verdict as to produce an excessive one”); *Soloria v. Atchison, Topeka & Santa Fe Ry. Co.* (10th Cir. 1955) 224 F2d 544, 547 (“strong appeals in the course of argument to sympathy, or appeals to passion, racial, religious, social, class, or business prejudice lie beyond the permissive range of propriety”); *Stone v. Foster*, 106 Cal. App. 3d 334, 355 (Cal. Ct. App. 1980) (“attempts to appeal to the prejudice, passions or sympathy of the jury are misconduct”).

One form of the prohibition on appeals to juror passion is barring counsel from asking the jurors to put themselves in a party’s place and to ask themselves how they individually would want to be treated or what compensation they would view as appropriate had they suffered the same injuries; this is known colloquially as an improper “Golden Rule” argument. E.g., *Granfield v. CSX Transp., Inc.*, 597 F.3d 474, 491 (1st Cir.2010) (A “Golden Rule” argument is “universally condemned because it encourages the jury to depart from neutrality and to decide the case on the basis of personal interest and bias rather than on evidence”); *Arnold v. E. Air Lines, Inc.*, 681 F.2d 186, 199 (4th Cir.1982) (“The Golden Rule and sympathy appeals are ... obviously improper arguments.... Having no legal relevance to any of the real issues, they were per se objectionable....”); *Loose v. Offshore Navigation, Inc.* (5th Cir. 1982) 670 F2d 493, 496 (a “Golden Rule” argument encourages the jury to depart from neutrality and to decide the case on the basis of personal interest and bias rather than on the evidence”); *Caudle v. District of Columbia* (DC Cir. 2013) 707 F3d 354, 359-60; *DuBois v. Grant*, 108 Nev. 478, 481, 835 P.2d 14, 16 (1992) (banned golden rule argument is the impermissible suggestion that the jurors trade places with the victim); *Boyd v. Pernicano*, 79 Nev. 356, 358, 385 P.2d 342, 343 (1963) (improper to ask the jurors to place themselves in the shoes of the victim because such argument interferes with the objectivity of the jury); *Seffert v. Los Angeles Transit Lines*, 56 Cal.2d 498, 511-12 (1961), Traynor, J. dissenting (““No rational being would change places with the injured man for an amount of gold that would fill the room of the court, yet no lawyer would contend that such is the legal measure of damages,”” emphasis added); *Horn v. Atchison, Topeka & Santa Fe Ry. Co.*, 61 Cal. 2d 602, 609 (1964) (“it was improper to appeal to the jurors to

fix damages as if they or a loved one were the injured party”); *Collins v. Union Pacific Railway Company*, 207 Cal.App.4th 867, 883-84 (2012) (“A ‘golden rule’ argument is one where counsel asks the jury to place itself in the victim’s shoes and award such damages as they would charge to undergo equivalent pain and suffering” and is prohibited as an improper appeal to passion); *Loth v. Truck-A-Way Corp.*, 60 Cal. App. 4th 757, 765 (1998) (“The appeal to a juror to exercise his subjective judgment rather than an impartial judgment predicated on the evidence cannot be condoned. It tends to denigrate the jurors’ oath to well and truly try the issue and render a true verdict according to the evidence. Moreover, it in effect asks each juror to become a personal partisan advocate for the injured party, rather than an unbiased and unprejudiced weigher of the evidence. Finally, it may tend to induce each juror to consider a higher figure than he otherwise might to avoid being considered self-abasing,” citations omitted); (Counsel “impermissibly asked the jurors to place themselves in [plaintiff’s] position when he asked them to ‘tap into feelings’ about [her] fears, in light of her physical condition, ... With respect to his “power broker” message, the fact that [counsel] did not expressly remind the jury that [plaintiff] is ‘people like you’ does not save him from a violation of the golden rule. He clearly asked the jurors to ‘allow such recovery as they would wish if in the same position.’ Moreover, [counsel’s] ‘testimony’ during his argument, that he personally would not want to trade ten million dollars for the use of his fingers, violated the golden rule. While making this argument, he asked the jurors, ‘How do you put a value on not using your fingers?’ He thus invited the jury to agree that neither would they make such a trade”).

The bar on “Golden Rule” arguments is near universal. The Reptile book itself has an appendix of cases from virtually every jurisdiction recognizing the Golden Rule, some attempting to skirt it. See The Reptile, at 267-326. Yet, ultimately, the underlying premise of The Reptile is that the jurors need to put themselves in the plaintiff’s place and to protect themselves and their loved ones from the same harm befalling them. There is some debate whether the “Golden Rule” prohibition extends to liability determinations or is limited to appeals as to damages. Compare, e.g., *Cordova v. City of Albuquerque* (10th Cir. 2016) 816 F3d 645, ___ 2016 WL 873347, *11 (although “Golden Rule” argument improper on damages issue, proper when argued on issue of ultimate liability to ask jurors to put themselves in officers’ shoes accused of unreasonable use of deadly force);

Shultz v. Rice (10th Cir. 1986) 809 F.2d 643, 652 (permitting defense argument that jurors place themselves in defendant physician's shoes with choices he faced); *Stokes v. Delcambre*, 710 F.2d 1120, 1128 (5th Cir. 1983) ("It is not improper when urged on the issue of ultimate liability"; not improper to ask jurors to put themselves into jailed plaintiff's shoes as to why he did not seek help from deputies in face of assault by other inmates); *Lopez v. Langer*, 114 Idaho 873, 879 (1988) ("Golden Rule" arguments prohibited as to damages; but "where such arguments merely appeal, in a moderate manner, to the jury's common sense by asking them to ascertain the reasonableness of a defendant's actions (or a plaintiff's actions) in the context of the case, they will be permitted," footnote omitted) *with Caudle v. D.C.*, 707 F.3d 354, 359–60 (D.C. Cir. 2013) (collecting cases going both ways; "Golden Rule" prohibition applies to both liability and damages; improper to ask jurors to put themselves in discrimination plaintiffs' shoes); *Edwards v. City of Philadelphia* (3rd Cir. 1988) 860 F.2d 568, 574, fn. 6 (same).

Despite The Reptile book's attempt to narrow its scope, the prohibition on appeals to jurors' self-interest are not limited strictly to direct or explicit appeals that jurors put themselves in a party's shoes. Thus, more generally, appeals to jurors' self-interest – the fundamental Reptile premise – are improper. E.g., *Allstate Ins. Co. v. James*, 845 F.2d 315, 318-19 (11th Cir. 1988) (defense argument that jurors policy premiums might be affected); *Roy v. Employers Mut. Cas. Co.*, 368 F.2d 902, 904-05 (5th Cir. 1966) (same); *Cassim v. Allstate Ins. Co.*, 33 Cal. 4th 780, 796 (2004) ("An attorney's appeal in closing argument to the jurors' self-interest is improper and thus is misconduct because such arguments tend to undermine the jury's impartiality"); *Brokopp v. Ford Motor Co.*, 71 Cal. App. 3d 841, 861 (Cal. Ct. App. 1977) (plaintiff's claim that defendant, rather than public healthcare [Veteran's Administration] should pay to treat plaintiff's injuries improperly appealed to self-interest).

In fact, some of the favorite Reptile attempts to avoid the "Golden Rule" prohibition fall within improper-argument precedent. Thus, counsel cannot simply say "I'm not going to ask you to put yourself in plaintiff's shoes" because doing so have just that effect. *Loose v. Offshore Navigation, Inc.*, 670 F.2d 493, 496–97 (5th Cir. 1982); *Woods v. Burlington N. R. Co.*, 768 F.2d 1287, 1292 (11th Cir. 1985), rev'd, 480 U.S.

1 (1987). Likewise, the “newspaper ad” gambit, asking the jury to think how much a newspaper advertisement (or these days eBay or the like) would have to offer for someone to agree to endure plaintiff’s injuries, is improper. ” *Collins, supra*, 207 Cal.App.4th at 883. These are simply not-to-subtle dodges of a prohibited Golden Rule argument.

So, too, the Reptile favorite that the jurors act as the “conscience of the community” and its fundamental premise that the jurors protect the community can cross the line and be improper argument. E.g., *Blue Grass Shows, Inc. v. Collins*, 614 So.2d 626, 627 quoting *Westbrook v. General Tire and Rubber Co.*, 754 F.2d 1233, 1238-39 (5th Cir.1985) (“you are conscience of community” argument improper); *Norman v. Gloria Farms, Inc.*, 668 So. 2d 1016, 1021 (Fla. Dist. Ct. App. 1996) (defense argument that verdict would put an end to local culture and hold jurors to community ridicule); and *Regalado v. Callaghan*, 3 Cal. App. 5th 582, 598-99, 207 Cal. Rptr. 3d 712, 725-26 (Ct. App. 2016) (“in our view the remarks from Regalado’s counsel telling the jury that its verdict had an impact on the community and that it was acting to keep the community safe were improper”) *United States v. Rogers*, 556 F.3d 1130, 1143 (10th Cir. 2009) (“Prosecutors are not permitted to incite the passions of a jury by suggesting they can act as the community conscience to society’s problems”); *Gilster v. Primebank*, 747 F.3d 1007, 1011 (8th Cir. 2014) (Counsel’s closing rebuttal argument “giving” to the jury “the power and responsibility for correcting injustices” akin to prosecutor’s improper plea that jury act as conscience of community); *Fyffe v. Massachusetts Bay Transp. Auth.*, 86 Mass. App. Ct. 457, 466-475, *review denied*, 470 Mass. 1105 (2014) (“conscience of community”/ “guardians of the guardians of the safety of all of the moms, all of the dads, and all of the children, and all of the grandparents that ride in these trains” so prejudicial as to not be cured by later instruction); but see *Freeman v. Blue Ridge Paper Prod., Inc.*, 229 S.W.3d 694, 712 (Tenn. Ct. App. 2007) (“‘An appeal to the jury to act as the community’s conscience is not necessarily improper argument,’” citation omitted); see also *Baldwin v. Adams*, 899 F.Supp.2d 889, 905-906 (N.D. Cal. 2012) (criminal habeas case; “A prosecutor may not urge the jurors to convict in order to protect community values, preserve civil order, or deter future law-breaking”; The vice in such an argument is that it increases the possibility that the defendant will be convicted for reasons unrelated to his own guilt. [*United States v. Sanchez*],

659 F.3d [1252], 1256 [(9th Cir. 2011)] (prosecutor committed misconduct in suggesting to jury that accepting defendant's duress defense would be tantamount to sending a memo to all drug couriers to use the duress defense and would lead to increased drug trafficking). In [*United States v. Weatherspoon*], 410 F.3d 1142 (9th Cir.2005)], the prosecutor repeatedly stated in his closing argument that finding the defendant guilty of being a felon in possession of a weapon would protect individuals in the community. 410 F.3d at 1149); *U.S. v. Reynolds*, 534 Fed.Appx. 347, 367-68 (6th Cir. 2013) The government's argument that the defendant brought Mexican drug cartels into the local community is the sort of appeal to the jury's passions or prejudices that would constitute misconduct. See Solivan, 937 F.2d at 1148 (finding that a prosecutor's request to the jury to "tell [the defendant] and all of the other drug dealers like her ... [t]hat we don't want that stuff in Northern Kentucky" constituted reversible error, especially in light of the heightened rhetoric surrounding the war on drugs). Here, although the prosecutor did not explicitly ask the jurors to send a message to other criminals with their verdict as was found impermissible in Solivan, the prosecutor did imply that the defendant represented a danger to the community and suggested that a conviction would result in the Mexican cartels leaving Knoxville. The prosecutor's statements clearly were an "attempt ... to associate the defendant with a feared and highly publicized group." *Id.* at 1154.)

Likewise, it is improper, in a nonpunitive damages case, to urge the jury to "send a message" or "to preserve the rights not just of [these] plaintiffs but of everyone." E.g., *Caudle, supra*, 707 F3d at 361 (preserve rights of everyone); *Nishihama v. City & County of San Francisco*, 93 Cal.App.4th 298, 305 (2001) ("any suggestion that the jury should 'send a message' by inflating its award of damages . . . would be improper where, as here, punitive damages may not be awarded"); *Gielow v. Strickland*, 185 Ga. App. 85, 86 (1987) (argument to punish defendant for wrongdoing).

A subtheme in Reptile presentations is often an attempt to demonize the defendant and defense counsel. This plays into the narrative that the defendant (and counsel) pose an ongoing danger to the jurors that must be stopped. Again, that is typically improper. E.g., *Cassim, supra*, 33 Cal.4th at 796 ("Nor may counsel properly make personally insulting or derogatory remarks directed at opposing counsel or impugn counsel's motives or

character”); *Las Palmas Associates v. Las Palmas Center Associates* (1991) 235 Cal.App.3d 1220, 1246 (“Personal attacks on opposing parties and their attorneys, whether outright or by insinuation, constitute misconduct. [Citation]. Such behavior only serves to inflame the passion and prejudice of the jury, distracting them from fulfilling their solemn oath to render a verdict based solely on the evidence admitted at trial”); *DeJesus, supra*, 116 Nev. at 819 (Counsel impermissibly asked jurors to “‘send a message’ to law firms that try to prevent injured persons from recovering (‘that’s what the power brokers of this world do to people like you’)”); *Kaas v. Atlas Chemical Co.*, 623 So. 2d. 525; (Fla. App. 1993) (“Other states have also held that improper comments made by counsel which accused a medical expert of perjury and accused opposing counsel of committing of fraud upon the court, caused a proceeding to be, ‘not in any meaningful sense a trial at all but a thoroughly unseemly name calling contest, reflecting a personal vendetta between a lawyer and an expert witness, in which the jury was essentially asked to choose between the combatants’”).

Finally, a related tactic is the psychological tactic of “anchoring,” that is, presenting to prospective jurors on voir dire with a large potential damages number in hopes of preconditioning them to a large result, even as a “discounted” or compromise figure. This may be prohibited, depending on the jurisdiction and the role counsel plays in juror voir dire. See Cal. Rules of Court, Standards of Judicial Administration, Standard 3.25(f).

The Need To Preserve Error And The Difficulty Of Obtaining Appellate Redress For Such Error.

The foregoing rules *should* act as a brake on much of the trial advocacy that the Reptile theorists promote. But the hard fact is that, in practice, appellate restraint is nominal. That is because of two generally applicable principles of appellate review: (1) error preservation and (2) prejudice.

Preservation. “‘Generally, to preserve for appeal an instance of misconduct of counsel in the presence of the jury, an objection must have been lodged at trial.’ In addition to objecting, a litigant faced with opposing counsel’s misconduct must also “move for a mistrial or seek a curative admonition” unless the misconduct is so persistent that an admonition would be inadequate to cure the resulting prejudice. This is so because

‘[o]ne of the primary purposes of admonition at the beginning of an improper course of argument is to avoid repetition of the remarks and thus obviate the necessity of a new trial.’ ... However, ‘the absence of a request for a curative admonition does not forfeit the issue for appeal if ‘the court immediately overrules an objection to alleged prosecutorial misconduct [and as a consequence] the defendant has no opportunity to make such a request.’” *Cassim v. Allstate Ins. Co.*, 33 Cal. 4th 780, 794–95 (2004), citations omitted; see *Horn v. Atchison, Topeka & Santa Fe Ry. Co.*, 61 Cal. 2d 602, 609–10 (1964) (The sum result of counsel’s remarks was such as to create an atmosphere of bias and prejudice which manifestly was calculated to deprive defendant of a fair trial. Certainly such conduct cannot be condoned. However we are nevertheless persuaded to the conclusion that defendant has waived its right to complain by its failure to make timely objections, and the instant judgment should not be reversed.”)

This is the general rule throughout the country, including in some of the above cited cases. E.g., *DeJesus, supra*, 116 Nev. 812, ___, 7 P.3d at 462 (“Generally, a failure to object to attorney misconduct precludes review”); *Millen v. Miller*, 224 Pa.Super. 569, 573-74, 308 A.2d 115 (1973) (“An indispensable element to finding such comment to have constituted reversible error is the requirement that opposing counsel make a prompt and specific objection on such grounds to give the trial court the opportunity to caution the jury to disregard the comments”); *Paragon Family Rest. v. Bartolini*, 799 N.E.2d 1048, 1057 (Ind. 2003) (no review of closing argument without objection); *Burns v. Prudential Sec., Inc.*, 167 Ohio App. 3d 809, 860 (2006) (“comments to the jury about the ‘close-knit community’ and the plaintiffs being the jurors’ ‘friends and neighbors,’” defense “counsel did not object to these classifications. ‘[T]he failure to object to misconduct of counsel at the time it occurs constitutes a waiver of the right to object on review of the case’”).

Nor is mere objection enough. To begin with, the objection must be timely. One recent California appellate decision, although expressly finding a “Reptile” argument –telling “the jury that its verdict had an impact on the community and that it was acting to keep the community safe were improper” – improper, held that an objection at a break in plaintiff’s counsel’s still uncompleted closing argument came too late. *Regalado, supra*, -3 Cal. App. 5th at 598-99, 207 Cal. Rptr. 3d at 725-26; but see

People v. Jasso (2012) 211 Cal.App.4th 1354, 1364 & fn. 5 (“Defense counsel’s objection, though not immediate, was timely, because it came in time for the trial court to cure any harm made by the remarks”).

And, “[i]n addition to objecting, a litigant faced with opposing counsel’s misconduct must either ‘move for a mistrial or seek a curative admonition’ [citation]” unless an admonition would have been inadequate under the circumstances. *Cassim*, at p. 795, 16 Cal.Rptr.3d 374, 94 P.3d 513; see *Smith v. Haugland*, 762 N.W.2d 890, 898, 900 (Iowa 2009) (plaintiff argued to the jury that “your decision will make a statement to this community and all the many, many patients who have this benign [medical condition] problem”; trial court sustained objection, but defense did not ask for curative instruction or timely ask for a mistrial; plaintiff reiterated statement once more; held on appeal: No abuse of discretion in not granting a new trial). Thus, where a curative admonition is given, it is often the case that counsel will have to move for a mistrial to preserve the issue for appellate review. See *Seabury-Peterson v. Jhamb*, 15 A.3d 746, 751 (Me. 2011) (trial court did not abuse discretion in giving curative instruction and denying mistrial).

Some jurisdictions may even require a new trial motion to preserve the issue for appellate review. See *Sauter v. Wasmiller*, 389 N.W.2d 200, 202 (Minn. 1986)

The preservation rules are not always absolute. Some jurisdictions permit “plain error” review even if there is no objection. *Bird v. Glacier Elec. Coop., Inc.*, 255 F.3d 1136, 1144 (9th Cir. 2001) (permitting “plain error”/due process review of closing arguments without contemporaneous objection; surveying circuits and finding that all but the Seventh Circuit allow such review); *Whitehead v. Food Max of Miss. Inc.*, 163 F.3d 265, 278 (1998) (reversing for plain error in closing arguments, including “Golden Rule” argument); contra *Kafka v. Truck Ins. Exch.*, 19 F.3d 383, 385 (7th Cir.1994) (“no plain error doctrine exists [in civil cases] to remedy errors which are alleged to have occurred during closing argument”).

Even then, the standard is incredibly high. E.g., *Lioce v. Cohen*, 124 Nev. 1, 19 (2008) (trial court may not grant a new trial for unobjected misconduct unless “no other reasonable explanation for the verdict exists’

except for the misconduct”; “[i]n the context of unobjected-to attorney misconduct, irreparable and fundamental error is error that results in a substantial impairment of justice or denial of fundamental rights such that, but for the misconduct, the verdict would have been different”); *Strickland v. Owens Corning*, 142 F.3d 353, 358–59 (6th Cir. 1998) (“we have also found that “the conduct of Plaintiffs' counsel was so outrageous as to warrant reversal of the verdict and [a] new trial,” despite opposing counsel's failure to object. Nonetheless, failure to object at trial to closing arguments does raise the degree of prejudice which must be demonstrated in order to get a new trial on appeal,” citations omitted.) see *Reese v. Mercury Marine Div. of Brunswick Corp.*, 793 F.2d 1416, 1429 (5th Cir.1986); *Mears v. Bethel Sch. Dist. No. 403*, 182 Wash. App. 919, 934 (2014), *review denied*, 182 Wash. 2d 1021 (2015) (“Where an attorney commits misconduct ‘so flagrant that no instruction could have cured the prejudicial effect,’ however, failure to timely object does not preclude appellate review”)

Prejudice. Even if the misconduct is objected to, reversals are rare. “The question is whether counsel's misconduct so permeated the trial as to lead to the conclusion the jury was necessarily influenced by passion and prejudice in reaching its verdict.” *Cooper v. Firestone Tire & Rubber Co.*, 945 F.2d 1103, 1107 (9th Cir. 1991) (although directed verdict striking punitive damages claim, counsel urged jury to inflict punishment on defendants and characterized a low verdict as a “hunting license” for defendants).

“Significantly, the test most often applied by appellate courts to these cases, holds that the use of a ‘Golden Rule’ argument is rendered harmless either by an immediate curative instruction, *see, e.g., Shultz v. Rice*, 809 F.2d 643, 652 (10th Cir.1986) (potential for prejudice adequately cured where, immediately following objection to use of ‘Golden Rule’ argument, the court ‘sufficiently admonished the jury to weigh [the offending attorney’s] argument against the whole of the evidence and the law presented them’), or by a complete final instruction to the jury concerning its proper role in the determination of liability and damages issues. *See, e.g., Joan W. v. City of Chicago*, 771 F.2d at 1023 (‘[a]lthough the judge did overrule the City's objection to the Golden Rule argument and did not give a limiting instruction, we have noted that any prejudice can often be cured simply by a general instruction that properly informs the jury

on the law of damages’); *Spray-Rite*, 684 F.2d at 1246 (harmless error where ‘the jury was properly instructed concerning the law it should apply in determining liability and damages’). *Edwards v. City of Philadelphia*, 860 F.2d 568, 574–75 (3d Cir. 1988); see *Brown v. Parker Drilling Offshore Corp.*, 410 F.3d 166, 180 (5th Cir.2005) (no prejudice where objection sustained and some admonition given).; cf. *Millen v. Miller*, 224 Pa.Super. 569, 308 A.2d 115 (1973) (only immediate admonishment would remove prejudice of Golden Rule argument; later instruction to jury insufficient). Thus, counsel faced with improper argument faces a no-win, Catch-22 situation. If counsel does not ask for an admonition or curative instruction, the error may be waived, at least in all but the most extreme cases, but if counsel does ask and the court agrees, the appellate court may find any prejudice cured.

And, even if objection and requests for an admonition and curative instructions are made, appellate courts are still reluctant to find prejudice. E.g. *U.S. v. Reynolds*, 534 Fed.Appx. 347 (6th Cir. 2013) (“But the misconduct was not flagrant. The statements were isolated. They ‘did not mislead the jury because it did not marshal them to punish all the drug dealers in their community by convicting [the defendant]; rather, the comment accurately identified [Reynolds] as [a] drug dealer[]’ who dealt with a Mexican cartel. *United States v. Wettstain*, 618 F.3d 577, 589–90 (6th Cir.2010). There is no evidence that the prosecutor intentionally sought to mislead or prejudice the jury. And, as noted above, the case against the defendant was strong. We do not find that the prosecutor’s statements ‘seriously affect[ed] the fairness, integrity, or public reputation of the judicial proceedings.’” *United States v. Henry*, 545 F.3d 367, 384 (6th Cir.2008); see *Nishihama*, *supra*, ____.

That doesn’t mean reversals never happen. But they are rare; and often involve multiple examples of misconduct or counsel disregarding specific trial court directives. E.g., *Caudle*, *supra*, 707 F.3d at ____ (repeated misconduct in face of sustained objections); *Whitehead*, *supra*, 163 F.3d at 278 (multiple misconduct, no objection); *Loose v. Offshore Navigation, Inc.*, *supra*, 670 F.2d at 496 (objection made and overruled); *Grosjean v. Imperial Palace, Inc.*, 125 Nev. 349, 369 (2009) (objected to and unobjected to misconduct including “Golden Rule” and “send a message” arguments [while counsel was crying] required new trial on

punitive damages). And, trial courts' exercise of discretion to grant a new trial are more favorably reviewed than asking the appellate court to reverse for misconduct in the first instance. E.g., *Collins, supra*, 207 Cal.App.4th at ____ (affirming trial court grant of new trial even though no contemporaneous objection during argument meant error would have been waived if trial court had denied new trial motion); *Baptist Mem'l Hosp., Inc. v. Bell*, 384 So. 2d 145, 146 (Fla. 1980) (affirming trial court grant of new trial based on "Golden Rule" argument where objection sustained and curative instruction given and subsequent arguably excessive damages); see *Lance, Inc. v. Ramanauskas*, 731 So. 2d 1204, 1216 (Ala. 1999) (remittitur, rather than new trial, can be proper remedy for improper argument).

What To Do.

Motions in Limine. Given the limited prospects for appellate recourse, the best defensive position to take on reptilian arguments is in the trial court. One place to start is with motions in limine. Such motions have the advantage, even if not fully successful, of educating the trial court as to likely tactics and their impropriety. To date, such motions appear to have met with limited success. *Jackson v. Asplundh Construction Corp.* 2016 WL 5941937 (E.D. Mo. 10/13/2016) (reptile motion in limine "held in abeyance": "The Court will not issue a ruling on this motion at this time. The Court will address any objections as the evidence is introduced"); *Turner v. Salem*, No. 3:14-CV-289-DCK, 2016 WL 4083225, at *2–3 (W.D.N.C. July 29, 2016) (Defendants move to prohibit Golden Rule argument and Reptile Theory questions and argument, arguing with respect to Reptile Theory that the arguments are meant to use a general sense of promoting safety to evoke an emotional response in the jury. Plaintiff agrees to the motion with respect to Golden Rule arguments, but objects with respect to Reptile Theory arguments on the grounds that safety and negligence are too interconnected, and Reptile Theory is not adequately defined. Defendants' motion is GRANTED in part and DEFERRED in part. The Court will not allow Golden Rule arguments. The Court also discourages Reptile Theory arguments, but will handle objections to statements purported to be Reptile Theory arguments as the need arises"); *Colman v. Home Depot*, 2016 WL 4543119 (S.D. Fla. 2/9/2016) (describing Reptile theory; granting "golden Rule" motion, but denying

reptile motion in limine: “the jury will be asked to determine whether Defendant failed to use reasonable care, which is the ‘degree of care that a reasonably careful person would use under like circumstances.’ Arguments about community safety standards and the extent that Defendant failed to comply with such standards may be relevant to this inquiry”); *Pracht v. Saga Freight Logistics, LLC*, No. 3:13-CV-529-RJC-DCK, 2015 WL 6622877, at *1 (W.D.N.C. Oct. 30, 2015) (granting “defendants’ motion to prohibit any Golden Rule argument and/or Reptile Theory questions and argument”); *Hensley v. Methodist Healthcare Hosps.*, No. 13-2436-STA-CGC, 2015 WL 5076982, at *4–5 (W.D. Tenn. Aug. 27, 2015) (denying motion, apparently without prejudice: “Defendants seek an order prohibiting Plaintiffs from offering testimony concerning violations of guidelines or safety rules or any other “scare tactics” in order to establish the standard of care. Defendants reference the “Reptile Theory,” which appears to be in use by the plaintiffs’ bar in some states as a way of showing the jury that the defendant’s conduct represents a danger to the survival of the jurors and their families. The Reptile Theory encourages plaintiffs to appeal to the passion, prejudice, and sentiment of the jury. [¶] Defendants have again not identified the specific evidence that is sought to be excluded. The Court will be cognizant of appeals to the jurors’ prejudice, and any attempt by either party to appeal to the prejudice or sympathy of the jury will not be condoned”).

Trial Briefs and Pocket Briefs. Motions in limine can be supplemented and expanded upon by a comprehensive trial brief that addresses, reptile issues. In addition, pocket briefs during trial at critical junctures, e.g., before expert testimony, before closing argument, can remind the trial court of the appropriate standards for conducting examination and for argument. In addition to reminding the trial court of applicable standards, such briefs provide a written record that objection to improper argument was made and provide a foundation for succinct objections during closing argument, e.g., “Objection, for the reason in yesterday’s brief.”

New trial motions. And, if there is an adverse result, there is the option (in some jurisdictions the requirement) of a new trial motion. See *Collins, supra*, 207 Cal.App.4th 867, 883-84 (affirming order granting new trial; in California trial court has broad discretion to grant new trial for

misconduct, even without a timely objection); *see Wahlstrom v. LAZ Parking Limited, LLC* 2016 WL 3919503 (Mass. Super. Ct. 5/19/2016) (describing Reptile book and “philosophy” but granting new trial by “focusing on particular actions of Plaintiff’s counsel without considering whether they were products of that philosophy”; counsel’s repeated violation of court orders meant to preclude inflammatory matters other than Reptile tactics required a new trial).

* * *

There is a theory that any new legal approach or argument takes a half dozen years or so to become generally known in the legal community. That theory seems to ring true with the Reptile approach. The addendum to that theory is that it takes as long again for the same argument to wend its way into judicial consciousness and into published judicial decisions. Key to defending against Reptile tactics is educating the bench, trial and appellate, on the true nature of Reptile arguments and unmasking those tactics for what they really are – a reprise of long-barred gambits.

Sources:

J. Crawford & B. Johnson, Outsmarting the Lizard, 57 No. 12 DRI for the Defense 70 (2015);

B. Kanasky, Debunking and Redefining the Plaintiff Reptile Theory, _____ DRI for the Defense 14 (2014);

Allen, Schwartz, and Wyzga’s “Atticus Finch Would Not Approve: Why a Courtroom Full of Reptiles is a Bad Idea” (2010)

<http://www.thejuryexpert.com/2010/05/atticus-finch-would-not-approve-why-a-courtroom-full-of-reptiles-is-a-bad-idea>;

A Greely, A Brief Primer on the Reptile Theory of Trial Strategy: Plaintiff Psychology and the Defense Response (ABA 2015 Section Annual Conference)

http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/2015-sac/written_materials/4_1_reptile_theory_of_trial_strategy.authcheckdam.pdf

B. Boggs, Combating Reptile Tactics in Litigation,
<http://www.namwolf.org/page/ReptileTactics/Combating-Reptile-Tactics-in-Litigation.htm>

J. Eckenrode & W. Kanasky, Defense Strategies to Confront the Reptile, DRI for the Defense course materials (2105)
http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjU0tucpZrQAhVQ9GMKHVuRDgEQFggdMAA&url=http%3A%2F%2Fwww.dri.org%2FDRI%2Fcourse-materials%2F2015-Medical%2Fpdfs%2F10_Eckenrode.pdf&usg=AFQjCNF3j5zQ_teP6zoSjRTMvJcQn8VwAA;

B. Howard, A Field Guide to Southern California Snakes: Identifying and Catching Plaintiffs' Reptile Theory In The Wild, Vol. 3 2013 Verdict 11 (Assn. of Southern California Defense Counsel 2013)

Marshall, D., "Lizards and Snakes in the Courtroom: What every Defense Attorney needs to know about the Emerging Plaintiff's Reptile Strategy," *For the Defense*, February, 2013.

UNITED STATES DISTRICT COURT FOR THE
SOUTHERN DISTRICT OF FLORIDA
MIAMI DIVISION

CASE NO.: 1:15-CV-21555-UU

CARLOS COLMAN, SR.,

Plaintiff,

v.

HOME DEPOT, U.S.A., INC.,

Defendant.

**DEFENDANT, HOME DEPOT, U.S.A., INC.’S MOTION IN LIMINE TO PREVENT
“GOLDEN RULE” ARGUMENTS AND “REPTILE STRATEGY”**

Defendant, HOME DEPOT U.S.A. INC. (hereinafter, “Defendant”), by and through the undersigned counsel, pursuant to the Federal Rules of Civil Procedure and Chapter 90 of the Florida Statutes, hereby moves this Honorable Court to enter an Order preventing the Plaintiff’s counsel from making “Golden Rule” arguments or employing “Reptile Strategy” and, as grounds therefor, states as follows:

INTRODUCTION

The Defendant anticipates that the Plaintiff’s counsel will, in *voir dire* and then throughout the course of the trial, attempt to argue to the prospective jurors and jury that they have the power to improve their own safety, as well as the safety of their family members and their community by rendering a verdict that will reduce or eliminate a dangerous conduct, such as that alleged against the Defendant in this matter. This trial tactic is being taught in plaintiff’s trial advocacy courses and is based on a book by authors David Ball and Don Keenan (hereinafter, “Reptile Strategy”). David Ball and Don Keenan, Reptile: The 2009 Manual of the

Plaintiff's Revolution (1st ed. 2009).

The psychological premise of the Reptile Strategy is that jurors, like all humankind, have brains consisting of various parts, one of which the authors refer to as the "Reptilian Complex." Id. The "Reptilian Complex," also known as the reptilian brain, includes the brain stem and the cerebellum, which control our basic life functions, such as breathing, hunger, and survival. Id. According to the authors, the reptilian brain instinctively overpowers the cognitive and emotional parts of the brain when those life functions become threatened. Id. at 17. The authors posit that "[w]hen the Reptile sees a survival danger, even a small one, she protects her genes by impelling the juror to protect himself and the community." Id. at 17, 19 and 73. They suggest that reducing danger in the community facilitates survival, which awakens the reptilian part of the brain in each juror and overcomes his or her logic or emotion. Id. at 45.

The authors further encourage plaintiff's lawyers to appeal to a juror's own sense of self-protection in order to persuade and prevail. According to Mr. Ball and Mr. Keenan, appealing to a juror's self-protective interests will reverberate and convince better than any other argument. Because the most powerful thinking occurs when one is protecting one's life, a lawyer can communicate most effectively by converting every issue into one of self-protection or its cousin—"community safety." By linking each argument in some way to a juror's sense of personal or community safety, the Reptile Strategy gives jurors a compelling, subliminal reason to rule in favor of a plaintiff over a defendant, despite what their logic and the evidence might tell them.

Mr. Ball and Mr. Keenan also instruct plaintiff's lawyers to "use the powerful Reptilian imperative to use devastating events as a springboard from which to create safety." Id. The authors further instruct that "[e]very injury presents a hope for a safer future. Position the jurors

as the cultivators of that hope." Id.

Accordingly, any mention, comment, reference, testimony or argument regarding "personal safety" or "community safety" should be precluded because they are akin to Golden Rule arguments which are expressly prohibited under Florida law. "Personal safety" and "community safety" arguments should also be precluded because they violate Florida's Standard Jury Instructions and undermine the Defendant's Due Process right to an impartial jury and fair trial. Finally, "personal safety" and "community safety" evidence should be precluded pursuant to Florida Statutes § 90.401 and § 90.403 because it is irrelevant and its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues and misleading the jury.

Examples of Reptile Strategy During *Voir Dire*

The following questions are examples of the types of questions that could be asked during *voir dire* that would fall within the gambit of Reptile Strategy:

- Q: Aside and apart from money for damages, **how do you feel verdicts might affect community safety** or things like that?
- Q: Do you feel you are a person that could be asked to decide some rules about **community safety** and to make those decisions?

These are just a couple of the types of questions that should not be asked of the prospective jurors during *voir dire*.

Examples of Reptile Strategy During Closing Argument

The following statements are examples of the types of arguments that could be made during closing that would fall within the gambit of Reptile Strategy:

- S: You chose to be here, and so **now you are here to decide what rules we are going to condone in this community**

for safety and what rules we're going to apply to the circumstances of this case.

- S: A jury is an incredibly powerful thing. I believe it is the most powerful group a person can belong to. For that reason, most countries do not have them. **Juries protect the community and set the safety standards.**
- S: The defendant's lack of understanding and caring about **community safety standards** caused harm to the plaintiff. The plaintiff never got to make those decisions. The decision is up to you.
- S: The defendant's conduct continues to threaten **everybody**. This type of conduct is a powder keg, okay. We have heard from every expert that talked about the standard of care. **This is a community problem, a state problem, and a national problem.**
- S: Now, your verdict is about the amount of money it will take to help and make up for the losses and the harms caused by the defendant. That is the first part of the verdict. **The second part is about deterring future negligence, protecting other people that are similarly situated.** That too, is part of your job.
- S: **Money communicates the message of what you and this community will tolerate or will not for safety.**

Again, these are just a few examples of the types of arguments that should not be made to the jury during closing argument.

STANDARD OF REVIEW

Under Florida law, it is axiomatic that the purpose and efficacy of a motion in *limine* is “to prevent the introduction of improper evidence, the mere mention of which at trial would be prejudicial.” See Dailey v. Multicon Development, Inc., 417 So. 2d 1106 (Fla. 4th DCA 1982) citing Adkins v. Seaboard Coast Line Railroad Company, 351 So. 2d 1088 (Fla. 2d DCA 1977). The Florida Statutes define “relevant” evidence as “evidence tending to prove or disprove a material fact.” Fla. Stat. § 90.401 (2005). Moreover, under Florida law, even relevant evidence

is “inadmissible if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of issues, misleading the jury, or needless presentation of cumulative evidence.” Fla. Stat. § 90.403.

SUMMARY OF THE ARGUMENTS

Having already established the underpinnings of the Reptile Strategy and its potential subliminal impact upon the minds of the prospective jurors and jury, the Plaintiff’s counsel should be precluded from asking questions or making arguments based upon the premises of “personal safety” and/or “community safety” for at least four (4) reasons. First, such arguments are tantamount to “Golden Rule” arguments, which are not permitted under Florida law. Second, such arguments violate Florida’s Model Jury Instructions. Third, such arguments would undermine the Defendant’s rights to due process and a fair trial. Fourth, arguments of “personal safety” and “community safety” are irrelevant and, to the extent they are relevant, should nonetheless be excluded because their relevancy is substantially outweighed by the danger of unfair prejudice, confusion of the issues and misleading the jury.

ARGUMENT AND CITATIONS OF AUTHORITY

I. Golden Rule Arguments Are Not Permitted Under Florida Law

A “Golden Rule” argument urges the jury to place themselves in a party’s position to allow recovery as they would want were they the party. Under Florida law, an impermissible argument strikes at that sensitive area of financial responsibility and hypothetically requests the jury to consider how much they would wish to receive in a similar situation. Stewart v. Cook, 218 So. 2d 491 (Fla. 4th DCA 1969); Seaboard Coastline Railroad Co. v. Addison, 481 So. 2d 3 (Fla. 1st DCA 1985), disapproved on other grounds, 502 So.2d 1241 (Fla.1987). Such an argument is improper because it encourages the jury to depart from neutrality and to decide the

case on the basis of personal interest and bias, rather than on the evidence. Schreidell v. Shoter, 500 So. 2d 228 (Fla. 3d DCA 1986). See also Bullock v. Branch, 130 So. 2d 74 (Fla. 1st DCA 1961).

As the court in Schreidell emphasized, the impropriety of a “Golden Rule” argument derives from the fact that it invites a juror to decide a case on the basis of personal interest and bias, rather than on the evidence. 500 So. 2d at 233. That is precisely the type of interest and bias that the Reptile Strategy invites. As its authors suggest, “[e]very injury presents a hope for a safer future. Position the jurors as the cultivators of that hope.” If the Plaintiff’s counsel employs Reptile Strategy, a juror could be persuaded to rely upon the juror’s own sense of self-protection.

In this sense, the Reptile Strategy is nothing more than a veiled Golden Rule argument because it seeks to have jurors decide a case not on the evidence presented at trial, but rather on the potential harms and losses that could have occurred within the “community,” which includes each juror and his or her family members.

Indeed, as evidenced by the following quotations taken from the Reptile Strategy book, the trial strategy is to directly or indirectly invoke the underpinnings of the Golden Rule by asking each juror to put themselves in the same position as a plaintiff—a position of jeopardy that calls upon survival instincts:

When the Reptile sees a survival danger, even a small one, she protects her genes by impelling the juror to protect himself and the community.

...

It gives jurors personal reason to want to see causation and dollar amount come out justly, because a defense verdict will further imperil him. Only a verdict [for the plaintiff] can make them safer.

...

The juror’s decision rests on the Reptilian question of which verdict will make her safer.

...

Just remember that the Reptile does not get involved unless she

sees that the danger is to her, and can be meliorated.

...

The Reptile ignores tragedy because she can't do anything about it. Instead, the trial...is an opportunity for jurors to use the horror of [the plaintiff's case] as a way to make their offspring safer.

...

So as with all things Reptilian, you show that the **safer decision for the community** (and thus the individual juror) is a fair verdict for your client.

...

No Reptile can protect herself alone. She protects herself by protecting the community. The concept of "No man is an island" shows the Reptile that what's good for the community connects directly to her, individually—and is good for her.

...

But the Reptile is not particularly concerned with your client. Our research revealed a different picture: the Reptile is concerned with *the Reptile*—meaning the individual juror—his world and family, their survival, and little else.

...

A case framed in terms of **community endangerment** is Reptilian. A hospital-acquired infection case turns Reptilian when jurors see that the victim could have been anyone who walked through the doors. "Anyone" means the community. "Community" includes Juror #3 and her children.

...

Jurors will do what they can to keep their communities (i.e. themselves) safe when they think their efforts will work.

David Ball and Don Keenan, Reptile: The 2009 Manual of the Plaintiff's Revolution (1st ed. 2009) at 17, 18, 39, 72, 73, 86, 99, 149, 170. (Emphasis added.)

Although the Plaintiff's counsel may not specifically ask jurors to put themselves in the shoes of the Plaintiff, presenting arguments regarding "personal safety" or "community safety" has the same intent and mischief—that is to have jurors base their deliberations and verdict not on the evidence of the case, but rather on the fear that they or other members of their family or community could be injured and to have them view compensating the Plaintiff as a means of diminishing that danger to themselves and the community of which they are a part.

“Golden Rule” arguments are impermissible in Florida. Where, as here, arguments regarding "personal safety" or "community safety" are veiled Golden Rule arguments, they too should be prohibited.

II. Reptile Strategies Violate Florida’s Standard Jury Instructions

During the trial of this matter, this Honorable Court will read certain instructions to the jury from the Florida Supreme Court’s Standard Jury Instructions. The most important of these instructions comes from Section 700, which reads:

In reaching your verdict, **do not let bias, sympathy, prejudice, public opinion, or any other sentiment** for or against any party to influence your decision. Your verdict must be based on the evidence that has been received and the law on which I have instructed you.

Florida Standard Jury Instructions – Civil Cases 700.

To be clear, the jury’s verdict must be based upon the evidence. In order to prevail on a negligence claim, the Plaintiff has to introduce evidence to prove the four elements: duty of care, breach of that duty, causation and damages. Gibbs v. Hernandez, 810 So. 2d 1034, 1036 (Fla. 4th DCA 2002). "Personal safety" and "community safety" are irrelevant to the legal issues raised in this negligence claim. Where, as here, no such evidence will be presented, the Plaintiff’s counsel should be precluded from making any arguments or presenting evidence concerning "personal safety" or "community safety."

Moreover, as the above-referenced Jury Instruction makes clear, a juror may not base his or her verdict on bias, sympathy, prejudice, public opinion, or any other sentiment. Those instructions were written to help ensure that every litigant receives the fair and impartial trial promised to them by the Constitution. Yet arguments of "personal safety" and "community safety" are premised on eliciting fear or passion in jurors of future harm if a verdict is not entered

in favor of the Plaintiff. Such arguments are a blatant appeal to the jury to abandon its duty to render an impartial verdict predicated on the evidence and the law of the case, and instead, to be influenced by fear or passion.

Furthermore, jurors are instructed not to be governed by public opinion. Yet, arguments of "personal safety" and "community safety" invite the jurors to base their verdict on public policy considerations. Any such strategy should not be countenanced by this Honorable Court.

III. Reptile Strategies Violate The Defendant's Right to Due Process And A Fair Trial

Under the due process clause of the Constitution of the United States and of the State of Florida, each and every person is guaranteed a fair and impartial trial. Castellano v. Travelers Ins. Co., 305 So. 2d 268 (Fla. 2d DCA 1974). This holds equally true for civil cases. Id. After all,

The ultimate goal of our court system to attain truth and justice demands unrelenting vigilance and dedication on the part of both bench and bar to keep every improper influence out of all legal proceedings.

City of Niceville v. Hardy, 160 So. 2d 535, 538 (Fla. 1st DCA 1964).

Reptile Strategy threatens the impartiality of the jury. As such, it undermines the Constitutional guarantees of the Defendant's right to a fair and impartial trial.

What is more, the Defendant's liability, if any, would be limited to liability for the damages that the Plaintiff can prove based upon competent and substantial evidence. Jenkins v. Plaza 3000, Inc., 2014 WL 537494 (Fla. 4th DCA 2014). "Competent, substantial evidence" is "such evidence as will establish a substantial basis of fact from which the fact at issue can be reasonably inferred" or such evidence as is "sufficiently relevant and material that a reasonable mind would accept it as adequate to support the conclusion reached." Heifetz v. Dep't of Bus.

Regulation, 475 So. 2d 1277, 1281 (Fla. 1st DCA 1985) (quoting De Groot v. Sheffield, 95 So.2d 912, 916 (Fla.1957)).

By contrast, the Defendant cannot be held liable for hypothetical damages to “the community.” Inviting the jury to consider how the Defendant’s alleged conduct violated “personal safety” or “community safety” would be tantamount to asking the jury to award damages for hypothetical wrongs done to others who are not even party to these proceedings. This too would violate the Defendant’s right to due process.

IV.Arguments Based On “Personal Safety” And/Or “Community Safety” Are Irrelevant

V.

Florida law defines “relevant” evidence as “evidence tending to prove or disprove a material fact.” Fla. Stat. § 90.401 (2005). Arguments concerning “personal safety” and/or “community safety” are not material to the Plaintiff’s claims; however, even if such an issue is relevant, under Florida law, it is “inadmissible if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of issues, misleading the jury, or needless presentation of cumulative evidence.” Fla. Stat. § 90.403.

For all of the reasons stated above, the obvious goal of Reptile Strategy is to create unfair prejudice, confuse the issues and mislead the jurors into believing that their verdict will protect themselves, their families and their communities from the threat of harm posed by the Defendant. Most respectfully, these types of tactics should not be permitted.

CONCLUSION

The goal of the Reptile Strategy is to have a subliminal impact upon the minds of the prospective jurors and jury that would create an inherent bias against the Defendant. Such arguments are tantamount to “Golden Rule” arguments, which are not permitted under Florida law. They also violate Florida’s Standard Jury Instructions and undermine the Defendant’s

rights to due process and a fair trial. Moreover, arguments of “personal safety” and “community safety” are irrelevant and, to the extent they are relevant, should nonetheless be excluded because of the danger of unfair prejudice, confusion of the issues and misleading the jury.

WHEREFORE the Defendant respectfully moves this Honorable Court to enter an Order granting this Motion in Limine and preventing the Plaintiff’s counsel from making “Golden Rule” arguments or employing “Reptile Strategy,” as well as any other relief deemed just and appropriate in light of the foregoing.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that I filed the foregoing document with the Clerk of the Court electronically on January 8, 2016, I also certify that the foregoing document is being served this day on all counsel of record identified on the attached Service List in the manner specified, either via transmission of Notices of Electronic Filing generated by CM/ECF or in some other authorized manner for those counsel who are not authorized to receive electronic Notices of Electronic Filing.

/s/ YAMILE TAMARGO
Yamile Tamargo

SERVICE LIST

WE HEREBY CERTIFY that we electronically filed the foregoing document with the Clerk of the Court using CM/ECF.

Plaintiff's Attorney:
Gregory A. Deutch, Esq.
Rubenstein Law, P.A.
9155 South Dadeland Blvd., Suite 1600
Miami, FL 33156
Tel: (305) 661-6000
Fax: (786) 230-2936
eservice@rubensteinlaw.com
gregory@rubensteinlaw.com
ssalvatierra@rubensteinlaw.com



Lighting the way to...

Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10



WEDNESDAY, MARCH 8, 2017

9:50 a.m. - 10:40 a.m.

PLENARY PROGRAM

What is your Tech Strategy?

Magnolia Ballroom

Speakers:

John J. Delany, III
Thomas G. Oakes
Robert L. Christie

USE OF TECHNOLOGY IN DEPOSITIONS

By: **Thomas G. Oakes**

THOMAS G. OAKES ASSOCIATES, LLC

With Special Thanks to: Francis J. Deasey, Esquire; Deasey, Mahoney & Valentini

INTRODUCTION

It goes without saying that the technological advantages of the last decade have changed the legal landscape dramatically. Applications of video technology have important implications for the future of the litigation process. Video depositions, almost universally permitted under Federal and State Rules of Civil Procedure, facilitate the transfer of information from pretrial events to the trial event. Traditionally, videotaped depositions were utilized for the depositions of testifying experts, particularly medical doctors. Today, most sophisticated plaintiff firms videotape every deposition. From the defense perspective this can create additional problems in preparing witnesses for depositions. Conversely, the savvy defense practitioner should make full use of the technology available to conduct video depositions.

In their formative years, most defense practitioners are taught that depositions are discovery tools designed to elicit facts. This way of thinking is obsolete. One of the major reasons most sophisticated plaintiff attorneys videotape depositions is to “Create a sound bite.” And, if permitted, this “sound bite” will be shown to a jury up to four times including:

- (a) During plaintiff counsel’s opening;
- (b) During plaintiff’s case-in-chief;
- (c) During cross-examination of the same witness (if called by the defense); and
- (d) During plaintiff counsel’s closing.

Every defense practitioner must understand how modern videotaped depositions work to prepare their witnesses for this experience. A video deposition brings to the forefront the concept of nonverbal communication, including concepts such as channeling, decoding,

encoding and rapport. All of these concepts impact how jurors will evaluate a witness' video deposition testimony,

However, it is important to remember that video deposition testimony is equally available to the defense and can be a tremendous weapon in defense counsel's arsenal when utilized effectively and professionally. This paper will explore the genesis of videotaped depositions up through and including interactive depositions, also known as smart depositions and will provide the defense practitioner with the tools to prepare their witnesses for video depositions and, at the same time, utilize videotaped depositions as part of their presentation.

GENESIS OF VIDEOTAPED DEPOSITIONS

In the early years of videotaping, the equipment was very antiquated. Cameras used VHS tapes only. Cameras were at least three times as large as today's cameras, bulky, heavy and the quality was not great. In fact, the lighting levels provided by the camera were so low, that additional lighting needed to be added. At times it resembled a mini movie set. Today, almost all videotaping is done digitally with digital cameras utilizing SD cards or directly to hard drives, and exporting the video to the format of counsel's choice, either Mpeg 1, 2 or 4.

In the early years, when the deposition was presented at trial and played to the jury, the videotaped deposition would not be edited, but any part of the deposition which was not to be shown to the jury would then be fast forwarded to the next part of the video to be played. The videographer would sit with a copy of the transcript with the portions not to be played X'd out. He/she would have a set of headphones on to listen and fast forward the VHS tape to the appropriate sections to be used.

While the process by which counsel and the court review objections or deposition designations has not changed, the ability to provide a more seamless edited file has made great strides in today's market. Years ago, the equipment used in the courtroom to play back the video was normally an old style television – not a flat panel – with a screen no more than 32 inches and the only audio came through the television. So that the audio could be heard better, one of the courtroom microphones would be placed close to the television audio output so it could be heard through the courtroom sound system. If we moved ahead a decade or two, we would find that

computers were fast enough, portable enough and software was developed for use in editing video. As a result, there was the advent of trial presentation software, such as Sanction and TrialDirector, which brought videotaped depositions to a new level. With this technology you could synchronize the audio, video and text file. The greatest part about having a video synched deposition is the ability to create clips or bites of the transcript. Delivery of videotaped depositions are now being made on CD, DVD, thumb drives and/or links. The video synched file that is received is a DVT file (digital video transcript). This portable DVT file allows the user to create their own clips of the deposition directly from the DVT and save the clips as either a PowerPoint file, MP4 file (iPad) or TrialDirector file to be imported into the full Trial Director Presentation software package.

SMART DEPOSITIONS – THE EARLY YEARS

First use of the smart deposition took place using an Elmo, which is a document camera. In the videotaped deposition, counsel would project onto a large screen a document to show the witness. Counsel would do the markings and/or have the witness make markings on a document or photo and capture this on videotape to be used later at trial. There are a number of issues using this type of technology. First, you needed to have multiple copies of the same document or photo for the witness or counsel to put markings on. Counsel would need to request the court reporter to put a sticker on each one of the files as they were made. You could not capture a digital copy of the document. You could only capture it on the video. The actual deposition was not being recorded to a hard drive and a video simultaneously. The video was the only recording. This could result in a very herky-jerky replay, since the video camera had to move its

focus from the witness to the document or the document camera and to the projection screen. However, this was a start and like any new technology, the bugs had to be worked out.

SMART INTERACTIVE OR SUPER DEPOSITIONS

If you intend to take a videotaped deposition of a witness using Smart, Interactive or Super Depositions, be sure that you take the time to either have your deposition exhibits pre-marked or numbered in such a way that the presenter (trial presenter) is able to offer up on the screen to the witness the document, x-ray or photo that you would like. A simple index of the documents with deposition exhibit numbers would work great. Also, even though the witness may using tools on the smart board or a monitor to do mark-ups on the exhibits, you will want to not only have this information recorded, but you will want to take screen shots of these documents for later use.

Screen shots can be used as a separate exhibit at trial. If you capture the document with its present markings, ask the presenter to capture the file for you. When asking that the file be captured, tell the presenter the number you want to give to the new exhibit. For example, if you offer the witness a photograph, which was pre-marked hypothetically Deposition Exhibit 3, the witness puts an X on the digital document denoting a location, etc., you would then tell the presenter to capture the new file, perhaps as Deposition Exhibit 3A. By capturing and numbering the exhibit at that time, you can then have that exhibit brought back at any time by just asking for 3A. You could also use this new exhibit with any other witness or in a PowerPoint presentation, etc. The file is captured as a PDF file.

A Smart/Interactive deposition provides you the ability to have a witness seen at trial exactly how the jury would see him/her on the witness stand, but you get the added benefit of being able to make clips of certain portions of the videotaped deposition to be used over and over again. You will also have the opportunity to have the witness pinpoint for you exactly what they are describing in words into a document, photograph, x-ray, etc. Thus, you create a picture which is “worth a thousand words.” Attached as Appendix A is information concerning terminology which will be helpful in understanding the intricacies of Smart depositions.

THE RULES

Federal Rule of Civil Procedure 30, provides impertinent part, as follows:

(3) Method of Recording.

(a) Method stated in the notice. The party who notices the deposition must state in the notice the method of recording the testimony. Unless the court orders otherwise, testimony may be recorded by audio, audio visual, or stenographic means. The noticing party bears the recording costs. Any party may arrange to transcribe a deposition.

(b) Additional Method. With prior notice to the deponent and other parties, any party may designate another method of recording the testimony and in addition to that specified in the original notice. That party bears the expense of the additional record or transcript unless the court orders otherwise.

(4) By Remote Means. The parties may stipulate – or the court may on motion order – that a deposition be taken by telephone or other remote means. For the purpose of this Rule and Rules 28(a), 37(a)(2) and 37(b)(1), the deposition takes place when the deponent answers the questions.

Many states have adopted verbatim or, in large measure, the Federal Rules of Civil Procedure including Rule 30. Before allowing your witness to be videotaped or noticing a

videotaped deposition, it is important to know the state's rules concerning videotaped depositions and, most importantly, restrictions on the use of videotaped depositions at trial.

NONVERBAL COMMUNICATION IN THE VIDEOTAPED DEPOSITION

Nonverbal communication is behavioral communication through facial expression, bodily movements and gestures, as well as vocal tone, hesitations, and pitch. Such communication is often subtle, uncontrollable and spontaneous. These cues are generally interpreted universally and cross-culturally. Thus, the advantage of allowing a jury to audio-visually perceive a witness' testimony through video tape means the jurors will be able to interpret nonverbal cues that they otherwise could not by simply hearing the testimony being read through a transcript. Another advantage is that the videotape is the most accurate way to relay the testimony, which alleviates concerns about objections that could be made regarding accuracy, inflection, tone, etc...when testimony simply is read from a transcript.

Of course, nonverbal communication can be controlled to achieve a purpose such as deception or impression management. This is a skill that some are better at than others. Actions such as nerves and anxiety can affect our ability to manage nonverbal communication. For example, a witness may attempt to project confidence, but the jury still might be able to sense nervousness from nonverbal cues, which may impact an assessment of the witness' credibility. Conversely, positive communication may establish mutual liking, empathy, rapport and most importantly, trust. A smile, direct gaze, forward lean, and warm vocal tone all convey interest and liking, when all are taken together. However, if you remove the smile or warm tone from that equation, the meaning could become entirely different. Nonverbal communication is imparted through a combination of these types of factors.

BASIC CHANNELS OF NONVERBAL COMMUNICATION

(a) Face

The face is the channel that is most easily controlled, and may be the most expressive channel of communication, particularly for emotions. Emotional expression occurs through movements of the mouth, eyebrows, cheek and eyes. Fear, surprise, anger, disgust, sadness and happiness are all conveyed in this matter, and have been observed universally in a variety of cultures. The direction and duration of a gaze is particularly important. We tend to associate direct eye contact with trustworthiness. Smiling and head nodding tend to be universal signs of empathy.

(b) Body

Bodily expression is less controllable than facial expression. Body orientation, positioning and postures are also key to emotional expression. Bodily expressions are also indicative of self-monitoring. High self-monitoring of one's behavior in relation to others and constant awareness of the social appropriateness of one's actions will likely be expressed through such cues. This is called postural mirroring and has been found to create empathy. Changes in posture can be indicative of aggression vs. passivity, as well as signs of emotions and/or mental conditions such as anxiety or depression. We tend to associate an erect posture with confidence and personal appearance.

(c) Gestures

Bodily expressions such as hand/arm gestures can have direct verbal meaning that replaces speech. The simplest example is a witness pointing to an object for

identification. Such movements can also be culture-specific, such as giving a “thumbs” up sign. The interpretation of these gestures can vary widely across cultures and serious misunderstandings can arise. Some gestures, such as crossing one’s arms, are universal signs of guardedness vs. openness. Hand wringing may be a sign of nervousness or anxiety.

(d) Voice

Voice is the least controllable channel of communication. Beyond the actual words spoken, a speaker’s voice, tone and inflection can mean expressions of emotion, mood, confidence and honesty. A harsh and loud vocal inflection such as a “command” voice will relay aggression, dominance and control. This is generally not the best way to establish empathy. A direct, warm and relaxed tone denotes confidence, genuineness and honesty.

IMPORTANCE OF NONVERBAL COMMUNICATION IN THE VIDEOTAPED
DEPOSITION

Studies have shown that jurors pick up nonverbal signs and cues unconsciously transmitted by the speaker. Up to 55% of the meaning of a speaker’s message is nonverbal. Nonverbal skill is the term used to describe individuals’ abilities to use nonverbal communication effectively and accurately. Nonverbal skills tend to be associated with enduring characteristics of people such as gender, personality and culture. Generally, nonverbal skills are conceptualized in terms of two separate sub skills: Encoding skills and decoding skills.

Encoding skills refer to the ability to communicate emotions, attitudes or other messages through nonverbal cues so that the observer (in this case the jury) can interpret the meaning of the message as the encoder intended. Thus, skilled encoders (the witness) tend to be judged as more empathic when they are being empathic and judged so purely from nonverbal channel such as the face or the voice. More-skilled encoders tend to be more popular, dominant and extraverted than less-skilled encoders.

Decoding skills refer to individuals' ability to interpret the nonverbal communication of other people. While the decoding skills of people vary all jurors will have decoding skills which will enable them, more or less, to interpret the nonverbal communications of witnesses. In general, women are more accurate encoders as well as decoders of nonverbal communication than men.

CREDIBILITY

Credibility is established in large part by the witness' confidence and rapport he/she is able to establish with his/her audience. Mutual involvement and interpretation of situations is key to establishing rapport. Witnesses who smile, nod their heads, lean forward, gaze directly at their subject, maintain direct body orientation, have an open as opposed to guarded posture, make few hand gestures, and speak with a warm and relaxed tone will most likely be able to establish a rapport with his/her audience and thus come across as more credible. Tone of voice, which is the most difficult channel to control, is important to establishing confidence. For example, a positive verbal message in a negative tone of voice may arouse suspicion, because we

generally expect a positive verbal message to be relayed in a positive tone. To the contrary, a negative verbal message in a positive tone of voice may communicate concern and acceptance.

DECEPTION

Deception occurs when one's behavioral expression is inconsistent with his/her true thoughts or feelings. Deception is not always considered unacceptable, as we often expect to mask non-verbal cues of our true feelings. The ability to mask these cues may vary from person to person. However, jurors can often times notice and react to deception. When lying, the witness tends to show more mismatch between the various channels of communication. More attention tends to be directed to managing facial expressions, which may not be synchronized with the bodily movement or voice inflection. People tend to move their face, hand and body more when lying. Also, facial expressions and eye contact can be quick and fleeting. While it is true that studies show that we tend to overrate our abilities to detect deception, it is also true that in the context of a witness' testimony, a jury's ability to detect deception is generally higher due to situational factors – primarily, the relationship of the witness to the parties and the motivation of that person to lie.

USES OF VIDEOTAPED DEPOSITIONS AT TRIAL

There are a number of reasons for using videotaped depositions at time of trial. Traditionally, testimony was preserved in case the deponent died, became too ill, fled or otherwise was unavailable to testify at trial. Deposition testimony was regularly used to impeach a witness if he/she changed his/her testimony at trial. Use of video depositions in these circumstances highlights the witness' inconsistencies. Seeing a witness make an unambiguously different statement on video than they did in court has much greater impact than simply reading the deposition transcript. Further, in the case of impeachment, particular segments are selected for presentation, which amounts to a mere fraction of the entire deposition. While these excerpts can be anticipated, they are only used when a witness unexpectedly alters his/her deposition testimony.

Today, the preservation of testimony via videotape is not only for provisional purposes but is used more and more to try to "catch the witness off guard." As an example, many skilled plaintiffs' attorneys do not begin a videotaped deposition in a traditional sense which would entail obtaining significant background information on the witness. Instead, the deposition may start with this question: "Isn't it true, sir, that your defective product has caused injuries to my client?" If your witness is not prepared for this style of questioning, then the normal response from the witness when asked a question like this is astonishment and his/her subsequent verbal and nonverbal communications can impart a lack of confidence, preparation and, worst of all, trustworthiness. The witness will typically look to counsel for help or an objection. But the video camera captures the witness' expression on his/her face. Thus, the defense practitioner

must be prepared and conduct research on their opponent. If possible, observe your opponent in action. Your opponent's use of videotaped depositions, whether clips, snippets or bites of your witness' testimony can provide your adversary with the ability to construct their case in a much more efficient and technologically advanced format.

EFFECTIVE PREPARATION OF YOUR WITNESS FOR THE VIDEOTAPED DEPOSITION

Traditionally, preparation for your client's deposition consisted of the standard instructions including:

- Tell the truth;
- Be concise;
- Don't guess;
- Speak clearly;
- Don't argue;
- Wait for the entire question before answering;
- Listen and understand the question before answering;
- Don't speculate; and
- Don't volunteer.

With the advent of videotaped depositions, preparation of your witness for a videotaped deposition must be taken to a much greater level. It is the general consensus of researchers that people do not see or hear themselves as others do. Most people have never been videotaped and, therefore, don't understand or appreciate how their nonverbal communication skills (or lack thereof) will affect how they are perceived by a jury. Therefore, it is important that as part of your deposition preparation your witness is videotaped both on direct and cross examination so that the witness can appreciate the strengths and weaknesses of his/her nonverbal communication skills. The weaknesses in your witness' testimony are magnified tremendously when their

testimony is videotaped. A dress rehearsal of the anticipated line of questioning by your adversary is essential for your witness to become comfortable “in their own skin” during videotaped deposition.

As the research described herein has shown, slouching, rapid eye movement, turning to the attorney for help, stammering, folding of the arms across the chest as well as other forms of body language impact the jury’s acceptance of your witness’ testimony much more than the words spoken by your witness. It is essential, therefore, for your witness to be prepared to develop the necessary rapport with the jurors by proper body language, voice control and inflection and body movement. Remember that the words spoken by your witness may become lost on the jury during the course of the trial but the jury’s perception of your witness as truthful or untrustworthy will remain.

Courts are split on whether videotaped deposition testimony can be utilized in openings. Therefore, it is important that you know the local rules of court for use of videotaped deposition during all phases of the trial. Alert your adversary well in advance of the trial that if he/she intends to utilize videotaped deposition testimony of your witnesses in his/her opening, they must provide you with the videotaped deposition well in advance of trial. While local court rules may permit use of videotaped depositions in openings objections can always be made on the grounds of relevancy or out of context.

EFFECTIVE USE OF VIDEOTAPED DEPOSITION AT TRIAL

The world we live in is moving faster and faster and, as a result, the attention span of most people is getting shorter and shorter. Consider, for example, why Superbowl ads are divided into 15 second segments. Effective advertisers can promote their product or message to the audience in as little as 15 seconds.

In the trial setting, jurors expect the attorneys will be polished, sophisticated and technologically savvy. Consider that almost 70% of today's jurors will be made up of GenX, GenY and Millennials. Many of your prospective jurors have grown up in our advanced technological age. T.V. shows and movies about lawyers show only snippets of courtroom drama. Your jurors will expect the same type of courtroom drama during your trial. Research over the past decade has demonstrated the following:

- Watching videotaped deposition testimony is much more boring than watching live testimony;
- If jurors are not engaged they are less likely to retain persuasive points;
- Jurors are most riveted by video clips that directly impeach or contain a dramatic nonverbal communication;
- Jurors are "turned off" by video clips that only marginally deviate from the testimony or where the contraindication was subtle.

Thus, when considering the use of videotaped deposition of your opponent consider the following:

- Important testimony should be broken down into “short clips” that can be repeated numerous times during openings, testimony and closing arguments;
- Avoid overuse of this valuable communication tool so that jurors will remain engaged and retain persuasive points;
- Combine videotaped deposition testimony with demonstrative evidence (exhibits, photos, x-rays, etcetera) to increase the jury’s understanding of your message;
- Use smart/super deposition techniques such as synchronized videotaped deposition so that the jury can see and hear the witnesses testimony.
- Follow the testimony through written word.
- Consider using your own “sound bites” during your opening and/or closing to emphasize your defense themes.
- If you have the ability to obtain the trial testimony of your adversary’s witnesses (daily copy) incorporate the written trial testimony into your cross-examination of the adversary’s witnesses highlighting the inconsistencies and/or contradictions between videotaped deposition testimony and trial testimony.
- Cue the jury during your opening to the importance of the videotaped deposition sound bites you will utilize to heighten the jury’s anticipation of your trial presentation.

Sophisticated use of videotaped deposition testimony using the most advanced technology methods available today can be one of the most persuasive elements of your trial presentation. Conversely, an ill prepared witness for a videotaped deposition can result in catastrophic consequences at time of trial. It is the responsibility of the defense practitioner to understand how technology, particularly with respect to videotaped depositions can impact their

case at trial either positively or negatively. Remember, in the final analysis the jury may not remember every word a witness said at trial or deposition. However, you can be assured that the jury will never forget the nonverbal communication expressed by a witness during their videotaped deposition or trial.

Appendix A

- Legal Videotaping – videotaping in the legal industry came about as a means to preserve for trial purposes the testimony of a witness who could not be at trial due to scheduling issues.
- Videotaped Deposition – The adjunct of videotaping the testimony provided by a witness at a deposition for preservation and presentation at trial.
- Video Synchronization – The result of combining the video, text and audio of a deposition into a searchable format which is synchronized by time, page and line number. Scrolling text can be turned on or off, in addition to linking exhibit files.
- DVT – Digital Video Transcript is the product that is produced as a video synched file. You can show the scrolling text under the witness if you would like – similar to closed captioning.
- Video Clips (depositions) – Individual portions of a deposition, such as a Question and Answer or multiple Questions and Answers in continuity, which can be as short or as long as necessary.
- Video Segments (depositions) – Portions or bytes of a deposition combined into one file to be played back to a finder of fact. This file would excise out portions not to be played, so that one complete stream is played without interruption.
- Smart Depositions (SuperDeps, Interactive Deps, iDeps) - Videotaped depositions with adjunct of trial presentation software, which allows the witness and/or counsel to interact with the document, photograph or X-ray applying mark ups and other iterations. All of the actions are recorded via video and also recorded digitally on the computer used by the

presenter, so that the final product shows the full video of the witness and the interaction of the witness with the documents. One important feature is that when viewing the video of the witness with the document offered to them, it can be in a split screen format or moving the witness into one of the four corners of the video, allowing the document to be shown almost full screen. After the witness is finished with the document, the document moves off the screen and the witness is then on the full screen.

- Smartboard – A computer monitor which allows the user to interact with anything presented on the monitor. An example is the weather person on your local newscast uses a Smartboard to draw arrows, circles, etc.
- Viewsonic Monitors – Touch Screen. Touch screen monitors are the newest generation of interactive monitors. Adding Windows 8 (Microsoft) provides the ability for you to use your fingers or a stylus to pinch open a file and markup a file.
- Videotaped Depositions – Linking Exhibits (split screen) - In post-production exhibits can be linked into the deposition to be shown to the jury. As an example, if you were discussing an animation with the witness, the way to present that to the jury would be when the exhibit is discussed, the screen would split into two so that the jury can see the witness testifying and the animation at the same time.
- Video Conferencing – The use of video conferencing for depositions and/or trial presentation is becoming more of a regular occurrence. Many times at trial the Court will allow a witness at an offsite location testify directly into the courtroom via video conference. The video conference is a two-way system, so that the video and audio is broadcast to both sides. You can also present documents to the witness in this situation for their view on the video conference screen.



WEDNESDAY, MARCH 8, 2017

11:00 a.m. - 12:00 p.m.

Closing Remarks - Leaving the Best Impression

Magnolia Ballroom

Moderator:

Vicki M. Smith

Speakers:

Deborah D. Kuchler

E. Paige Sensenbrenner

Joseph Fasi, II

FROM THE LIPS OF THE CLOSING ARGUMENT PROS

Authored by Vicki M. Smith, Bodyfelt Mount, Portland, Oregon

With the FDCC's distinguished group of trial attorneys and savvy industry members, how does one write a paper on closing arguments? There are hornbooks, treatises and articles galore written on the subject. We already know the textbook goal of a closing argument is to persuade the jury to rule in favor of your client by summarizing and arguing how the evidence presented at trial supports your client. With enough experience, we learn there is a practical goal of closing argument and that is to provide ammunition and arguments for those jurors who already agree with you to use in the jury room to try to convince those jurors who are still on the fence.

In law school trial practice class, we are taught how to organize and present a closing argument. We are also given tips and strategies. Create a theory of your case and present it throughout the case. Define and use themes and labels. Start your closing with a powerful statement. End it on a powerful note too. Avoid personal opinions. Use exhibits. Then, as we develop our closing argument skills, we learn more advanced strategies. Believe in your case/client/story. Be passionate or confident. Simplify any case to its core issues and repeat those issues in closing argument. And a little theater may be helpful.

As experienced trial lawyers, we can still improve our closing arguments. The best method is through practice and giving closing arguments. But, we can also learn from other attorney's closing arguments. We can see how they successfully assembled their arguments or dealt with a particular issue. Some closing argument strategies are exemplified in the memorable closing arguments below.

Argue your theory and be passionate about your case.

Clarence Darrow's 12-hour closing argument in the *State of Illinois v. Leopold and Loeb* trial of 1924 has been described as "masterful" and "brilliant."¹ Darrow defended

¹ *Wade v. Calderon*, 29 F3d 1312, 1331 (9th Cir. 1994)(Reinhardt, J. dissenting).

two wealthy teenagers in the thrill killing of their 14-year old neighbor. Their guilt was never an issue. Darrow made his emotional argument during the penalty phase of trial.

I have heard in the last six weeks nothing but the cry for blood. I have heard from the office of the state's attorney only ugly hate. I have heard precedents quoted which would be a disgrace to a savage race. I have seen a court urged almost to the point of threats to hang two boys, in the face of science, in the face of philosophy, in the face of humanity, in the face of experience, in the face of all the better and more humane thought of the age.

Why did they kill little Bobby Franks? Not for money, not for spite; not for hate. They killed him as they might kill a spider or a fly, for the experience. They killed him because they were made that way. Because somewhere in the infinite processes that go to the making up of the boy or the man something slipped, and those unfortunate lads sit here hated, despised, outcasts, with the community shouting for their blood. Mr. Savage [the prosecutor], with the immaturity of youth and inexperience, says that if we hang them there will be no more killing. This world has been one long slaughterhouse from the beginning until today, and killing goes on and on and on, and will forever.

Do I need to argue to Your Honor that cruelty only breeds cruelty? That hatred only causes hatred; that if there is any way to soften this human heart which is hard enough at its best, if there is any way to kill evil and hatred and all that goes with it, it is not through evil and hatred and cruelty; it is through charity, and love, and understanding? I am not pleading so much for these boys as I am for the infinite number of others to follow, those who perhaps cannot be as well defended as these have been, those who may go down in the storm, and the tempest, without aid. It is of them I am thinking, and for them I am begging of this court not to turn backward toward the barbarous and cruel past.

Your Honor, if in this court a boy of eighteen and a boy of nineteen should be hanged on a plea of guilty, in violation of every precedent of the past, in violation of the policy of the law to take care of the young, in violation of all the progress that has been made and of the humanity that has been shown in the care of the young; in violation of the law that places boys in reformatories instead of prisons, if Your Honor in violation of all that and in the face of all the past should stand here in Chicago alone to hang a boy on a plea of guilty, then we are turning our faces backward, toward the

barbarism which once possessed the world. If Your Honor can hang a boy at eighteen, some other judge can hang him at seventeen, or sixteen, or fourteen. Someday, if there is any such thing as progress in the world, if there is any spirit of humanity that is working in the hearts of men, someday men would look back upon this as a barbarous age which deliberately set itself in the way of progress, humanity, and sympathy, and committed an unforgivable act....²

Throughout his closing argument, Darrow stayed with his theory and argued that executing his clients would serve no legitimate purpose. There was no question that he wholeheartedly believed in this position. His conviction and passion transferred to his audience and moved the jurors and judge to tears. It is commonly believed that his closing argument convinced the trial judge to spare the lives of his clients, who were sentenced to life in prison.³

Keep your theory simple and state it clearly and succinctly.

Your theory must be focused and presented in clear and concise language to the jury. In the *Silkwood v. Kerr-McGee Corp.* case, Gerry Spence represented the family of a nuclear energy facility employee. The employee died on her way to meet with a reporter where she intended to expose her employer's failure to follow safety protocols, which allowed employees to be exposed to hazardous materials. In his closing, Spence succinctly defined the case and his theory for the jury.

What is the case not about? The case is not about being against the nuclear industry. You will never hear me say that I stand here against the nuclear industry—I do not. But it is about being responsible, about responsible progress....And without the truth, the progress that we all need, and want, can't be had. It is that simple—that is what the case is not about.⁴

Simplifying a case to the essential issues is key to helping a jury understand the case and your position but is not easy to achieve in some cases. In the 1945 Nuremberg Trials, Robert Jackson was challenged to simplify and focus the prosecution case against

² Michael S. Lief, *et al.*, Ladies and Gentlemen of the Jury: Greatest Closing Arguments in Modern Law Ch 5 (1998).

³ Read the full transcript of Darrow's closing on the University of Missouri-Kansas City School of Law's Famous Trials page at: <http://law2.umkc.edu/faculty/PROJECTS/FTRIALS/leoploeb/darrowclosing.html>. This webpage is an excellent resource.

⁴ Lief, Ladies and Gentlemen of the Jury, Ch 4.

22 Nazi leaders. That trial lasted 216 days and included 237 witnesses plus testimony from 19 of the defendants.

Of one thing we may be sure. The future will never have to ask, with misgiving: "What could the Nazis have said in their favor?" History will know that whatever could be said, they were allowed to say. They have been given the kind of a trial which they, in the days of their pomp and power, never gave to any man.

But fairness is not weakness. The extraordinary fairness of these hearings is an attribute of our strength. The prosecution's case, at its close, seemed inherently unassailable because it rested so heavily on German documents of unquestionable authenticity. But it was the weeks upon weeks of pecking at this case by one after another of the defendants that has demonstrated its true strength. The fact is that the testimony of the defendants has removed any doubts of guilt which, because of the extraordinary nature and magnitude of these crimes, may have existed before they spoke. They have helped write their own judgment and condemnation.

We are not trying them for possession of obnoxious ideas. It is their right, if they choose, to renounce the Hebraic heritage in the civilization of which Germany was once a part. Nor is it our affair that they repudiated the Hellenic influence as well. The intellectual bankruptcy and moral perversion of the Nazi regime might have been no concern of International Law had it not been utilized to goose-step the Herrenvolk across international frontiers. It is not their thoughts, it is their overt acts which we charge to be crimes. Their creed and teachings are important only as evidence of motive, purpose, knowledge and intent....⁵

Jackson focused the jury on the "overt acts" of the defendants and, at the conclusion of trial, only three were acquitted.

End with a strong statement.

The start and conclusion of a presentation tend to be most memorable. As defense counsel, we generally get one time to present closing argument to the jury. You want to leave it on a high note with something that strongly stays in the jury's mind throughout a plaintiff's rebuttal and for the jury to take back to the jury room. Gerry Spence would often

⁵ *Id.* at Ch 1.

end his closing arguments with his Bird Story, which he used to make the jury understand the weight of their decision and that his client's fate was in their hands.

Once there was a wise old man and a smart-aleck boy. The boy was driven by a single desire-to expose the wise old man as a fool. The smart aleck had a plan. He had captured a small and fragile bird in the forest. With the bird cupped in his hands so that the old man could not see it, the boy's scheme was to approach the old man and ask, "Old man, what do I have in my hand?" To which the wise old man would reply, "You have a bird, my son."

Then the boy would ask, "Old man, is the bird alive or dead?" If the old man replied that it was dead, the boy would open his hands and allow the bird to fly off into the forest. But if the old man replied that the bird was alive, the boy would crush the bird inside his cupped hands until it was dead. Then the boy would open his hands and say, "See, the bird is dead!"

And so, the smart-aleck boy went to the old man, and he said, as planned, "Old man, what do I have in my hands?"

The old man, as predicted, replied, "You have a bird, my son."

"Old man," the boy then said with disdain, "is the bird alive or is it dead?"

Whereupon the old man looked at the boy with his kindly old eyes and replied, "The bird is in your hands, my son."

It is then that I turn to the jury and say, "And so, too, ladies and gentlemen, the life of my client is in yours."⁶

He closed with this story in the Randy Weaver trial that arose out of the standoff between Weaver and his family and the FBI at Ruby Ridge in Idaho.⁷ Spence's client, Weaver, was acquitted of all major charges. He also used the Bird Story to conclude his closing argument in the *Silkwood v. Kerr-McGee Corp.* trial.⁸ Certainly, the award in *Silkwood* was the result of more than simply telling the Bird Story but Spence did sway the jury not just to find for his clients but to award \$10 million in punitive damages.⁹

⁶ Kevin C. Kennedy, *Closing Argument: Through the Eyes of a Trial Advocate*, 20 Am J Trial Advoc 593, 606 (2006-07).

⁷ <http://law2.umkc.edu/faculty/projects/ftrials/weaver/spencesummation.html>.

⁸ Lief, *Ladies and Gentlemen of the Jury*, Ch 4.

⁹ *Silkwood v. Kerr-McGee Corp.*, 464 US 238, 245 (1984).

Try to connect with the jury.

We all know that you want to talk “with” the jury and not “at” them. Finding a way to connect with the jury can help them feel like they are part of the process and part of the discussion. D’Lesli Davis’ closing argument in the 2013 trial of *Alsabagh v. Takeda Chemical Industries Ltd.* is a good example of using your case themes and also connecting with the jury. It was a product liability case where Davis represented a defendant drug manufacturer. Davis made a personal connection between the defense theme of “choices and consequences” and the Las Vegas, Nevada jury.¹⁰

This great city, this great state in fact, is all about personal choice. And personal choice without judgment... This state and this city (are) founded on the idea that people can make their own personal decisions.

*But we also understand that, with the freedom to make personal decisions about our lives about our health, about our families, comes a personal responsibility.*¹¹

Davis obtained a defense verdict for her client.

Use the Rule of Three.

Three is a magic number. People are more likely to remember information or an idea if it is presented three times or if a presentation is organized around three, such as three concepts, three issues, three arguments. Litigators use this age-old principle in closing arguments to emphasize an important point, fact or argument. Of course, it also helps if the point you want the jury to remember is a snappy tag line. Johnny Cochran effectively used this principle in the OJ Simpson trial.

Like the defining moment in this trial, the day Mr. Darden asked Mr. Simpson to try on those gloves and the gloves didn't fit, remember these words; if it doesn't fit, you must acquit.

Where is all that blood trail they've been banting about in this mountain of evidence? You will see it's little more than a river or a stream. They don't have any mountain or ocean of evidence. It's not so because they say so.

¹⁰ <http://blog.cvn.com/courtroom-masters-show-you-three-crucial-tweaks-to-perfect-your-closing-argument>. CVN is the Courtroom View Network.

¹¹ *Id.*

That's just rhetoric. We this afternoon are talking about the facts. And so it doesn't make any sense. It just doesn't fit. If it doesn't fit, you must acquit.

It occurred to me how they [the prosecution] were going to come here, stand up here and tell you how O.J. Simpson was going to disguise himself. He was going to put on a knit cap and some dark clothes, and he was going to get in his white Bronco, this recognizable person, and go over and kill his wife. That's what they want you to believe. That's how silly their argument is. And I said to myself, maybe I can demonstrate this graphically. Let me show you something. This is a knit cap. Let me put this knit cap on (Indicating). You have seen me for a year. If I put this knit cap on, who am I? I'm still Johnnie Cochran with a knit cap. And if you looked at O.J. Simpson over there--and he has a rather large head--O.J. Simpson in a knit cap from two blocks away is still O.J. Simpson. It's no disguise. It's no disguise. It makes no sense. It doesn't fit. If it doesn't fit, you must acquit.¹²

A little theater may be helpful, if done appropriately.

Richard "Racehorse" Haynes of Texas was involved in a criminal trial in the 1970s. The prosecutor refused to call a key witness, knowing Haynes' cross-examination would be brutal. Haynes did not let that stop him but cross-examined the empty witness chair in his closing argument by asking it the pointed questions he would have asked the witness. This tactic was effective. The jury acquitted his client.¹³

We know that our closing arguments should mostly be prepared well in advance and rehearsed often. We also know that we need to remain flexible and be willing to respond to circumstances outside of our control. Consider another trial by Richard Haynes where he defended a client accused of murdering her well-known husband. Just as Haynes rose to present his closing argument, the *William Tell Overture* floated in through the open courthouse windows. A high school band had started practicing near the courthouse. The prosecutor objected and accused Haynes of arranging the event to which Haynes responded "I wish I had, because it is a marvelous idea."¹⁴

¹² <http://law2.umkc.edu/faculty/projects/ftrials/simpson/cochranclose.html#gloves>.

¹³ http://www.abajournal.com/magazine/article/richard_racehorse_haynes.

¹⁴ *Id.*

Or consider this incredible exchange during closing arguments in a 1890 criminal trial in California.

*She is a WOMAN, she cannot be expected to reason; God Almighty decreed her limitations, but you can reason and you must use your reasoning faculties against this young woman who will lead you by her sympathetic presentation of this case to violate your oaths and let a guilty man go free.*¹⁵

You can imagine that opposing counsel Clara Shortridge Foltz did not take too kindly to Colonel Thetas Stonehill's closing argument.

If Your Honor please and gentlemen of the jury: You well know that I am not before you by my own choice! That in obedience to time-honored rule I am here by order of this court trying as best I can to represent this despairing man. Is it not strange then that the district attorney should make me an object of his displeasure and challenge my presence at this bar because only that I am a woman? The kind indulgence of the court has permitted counsel to range over much matter that is neither of record nor part of the evidence in this case. I would rather the immaterial and irrelevant part of his speech had remained unspoken, for I take no pleasure in the wanton abuse of a jury's patience nor in burdening them with matter wholly foreign to the case.

Counsel tells you that I am a woman. I wonder that the planets did not stand still in their course and rivers cease to run to the sea at the announcement of this startling discovery. I am amazed that His Honor did not faint upon the bench and that you gentlemen of the jury have survived this awful shock to your nervous systems.

Counsel intimates with a curl on his lip that I am called the lady lawyer. I am sorry I cannot return the compliment, but I cannot. I never heard anybody call him any kind of lawyer at all.

And now let us take it all together. I am a woman and I am a lawyer—and what of it? It is not so new or wonderful a thing. I am practicing law in this city; I have offices in one of its largest buildings, and I go daily to and from those offices in my right mind. I am certainly not unknown to the bench and bar of California. And gentlemen, I came into the practice of my profession under the laws of this state, regularly and honestly, and not by the certificate

¹⁵ <https://www.countyofsb.org/defender/asset.c/54> , citing Mortimer D. Schwartz, et al., The Battles of Clara Shortridge Foltz, California Defender Vol 1, Issue 1 (1985).

*of another state that required no learning to secure, and I have come to stay. I am neither to be bullied out nor worn out. I ask no special privileges and expect no favors, but I think it only fair that those who have had better opportunities than I, who have had fewer obstacles to surmount and fewer difficulties to contend with should meet me on even ground, upon the merits of the law and fact without this everlasting and incessant reference to sex—reference that in its very nature is uncalled for and is as unprofessional as it is unmanly...*¹⁶

Foltz won her case.

We may not all be as eloquent as Clarence Darrow, as witty as Richard Haynes, or be given such a great opportunity to respond to opposing counsel as Clara Shortridge Foltz, but there are lessons in these lawyers' closing arguments. We can learn that the power of conviction in one's case and the strength of good themes are persuasive; a simple, direct theory guides the jury; beginning and ending a closing argument with strong points leaves an impact on the jury; and incorporating the Rule of Three and connecting with the jury can lead to a successful closing argument.

¹⁶ Lief, Ladies and Gentlemen of the Jury, Ch 6.



Lighting the way to...

Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10

WEDNESDAY, MARCH 8, 2017

12:00 p.m. – 2:00 p.m.

Trial Technology Learning Laboratory

Jenkins

Moderator:

Thomas G. Oakes

USE OF TECHNOLOGY IN DEPOSITIONS

By: **Thomas G. Oakes**

THOMAS G. OAKES ASSOCIATES, LLC

With Special Thanks to: Francis J. Deasey, Esquire; Deasey, Mahoney & Valentini

INTRODUCTION

It goes without saying that the technological advantages of the last decade have changed the legal landscape dramatically. Applications of video technology have important implications for the future of the litigation process. Video depositions, almost universally permitted under Federal and State Rules of Civil Procedure, facilitate the transfer of information from pretrial events to the trial event. Traditionally, videotaped depositions were utilized for the depositions of testifying experts, particularly medical doctors. Today, most sophisticated plaintiff firms videotape every deposition. From the defense perspective this can create additional problems in preparing witnesses for depositions. Conversely, the savvy defense practitioner should make full use of the technology available to conduct video depositions.

In their formative years, most defense practitioners are taught that depositions are discovery tools designed to elicit facts. This way of thinking is obsolete. One of the major reasons most sophisticated plaintiff attorneys videotape depositions is to “Create a sound bite.” And, if permitted, this “sound bite” will be shown to a jury up to four times including:

- (a) During plaintiff counsel’s opening;
- (b) During plaintiff’s case-in-chief;
- (c) During cross-examination of the same witness (if called by the defense); and
- (d) During plaintiff counsel’s closing.

Every defense practitioner must understand how modern videotaped depositions work to prepare their witnesses for this experience. A video deposition brings to the forefront the concept of nonverbal communication, including concepts such as channeling, decoding,

encoding and rapport. All of these concepts impact how jurors will evaluate a witness' video deposition testimony,

However, it is important to remember that video deposition testimony is equally available to the defense and can be a tremendous weapon in defense counsel's arsenal when utilized effectively and professionally. This paper will explore the genesis of videotaped depositions up through and including interactive depositions, also known as smart depositions and will provide the defense practitioner with the tools to prepare their witnesses for video depositions and, at the same time, utilize videotaped depositions as part of their presentation.

GENESIS OF VIDEOTAPED DEPOSITIONS

In the early years of videotaping, the equipment was very antiquated. Cameras used VHS tapes only. Cameras were at least three times as large as today's cameras, bulky, heavy and the quality was not great. In fact, the lighting levels provided by the camera were so low, that additional lighting needed to be added. At times it resembled a mini movie set. Today, almost all videotaping is done digitally with digital cameras utilizing SD cards or directly to hard drives, and exporting the video to the format of counsel's choice, either Mpeg 1, 2 or 4.

In the early years, when the deposition was presented at trial and played to the jury, the videotaped deposition would not be edited, but any part of the deposition which was not to be shown to the jury would then be fast forwarded to the next part of the video to be played. The videographer would sit with a copy of the transcript with the portions not to be played X'd out. He/she would have a set of headphones on to listen and fast forward the VHS tape to the appropriate sections to be used.

While the process by which counsel and the court review objections or deposition designations has not changed, the ability to provide a more seamless edited file has made great strides in today's market. Years ago, the equipment used in the courtroom to play back the video was normally an old style television – not a flat panel – with a screen no more than 32 inches and the only audio came through the television. So that the audio could be heard better, one of the courtroom microphones would be placed close to the television audio output so it could be heard through the courtroom sound system. If we moved ahead a decade or two, we would find that

computers were fast enough, portable enough and software was developed for use in editing video. As a result, there was the advent of trial presentation software, such as Sanction and TrialDirector, which brought videotaped depositions to a new level. With this technology you could synchronize the audio, video and text file. The greatest part about having a video synched deposition is the ability to create clips or bites of the transcript. Delivery of videotaped depositions are now being made on CD, DVD, thumb drives and/or links. The video synched file that is received is a DVT file (digital video transcript). This portable DVT file allows the user to create their own clips of the deposition directly from the DVT and save the clips as either a PowerPoint file, MP4 file (iPad) or TrialDirector file to be imported into the full Trial Director Presentation software package.

SMART DEPOSITIONS – THE EARLY YEARS

First use of the smart deposition took place using an Elmo, which is a document camera. In the videotaped deposition, counsel would project onto a large screen a document to show the witness. Counsel would do the markings and/or have the witness make markings on a document or photo and capture this on videotape to be used later at trial. There are a number of issues using this type of technology. First, you needed to have multiple copies of the same document or photo for the witness or counsel to put markings on. Counsel would need to request the court reporter to put a sticker on each one of the files as they were made. You could not capture a digital copy of the document. You could only capture it on the video. The actual deposition was not being recorded to a hard drive and a video simultaneously. The video was the only recording. This could result in a very herky-jerky replay, since the video camera had to move its

focus from the witness to the document or the document camera and to the projection screen. However, this was a start and like any new technology, the bugs had to be worked out.

SMART INTERACTIVE OR SUPER DEPOSITIONS

If you intend to take a videotaped deposition of a witness using Smart, Interactive or Super Depositions, be sure that you take the time to either have your deposition exhibits pre-marked or numbered in such a way that the presenter (trial presenter) is able to offer up on the screen to the witness the document, x-ray or photo that you would like. A simple index of the documents with deposition exhibit numbers would work great. Also, even though the witness may using tools on the smart board or a monitor to do mark-ups on the exhibits, you will want to not only have this information recorded, but you will want to take screen shots of these documents for later use.

Screen shots can be used as a separate exhibit at trial. If you capture the document with its present markings, ask the presenter to capture the file for you. When asking that the file be captured, tell the presenter the number you want to give to the new exhibit. For example, if you offer the witness a photograph, which was pre-marked hypothetically Deposition Exhibit 3, the witness puts an X on the digital document denoting a location, etc., you would then tell the presenter to capture the new file, perhaps as Deposition Exhibit 3A. By capturing and numbering the exhibit at that time, you can then have that exhibit brought back at any time by just asking for 3A. You could also use this new exhibit with any other witness or in a PowerPoint presentation, etc. The file is captured as a PDF file.

A Smart/Interactive deposition provides you the ability to have a witness seen at trial exactly how the jury would see him/her on the witness stand, but you get the added benefit of being able to make clips of certain portions of the videotaped deposition to be used over and over again. You will also have the opportunity to have the witness pinpoint for you exactly what they are describing in words into a document, photograph, x-ray, etc. Thus, you create a picture which is “worth a thousand words.” Attached as Appendix A is information concerning terminology which will be helpful in understanding the intricacies of Smart depositions.

THE RULES

Federal Rule of Civil Procedure 30, provides impertinent part, as follows:

(3) Method of Recording.

(a) Method stated in the notice. The party who notices the deposition must state in the notice the method of recording the testimony. Unless the court orders otherwise, testimony may be recorded by audio, audio visual, or stenographic means. The noticing party bears the recording costs. Any party may arrange to transcribe a deposition.

(b) Additional Method. With prior notice to the deponent and other parties, any party may designate another method of recording the testimony and in addition to that specified in the original notice. That party bears the expense of the additional record or transcript unless the court orders otherwise.

(4) By Remote Means. The parties may stipulate – or the court may on motion order – that a deposition be taken by telephone or other remote means. For the purpose of this Rule and Rules 28(a), 37(a)(2) and 37(b)(1), the deposition takes place when the deponent answers the questions.

Many states have adopted verbatim or, in large measure, the Federal Rules of Civil Procedure including Rule 30. Before allowing your witness to be videotaped or noticing a

videotaped deposition, it is important to know the state's rules concerning videotaped depositions and, most importantly, restrictions on the use of videotaped depositions at trial.

NONVERBAL COMMUNICATION IN THE VIDEOTAPED DEPOSITION

Nonverbal communication is behavioral communication through facial expression, bodily movements and gestures, as well as vocal tone, hesitations, and pitch. Such communication is often subtle, uncontrollable and spontaneous. These cues are generally interpreted universally and cross-culturally. Thus, the advantage of allowing a jury to audio-visually perceive a witness' testimony through video tape means the jurors will be able to interpret nonverbal cues that they otherwise could not by simply hearing the testimony being read through a transcript. Another advantage is that the videotape is the most accurate way to relay the testimony, which alleviates concerns about objections that could be made regarding accuracy, inflection, tone, etc...when testimony simply is read from a transcript.

Of course, nonverbal communication can be controlled to achieve a purpose such as deception or impression management. This is a skill that some are better at than others. Actions such as nerves and anxiety can affect our ability to manage nonverbal communication. For example, a witness may attempt to project confidence, but the jury still might be able to sense nervousness from nonverbal cues, which may impact an assessment of the witness' credibility. Conversely, positive communication may establish mutual liking, empathy, rapport and most importantly, trust. A smile, direct gaze, forward lean, and warm vocal tone all convey interest and liking, when all are taken together. However, if you remove the smile or warm tone from that equation, the meaning could become entirely different. Nonverbal communication is imparted through a combination of these types of factors.

BASIC CHANNELS OF NONVERBAL COMMUNICATION

(a) Face

The face is the channel that is most easily controlled, and may be the most expressive channel of communication, particularly for emotions. Emotional expression occurs through movements of the mouth, eyebrows, cheek and eyes. Fear, surprise, anger, disgust, sadness and happiness are all conveyed in this matter, and have been observed universally in a variety of cultures. The direction and duration of a gaze is particularly important. We tend to associate direct eye contact with trustworthiness. Smiling and head nodding tend to be universal signs of empathy.

(b) Body

Bodily expression is less controllable than facial expression. Body orientation, positioning and postures are also key to emotional expression. Bodily expressions are also indicative of self-monitoring. High self-monitoring of one's behavior in relation to others and constant awareness of the social appropriateness of one's actions will likely be expressed through such cues. This is called postural mirroring and has been found to create empathy. Changes in posture can be indicative of aggression vs. passivity, as well as signs of emotions and/or mental conditions such as anxiety or depression. We tend to associate an erect posture with confidence and personal appearance.

(c) Gestures

Bodily expressions such as hand/arm gestures can have direct verbal meaning that replaces speech. The simplest example is a witness pointing to an object for

identification. Such movements can also be culture-specific, such as giving a “thumbs” up sign. The interpretation of these gestures can vary widely across cultures and serious misunderstandings can arise. Some gestures, such as crossing one’s arms, are universal signs of guardedness vs. openness. Hand wringing may be a sign of nervousness or anxiety.

(d) Voice

Voice is the least controllable channel of communication. Beyond the actual words spoken, a speaker’s voice, tone and inflection can mean expressions of emotion, mood, confidence and honesty. A harsh and loud vocal inflection such as a “command” voice will relay aggression, dominance and control. This is generally not the best way to establish empathy. A direct, warm and relaxed tone denotes confidence, genuineness and honesty.

IMPORTANCE OF NONVERBAL COMMUNICATION IN THE VIDEOTAPED
DEPOSITION

Studies have shown that jurors pick up nonverbal signs and cues unconsciously transmitted by the speaker. Up to 55% of the meaning of a speaker’s message is nonverbal. Nonverbal skill is the term used to describe individuals’ abilities to use nonverbal communication effectively and accurately. Nonverbal skills tend to be associated with enduring characteristics of people such as gender, personality and culture. Generally, nonverbal skills are conceptualized in terms of two separate sub skills: Encoding skills and decoding skills.

Encoding skills refer to the ability to communicate emotions, attitudes or other messages through nonverbal cues so that the observer (in this case the jury) can interpret the meaning of the message as the encoder intended. Thus, skilled encoders (the witness) tend to be judged as more empathic when they are being empathic and judged so purely from nonverbal channel such as the face or the voice. More-skilled encoders tend to be more popular, dominant and extraverted than less-skilled encoders.

Decoding skills refer to individuals' ability to interpret the nonverbal communication of other people. While the decoding skills of people vary all jurors will have decoding skills which will enable them, more or less, to interpret the nonverbal communications of witnesses. In general, women are more accurate encoders as well as decoders of nonverbal communication than men.

CREDIBILITY

Credibility is established in large part by the witness' confidence and rapport he/she is able to establish with his/her audience. Mutual involvement and interpretation of situations is key to establishing rapport. Witnesses who smile, nod their heads, lean forward, gaze directly at their subject, maintain direct body orientation, have an open as opposed to guarded posture, make few hand gestures, and speak with a warm and relaxed tone will most likely be able to establish a rapport with his/her audience and thus come across as more credible. Tone of voice, which is the most difficult channel to control, is important to establishing confidence. For example, a positive verbal message in a negative tone of voice may arouse suspicion, because we

generally expect a positive verbal message to be relayed in a positive tone. To the contrary, a negative verbal message in a positive tone of voice may communicate concern and acceptance.

DECEPTION

Deception occurs when one's behavioral expression is inconsistent with his/her true thoughts or feelings. Deception is not always considered unacceptable, as we often expect to mask non-verbal cues of our true feelings. The ability to mask these cues may vary from person to person. However, jurors can often times notice and react to deception. When lying, the witness tends to show more mismatch between the various channels of communication. More attention tends to be directed to managing facial expressions, which may not be synchronized with the bodily movement or voice inflection. People tend to move their face, hand and body more when lying. Also, facial expressions and eye contact can be quick and fleeting. While it is true that studies show that we tend to overrate our abilities to detect deception, it is also true that in the context of a witness' testimony, a jury's ability to detect deception is generally higher due to situational factors – primarily, the relationship of the witness to the parties and the motivation of that person to lie.

USES OF VIDEOTAPED DEPOSITIONS AT TRIAL

There are a number of reasons for using videotaped depositions at time of trial. Traditionally, testimony was preserved in case the deponent died, became too ill, fled or otherwise was unavailable to testify at trial. Deposition testimony was regularly used to impeach a witness if he/she changed his/her testimony at trial. Use of video depositions in these circumstances highlights the witness' inconsistencies. Seeing a witness make an unambiguously different statement on video than they did in court has much greater impact than simply reading the deposition transcript. Further, in the case of impeachment, particular segments are selected for presentation, which amounts to a mere fraction of the entire deposition. While these excerpts can be anticipated, they are only used when a witness unexpectedly alters his/her deposition testimony.

Today, the preservation of testimony via videotape is not only for provisional purposes but is used more and more to try to "catch the witness off guard." As an example, many skilled plaintiffs' attorneys do not begin a videotaped deposition in a traditional sense which would entail obtaining significant background information on the witness. Instead, the deposition may start with this question: "Isn't it true, sir, that your defective product has caused injuries to my client?" If your witness is not prepared for this style of questioning, then the normal response from the witness when asked a question like this is astonishment and his/her subsequent verbal and nonverbal communications can impart a lack of confidence, preparation and, worst of all, trustworthiness. The witness will typically look to counsel for help or an objection. But the video camera captures the witness' expression on his/her face. Thus, the defense practitioner

must be prepared and conduct research on their opponent. If possible, observe your opponent in action. Your opponent's use of videotaped depositions, whether clips, snippets or bites of your witness' testimony can provide your adversary with the ability to construct their case in a much more efficient and technologically advanced format.

EFFECTIVE PREPARATION OF YOUR WITNESS FOR THE VIDEOTAPED DEPOSITION

Traditionally, preparation for your client's deposition consisted of the standard instructions including:

- Tell the truth;
- Be concise;
- Don't guess;
- Speak clearly;
- Don't argue;
- Wait for the entire question before answering;
- Listen and understand the question before answering;
- Don't speculate; and
- Don't volunteer.

With the advent of videotaped depositions, preparation of your witness for a videotaped deposition must be taken to a much greater level. It is the general consensus of researchers that people do not see or hear themselves as others do. Most people have never been videotaped and, therefore, don't understand or appreciate how their nonverbal communication skills (or lack thereof) will affect how they are perceived by a jury. Therefore, it is important that as part of your deposition preparation your witness is videotaped both on direct and cross examination so that the witness can appreciate the strengths and weaknesses of his/her nonverbal communication skills. The weaknesses in your witness' testimony are magnified tremendously when their

testimony is videotaped. A dress rehearsal of the anticipated line of questioning by your adversary is essential for your witness to become comfortable “in their own skin” during videotaped deposition.

As the research described herein has shown, slouching, rapid eye movement, turning to the attorney for help, stammering, folding of the arms across the chest as well as other forms of body language impact the jury’s acceptance of your witness’ testimony much more than the words spoken by your witness. It is essential, therefore, for your witness to be prepared to develop the necessary rapport with the jurors by proper body language, voice control and inflection and body movement. Remember that the words spoken by your witness may become lost on the jury during the course of the trial but the jury’s perception of your witness as truthful or untrustworthy will remain.

Courts are split on whether videotaped deposition testimony can be utilized in openings. Therefore, it is important that you know the local rules of court for use of videotaped deposition during all phases of the trial. Alert your adversary well in advance of the trial that if he/she intends to utilize videotaped deposition testimony of your witnesses in his/her opening, they must provide you with the videotaped deposition well in advance of trial. While local court rules may permit use of videotaped depositions in openings objections can always be made on the grounds of relevancy or out of context.

EFFECTIVE USE OF VIDEOTAPED DEPOSITION AT TRIAL

The world we live in is moving faster and faster and, as a result, the attention span of most people is getting shorter and shorter. Consider, for example, why Superbowl ads are divided into 15 second segments. Effective advertisers can promote their product or message to the audience in as little as 15 seconds.

In the trial setting, jurors expect the attorneys will be polished, sophisticated and technologically savvy. Consider that almost 70% of today's jurors will be made up of GenX, GenY and Millennials. Many of your prospective jurors have grown up in our advanced technological age. T.V. shows and movies about lawyers show only snippets of courtroom drama. Your jurors will expect the same type of courtroom drama during your trial. Research over the past decade has demonstrated the following:

- Watching videotaped deposition testimony is much more boring than watching live testimony;
- If jurors are not engaged they are less likely to retain persuasive points;
- Jurors are most riveted by video clips that directly impeach or contain a dramatic nonverbal communication;
- Jurors are "turned off" by video clips that only marginally deviate from the testimony or where the contraindication was subtle.

Thus, when considering the use of videotaped deposition of your opponent consider the following:

- Important testimony should be broken down into “short clips” that can be repeated numerous times during openings, testimony and closing arguments;
- Avoid overuse of this valuable communication tool so that jurors will remain engaged and retain persuasive points;
- Combine videotaped deposition testimony with demonstrative evidence (exhibits, photos, x-rays, etcetera) to increase the jury’s understanding of your message;
- Use smart/super deposition techniques such as synchronized videotaped deposition so that the jury can see and hear the witnesses testimony.
- Follow the testimony through written word.
- Consider using your own “sound bites” during your opening and/or closing to emphasize your defense themes.
- If you have the ability to obtain the trial testimony of your adversary’s witnesses (daily copy) incorporate the written trial testimony into your cross-examination of the adversary’s witnesses highlighting the inconsistencies and/or contradictions between videotaped deposition testimony and trial testimony.
- Cue the jury during your opening to the importance of the videotaped deposition sound bites you will utilize to heighten the jury’s anticipation of your trial presentation.

Sophisticated use of videotaped deposition testimony using the most advanced technology methods available today can be one of the most persuasive elements of your trial presentation. Conversely, an ill prepared witness for a videotaped deposition can result in catastrophic consequences at time of trial. It is the responsibility of the defense practitioner to understand how technology, particularly with respect to videotaped depositions can impact their

case at trial either positively or negatively. Remember, in the final analysis the jury may not remember every word a witness said at trial or deposition. However, you can be assured that the jury will never forget the nonverbal communication expressed by a witness during their videotaped deposition or trial.

Appendix A

- Legal Videotaping – videotaping in the legal industry came about as a means to preserve for trial purposes the testimony of a witness who could not be at trial due to scheduling issues.
- Videotaped Deposition – The adjunct of videotaping the testimony provided by a witness at a deposition for preservation and presentation at trial.
- Video Synchronization – The result of combining the video, text and audio of a deposition into a searchable format which is synchronized by time, page and line number. Scrolling text can be turned on or off, in addition to linking exhibit files.
- DVT – Digital Video Transcript is the product that is produced as a video synched file. You can show the scrolling text under the witness if you would like – similar to closed captioning.
- Video Clips (depositions) – Individual portions of a deposition, such as a Question and Answer or multiple Questions and Answers in continuity, which can be as short or as long as necessary.
- Video Segments (depositions) – Portions or bytes of a deposition combined into one file to be played back to a finder of fact. This file would excise out portions not to be played, so that one complete stream is played without interruption.
- Smart Depositions (SuperDeps, Interactive Deps, iDeps) - Videotaped depositions with adjunct of trial presentation software, which allows the witness and/or counsel to interact with the document, photograph or X-ray applying mark ups and other iterations. All of the actions are recorded via video and also recorded digitally on the computer used by the

presenter, so that the final product shows the full video of the witness and the interaction of the witness with the documents. One important feature is that when viewing the video of the witness with the document offered to them, it can be in a split screen format or moving the witness into one of the four corners of the video, allowing the document to be shown almost full screen. After the witness is finished with the document, the document moves off the screen and the witness is then on the full screen.

- Smartboard – A computer monitor which allows the user to interact with anything presented on the monitor. An example is the weather person on your local newscast uses a Smartboard to draw arrows, circles, etc.
- Viewsonic Monitors – Touch Screen. Touch screen monitors are the newest generation of interactive monitors. Adding Windows 8 (Microsoft) provides the ability for you to use your fingers or a stylus to pinch open a file and markup a file.
- Videotaped Depositions – Linking Exhibits (split screen) - In post-production exhibits can be linked into the deposition to be shown to the jury. As an example, if you were discussing an animation with the witness, the way to present that to the jury would be when the exhibit is discussed, the screen would split into two so that the jury can see the witness testifying and the animation at the same time.
- Video Conferencing – The use of video conferencing for depositions and/or trial presentation is becoming more of a regular occurrence. Many times at trial the Court will allow a witness at an offsite location testify directly into the courtroom via video conference. The video conference is a two-way system, so that the video and audio is broadcast to both sides. You can also present documents to the witness in this situation for their view on the video conference screen.



THURSDAY, MARCH 9, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

CIVIL RIGHTS AND PUBLIC ENTITY LIABILITY

Balancing Interests in an Armed Society

Colleton

Speakers:

David J. MacMain

Casey C. Stansbury

Jane M. Lynch

BALANCING INTERESTS IN AN ARMED SOCIETY

FDCC Winter Meeting
Charleston, South Carolina
March 6-10, 2017

Tots and Glocks
Casey C. Stansbury
Mazanec, Raskin, & Ryder, Co., L.P.A.
230 Lexington Green Circle, Suite 605
Lexington, KY 40503
859-899-8514
cstansbury@mrrlaw.com

**Political Subdivision Liability for Civil Rights Claims Arising from Stops,
Detentions, and Arrests of Open Carriers**

Jane M. Lynch
Green & Green, Lawyers
109 North Main Street
Dayton, OH 45402
937-224-3333
jmlynch@green-law.com

Open Carry on Public/Municipal Property

David J. MacMain
The MacMain Law Group, LLC
101 Lindenwood Drive, Suite 160
Malvern, PA 19355
484-318-7703
dmacmain@macmainlaw.com

**Tots and Glocks:
School District Concerns When Arming School Staff**

**FDCC 2017 WINTER MEETING
March 6-10, 2017
Charleston, South Carolina**

**Presented by
Casey C. Stansbury**

**Manuscript by
Casey C. Stansbury
Tia J. Combs**

**Mazanec, Raskin & Ryder, Co., L.P.A.
Cleveland, OH
Columbus, OH
Lexington, KY**

1. Sandy Hook Changes Everything

On December 14, 2012, at approximately 9:30 a.m., 20-year-old Adam Lanza walked into Sandy Hook Elementary School in Newtown, Connecticut armed with three guns--a semi-automatic rifle and two handguns. Steve Vogel, Sari Horwitz, and David A. Fahrenthold, *Sandy Hook Elementary Shooting Leaves 28 Dead, Law Enforcement Sources Say*, Wash. Post, Dec. 14, 2012. There were 700 hundred elementary students present at school that day. By midmorning, twenty students and six school staff members were dead. *Id.*

While that December day was not the first school shooting or, unfortunately, the last, it marked a turning in the national consciousness. For many, school shootings, while never an acceptable part of American life, now called for dramatic action.

One response was an increased push for gun control. In Connecticut, Gov. Dannel P. Malloy signed into law “sweeping new restrictions on weapons and ammunition magazines similar to the ones used...at Sandy Hook” in April of 2013. Associated Press, N.Y. Times, April 14, 2013. Over 100 new firearms were added to the state’s assault weapons ban, the state now has a weapon offender registry, and there are new eligibility rules for buying ammunition. Associated Press, *Connecticut Governor Signs Gun Measures*, N.Y. Times, April 4, 2013.

Another response has been increased demand to arm teachers and staff in schools, putting them on the front lines of preventing school shootings. In 2013, lawmakers in more than thirty states proposed bills that would have authorized school districts to arm non-law enforcement in schools, mostly teachers and other staff members. Danielle Weatherby, *Opening the "Snake Pit": Arming Teachers in the War Against School Violence and the Government-Created Risk Doctrine*, 48 Conn. L. Rev. 119 (2015). These laws passed in at least eleven states. *Id.*

This article examines the legal responsibility of schools districts, schools, and teachers to protect students from active shooter situations and the legal problems created when districts chose to arm non-law enforcement school staff.

2. The Legal Problem of School Safety

When considering arming teachers and staff, the first question for districts should be: What is the legal liability of schools for failure to protect students from the dangers posed by third party actors.

A. Federal Due Process Litigation

i. *DeShaney* and Third Party Violence

As a general matter, the United States Supreme Court has held that the Due Process Clause of the Fourteenth Amendment does not require the State to protect the life, liberty, and property of citizens from private violence. *DeShaney v. Winnebago Cty. Dep't of Soc. Servs.*, 489 U.S. 189, 195 (1989). In *DeShaney*, the Petitioner, Joshua, was a young boy injured by his biological father's abuse. *Id.* at 191. The Respondents were social workers and other officials who received complaints Joshua was being abused by his father, but who failed to stop the mistreatment. *Id.* As a result of his father's repeated abuse, Joshua eventually suffered brain hemorrhaging, causing irreparable damage and mental retardation. *Id.* Joshua's mother brought suit, on behalf of herself and Joshua, under 42 U.S.C. 1983 alleging violation of the Fourteenth Amendment Due Process Clause for the officials' failure to protect Joshua from a risk of which they knew or should have known. *Id.* The District Court granted, and the Seventh Circuit and United States Supreme Court upheld, summary judgment in favor of the officials holding the Due Process Clause does not require states to protect individuals from private violence. *Id.* 194-95.

In *DeShaney*, the Court left open the possibility that states might be liable to those injured by third parties by creating two exceptions to non-liability: 1) when the state and the individual have a special relationship and 2) when the state has created the danger.

ii. The *DeShaney* Exceptions Applied to Violence in Schools

Awareness of violence in schools is higher than ever. In one case, the Tenth Circuit lamented:

We are poignantly aware of the seeming transformation of our public schools from institutions of learning into crucibles of disaffection marred by increasing violence from which anguish and despair are often brought to homes across the nation.

Graham v. Indep. Sch. Dist. No. 1-89, 22 F.3d 991, 992 (10th Cir. 1994).

However, despite this growing cognizance of the violence perpetrated in America's schools, and explicit acknowledgment of the sadness of the situation, circuit courts have largely held in a variety of situations that states have no duty under the exceptions enumerated in *DeShaney* to do more.

a. The Special Relationship Exception

Despite compulsory attendance laws and the fact that schools act *in loco parentis* for their students, nearly all courts addressing the question of whether schools stand in a *DeShaney* special relationship with their students have held they do not.

The analysis concerning special relationships largely stems from the Supreme Court's language in *DeShaney* itself. In *DeShaney*, the Supreme Court held that while generally there is no duty for the state to protect individuals from private violence, a special relationship between the state and the individual might give rise to such a duty. *DeShaney*, 489 U.S. at 198. The Court recognized such a right to protection in the case of prisoners, because the prisoner's lack of liberty made it impossible to care for himself, and, therefore, made it just that the state would provide such care. *Id.* at 199, citing *Estelle v. Gamble*, 429 U.S. 97 (1976). The Court also recognized such a duty for the state in the case of involuntarily committed mental patients because these individuals similarly could not completely care for themselves due to their custodial relationship with the state. *DeShaney*, 489 U.S. at 199, citing *Youngberg v. Romeo*, 457 U.S. 307 (1982).

Case law concerning violence in schools shows it is notoriously difficult to establish this type of relationship between public schools and their students. Even in cases where the students are disabled and significantly impaired in their abilities to care for themselves, most courts hold that the relationship between schools and students is not sufficiently custodial to allow this type of liability to attach.

In *Walton v. Alexander*, 20 F.3d 1350 (5th Cir. 1994), rehearing *en banc*, *Walton v. Alexander*, 44 F.3d 1297 (5th Cir. 1995), the plaintiff was a male student at the Mississippi School for the Deaf, a residential boarding school for deaf and hard of hearing students. *Walton*, 20 F.3d at 1352. The plaintiff was described as "a handicapped child who lacks the basic communications skills that a normal child would possess." *Id.* at 1355. He was twice sexually assaulted by another male student at the school. *Id.* at 1353.

A panel of the Fifth Circuit originally held that the school's twenty-four hour custody of the student, the strict rules that the student was not free to leave, and the fact that most Mississippi families of deaf students could not afford to send their children to alternative private schools created a "significant custodial component" and a special relationship between the school and the student. *Id.* As such, the plaintiff's abuse at the hands of the other student created a Fourteenth Amendment Due Process violation. *Id.* This decision, however, was reversed by an *en banc* Fifth Circuit the next year. *Walton*, 44 F.3d at 1304-05. The court held that the student was not involuntarily confined by the school because the

student had voluntarily enrolled in the school without coercion by the state. *Id.* at 1305. The court therefore held that the student could not assert a due process claim.

In a similar case, the Ninth Circuit also declined to find that the disabled condition of a student created a special relationship. *Patel v. Kent Sch. Dist.*, 648 F.3d 965 (9th Cir. 2011). In *Patel*, the victim was a developmentally disabled high school student. *Id.* at 968. The Ninth Circuit noted that the student's disabilities "affected her day-to-day life in various ways" and "[s]he was sometimes unable to complete basic tasks like holding her eating utensils correctly, blowing her nose, and zipping her clothes." *Id.* An Individualized Education Plan ("IEP") was drawn up for the student during her freshman year calling for her to be escorted by adults to and from all classes and to the bathroom. *Id.* at 969. Despite this, the plaintiff was sent to the bathroom alone by her special education teacher up to five times a day. *Id.* at 969. By the spring of her sophomore year, the plaintiff's mother learned that she was having sex in the bathroom with another developmentally disabled student. *Id.*

Despite the IEP and the developmental condition of the plaintiff, the Ninth Circuit held that the school and the plaintiff's teacher did not have a special relationship with the plaintiff and that there could therefore not be a due process violation. *Id.* at 973-74. The court held specifically that compulsory attendance and the school's status as in loco parentis did not confer a special relationship. *Id.* at 973. The court further held that the plaintiff's IEP did not create a greater obligation because it did not increase the school's custody or restraint over her. *Id.*

b. The State-Created Danger Exception

While the elements of state-created danger vary somewhat between the circuits, in general the elements are 1) foreseeable harm; 2) affirmative state action creating or increasing the risk to the victim; 3) a relationship between the state and the plaintiff that created a special danger to the victim greater than the risk to the public at large; and 4) a degree of state culpability, usually deliberate indifference.

An illustration of a case where state-created danger theory was found not applicable is *McQueen v. Beecher Cmty. Sch.*, 433 F.3d 460 (6th Cir. 2006). In *McQueen*, a student was fatally shot when her teacher left her and a few other students unsupervised in a classroom and one of the students pulled out a gun. *Id.* at 463. The shooter had previously been involved in several violent incidents at school, which the *McQueen* Plaintiffs claim should have gotten him expelled. *Id.* at 462. The plaintiff brought a 1983 against the teacher under a state-created danger theory. *Id.* at 463. The Sixth Circuit dismissed the plaintiff's claims on

summary judgment. *Id.* at 470. The court held that the plaintiff had shown that she was more likely to be injured than the general public--obviously the shooter was more likely to shoot someone in the room than members of the general public. *Id.* at 468. However, the plaintiff had failed to prove that the teacher took affirmative action putting her at risk--it was pure speculation to say that the shooting would not have taken place had the teacher been in the room--and had failed to prove the teacher acted with deliberate indifference--there was no evidence the shooter either had a gun or would use it against his classmates. *Id.* at 466; 469-70.

A different holding was reached by the Third Circuit in *L.R. v. Sch. Dist. of Philadelphia*, 836 F.3d 235 (3d Cir. 2016). In *L.R.*, a kindergarten student was sexually assaulted off school premises after her teacher allowed her to leave her classroom with an unidentified adult. *Id.* at 240. The adult had come to pick up the child and the teacher had, per district policy, requested to see his identification. *Id.* When he did not produce it, the teacher allowed the child to leave with the man anyway. *Id.* The court held that there was state-created danger because the teacher had taken affirmative action and greatly changed the child's status quo by releasing her to the perpetrator. *Id.* The court noted that kindergarten classrooms are often very tightly controlled, highly protective environments and that in releasing the student the teacher had taken affirmative action to change the child's level of protection. *Id.* at 244. The court also held the harm was a direct result of the teacher's conduct, as the perpetrator would have had no access to the child had the teacher not released her. *Id.* The court also believed the teacher's actions shocked the conscience and was a case of deliberate indifference, as the teacher had plenty of time to make a decision about whether or not to release the student and knew or should have known of the grave risk of releasing the child to an unidentified adult. *Id.* The court also held the student was a foreseeable victim as the district's policy of checking identification was enacted specifically for the benefit of young children such as the plaintiff. *Id.* at 247.

B. State Court Litigation

There has also been significant state court litigation about school shootings, most notably, a case brought by the families of two victims of the Virginia Tech shooting went to the Virginia Supreme Court in 2013. While the case was eventually decided in favor of the school, the original jury trial awarded \$4,000,000 to the families. *Commonwealth of Virginia v. Peterson*, 749 S.E.2d 307, 310 (Va. 2013).

Notably, the trial court in the Virginia Tech shooting was mostly persuaded by the ability the school had to warn students of a live shooter situation and its failure to give the students any warning. The shooting began at 7:30 a.m. in a residence hall. *Id.* at 308. When the incident was investigated by the Virginia Tech Police Department, the investigators did not find the shooter and believed the shooting was a domestic incident perpetrated by the female victim's gun-enthusiast boyfriend. *Id.* The investigators did not send out a blast email that would have warned all students of the possibility of a live shooter. *Id.* The University Police department continued with this stance even after it became clear the boyfriend was not the shooter. *Id.* The University President and other administrators were also notified of the events, but they chose not to release the information about the shooting to students until 9:26 a.m., and they still did not notify students that there had been a fatality or call for a campus lockdown. *Id.* At around 9:45 a.m., the same shooter opened fire in a classroom building, killing several additional students, including the students whose estates brought the suit. *Id.* at 310. The case was tried before a jury who awarded \$4,000,000 to the victims' families.

The Supreme Court of Virginia reversed the verdict, holding that the facts did not give rise to a duty to warn students of the danger of third party criminal acts. *Id.* at 311. The court noted that Virginia law does not generally confer a duty to warn or protect others from the criminal acts of a third party unless there is "an imminent probability of injury" from a third party criminal act." *Id.* at 312. The court went on to hold that in this case, no such probability existed as the school did not know who the shooter was or that he continued to pose a threat to others. *Id.* at 313.

Thus, evidence shows that it is unlikely, but not impossible, for a school district, teacher, or administrator to be held liable for violence toward a student by a third party, non-state actor.

3. Legal and Practical Issues Concerning Use of Armed School Marshalls

Despite a lack of liability, many school officials feel that they have a moral imperative to protect students using armed guards. As such, the next question for districts and their counsel is whether such a plan is legally and practically feasible.

A. Legal Issues

i. The Gun Free Schools Act 18 U.S.C. 922(q)

The Gun Free Schools Act prohibits the knowing possession of a firearm within a “school zone” as defined by the Act. 18 U.S.C. 922(q). A “school zone” under the Act is defined as “in, or on the grounds of, a public, parochial or private school” and “within a distance of 1,000 feet from the grounds of a public, parochial or private school.” 18 U.S.C. 921(25). “School” is defined as “a school which provides elementary or secondary education, as determined under State law.” 18 U.S.C. 921(26).

Pursuant to the Gun Free Schools Act, exceptions are made if:

(ii) if the individual possessing the firearm is licensed to do so by the State in which the school zone is located or a political subdivision of the State, and the law of the State or political subdivision requires that, before an individual obtains such a license, the law enforcement authorities of the State or political subdivision verify that the individual is qualified under law to receive the license;

...

(iv) by an individual for use in a program approved by a school in the school zone;

(v) by an individual in accordance with a contract entered into between a school in the school zone and the individual or an employer of the individual;

(vi) by a law enforcement officer acting in his or her official capacity; or

18 U.S.C. 922(q).

Thus, the Gun Free Schools Act does not prevent schools from implementing programs allowing non-law enforcement to provide armed security in their schools.

ii. State Laws Authorizing Guns on Campus

In addition to federal laws, school districts wishing to provide schools with armed guards will want to look to their individual state laws concerning guns on school property. Most states have laws prohibiting guns on campus, however, similar to the Gun Free Schools Act, most state laws provide an exception for those authorized by a school district to carry guns. In addition, many states have newly enacted statutes outlining procedures to be followed by districts authorizing teachers and staff to carry firearms in their schools. A few of these are detailed below:

Alabama: Ala. Code § 45-30-103 allows principals of schools in Franklin County Alabama to create volunteer emergency security forces consisting of current employees of the school, retired employees of the school, and residents of the school district to protect schools.

Arkansas: Ark. Code Ann. § 5-73-119 allows authorized persons to carry concealed handguns onto the property of private schools.

Kansas: Kan. Stat. Ann. § 75-7c10 allows the governing body of a unified school district to permit employees legally qualified to carry concealed handguns to carry a concealed handgun in any building of such institution, if the employee meets such institution's own policy requirements.

Ohio: Ohio Rev. Code. Ann. § 2923.122 prohibits the possession of firearms, deadly weapons, dangerous ordnance, and objects indistinguishable from firearms within a “school safety zone,” which is defined as a school building, premises, or activity. The statute specifically does not apply to a law enforcement officer who is “authorized to carry deadly weapons or dangerous ordnance and is acting within the scope of the[ir] duties, a security officer employed by a board of education or governing body of a school during the time that the security officer is on duty pursuant to that contract of employment, or any other person who has written authorization from the board of education or governing body of a school . . . and who conveys or possesses the deadly weapon or dangerous ordnance in accordance with that authorization”

Oklahoma: Okla. Stat. Ann. tit. 21, § 1280.1 allows private schools to authorize a person licensed pursuant to the Oklahoma Self-Defense Act to carry concealed or unconcealed weapons onto private school property or private school buses or other vehicles. The statute also stipulates, “Except for acts of gross negligence or willful or wanton misconduct, a governing entity of a private school that adopts a

policy which authorizes the possession of a weapon on private school property, a school bus or vehicle used by the private school shall be immune from liability for any injuries arising from the adoption of the policy.”

South Dakota: S.D. Codified Laws § 13-64-1, et seq. lays out a plan for school boards to implement a “school sentinels” program. The program allows a board to “create, establish, and supervise the arming of school employees, hired security personnel, or volunteers in such manner and according to such protocols as the board may believe to be most likely to secure or enhance the deterrence of physical threat and defense of the school, its students, its staff, and members of the public on the school premises against violent attack.”

Tennessee: Tennessee has three statutes concerning the authorization of school marshals. Tenn. Code Ann. § 49-50-803 allows for carrying of firearms on private school property by persons authorized by the board or governing entity of the school. Tenn. Code Ann. § 49-6-815 allows for authorized faculty and staff who are former law enforcement with proper training to carry firearms on public school property. Tenn. Code Ann. § 49-6-816 allows “distressed rural counties” to authorize properly trained faculty or staff who are not former law enforcement to carry firearms on school property.

Texas: Texas state law specifically addresses arming non-law enforcement in schools, terming them “school marshals.” Tex. Crim. Proc. Code Ann. art. 2.127. These officials are given the authority to “make arrests and exercise all authority given peace officers.” *Id.* Texas’ statutes call for the Texas Commission on Law Enforcement to establish and maintain a training program for school marshals to certify them. Tex. Occ. Code Ann. § 1701.260. The statutes also limit the number of marshals that may be appointed by districts, conditions under which the appointed marshals may carry concealed weapons, and state that the names of those appointed as marshals can be maintained as confidential by the district and are not subject to open records requests under Texas law.

iii. Liability for Arming School Staff

Once it is established that it is legal to arm non-law enforcement in schools, the next concern is what liability is created for the individuals armed, school administrators, and the district. While the intentions of administrators in arming school staff and those of the individuals carrying guns on campus are undoubtedly pure, it is not difficult to imagine that arming teachers and other non-law enforcement opens a veritable Pandora’s box of liability. For example, improperly (or even properly) stored guns may fall into the wrong hands and

being used for nefarious purposes. Additionally, in the case of an emergency, tensions and adrenaline run high creating an apt case for bystander injury.

a. Unauthorized Use

In the case of the guns falling into unauthorized hands, the issue is once again the responsibility of the district to protect students from the wrongful acts of a third party under the Fourteenth Amendment's Due Process Clause. Thus, the analysis to be undertaken is similar to that of *DeShaney* and its progeny explained, *supra*. As noted above, liability for districts under the *DeShaney* exceptions has previously been very low risk. However, that may not continue if districts authorize and encourage staff to carry firearms.

Nothing about arming teachers would change the analysis of whether students and schools have a special relationship. Giving guns to staff does not make the relationship between teachers and their students any more custodial as parents still have the primary responsibility for their care.

However, a policy and practice of putting guns on school property might change the analysis for the state-created danger exception. If districts enact policies bringing guns onto campus, this changes the current situation significantly. Similar to the kindergarten classroom in *L.R. v. Sch. Dist. of Philadelphia*, schools are traditionally a place where guns are forbidden or allowed only under very limited circumstances. *L.R.*, 836 F.3d at 247. Similar to the safety of a kindergarten student in her classroom, if a district enacts a policy to arm school staff, it has arguably put a gun within firing distance of children who did not previously face that risk, making a better case for state-created danger than previously existed.

b. Liability for Misfire

In the case of a staff misfire, it is a state actor who has created the harm, thus *DeShaney* and its progeny would not be applicable. Instead, the liability would more likely be comparable to liability for police liability for accidental bystander shootings. In such cases, courts will normally not hold officers responsible unless their actions "shock the conscience." For example, in *Claybrook v. Birchwell*, 199 F.3d 350, 360 (6th Cir. 2000), a bystander was struck by a stray bullet during the course of a police shootout. *Id.* at 354. The Sixth Circuit refused to hold officers liable for her because the officer had not acted "maliciously or sadistically" toward the injured party and his actions therefore did not violate the Fourteenth Amendment Due Process clause.

c. *Monell* Liability

In addition, a person injured by a gun on campus might also attempt to make out a claim under *Monell v. Dep't of Soc. Servs. of City of N.Y.*, 436 U.S. 658, 694 (1978). As a local governmental entity, a school district cannot be held vicariously liable under 42 U.S.C. 1983 for an injury inflicted solely by its employees or agents. *Id.* at 694. But, under the Supreme Court's decision in *Monell*, a school district could only be liable for an accidental injury as a result of its armed guards if execution of its policy or custom caused the injury. *Id.*

In *Monell* cases, plaintiffs generally establish municipal liability by 1) pointing to an officially adopted policy, 2) pointing to a custom or practice so pervasive and long-standing so as to have the force of law, 3) pointing to a policy of inadequate training or supervision, or 4) pointing to a particular decision or act by a final policymaker.

In the cases of unauthorized use or armed personnel hitting bystanders, the most likely *Monell* claim is that the school district failed to train and supervise armed staff. Under this approach, a municipality may be held liable if "the failure to train amounts to deliberate indifference to the rights" of people with whom the municipal employee or agent comes into contact. *City of Canton, Ohio v. Harris*, 489 U.S. 378, 388 (1989). To prove deliberate indifference, the plaintiff may argue 1) there was an obvious need to train or 2) a pattern of constitutional violations is apparent putting the entity on constructive notice of a need to train. *Blum*, *supra*, at 843. In addition, the plaintiff must prove that the inadequate training caused the underlying violation. *City of Canton*, 489 U.S. at 391.

If a district wishes to arm teachers and staff, there is a great need to provide adequate training and supervision. Using a weapon under stress is a very difficult proposition for which most educators are not prepared. Law enforcement officers have a missed shot rate between 52 and 82%. *See Weatherby, supra*, at 142. It's not hard to imagine that the misfire rate for teachers, who do not use weapons as part of their jobs everyday and have considerably less training, would be much higher, creating much greater liability for districts. In one highly publicized case, Arkansas State Senator Jeremy Hutchinson, a vocal advocate for arming school personnel, accidentally shot a "teacher" when participating in an active shooter training scenario. Brenda Bernet, *School Districts Hoping to Keep Security Licenses*, Ark. Dem. Gaz. August 28, 2013. Notably, Senator Hutchinson said that the experience did not change his opinion on arming teachers.

B. Practical Issues

i. Insurance Coverage

One of the most practical and pressing problems of a school district that wishes to arm its teacher or other staff is providing insurance for that risk through the procurement of insurance.

Unfortunately, finding coverage for armed guards in schools is not always easy. For example, at the beginning of 2013, at a time when thirty legislatures were considering new statutes detailing parameters for arming teachers and staff, some insurance companies simply said “no.” EMC, the largest school insurer in Kansas, wrote a letter to all of its agents telling them that the company would not continue to provide insurance coverage to any district that armed its staff. Steven Yaccinno, *Schools Seeking to Arm Employees Hit Hurdle on Insurance*, N.Y. Times, July 7, 2013. Still other companies warned that increased premiums would follow district decisions to arm teachers and staff. *Id.*

ii. District Policy

A district looking to arm their teachers and staff would like need to answer, at a minimum, the following questions in district policy:

- Does state law state allows civilian staffers to carry firearms?
- What individuals within the district will be authorized? What is the approval process?
- What screening should be required for those individuals authorized to carry firearms (background checks and mental health examinations)? How will the district revoke this authorization if that becomes necessary? Is such authorization is automatically revoked if such employee receives any form of discipline related to a firearm and the revocations are not subject to any grievance or hearing process or procedure?
- What procedures will be used to secure the firearms during and after school hours?
- How will the district keep track of records relating to the authorization of individuals to carry firearms on campus? (i.e. valid, current permits, annual criminal background check requirements, and annual mental health examination)
- What type of firearms will be allowed?
- Who will purchase the firearms? Who will pay for their upkeep? How with the district verify upkeep if the firearms are privately owned?

- What type of ammunition will be authorized? (Is the district going to specify only frangible ammunition to prevent ricochets? Does the damage done by frangible munitions in the event of a misfire present too great a risk?)
- How is the district going to train staff on appropriate use of force and use of deadly force, storage, and security?
- Will the district shared its policy with local law enforcement agencies likely to respond to an event involving firearms? What will be the interaction between local law enforcement and armed staff?
- Does the district have a communication plan in place to deal with parents and media inquiries in the event of firearm discharge?

**POLITICAL SUBDIVISION
LIABILITY FOR CIVIL
RIGHTS CLAIMS ARISING
FROM STOPS, DETENTIONS,
AND ARRESTS OF OPEN
CARRIERS**

FDCC Winter Meeting
Charleston Place Hotel
Charleston, South Carolina
March 6 – March 10, 2017

Presented By:
Jane M. Lynch
GREEN & GREEN, LAWYERS
Dayton, Ohio

I. WHAT IS OPEN CARRY?

A. Open Carry Defined

In the vernacular, “open carry” is a manner of carrying a firearm where the firearm, or some part of it, is visible to the public. The legal definition of “open carry” varies by jurisdiction.

Some jurisdictions affirmatively define open carry in order to prohibit it. For example, in Florida:

“[e]xcept as otherwise provided by law . . . it is unlawful for any person to openly carry on or about his person any firearm It is not a violation of this section for a person licensed to carry a concealed firearm . . . to briefly and openly display the firearm to the ordinary sight of another person, unless the firearm is *intentionally* displayed in an *angry or threatening manner*, not necessarily in self-defense.”

Fla. Stat. 790.053(1).

In other jurisdictions, open carry may be legal simply because it is not prohibited by state or local law. *Compare* Ohio Const. Art. I, § 4, *with* Ohio Revised Code Chapter 2923 (Ohioans have a right to bear arms generally, but nothing in the Weapons Control Act prohibits bearing arms openly.) In other jurisdictions still, open carry may be illegal because the carrying of firearms is generally prohibited, and no exception exists. *See generally* 430 ILCS 65 (Illinois law prohibits carrying firearms unless the actor has a firearms owner ID card, which itself only allows the actor to carry a firearm that is “completely or mostly concealed from view of the public.”)

B. Open Carry Trends

Many more jurisdictions than ever before now recognize open carry as a lawful activity. The Washington Post declares America a “country with relaxing gun laws.” *In Jim Cooley’s open carry America, even a trip to Walmart can require an AR-15*, September 17, 2016. Open carry is legal in the overwhelming majority of jurisdictions (though some require a license). According to the Law Center to Prevent Gun Violence, only three states (California, Florida, and Illinois) prevent open carry altogether. New York and South Carolina prohibit open carry of handguns, but not long guns. Massachusetts, Minnesota, and New

Jersey prohibit open carry of long guns, but not handguns. In every other jurisdiction, open carry is lawful, though sometimes only with a license.

There is disagreement, even among Second Amendment supporters, as to whether open carry is prudent. Alan Gottlieb, the founder of the pro-gun Second Amendment Foundation, noted that while he is “all for open carry laws,” he believes “flaunting it is [not] very productive for our cause” and “just scares people.” Ian Urbina, *Locked, Loaded, and Ready to Caffeinate*, N.Y. Times, March 8, 2010, at A11. Gottlieb’s sentiment is reflected in the significant increase in not only the percentage of Americans who openly carry firearms, but also the significant increase in other citizens who call police to complain of a “man with a gun” when they encounter open carriers. As officers come into contact with open carriers more frequently, we can expect an increase in the number of civil rights suits filed against officers who are attempting to investigate possible threats and/or keep the peace at the intersection of a citizen’s right to open carry and the officer’s duty to ensure public safety.

II. THE CHANGING LEGALITY OF OPEN CARRY.

Open carry is a highly politicized issue that has seen significant recent changes at the federal, state, and local levels.

A. D.C. v. Heller, 554 U.S. 570, 128 S.Ct. 2783, 171 L.Ed.2d 637 (2008)

This case declared the federal right to keep and bear arms a *fundamental, individual right*, but failed to provide a standard of review for evaluating the validity of subsequent laws that are designed to or have the practical effect of restricting the free exercise of that right. The Circuit Courts are split as to whether that standard should be *strict scrutiny*, *intermediate scrutiny*, or *rational basis*. It is unlikely the split will be resolved until the Supreme Court once again has a full bench. Nevertheless, practitioners must monitor the standard of review for firearms laws to gauge the number of open carry / civil rights cases that may be coming in the future. If *strict scrutiny* applies, state and local statutes which presently limit open carry may be invalidated, leading to a rise in open carry / civil rights suits against municipalities and law enforcement officers.

B. Strict Scrutiny of Laws That Restrict Firearms Rights

The most stringent standard of review is strict scrutiny, under which a statute will be struck down unless the law is “narrowly tailored” to advance a “compelling” governmental interest, and is the “least restrictive means” to

achieve that interest. *See, e.g., U.S. v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, 813, 120 S.Ct. 1878, 146 L.Ed.2d 865 (2000). Virtually all laws that are examined under strict scrutiny are struck down. In evaluating the constitutionality of laws that restrict the right to keep and bear arms, the Sixth Circuit originally “prefer[red] strict scrutiny over intermediate scrutiny.” *Tyler v. Hillsdale County Sheriff’s Dept.*, 775 F.3d 308, 328 (6th Cir. 2014). However, on *en banc* review the Sixth Circuit reversed and vacated that decision cautioning “against imposing too high a burden on the government to justify its gun safety regulations, particularly where Congress has chosen to rely on prior judicial determinations that individuals pose a risk of danger to themselves or others.” *Tyler v. Hillsdale Cty. Sheriff’s Dept.*, 837 F.3d 678, 2016 WL 4916963, at *9 (6th Cir. 2016) (*en banc*).

The Fourth Circuit applied strict scrutiny to an assault weapons ban, and noted that the standard of review was only appropriate because the ban limited possession of weapons within the home. *Kolbe v. Hogan*, 813 F.3d 160, 182 (4th Cir. 2016) (*reh’g granted*) 636 F. App’x. 880 (4th Cir. 2016). This matter has been reheard, but as of October 31, 2016, no decision has been filed.

Judge Leon of the D.C. District Court also applied strict scrutiny review to a statute allowing the chief of police to refuse issuance of concealed carry licenses for “good reason” or “proper reason.” *Grace v. D.C.*, No. CV 15-2234 (RJL), 2016 WL 2908407, at *11 (D.D.C. May 17, 2016). Judge Leon also recognized that under the DC Circuit’s precedent, a means-end analysis should be used to consider whether strict or intermediate scrutiny is appropriate when determining the application of the Second Amendment. “This requires examining the nature of the conduct being regulated and the degree to which the challenged law burdens the right. A regulation that imposes a substantial burden upon the core right of self-defense protected by the Second Amendment must have a strong justification, whereas a regulation that imposes a less substantial burden should be proportionately easier to justify. In other words, the former receives strict scrutiny, while the latter receives intermediate scrutiny.” *Id.* An appeal has been taken from that decision, but as of February 16, 2017, the matter is still under the DC Circuit’s consideration.

C. Intermediate Scrutiny of Laws That Restrict Firearms Rights

Under intermediate scrutiny, a law will be struck down unless the state can establish that the statute is “substantially related” to an “important governmental objective.” *Clark v. Jeter*, 486 U.S. 456, 461, 108 S.Ct. 1910, 100 L.Ed.2d 465 (1988). This is the majority rule for evaluating whether laws that restrict the right to keep and bear arms are unconstitutional. *See, e.g., Tyler*, 2016

WL 4916963, at *9; *U.S. v. Booker*, 644 F.3d 12 (5th Cir. 2011); *U.S. v. Yancey*, 621 F.3d 681 (7th Cir. 2010); *Friedman v. City of Highland Park, Illinois*, 784 F.3d 406 (7th Cir. 2015) (refusing to characterize its test as intermediate scrutiny, but effectively imposing a variant of intermediate scrutiny); *Heller v. D.C.*, 670 F.3d 1244 (D.C. Cir. 2011) (not the original *Heller* case, but a subsequent appeal challenging further aspects of the District’s firearms regulations); and *Fyock v. Sunnyvale*, 779 F.3d 991 (9th Cir. 2015). States have also implemented intermediate scrutiny for review of state and local statutes that restrict the right to keep and bear arms. *See, e.g., Norman v. State*, 195 So.3d 205, 212 (Fla. 4th DCA 2015).

D. Rational Basis Review of Laws That Restrict Firearms Rights

The least restrictive standard of review is rational basis, under which a statute will be affirmed so long as it is “rationally related” to a “legitimate government interest.” *See U.S. v. Carolene Products Co.*, 304 U.S. 144, n.4, 58 S.Ct. 778, 82 L.Ed. 1234 (1938). Virtually all statutes are affirmed under the rational basis standard of review. The Supreme Court suggested that rational basis is an improper test for assessing the validity of laws that limit the right to keep and bear arms. *Heller*, 554 U.S. at n.27 (rational basis “could not be used to evaluate the extent to which a legislature may regulate a specific, enumerated right, be it the freedom of speech, the guarantee against double jeopardy, the right to counsel, or the right to keep and bear arms.”) No jurisdictions have attempted to use rational basis as the standard of review since the *Heller* decision was released.

III. DEFENDING AN OPEN CARRY 1983 CLAIM

A. Open Carry As *Ipsa Facto* Illegal

Defending a civil rights suit against an officer for stopping, detaining, and/or arresting an open carrier is a straightforward task when open carry itself is a crime. Qualified immunity protects government officials “from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.” *Harlow v. Fitzgerald*, 457 U.S. 800, 818, 102 S.Ct. 2727, 73 L.Ed.2d 396 (1982). A stop, detention, or arrest based on probable cause does not give rise to liability under 42 U.S.C. § 1983. *See, e.g., Devenpeck v. Alford*, 543 U.S. 146, 152-53, 125 S.Ct. 588, 160 L.Ed.2d. 537 (2004); *Safford Unified Sch. Dist. No. 1 v. Redding*, 557 U.S. 364, 370, 129 S.Ct. 2633, 174 L.Ed.2d 354 (2009). As such, the arrest of a person openly carrying in a jurisdiction that criminalizes open carry would most likely not be constitutionally prohibited.

However, there remains a very real possibility that the right to openly carry may be protected under the Second Amendment. At this point, it does not appear that any courts have directly addressed this issue. *See Peruta v. Cty. of San Diego*, 824 F.3d 919, 942-25 (9th Cir. 2016) (determining that the Second Amendment does not protect the right to carry a **concealed** firearm outside the home but reserving the question of open carry); *see also Grace*, 2016 WL 2908407, at *7 (recognizing that the Second Amendment protects the right to carry a firearm outside of the home and historically allowed for prohibition of concealed carry so long as open carry was permitted, but not directly addressing the issue of whether open carry is specifically protected under the Second Amendment). If the Second Amendment does indeed provide a right to openly carry, then the state law prohibitions against open carry would most likely be determined to be unconstitutional, thereby eliminating the fact that a person was openly carrying as being a valid basis for an arrest, even in jurisdictions where such actions are prohibited. Nevertheless, given the fact that the law is currently not clear as to whether the Second Amendment includes the right to openly carry, the arrest of a person for openly carrying firearms *before* that right is recognized would not violate the plaintiff's *clearly established* rights and the officer would still be entitled to immunity. *Chesney v. City of Jackson*, 171 F.Supp.3d 605, 619-22 (E.D. Mich 2016).

B. Open Carry As Illegal Under Other Statutes.

Even if open carry is generally legal in a particular jurisdiction, other factors—including the manner and location of an incident—may bring the plaintiff's conduct within the scope of criminal laws, such as those that criminalize brandishing, disorderly conduct, and trespassing. For purposes of the civil rights act, it is immaterial whether the officer subjectively realized that the plaintiff's conduct was potentially criminal under other statutes; the reasonableness of a stop, detention, arrest, or use of force is evaluated for objective reasonableness. *See, e.g., Graham v. Connor*, 490 U.S. 386, 109 S.Ct. 1965, 104 L.Ed.2d 443 (1989). Accordingly, it is imperative to determine whether a plaintiff's conduct in openly carrying a firearm resulted in the violation of any other criminal statutes.

The question of whether an officer is entitled to qualified immunity depends on whether there was **objective** evidence supporting either reasonable suspicion sufficient to justify an investigatory detention or pat down and/or probable cause to sufficient to justify an arrest. Reasonable suspicion is defined as “specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant” an intrusion upon the constitutional rights of a suspect. *Terry v. Ohio*, 392 U.S. 1, 21, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968).

Probable cause “is incapable of precise definition” but includes “a reasonable ground for belief of guilt . . . particularized with respect to the person to be searched or seized.” *Maryland v. Pringle*, 540 U.S. 366, 370, 124 S.Ct. 795, 157 L.Ed.2d 769 (2003). An officer’s **subjective** intent, even if improper (i.e. he stopped and/or arrested the plaintiff for openly carrying a firearm) is not determinative of whether the officer is entitled to qualified immunity. *Boyd v. Baeppler*, 215 F.3d 594, 600 (6th Cir. 2000) (the relevant inquiry is “what a reasonable police officer would believe to be lawful based upon the information then possessed, not what the officer subjectively may have believed.”)

Accordingly, practitioners must use care to investigate all the facts and circumstances surrounding the interaction described in the complaint. An officer’s liability may hinge on particular details that the officer may have overlooked at the time the decision was made to detain or arrest an open carrier, or which the officer may not feel are worthy of discussion during an initial interview.

Below is a brief discussion of several laws that may become relevant in evaluating whether a stop, detention, or arrest of an open carrier may have been lawful even in a jurisdiction where open carry is a legal activity. This list is merely illustrative and by no means exhaustive. Lawyers should take into consideration the unique facts and circumstances of every case, along with the criminal laws in the particular jurisdiction where a case originates.

1. Open Carry As “Brandishing”

Brandishing is an offense in several jurisdictions. *See, e.g.* Wash. Rev. Code Ann. 9A.41.270 (criminalizing “display with an intent to intimidate” or in a manner such as to “warrant alarm for the safety of other persons.”)

2. Open Carry As “Disorderly Conduct”

Most states have some version of a crime usually called disorderly conduct, which criminalizes an assortment of relatively minor behaviors that society generally deems inappropriate including: begging, public intoxication, loitering, and notably, causing public disturbances. *See, e.g.*, Cal. Penal Code § 647.

An example of the application of disorderly conduct violations in the context of open carrying can be found in the case of Jesus Gonzales—someone who was “active in Wisconsin’s ‘open carry’ movement”—was the subject of two open carry arrests that culminated in one civil action. The first incident occurred in 2008 when Gonzales openly carried a handgun into a home improvement store.

Gonzalez v. Village of West Milwaukee, 671 F.3d 649 (7th Cir. 2012). A store employee asked Gonzalez to put his gun in his car if he wanted to keep shopping. Gonzalez initially refused, and then agreed after employees said they would call the police if he did not comply. Meanwhile, an employee did call the police to complain that Gonzalez was “creeping people out” and making customers uncomfortable and nervous. By the time police arrived, Gonzalez had already disarmed, finished shopping, and was putting his purchases in his car. Police asked Gonzalez where his gun was and Gonzalez refused to answer. Police then arrested Gonzalez for disorderly conduct. In 2009, a similar incident occurred at a Wal-Mart. A manager called police to express concern over the fact that it was very late, Gonzalez was visibly armed, and was attempting to purchase ammunition. The responding officer located Gonzalez, and commanded him, at gunpoint, to “Freeze.” Gonzalez evidently complied, and the officer arrested Gonzalez for disorderly conduct. The officer called the prosecutor for guidance on how to proceed with booking, but released Gonzales the same evening when nobody answered his call. He did not return Gonzales’ gun. Two weeks later, the prosecutor called Gonzalez to say that the charges would be dismissed and that Gonzalez could retrieve his gun from the police. Gonzalez eventually sued for both incidents. The officers moved for summary judgment on qualified immunity, and the district court granted the motions. At the time, Wisconsin’s disorderly conduct statute prohibited conduct that “. . . tends to cause or provoke a disturbance.” Wis. Stat. Ann. § 947.01(1). The District Court ultimately found that Gonzalez’ conduct had such a tendency, and that officers had reasonable suspicion to detain and even arrest Gonzalez for disorderly conduct. On Appeal, the Circuit Court disapproved of the District Court’s “categorical” reasonable suspicion analysis, and suggested that it was improper to find that openly carrying a firearm was or could be disorderly conduct in all scenarios. However, the Circuit Court affirmed summary judgment on qualified immunity because Wisconsin’s constitutional right to keep and bear arms was new, and even if there was an implicit right to openly carry firearms, that right was not clearly established at the time of Gonzalez’ arrest.

Between the District Court’s order of summary judgment in favor of the defendants and the 7th Circuit’s opinion affirming it, the state of Wisconsin amended the disorderly conduct statute such that, in the absence of other “facts and circumstances that indicate a criminal or malicious intent,” a person does not commit disorderly conduct by going armed with a firearm, whether carried openly or concealed. 2011 Wisc. Act 35, § 86. Accordingly, the law in Wisconsin is now that open carry, by itself, is not disorderly conduct. However, carrying a firearm openly or concealed may become disorderly conduct if there are other factors from which an officer might infer a criminal or malicious intent on the part of the

armed citizen. Interestingly, Gonzales was convicted for a homicide during that same interval of time—something that may have had an impact on the Circuit Court’s analysis (though the Court specifically denied it at the outset of the opinion).

In another applicable case, in 2010 Richard Burgess openly carried a pistol into a pool hall. *Burgess v. Town of Wallingford*, 569 Fed.Appx. 21 (2d Cir. 2014). He refused the manager’s request to conceal the weapon, and refused a request from another patron to the same effect. Shortly after, Burgess decided to leave. Both the manager and the other patron had already called the police, who arrived after Burgess left, but while he was standing outside the pool hall. They detained Burgess, and called their lieutenant to find out whether Burgess’ conduct amounted to an offense. The police arrested Burgess and charged him with disorderly conduct. Later the same evening his weapon was returned and he was released. The charge was later dropped. Under Connecticut law, disorderly conduct occurs when a person “with intent to cause inconvenience, annoyance or alarm, or recklessly creating a risk thereof . . . by offensive or disorderly conduct, annoys or interferes with another person” Conn. Gen. Stat. 53a-182. The District Court found that the officers had probable cause to believe that Burgess intended or was reckless to the fact that his conduct annoyed and/or interfered with others, and therefore, that Burgess’ detention and arrest for disorderly conduct was lawful.

3. Open Carry as Trespassing

In 2014, the manager of a Dunkin’ Donuts called police to report that there was a man in the restaurant armed with an assault rifle. *Baker v. Smiscik*, 49 F.Supp.2d 489, 492 (E.D. Mich. 2014). The manager wanted police to help him ask the armed customer to leave. Police arrived to find James Baker having a cup of coffee and a donut “while openly carrying a pistol, a rifle, a copy of the U.S. Constitution, and a ‘recording device.’” One officer approached Baker with a weapon drawn. Police questioned Baker on why he was openly armed, and after Baker replied that he “open carries,” officers ordered Baker to place his hands on his head, and disarmed him. Officers demanded Baker’s ID, and when Baker refused to provide it, an officer took Baker’s wallet and searched for Baker’s ID. Officers restricted Baker’s movement within the shop. At some point during the stop, Baker attempted to put his copy of the Constitution in his pocket, but an officer forcibly prevented him from doing so. Approximately thirty minutes after the encounter began, a manager asked Baker to leave, officers escorted Baker to his car, returned his weapons, and watched him leave. Baker filed suit for violations of his Fourth and Fourteenth Amendment rights. Officers filed for summary judgment, claiming qualified immunity. The District Court (Judge

Goldsmith) found that the 911 call asking for help in making Baker leave might have given rise to a reasonable suspicion that Baker had violated the state's criminal trespass statute. More emphatically, the District Court seemed to believe that the mere fact Baker was armed justified a reasonable suspicion that "something was amiss" and there was a "risk to officer or public safety" that justified a detention and investigation. The District Court also mentioned "exigent circumstances" as a justification for the stop

4. Open Carry As Firearms Under Disability

James Baker surfaced again in *Baker v. Schwarb*, 40 F.Supp.3d 881 (E.D. Mich. 2014). In that case, police received a tip that "two teenage guys" were walking around with rifles. Police stopped Baker and his friend Shyama Nixon, both openly carrying rifles and handguns; Baker was dressed in all-black with sunglasses. The Court evidently found Baker and Nixon's appearance pertinent enough to include this photograph, taken at the time of the stop, in the official recorded opinion:



During a twenty-minute stop, officers verified Baker's identity and age, confirmed that the firearms were lawfully possessed, and then released both men. Baker again filed suit for violations of his Fourth and Fourteenth Amendment rights. Officers asserted qualified immunity, and moved for summary judgment. The District Court (Judge Cleland) found that officers had reasonable suspicion to justify the stop. While open carry itself was not illegal in Michigan, there was a state statute prohibiting minors from possessing firearms. The District Court zeroed in on the fact that the tipster reported "teenage guys" carrying firearms. When combined with Baker's particularly youthful appearance, the Court concluded that officers had reasonable suspicion to believe Baker and his friend

may have been minors. Additionally, the Court noted that the possession of firearms may have been a violation of city ordinances against creating a “public disturbance” and loitering. Judge Cleland appears to have drawn heavily from an unreported decision from Judge Roberts, of the same District Court, in a case involving virtually identical facts (but different plaintiffs and defendants) one year earlier. *See Combs v. City of Birmingham*, No. 12-14528, 2013 WL 4670699 (E.D. Mich. Aug. 30 2013).

5. Open Carry Of Potentially Illegal Guns

In 2012, Tennessee allowed openly carrying handguns, but not long guns, in state parks. *Embry v. Ward*, 695 F.3d 577 (6th Cir. 2012). After several citizen complaints of a man carrying an assault rifle in Radnor Lake State Natural Area, a park ranger arrived and spoke to Leonard Embry about the weapon Embry was openly carrying: an AK-47 pistol—essentially an AK-47 with a short barrel and no shoulder stock. Embry told the ranger the weapon was a pistol and therefore lawful, but the ranger was unsure. He released Embry and called his supervisor for guidance. Embry was directed to perform a “felony take down,” disarm Embry, and check the weapon. The ranger ordered Embry to the ground at gunpoint and took the weapon. Backup arrived from Nashville. After some communications with experts in Nashville, the ranger and his backup verified that the rifle met the definition of a pistol under Tennessee law, returned the weapon to Embry, and released him. Embry later filed suit for Fourth and Fourteenth Amendment violations. The Sixth Circuit found that the ranger had reasonable suspicion that Embry was illegally openly carrying a rifle because the weapon was only ½ inch shorter than the cut-off for making it a “rifle” under state law, and when viewed with the drum magazine Embry had loaded into the weapon, it was easily confused for a rifle. Further, Embry painted the tip of the weapon orange. The ranger felt that may have constituted a crime and wanted an opportunity to check the law. The Court found the ranger’s actions rooted in reasonable suspicion.

C. Consensual Stop of an Open Carrier

There is no liability for a police officer who approaches an open carrier and engages in a consensual conversation / investigation. *See Florida v. Bostick*, 501 U.S. 429, 434 111 S.Ct. 2382, 115 L.Ed.2d 389 (1991). While open carriers may balk at being questioned or “hassled” by police, as long as the exchange does not amount to more than a consensual encounter, there is no civil rights violation.

D. Detention Under Community Caretaker Standard

Since the Supreme Court of the United States ratified the notion that police have a function as “community caretakers” in *Cady v. Drombrowski*, 413 U.S. 433, 93 S.Ct. 2523, 37 L.Ed.2d 706 (1973), lower courts have experimented with this exception to the warrant requirement as an excuse for several otherwise illegal searches and seizures. In appropriate circumstances, the community caretaker exception may also serve as a defense for officers sued for detaining and/or searching open carriers.

In yet another case from Michigan, *Deffert v. Moe*, 111 F.Supp.3d 797 (W.D. Mich. 2015), Plaintiff Johann Deffert was walking down the street openly carrying a handgun in a leg holster. He was wearing camouflage pants and, according to a citizen who called 911, appeared to be “talking to nobody.” The dispatcher told the caller that open carry was legal, but they would dispatch a patrol. Officers responded and, after looking at Deffert and noting that he appeared to be talking to himself, advised dispatch that they would make contact. Officers stopped their cruiser in the middle of the street, and approached Deffert with their weapons drawn. They ordered Deffert to the ground (he complied), handcuffed his hands behind his back, and disarmed him. Deffert was detained for approximately thirteen minutes while officers verified that he was not prohibited from possessing the weapon, that the weapon was registered, and that he was not talking to himself, but simply singing. Deffert sued and Defendants moved for summary judgment, arguing in part that their interest in making sure Deffert was not about to use his weapon to harm himself or others outweighed Deffert’s interest in not being disturbed. The District Court found Defendants’ argument meritorious, particularly given Deffert’s attire, the fact that he was singing (*Hakuna Matata*, from the Lion King) loudly enough to be heard from a distant police cruiser, was not known to be a resident of the area, and the fact that one responding officer testified he felt Deffert might have been suffering from mental issues. The Court concluded that “Officer Moe was justified in following up on the neighbor’s 911 call and using swift action to determine whether Plaintiff’s behavior gave rise to a need to protect or preserve life or avoid serious injury, either of Plaintiff or of others in the neighborhood.”

The New Mexico District Court examined a similar case, and reached a different conclusion. In *St. John v. McColley*, 653 F.Supp.2d 1155 (D. New Mexico 2009), Plaintiff Matthew St. John was openly carrying a firearm in a movie theater. The theater manager called police to report that the presence of St. John’s firearm was “making customers upset.” Police went into the theater and asked St. John if he was carrying a firearm. St. John said he was. Police told St. John to keep his hands in plain sight, then took him out of the theater in an “escort

hold.” Police continued to hold one of St. John’s arms while disarming him outside of the theater. St. John was placed against a wall and patted down. After verifying he owned the weapon lawfully, police told St. John he could return to the theater if he left the weapon in his truck. St. John agreed. The incident took thirty minutes. Later, St. John filed suit. Defendants moved for summary judgment on qualified immunity. The District Court found that police lacked reasonable suspicion to believe St. John had committed a crime—open carry is legal in New Mexico—when they detained him. Defendants argued, alternatively, that they properly exercised their community caretaker function in seizing St. John “to ensure the safety of the public and/or the individual.” The Court denied that the community caretaker function was a valid defense to liability because police had no basis to believe St. John was a risk to himself or others. A report that an individual is armed, in a jurisdiction where individuals are allowed to be armed, does not trigger a community caretaker privilege to detain the individual and inquire into the reason for his decision to be armed.

IV. RECENT NOTABLE CASES.

Until very recently, precedent almost universally suggested that open carriers have a tremendous burden of proof in establishing police officer liability. However, two recent cases suggest a trend toward liability for officers who effect stops and/or detentions of open carriers for no reason other than the simple fact that a person was openly carrying a firearm. Additionally, one open carrier recently attempted (unsuccessfully) to characterize his act of openly carrying a firearm as constitutionally protected speech.

A. *Northrup v. City of Toledo Police Dept.*, 785 F.3d 1128 (6th Cir. 2015)

Shawn Northrup went for a walk while open carrying. Northrup had a disagreement with a passing motorist about the legality of open carry (involving an exchange of profanity), after which the motorist called the police. A police dispatcher told the motorist that open carry was legal in Ohio (which was correct) if you have a concealed handgun license (which was incorrect—no license is required to open carry in Ohio). Nevertheless, the dispatcher promised to send someone to investigate. The officer initially attempted a consensual stop, which became an involuntary encounter after Northrup reached for his cell phone and the officer interpreted his actions as “furtive movements.” The officer ordered Northrup to place his hands above his head. Northrup refused, and the officer disarmed him. The officer demanded Northrup’s driver’s and concealed handgun licenses. Northrup produced his driver’s license, but refused to provide his concealed handgun license. In response, the officer threatened to arrest Northrup

“right now” for inducing panic. The officer then put Northrup in handcuffs and, after a half-hour investigation, cited him for failing to disclose personal information in violation of Ohio statutes. The charge was later dismissed.

Northrup sued for violations of his First and Fourteenth Amendment rights. Defendants asserted qualified immunity, and particularly argued that the arresting officer had reasonable suspicion to believe that Northrup was engaged in criminal activity—namely disorderly conduct—because Northrup was openly carrying a gun and because there had been a 911 call. The Court rejected Defendants’ conclusion with respect to reasonable suspicion. In a detailed analysis, the Court explained that a police officer may not presume illegal conduct from the simple fact that a person is visibly armed. Nevertheless, the Court found there was an issue of fact as to whether Northrup immediately raised his hands when the officer initially approached (as Northrup testified) or engaged in furtive movements on the officer’s approach (as Defendants claim), and remanded the case for further proceedings. The case settled on remand.

Most notably, this decision stands for the proposition that officers cannot presume illegal conduct from the mere fact that a person is openly carrying a firearm. “Where it is lawful to possess a firearm, unlawful possession ‘is not the default status’” and cannot be presumed by police officers. *Id.* at 1132.

B. *Duffie v. City of Lincoln*, 834 F.3d 877 (8th Cir. 2016) reh’g and reh’g en banc denied

A young black man with a white t-shirt and dreadlocks “kept looking at the cash register” during a purchase at a gas station. Later, when the cashier took out the trash, he saw the same young man hold up a silver handgun and gesture as if blowing smoke from the barrel. The young man was a passenger in a relatively distinct 90’s Astro van. The cashier called the police, who put out an APB. Later, police spotted a van matching the description. The officer could only verify that the driver was a black male. He called for backup and performed a “high risk traffic stop,” which included a demand that the driver exit the vehicle with his hands up. The driver shouted that he was unable, and police reiterated their demand. The driver then tried to comply, and fell out of the van onto his face. The driver, Leroy Duffie, turned out to be a double amputee, older, bald, black man. Police cuffed him on the ground and verified that nobody else was in the car. According to the court, it was clear at that point that the driver was not the man described in the APB.

Nevertheless, police continued to search the van while the driver remained on the ground. They found a silver paintball gun and confiscated it, stating that

they intended to question the driver's son about the weapon. Duffie filed suit for violations of his Fourth and Fourteenth Amendment rights. The police officers moved for summary judgment, stating that they had reasonable suspicion to believe a crime had been committed. The District Court granted summary judgment for the officers, but the Circuit Court reversed, writing that nothing the clerk reported to police could give rise to a reasonable suspicion that a crime had been committed. The Court noted that Nebraskans over the age of eighteen are allowed to possess handguns, and the fact that the clerk saw a young man with a handgun, without more, could not give rise to reasonable suspicion that the handgun possession was unlawful. Further, the Court noted that the clerk's tip did not indicate that the suspect's gesture of blowing smoke from the barrel was directed at the clerk, so the gesture could also not give rise to reasonable suspicion that the suspect had made a threat to the clerk.

C. Chesney v. City of Jackson, 171 F.Supp.3d 605 (E.D. Mich 2016)

Jeremiah Chesney openly carried a firearm into the Michigan Secretary of State's office, where he was attempting to obtain a motorcycle title. After waiting for twenty minutes, Chesney went to his car and returned with a backpack and lunch box. After sitting for a few minutes, Chesney left the backpack and lunch box at a desk, and began to walk around the waiting room. Someone at the Secretary's office became concerned and called the police to report "a suspect with long hair was possibly in possession of a handgun in a backpack . . . [and that] the subject was pacing back and forth." This caused the caller to feel "nervous that something else was going on." Officers arrived and recognized Chesney from "a prior contact." They initially asked him to step outside the office to talk, but Chesney refused. Officers reported that Chesney became increasingly agitated and began to raise his voice before they made the decision to forcibly escort him outside of the crowded office. Chesney was arrested for resisting arrest and obstructing a police officer after he "tensed up" during the escort, and his refusal to provide identification once outside of the office. The charges were later dismissed.

Chesney filed suit, which included a novel claim for violations of his First Amendment rights in addition to his Second and Fourth Amendment rights. Chesney argued that openly carrying a firearm was a constitutionally protected form of speech, which he used "to promote awareness of and educate others . . . on the legality of open carry." Chesney claimed that officers retaliated against him for engaging in speech they deemed objectionable. The District Court rejected Chesney's arguments, finding that nothing Chesney did evidenced an intent to convey a particularized message, and that there was no evidence to suggest any message he wanted to express would be understood by the audience

at the Secretary's office. Rather, the evidence showed that Chesney was on a routine trip to the Secretary's office for a personal errand, that he carried a gun everywhere he went, and Chesney was not carrying any signs or wearing any clothing to advocate for his message. Accordingly, the Court granted summary judgment in favor of the defendants on Chesney's First Amendment retaliation claims. The Court disposed of Chesney's Second Amendment claims on qualified immunity grounds (the right to openly carry a firearm was not "clearly established" in Michigan at the time of Chesney's arrest) and Fourteenth Amendment claims on the ground that there was reasonable suspicion and probable cause to support Chesney's detention and arrest.

V. RECENT NOTABLE STATUTES

A. Florida HB 163 / SB 300

Originally introduced to legalize open carry in Florida, the bill also included several provisions which would have significantly added to the burden of defending officers accused of civil rights violations resulting from interactions with open carriers. Under existing Florida law an officer with "reasonable grounds" to believe a person is illegally carrying a concealed weapon may effect a warrantless arrest of that person. As originally introduced, the bill struck "reasonable grounds" and substituted "probable cause." The bill also included a provision expressly imposing a civil fine of up to \$5,000.00 against any local government official or administrative agency head under whose jurisdiction a knowing and willful violation of firearms preemption occurs, and imposing liability for up to \$100,000 in actual damages, plus attorney fees and costs, *including a contingency fee multiplier*, for any plaintiff found to have been adversely affected by any statute, regulation, or policy in violation of firearms preemption. The bill also stripped officers of their immunity for violations of the firearms laws.

A Florida non-profit called Florida Carry, Inc. claims responsibility for drafting, advocating for, and procuring sponsors for the bill. The organization describes itself as a "nonprofit, non-partisan, grassroots organization dedicated to advancing the fundamental civil right of all Floridians to keep and bear arms for self-defense"

The bill was first introduced on September 14, 2015 in the Florida House by Rep. Matt Gaetz (R. 1st Dist.) and seventeen co-sponsors. According to Rep. Gaetz' campaign website, he is "one of the most pro-gun members of the Florida legislature." Among his other accomplishments, Rep. Gaetz claims to have "led the fight to bring open carry to Florida," "led the fight to keep [stand

your ground laws] in place,” and “passed legislation stopping insurance companies from discriminating against gun owners.” In November, 2016, Gaetz won election to the United States House of Representatives for Florida’s First Congressional District.

A companion bill was introduced in the Florida Senate by Sen. Don Gaetz (R. 1st Dist.), who happens to be Rep. Gaetz’ father. Sen. Gaetz’ political views are much more muted than his son. He has served in the Florida Senate since 2006, including a two-year term as Senate President. He is not seeking re-election and his term will end in 2016.

The Florida Sheriff’s Association strongly opposed the bill from its introduction. Perhaps because the primary purpose of the bill was to legalize open carry, which had a great deal of popular support among Floridians, it appeared quite likely to pass. Eventually, the Florida Police Chiefs Association publically announced its support for the legislation *provided* sponsors would agree to several amendments to protect officers from civil suit. Specifically, those amendments included provisions criminalizing open carry if the individual displays the firearm in an “angry or threatening manner, not necessarily in self-defense,” reduced the threshold for warrantless arrests from “probable cause” to “reasonable suspicion,” and provided immunity for officer’s conduct if the officer was acting as part of a lawful investigation.

The House Bill, as amended above, passed the House by a vote of 80-38. The Senate Bill died in committee. The Florida legislature only convenes in regular session for a sixty-day period beginning in March. Thereafter, the legislature is only in special sessions convened by the Governor, or jointly by the leaders of both chambers. It is unclear whether the Florida Senate deliberately failed to act on this legislation, or if it was simply not moved forward because of more pressing legislative concerns. Regardless, the bill did not become law.

B. Texas H.B. 190

This legislation was originally introduced by Texas Assemblyman Craig Estes, a Republican, to legalize open carry. Two non-profit organizations—Open Carry Texas and Texas Carry—claim responsibility for moving the legislation forward. The bill allows open carry, provided the open carrier first obtains a state license, completes a course on firearms safety, and keeps the weapon in a hip or shoulder holster (if the weapon is a handgun). The legislation was opposed by a majority of Texas law enforcement officers (as many as 75%, according to a February, 2015 survey by Dallas News), particularly after an amendment was offered which would have prevented law enforcement from stopping a person

solely to verify the open carrier had a firearms license. Interesting, the amendment had significant support from the Democratic caucuses, which felt that police might use the stops in a racially discriminatory manner. Eventually, however, that amendment was withdrawn after a state senator threatened to filibuster the entire legislation. The Governor signed H.B. 190 into law, and open carry became legal in Texas on January 1, 2016.

Two months later, police arrested open carrier Brett Sanders after he refused to produce his handgun license when police stopped him for questioning. The charges were dropped in late 2016. According to Sanders' website, he is a "notable First and Second Amendment activist," who has previously sued police for allegedly refusing to allow him to film their activities, and also paid a \$200 traffic ticket with several buckets of pennies. As of February 21, 2017, Sanders has not yet filed suit against the officers who arrested him, but suit seems likely given his history, and his stated willingness to be a test case on whether police can detain open carriers and request identification. The suit, if it materializes, will be an interesting test of whether and under what circumstances Texas law enforcement officers may detain or arrest open carriers.

VI. CAN AN OPEN CARRIER WIN?

A quick web search produces numerous hits for reports of civil suits settled in favor of open carriers, typically in the low to mid five-figure range. However, we found no evidence of a jury verdict—for plaintiff or defendant—in any open carry civil rights suit. This seems to suggest that cases on facts less favorable to a plaintiff are being resolved through motions practice, and that cases on facts more favorable to a plaintiff are being settled.

VII. DISCUSSION HYPOTHETICAL: A mass shooting occurs at the scene of an open carry rally. Police are present at the scene, and detain/disarm open carriers, who later file suit for First, Second, and Fourth Amendment violations. What is the defense strategy?

A. Argue that there was no constitutional violation.

1. No court has recognized a First Amendment right to openly carry a firearm, and in fact at least one court has found that such a right does not exist. *Chesney v. City of Jackson*, 2016 WL 1090372, *1 (E.D. Mich. Mar. 21, 2016)

2. Likewise, the right to openly carry a firearm has not been recognized under the Second Amendment. *Id.* In fact, Courts are still in disagreement about whether the individual right to carry a firearm, recognized in *Heller*, extends outside of the home.

3. While the Fourth Amendment usually requires police to have reasonable suspicion that the *particular* person being detained has engaged in some criminal conduct, there is authority for the proposition that “even absent particularized reasonable suspicion, innocent bystanders may be temporarily detained where necessary to secure the scene of a valid search or arrest and ensure the safety of officers and others.” *Bletz v. Gribble*, 641 F.3d 743, 755 (6th Cir. 2011).

Further, the court will look to the unique facts of the case to determine whether there was particularized reasonable suspicion and/or probable cause sufficient for each detention (i.e. were the persons detained coming from the direction of the area from which the shots were fired, were the persons brandishing and/or reaching for their weapons, and whether the detained person engaged in furtive movements, etc.).

B. Argue that the right was not clearly established.

1. As discussed above, the case law is unclear regarding the scope of the individual right to bear a firearm recognized in *Heller*. Courts cannot even agree upon whether that right extends to carrying a firearm outside of the home, let alone whether the Second Amendment extends to the right to openly carry or whether the right to openly carry is also protected by the First Amendment. Moreover, there is at least some case law supporting the proposition that neither the First nor the Second Amendment encompass the right to openly carry a firearm and there does not currently appear to be any case law otherwise. Thus, at least for the time being, the issue is not clearly established even in a general sense, and officers should be entitled to qualified immunity. As noted by the Supreme Court, officers should not be subject to civil liability for choosing the wrong side in a constitutional debate.

2. Regarding the Fourth Amendment, the right of a citizen who is openly carrying a firearm to be free from detention and disarmament at the scene of a mass shooting has not been addressed by any court. Thus, while citizens enjoy a clearly established generalized right to be free from unreasonable seizures, it is not clearly established whether the seizure of a person under these circumstances would be clearly established in the particularized sense that all reasonable officers would understand such a seizure to violate the Fourth

Amendment. The Supreme Court has repeatedly, including recently in *White*, emphasized the need to consider the clearly established prong in a particularized rather than general manner. Without any comparable prior case law, and noting that officers have at least an arguable reasonable basis for the seizure in this hypothetical, the officers should be entitled to qualified immunity even if the detentions are ultimately found to constitute a Fourth Amendment violation.

- C. Argue that the detentions were appropriate under the community caretaker exception.

- 1. Law enforcement officers have a duty to protect the public, which is entirely separate from their duty to prevent crime and collect evidence for use in criminal prosecutions. The community caretaker defense has been asserted successfully in several civil rights cases, and should be raised in this scenario. But as highlighted in *St. John*, the defense may fail unless a defendant can articulate a reason why he or she believed the plaintiff was a threat to himself or others. It has yet to be determined if it is appropriate to detain an armed person because of the possibility that he or she is in a panic and acting scared and/or irrationally at the scene of an emergency.

VIII. SUMMARY OF DEFENSE TIPS

- A. Find out if open carry was legal in the jurisdiction. If not, defending the civil suit is more straightforward.

- B. Investigate all of the facts surrounding the open carry incident. Using those facts, find out if there are objective grounds upon which an officer could have acquired the probable cause or reasonable suspicion necessary to justify a stop or detention. If open carry itself is legal, but the particular facts of the case might have supported a detention, search, or arrest for another crime, such as brandishing, disorderly conduct, or criminal mischief, the law enforcement officer may not have committed a constitutional violation. This is true whether or not the officer subjectively intended to use the stop to question the plaintiff about an openly carried firearm.

- C. Find out if open carry is “clearly established” in the jurisdiction. In most jurisdictions it is not... yet, at least with regard to the specific scope of that right and how it relates to other laws and rights. Additionally, it has not yet been clearly established whether the Second Amendment protects the open carrying of firearms and, if so, to what extent. As noted by the Supreme Court, “[i]f judges thus disagree on a constitutional question, it is unfair to subject police to money damages for picking the losing side of the controversy.” *Wilson v. Layne*, 526

U.S. 603, 617 (1999). Therefore, in most instances the right to openly carry, especially in the specific circumstances of that incident, may not be clearly established and the officer would be entitled to qualified immunity. However, the longer open carry is recognized as a right, and the more case law that is created with analyzing that right, the more difficult it will become to argue that the plaintiff's rights were not "clearly established".

D. Consider the Community Caretaker Exception. The law with respect to community caretaker immunity is not well-defined as it pertains to open carrier detentions. Nevertheless, asserting community caretaker immunity should not be overlooked, as it may provide a viable defense for an officer who believed an open carrier was a threat to himself or others, but who otherwise lacked reasonable suspicion that a crime was afoot or about to be committed.

**OPEN CARRY LAW ON
PUBLIC/MUNICIPAL PROPERTY**

Paper prepared by

David J. MacMain

Tricia M. Ambrose



**The MacMain
Law Group LLC**

101 Lindenwood Drive - Suite 160

Malvern, PA 19355

484.318.7703

dmacmain@macmainlaw.com

www.macmainlaw.com

OPEN CARRY IN PUBLIC/MUNICIPAL PLACES

I. Introduction

In the case of *District of Columbia v. Heller*, 554 U.S. 570 (2008), the Supreme Court, in a 5-4 decision authored by the late Justice Antonin Scalia, and joined by Justices Roberts, Kennedy, Thomas and Alito, reiterated that the 2nd Amendment protects an individual's right to bear arms as a fundamental right, unrelated to military or 'militia' service, and is for the purpose of, *inter alia*, self-defense. While *Heller* did not directly address the issue of 'open carry', some discussion and analysis of *Heller* is instructive as to how courts review regulations involving firearms, and may likely view "open carry" issues if presented with a case.

In *Heller*, the District of Columbia passed legislation that prohibited the possession of an unregistered firearm, placed certain restrictions on the registration of firearms, and prohibited handguns to be kept in the home unless they were rendered inoperable. While the *Heller* Court opined that the right to keep and bear arms is a fundamental right, it added that such right is not without limitation – noting that it is long been held that "a person cannot keep and carry any weapon whatsoever, in any manner whatsoever, and for any purpose whatsoever."

As to the District of Columbia's prohibition, the Court held that it amounted to a prohibition on an entire class of weapons (i.e. handguns) that is overwhelming chosen as the weapon of choice by citizens for a lawful purpose that the 2nd Amendment intended – self-defense. Further, the majority was troubled that the ban extended to citizen's home, where that lawful purpose and protected right is most sacred. The Court held that the blanket ban on handguns in the home failed constitutional muster regardless of the level of scrutiny that the court could apply.

Justices Stevens and Breyer filed dissenting opinions, with Justices Souter and Ginsburg joining. In short, the dissent focused on the language that 2nd Amendment gun rights are not absolute, and permits governmental regulation. The dissent further noted that many states have regulations with regard to possession and use of handguns, and that the Court ought to give some deference to the local legislatures as to what they felt was best in this area, and apply an 'interest balancing' test.

While the majority in *Heller* was very clear that the 2nd Amendment provided protection of the right to bear arms – a fundamental right – it also pointed out that it was lawful and proper to forbid the carrying of firearms in "sensitive places" such as schools and government buildings and that such regulations and prohibitions are presumptively lawful. It is this so-called 'sensitive places' exception that the balance of open carry rights vs. government regulation of same collides and the battle is waged.

II. Arguments For and Against Open Carry

Proponents of open carry argue that it provides a deterrent to potential criminals and makes them aware that potential victims are able to protect themselves, their property and others.

Further, those who open carry pose less of a risk to the public because they are not carrying their firearm concealed or in secret, and all are aware that the person is armed. And, above all, proponents argue, the right of self-protection – through self-arming – is a fundamental right provided by the 2nd Amendment.

Opponents of open carry argue that there is no benefit or advantage to openly carrying a firearm in an urban setting, or every day situation. Having citizens with open weapons serves to intimidate and scare, possibly escalate verbal arguments into violent physical encounters, with concomitant risks to all involved and uninvolved bystanders and law enforcement.

The issues surrounding guns and gun control has become increasingly contentious and heated in the last few years as a result of the mass shootings that have taken center stage in movie theaters, schools and county buildings. Moreover, with the ever-changing laws in the area, states and municipalities attempting to regulate firearms, and the make-up of the Supreme Court – the regulation and analysis of the 2nd Amendment is likely to become a fluid issue with changes possible with the incoming presidential administration.

III. Federal Law

There are no federal restrictions on open carrying of firearms in public. However, pursuant to 18 U.S. Code § 930 possession of a firearm or other dangerous weapon in a Federal facility is against the law. This includes among other places, Federal Courthouses, Post Offices and Federal prisons. Federal law *does permit* the possession of firearms in National Parks.

IV. State Law

A. Generally

California, Florida, Illinois, South Carolina, New York and D.C. prohibit the open carrying of a firearm in public.

Connecticut, Georgia, Hawaii, Indiana, Iowa, Maryland, Massachusetts, Minnesota, Missouri, New Jersey, Oklahoma Rhode Island, Tennessee, Texas and Utah require a permit or license to openly carry.

Arkansas, Colorado, Delaware, North Dakota, Pennsylvania, Utah, Virginia, Washington permit open carry with some restrictions. Generally, these restrictions deal with prohibiting open carry in populous cities, such as Philadelphia, openly carrying long guns, not permitting guns in a local government's jurisdiction or only allowing unloaded open carry.

Alabama, Alaska, Arizona, Idaho, Kansas, Kentucky, Louisiana, Maine, Michigan, Mississippi, Missouri, Montana, Nebraska, New Hampshire, New Mexico, North Carolina, Ohio, Oregon, South Dakota, Vermont, West Virginia, Wisconsin and Wyoming allow open carry with no restrictions.

B. State Preemption

Many states have passed regulations that preempt *local* regulation of firearms. However, some states permit the local regulation of concealed carry – but not of open carry. This means that if your state permits the possession and carrying of a firearm - a municipality, township or county cannot pass its own regulation regarding the lawful possession of firearms.

Some states do not preempt local regulation including Oregon, Connecticut, New York, New Jersey, California, and Massachusetts. As such, these states permit local agencies and governments to prohibit or regulate the possession of firearms in their public entity as they see fit. Local regulation can cause significant issues regarding a citizen's right to possess a firearm. For example, if one township prohibits open carry in their local park, but the next township over does not, a citizen may be required to keep abreast of various local regulations so as not to face criminal prosecution or fines for violating local regulations.

Many states have a preemption clause, but also permit local municipalities to regulate the possession of firearms in certain situations. Most of these states permit local regulations in very specific circumstances, and do not *require* that a municipality locally regulate, rather, it permits regulation if the municipality chooses to do so.

Alaska has a preemption clause, but permits municipalities to prohibit guns in municipal buildings.

Delaware permits local agencies to regulate the possession of open firearms in police, state, county and municipal buildings.

Indiana permits local governments to enact laws prohibiting firearms in buildings with courtrooms, and in county and municipal buildings.

Kansas permits cities, counties and political subdivisions to restrict or prohibit the possession of firearms in public buildings.

Louisiana gives political subdivisions the authority to prohibit possession of a weapon in certain commercial establishments and public buildings. Commercial establishments such as bars or other businesses that serve alcohol have had regulations imposed regarding possession of firearms.

Maryland permits local governments to regulate possession of a firearm within 100 yards of a park, public building or other place of public assembly.

Nebraska allows local municipalities to regulate concealed firearms.

North Carolina allows cities and counties to regulate possession of firearms in publicly owned buildings, parks and recreation areas

In Texas, guns can be prohibited in any county building that houses a court or any office used by the courts.

On the other hand, some states prohibit any local regulations with regard to the possession of firearms.

For example, Georgia state law preempted a county ordinance prohibiting firearms on County property.

Iowa local governments cannot prohibit firearms in county buildings or those controlled by the local government.

In Michigan, a city ordinance that attempted to make public buildings gun free zones was preempted by state law.

Kentucky law states that only the state can regulate firearms; local municipalities cannot enact ordinances and restrictions regulating firearms. Further, state law permits open carry in any city-owned facility, including libraries, parks, the zoo, city hall and city council.

V. Examples

A. State Courthouses/City Halls

In Pennsylvania, guns are not permitted in state or municipal buildings. However, in Texas guns are permitted, but not if the citizen is going to city council meetings, commission or board meetings, polling places or municipal court. In Nevada, firearms are only prohibited in legislative buildings.

B. Police Stations

In Texas, a citizen can have a firearm in a police station, but only in the portions of the police station open to the public. In Pennsylvania firearms are permitted in police stations.

C. Public Parks

In Pennsylvania, firearms are not permitted in state parks with some exceptions for hunting, however, they are permitted in local public parks. In Nevada, firearms are permitted in public parks.

VI. The Heller “Sensitive Places” Analysis

In *Heller*, the Court held that laws forbidding the carrying of firearms in “sensitive places” such as schools and government buildings are presumptively lawful. Sensitive places have been defined as places where youth and children recreate and are most likely to be present and/or places where the possession of firearms would place large number of defenseless people

at risk of danger. *Nordyke v. King*, [563 F.3d 439 \(9th Cir. 2009\)](#), *vacated by* [611 F.3d 1015 \(9th Cir. 2010\)](#); *Warden v. Nickels*, [697 F. Supp. 2d 1221 \(W.D. Wash. 2010\)](#); ¹ open-space venues, where large numbers of people might congregate; places used for government business or important to government functioning, and certain colleges.

In *Digiacinto*, 281 Va. 127, 704 S.E.2d 365 (2011) the Supreme Court of Virginia determined that George Mason University qualified as a “sensitive place” because it is an agency of the state and its property is owned by the government; (2) the statutory structure creating the university indicated its sensitive nature; and (3) people on university property have “a reasonable expectation that the university will maintain a campus free of foreseeable harm. The Court opined that because it is a school **and** government owned – it is a sensitive place.”²

“Sensitive places” can be a broad term and can be case and situation specific. *Nordyke* held that prohibiting firearm possession on municipal property fits within the sensitive places exception that *Heller* recognized. Plaintiffs in *Nordyke* challenged a County ordinance that bans firearms on County property. The *Nordyke* Court held that the 2nd Amendment does not protect a right to keep and bear arms onto government property. Further, the Court held that the ordinance was permitted because it did not impede the ability of people to defend themselves in their homes with firearms – the core right that *Heller* addressed.

VII. The Municipality Acting As A “Property Owner”

Some courts have balanced the municipality’s attempt to regulate firearms as a ‘municipality’ versus as a ‘property owner’. If a municipality can successfully argue that they are attempting to act as a property owner, they may be able overcome preemption.

To make this argument the municipality must ask if the regulation is specific to certain property or to the municipality more generally and in other places. For example, is there a prohibition on a particular park in the township or city, or will it apply to all parks. Does the penalty involve a citation or prosecution?

VIII. Recent Law

In *Firearm Owners Against Crime v. Lower Merion Township*, 2016 Pa. Commw. LEXIS 545, Lower Merion Township in suburban Philadelphia passed an ordinance prohibiting persons from carrying or discharging firearms in a park without a special permit. Pennsylvania law preempts local regulation of firearms. The township argued that it was only regulating unlawful firearms – however, the statute did not delineate that. The Township also argued it was regulating pursuant to its “property owner” rights, not as a municipality.

The Pennsylvania Commonwealth Court disagreed finding that Lower Merion’s Ordinance sought to regulate in *all* parks and authorized police involvement for anyone who

¹ The *Nordyke* decision has been vacated, but the Court’s analysis on regulation of guns in sensitive places continues to be recognized.

² One wonders if the then-recent April 16, 2007 Virginia Tech massacre had any effect on the Court’s analysis.

violates the ordinance – thereby tending towards the Township operating pursuant to its police powers, not powers as a “property owner.” Further, since Pennsylvania law preempts local regulation of firearms, the Township could not pass a statute prohibiting firearms in public parks.

IX. What Does This Mean For Municipalities?

Understand your state regulations on guns. Does your state give local municipalities the right to regulate and if so, what specific areas can the municipality regulate? Even if local regulation is permitted, a citizen could make a 2nd Amendment challenge. However, based on the case law, and provided the regulation is not a blanket ban, the regulation would likely stand.

Recently in Arizona – a state which has a preemption clause – the state has been finding that local municipalities are ignoring the state preemption law and regulating firearms. Arizona has advised that will be withholding funding to those local municipalities who are thumbing their nose at state law preemption of firearms.

In considering local regulation if you are in a state that permits it, consider if the proposed regulation or ban fits into a “sensitive place” scenario. If so, this could avoid a 2nd Amendment claim but would not likely be enough to overcome state preemption if it applies to your state.



Mazanec, Raskin & Ryder Co., L.P.A.

Attorneys and Counsellors at Law

Casey C. Stansbury

PARTNER

AREAS OF PRACTICE

Auto & Commercial Trucking	Employment & Labor Law
Business & Commercial Law	General Liability
Civil Rights & Governmental Liability	Insurance Coverage & Bad Faith
Construction Litigation	Professional Liability & Licensing
	Public Sector Law

Lexington Office

230 Lexington Green Cir.
Suite 605
Lexington, KY 40503
Direct: 859.899.8514
Fax: 859.899.8498
cstansbury@mrrlaw.com

EDUCATION

- J. D., 2001, Ohio
Northern University
College of Law
 - National Environmental Moot Court Team
 - The Order of Barristers
- B.A., 1998, Louisiana
State University
 - Pi Kappa Alpha Fraternity

BAR ADMISSIONS

- Kentucky Supreme Court
- U.S. District Court,
Eastern District of
Kentucky
- U.S. District Court,
Western District of
Kentucky
- U.S. Court of Appeals,
Sixth Circuit
- Indiana

Mr. Stansbury focuses his practice on insurance defense, civil rights and governmental liability issues. He represents insurance companies/risk pools and their insureds with respect to both first and third-party claims, including employment discrimination, professional liability, municipal liability, automobile negligence claims, general commercial matters, bad faith claims, uninsured claims, products liability, wrongful death claims, commercial premises liability claims, and property and casualty claims. He also has significant experience counseling clients in insurance coverage matters, including the securing of declaratory judgments on policy interpretations. He regularly counsels and represents police officers, correctional officials, municipalities, and public officials in a variety of matters including employment concerns, contract disputes, and civil rights actions. Casey has a diverse practice including the defense of employers, both public and private. In addition to his representation of public entities and officials, he has experience in handling various other types of litigation matters including cases concerning construction disputes, commercial law, and motor vehicle accidents.

Casey is a frequent presenter and has received numerous awards, including the Defense Research Institute's 2014 Albert H. Parnell Outstanding Program Chair Award. He also serves as the DRI Government Liability Committee Chair.

PROFESSIONAL ORGANIZATIONS

- Fayette County Bar Association
- Kentucky Defense Counsel
 - President (2014-2015)
 - President Elect (2013-2014)
 - Vice President (2012-2013)
 - Secretary (2011-2012)
 - Board of Directors (2010-2011)



- Defense Research Institute (DRI)
 - Governmental Liability Committee
 - Chair (current)
 - Vice Chair (2014-2016)
 - Program Chair (2013-2014)
 - Online Committee Chair (2013-2014)
 - Vice-Program Chair (2012-2013)
 - Chair of Publications (2011-2012)
 - Annual Meeting Chair (2010-2011)
- Federation of Defense and Corporate Counsel (FDCC)
- Risk and Insurance Management Society
- Bluegrass Claims Association

COMMUNITY INVOLVEMENT

- Faith First Soccer, Coach
- First United Methodist Church, Member

ACCOMPLISHMENTS

- AV® Preeminent™ rating from *Martindale-Hubbell Law Directory*
- Named a Kentucky “Super Lawyer” (2015 & 2016)
- Named a Kentucky “Super Lawyer Rising Star” (2013-2014)
- DRI Albert H. Parnell “Outstanding Program Chair Award” (2014)

PRESENTATIONS

- “Section 1983 Claims – Kentucky Jailers’ Association Conference
- “Law Enforcement Encounters with the Mentally Ill and Potential Liability under the ADA: Analysis of *Sheehan v. City of San Francisco*” – Travelers Insurance Company, Public Sector
- “The Perfect Storm – The True Story of How Inexcusable Mistakes and Failures at All Levels of City Government Led to the Payment of a Merit-less Claim” – Defense Research Institute Annual Meeting (2011)
- “Mock Trials” – Bluegrass Claims Association/Kentucky Claims Association Annual Conference
- “Bonding and Surety Issues Concerning Construction” and “Insurance and Indemnity Issues Involving Construction.” – Blue Moon Seminar
- “Evaluating and Settling Personal Injury Claims” – National Business Institute Seminar
- “Utilizing Paralegals Effectively” – Greater Lexington Paralegal Association, *Voted Most Outstanding Speaker*
- “Cyber Insurance & Cyber Liability” – Bluegrass Claims
- “Politically Correct, Defending Political Government Officials” – Kentucky Paralegal Association



PUBLICATIONS

- “Evaluation of a Motor Vehicle Claim from the Defense Perspective” – *Kentucky Justice Association*
- “Iqbal Energizes Motion to Dismiss Practice” – *International Society of Primerus Law Firms*

**JANE M. LYNCH, ESQUIRE
GREEN & GREEN, LAWYERS
800 PERFORMANCE PLACE
109 N. MAIN STREET
DAYTON, OHIO 45402**

Jane has practiced extensively in the areas of political subdivision liability claims, construction litigation, personal injury, premises liability, civil rights, and insurance. She is admitted to practice in Ohio as well as before the U.S. District Courts for the Southern and Northern Districts of Ohio, the Sixth Circuit Court of Appeals, and the U.S. Supreme Court.

Jane is a member of the American, Ohio State and Dayton Bar Associations, Defense Research Institute, Ohio Association of Civil Trial Attorneys, Litigation Counsel of America, Federation of Defense and Corporate Counsel (FDCC) and Claims & Litigation Management Alliance (CLM), and the President of the Lawyers Club of Dayton. She is also a Master of the Carl D. Kessler Inn of Court, an organization of trial counsel and judges. Jane has been recognized as an Ohio Super Lawyer® annually since 2006. She is a Fellow of the American Bar Association, the Ohio State Bar Association, and the Dayton Bar Association. She has served in leadership roles on many professional and community committees and boards, including serving as Chair for the Southern District of Ohio Federal Court Rules Committee. She was also an invited participant in the 2013 Air War College, National Security Forum.

Jane was honored to be selected by her peers to be included since 2015 in the Edition of The Best Lawyers in America©. She is rated AV Preeminent® by Martindale Hubbell.



THURSDAY, MARCH 9, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

CONSTRUCTION LAW and PROFESSIONAL LIABILITY SECTIONS

What lies beneath - Beware the Meaning and Implications of “Incorporation by Reference”

Dogwood

Moderator:

Marc H. Harwell

Speaker:

Robert C. Moore

“SO, WHAT DID I JUST AGREE TO?” THE INCORPORATION BY REFERENCE DOCTRINE

I would like to say it all started with the famous television Series “Lost in Space” with the line “Danger Will Robinson Danger,” but history tells us that the Doctrine of Incorporation by Reference started a long time before this series. However, this well known line is more appropriate now than ever before. When reviewing contracts for various parties, it never ceases to amaze me at the amount of documents and issues that are incorporated by reference that have nothing to do with the subcontractor's work.

Commercial contracts, including construction contracts, have become intricate, detailed and hypertechnical. The doctrine of incorporation by reference addresses this complexity by allowing a reference to incorporate into the agreement extrinsic materials which are given equal weight with provisions directly contained in the agreement. Utilizing such an incorporation, may have the advantage of (1) speed and efficiency in drafting; (2) achievement of greater uniformity; (3) a clearer and more complete statement of intent; and (4) the convenience of the parties. On the other hand, employment of an incorporation by reference has the potential to cause problematic results. A court can misinterpret an ambiguous or inadequate clause, as the presence or absence of an intent to incorporate, or the desired scope of the reference may be misconstrued. Further, an indiscriminate use of incorporation may create conflicts between contractual provisions. Finally, incorporation discourages careful scrutiny of all the contract's terms, as extrinsic materials may be unavailable or voluminous and this may result in an unequal advantage for one of the parties.

The Doctrine of Incorporation by Reference really caught on in the early 1900's when the US Supreme Court stated that it is critical to know the exact language of any reference to another document. In *Guerini Stone Co. v. P.J. Carlin Constr. Co.*, 240 U.S. 264 (1916), a reference to “drawings and specifications” was held not sufficient to bind the subcontractor to the owners' changes and time extension clauses. In that case the court stated:

...in our opinion the true rule, based upon sound reason and supported by the greater weight of authority, is that in the case of subcontracts, as in other cases of express agreements in writing, a reference by the contracting parties to an extraneous writing for a particular purpose makes it a part of their agreement only for the purpose specified. *Id* at 277.

Since then, states have taken the United States Supreme Court's opinion and made some major and minor modifications. Most states have the following concept as part of their incorporation by reference doctrine: contracts, clauses,

designs, drawings, agreements, writings, URL sites or matters, which are clearly and unambiguously referred to in a written contract/agreement may be regarded as incorporated by reference as a part of the contract/agreement and, therefore, may be used by the parties to express duties and obligations. The drafter must clearly indicate, show, establish, substantiate, corroborate, and confirm an intent to incorporate an outside document into the written contract/agreement. Where a written contract that refers to a document, URL site, or agreement and makes the terms and conditions of such other instrument a part of the subcontract, then it becomes a part of understanding, or as we say in law school, the “meeting of the minds” of the parties. However, if in a written contract, a reference is not clear or is made to or for only a particularly designated purpose, the other writing becomes a part of the contract only for the purpose specified, and will not be considered for purposes other than the one specified, the “Reasonably Clear Standard.”

Some form of assent to the terms of the incorporation by reference is also usually necessary. We often times see the form of assent in the opening paragraph of an agreement or right above the signature line. However, the assent can be stated as part of the course and conduct of the parties undertaken previously.

Some states allow a double incorporation by reference. A double incorporation by reference, incorporates a contract into a contract, not only is the contract that is incorporated by reference part of the contract, but if the contract incorporated by reference has another document that is incorporated by reference, the double incorporation by reference doctrine allows that other document to be incorporated as well and is a part of the agreement.

AIA “Standard Form of Contract Between Contractor and Subcontractor” (A401) 2007 is a classic example of the double incorporation by reference doctrine. Since this contract is copyrighted, I can tell you and reminisce about the client meeting that I had some years ago where the client found out the hard way about the double incorporation by reference doctrine. The contract had some interesting twists and turns. In essence the contract stated:

Article 2

The Subcontract Documents

1. The Subcontract Documents consist of (1) this Agreement; (2) All upper tier contracts including the Prime Contract, consisting of the Agreement between the Owner and General Contractor and any other Contract Documents enumerated in those agreements, including Conditions of the Contract (General, Supplementary and other Conditions), Drawings, Specifications, Addenda issued prior to the execution of the Agreement between the Owner and General Contractor and all Modifications issued subsequent to the execution of

the Agreement between the Owner and General Contractor, whether before or after the execution of this Agreement, and all other Contract Documents, if any, listed in the Owner-General Contractor Agreement; (3) other documents listed in Exhibit "B" of this Agreement; and (4) Modifications to this Agreement issued after execution of this Agreement. All of these documents including the ones listed on Exhibit "B" are a part of the Subcontract as if all the documents were attached to this Agreement or repeated herein. The Subcontract represents the entire and integrated agreement between the parties hereto and supersedes prior negotiations, representations, or agreements, either written or oral. All documents are available for review upon request.

My client never reviewed any of these documents, nor did they ever ask to see the documents. You ask how someone could do that; how could they "NOT REVIEW ALL THE DOCUMENTS?" The answer is simple, there is just not enough time for subcontractors to read all the documents especially documents that have items that are not relevant to my subcontractors work. Buried in the double incorporated documents, were various construction clauses that were clearly in favor of the Owner/General Contractor, including that the subcontractor waived a jury trial, agreed to submit to arbitration, agreed to arbitration only in the county where the General Contractor was well regarded, Texas law applied to the contract, and finally that if there was litigation that it could only be brought in the Texas county where the General Contractor was located. So what's the big deal—well all the work was done in Chicago...nothing was done in Texas. These clauses turned the case on its head. I think that you get the point.

One way that I have suggested to my subcontractor insured's is to try to insert into the contract the following at the end of the incorporation by reference Article: "The Subcontractor hereby requests that the General Contractor submit non-digital or non-electronic versions (hereafter referred to as "Paper Documents") of all incorporated documents to the Subcontractor for review. The parties agree that it is the intention of the parties that all Paper Documents submitted to the Subcontractor for review shall deal only with the scope of the subcontractors work and should take no longer than two (2) hours to review. Any document not given as a Paper Document will not be incorporated by reference into this subcontract."

We have drafted this type of a clause for use with heavy handed upper tier contracts that are over-bearing, so as to establish the parties intent that the contract be fair and reasonable. We have not tried to change the article, since often times trying to get something changed, is much more difficult than just adding a clause. When interpreting a contract, a court must determine and give effect to the parties' intent through the language they use to express their rights

and duties under the contract. Absent ambiguity, the terms of a contract are given their plain and ordinary meaning. In this day and age if a contractor is performing work on a large scale billion dollar project and all of the documents for the project are incorporated by reference, there is a potential that your contractor won't have the time to read through all the documents, especially if your contractor is a specialty contractor who is performing small part of the work taking place on the billion dollar project. By using this language, we try to create a reasonable and fair contract by putting caps on the amount of work that has to go into reviewing the contract documents. Our additional language gives the subcontractor a basis for negotiation, also; Why should a subcontractor look at the roadwork specs, when that subcontractor is the finish carpenter for the project.

Another pitfall is that the tendered contract will contain a "conflict of terms and conditions" clause that says that the terms and conditions of the upper tier contract will control if there is a conflict. This language will also apply to documents incorporated by reference and also those subject to double incorporation. This means that the subcontract governing the work at hand, can be trumped by documents that are completely unrelated to this work and are often never seen. We would suggest that these clauses be amended to make the subcontract terms and conditions control, not the upper tier contract. This will serve to protect the lower tier contractor, by making sure that the terms they must follow are tied to their actual work.

Another potential argument is that there is an ambiguity in the contract. Typically an ambiguity exists when "reasonable people could come to different conclusions about the contract's meaning." In such cases, we are often forced to use extrinsic evidence, also known as evidence from outside the written agreement, since it is "relating to a contract but not appearing on the face of the contract because it comes from other sources." Black's Law Dictionary 578 (7th ed.1990.) A situation such as this, leads right into the one of the best arguments to the court, given the often overwhelming amount of documents typically incorporated by reference, and that is the "Taint Fair Argument." Said another way, if the incorporation reference language is ambiguous, a party will often be heard to complain that it isn't fair to hold them to all of these extraneous documents. They will contend that there is no way they could have known about these documents and what they say and courts will often be swayed by these arguments. While an ambiguity may provide a defense, it is not ideal, as both parties should know clearly what they are agreeing to before starting the work. If at all possible, negotiations should result in clear unambiguous language.

CONCLUSION

If you want to be clear about what has been included in your agreements by

reference, you need to pay attention to these types of terms. If the contract terms offered to you are unacceptable, you should recall, and use, the incorporation principles discussed in this article. As part of your negotiations, add language to your agreement, including the suggested language to require incorporated documents to be provided to you. You might also consider adding language to your subcontract that says that its terms take precedence over the clauses in the upper tier contract. That way, if there is a contradiction and a dispute arises, the meaning expressed in your subcontract should prevail. dispute dispute arises, the meaning expressed in your subcontract should prevail.



THURSDAY, MARCH 9, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

HEALTHCARE PRACTICE and LIFE, HEALTH & DISABILITY SECTIONS

Telemedicine Liability and Compliance

Jenkins

Speakers:

Thayla P. Bohn

Jay D. Davis, Jr.

James A. Hoover

TELEMEDICINE, LIABILITY, AND THE NEW LEGAL FRONTIER

Authors: D. Jay Davis, Jr., Esq. and J. Camden Hodge, Esq.
YOUNG CLEMENT RIVERS, LLP
Charleston, SC

Presented by:

D. Jay Davis, Jr. Esq.

FDCC 2017 WINTER MEETING
Charleston, South Carolina
March 6 – 10, 2017

Telemedicine, Liability, and the New Legal Frontier

**D. Jay Davis, Jr.¹
J. Camden Hodge**

INTRODUCTION

Imagine a 50 year old man living in rural middle America, 2 hours and 100 miles from any medical specialist or intensive care unit. After a late dinner with his family, the man's vision begins to blur. His head starts to ache with the force of a migraine, and he becomes nauseas. The symptoms worsen, and the man's family drives him to the local emergency room. The ER doctor performs a physical examination and takes the man's vitals; the differential diagnosis includes the possibility of a stroke. A CT scan is ordered. Knowing that time is of the essence, the doctor queues up his hospital's new videoconference "telemedicine" system and is instantly connected to a neurologist and stroke specialist in the state's closest level one trauma center. With the help of the ER doctor, the specialists interactively examine the man, review his brain scan, and determine that he is suffering from an ischemic stroke. The specialists order a clot-dissolving IV drip that is in turn administered by ER staff, and the patient's symptoms begin to alleviate. Had a proper diagnosis not been made and the clot-dissolving drug not been provided within the first 3 hours of the stroke's onset, the man could have suffered life-altering consequences or death.

Innovations in data communication and technology have nurtured the advent of telemedicine – a practice that allows doctors to treat patients located in disparate locations and across great distances. Despite the term being used since the 1970's, telemedicine is not uniformly defined. Indeed, a study cited by the World Health Organization found 104 separate, peer-reviewed definitions of the word. Bradley J. Kaspar, *Legislating for A New Age in Medicine: Defining the Telemedicine Standard of Care to Improve Healthcare in Iowa*, 99 IOWA L. REV. 839, 844 (2014). The American Telemedicine Association (ATA) defines it as "the use of medical information exchanged from one site to another via electronic communications to improve a patient's clinical health status." American Telemedicine Association, *What is Telemedicine?* (2012)(available at goo.gl/tOuL7z). The Centers for Medicare and Medicaid Services (CMS) defines telemedicine more narrowly, describing it as the "two-way, real time interactive communication between the patient, and the physician or practitioner at the distant site to improve a patient's health." Centers for Medicare & Medicaid Services, *Telemedicine* (available at goo.gl/tOuL7z). Telemedicine generally is thought to include two distinct modalities: store-and-forward (also known as "asynchronous communication") and real time communication. Diane Hoffmann, Virginia Rowthorn, *Legal Impediments to the Diffusion of Telemedicine*, 14 J. HEALTH CARE L. & POL'Y 1, 2 (2011). Store-and-forward telemedicine involves the transmission of medical information (such as radiologic images) to a specialist for offline assessment. *Id.* This method commonly is used for diagnostic purposes in specialties such as pathology, dermatology, and radiology, to name a few. *Id.* Real-time telemedicine refers to communication that is instantaneous, involving the use of interactive telecommunication

¹ Jay Davis is a partner at Young Clement Rivers, LLP in Charleston, SC. He is Chair of the Healthcare Practice Group. Camden Hodge is an associate within the firm.

devices most often equipped with video, audio, and interactive capabilities. Avery Schumacher, *Telehealth: Current Barriers, Potential Progress*, 76 OHIO ST. L.J. 409, 416 (2015). Modern telemedicine “carts” even can come equipped with electronic stethoscopes and special, condition-specific diagnostic instruments. Dawn Brazell, *Telemedicine to Help Save More Lives*, Medical University of South Carolina Public Relations (August 2, 2013)(available at: goo.gl/El6y2r).

The reasons for telemedicine’s allure are legion. It has the potential to increase access to quality healthcare in rural and underserved areas; allow patients with chronic conditions to receive care in their own homes; reduce hospital visits; and increase continuity of care among providers. *See Hoffman, supra*. Proponents of telemedicine harp on its cost efficiencies, citing studies asserting that telemedicine could save the United States more than \$4 billion a year in healthcare spending. *See Schumacher, supra*.

Telemedicine has been well-received in the United States, and its ubiquity and use in the American healthcare system is only going to increase. Bill Marino, J.D. et. al., *A Case for Federal Regulation of Telemedicine in the Wake of the Affordable Care Act*, 16 COLUM. SCI. & TECH. L. REV. 274, 275 (2015). A number of factors are driving that growth. Foremost among them, of course, is money: by 2018, the value of the U.S. telemedicine market is expected to reach nearly \$ 2 billion. Bruce Japsen, *ObamaCare, Doctor Shortage to Spur \$2 Billion Telehealth Market*, FORBES (Dec. 22, 2013, 9:30AM) (available at: goo.gl/CxPYNp)(citing a forecast by business analytics firm IHS). The federal government has continually supported the use of telemedicine through developmental grants and research, with countless government agencies championing telemedicine and pushing the boundaries of its use. *See Hoffman, supra*. The Patient Protection and Affordable Care Act (more commonly known as Obamacare) contains at least seven separate provisions directing federal healthcare officials to “explore, consider, or implement telemedicine practices.” *Marino, et al., supra* at 277. Our national news apparatus keeps the practice in the spotlight, simultaneously extolling its virtues and critically examining its potential downfalls. Even the 2016 presidential candidates pushed for its use during campaign season. At a campaign stop in Iowa, Hillary Clinton called for telemedicine services to be readily reimbursable under Medicare; in Nevada, Jeb Bush cited it as a potential tool for supporting healthcare needs of rural populations. Carrie Pallardy, *Thoughts on Telemedicine from 2016 Presidential Candidates Hillary Clinton and Jeb Bush* (February 5, 2016)(available at: goo.gl/bCWxok).

But with its quick development and burgeoning use come unique legal considerations that must be taken into account by litigators, transactional attorneys, advisers, in-house counsel, and insurers alike. This article addresses three chief challenges and the attendant legal consequences that must be considered in advising and representing telemedicine providers and practitioners. First, the article begins with a discussion of medical malpractice considerations in the world of telemedicine. Next, it discusses the current state of reimbursement and coverage of telemedicine services, including concerns surrounding anti-kickback statutes and the Stark Law. Finally, this article examines the patchwork of rules and regulations that control physician licensure regarding the practice of telemedicine.

I. MEDICAL MALPRACTICE

To date, there has been a dearth in medical malpractice cases directly involving the practice of telemedicine. The majority of legal opinions associated with telemedicine regard disciplinary and criminal actions stemming from the prescription of medication over the internet, rather than claims brought against practitioners for medical malpractice. Telemedicine also is mentioned in a growing body of 42 U.S.C. § 1983 cases involving federal prisoners, but those cases fail to address malpractice by way of a breach of “telemedical standards of practice.” Despite this lack of case law, there is a “widespread assumption” that telemedicine is bringing with it new complications to traditional medical malpractice claims, including choice of law issues, jurisdictional problems, and concerns in defining the applicable standard of care. See *Hoffman, supra*. This section will briefly address those issues. As a refresher, medical malpractice cases mirror traditional negligence claims in that they require the proving of (1) a duty owed by the physician to the patient; (2) a breach of that duty; (3) injury to the patient; and (4) a causal link between the breach and the injury.

A. Creating a Duty and Establishing the Standard of Care

“Malpractice law dictates that a physician’s duty exists if there is a patient-physician relationship.” *Kasper, supra* at 845. Thus, the first step in evaluating a potential medical malpractice claim regarding the provision of telemedicine services involves determining when the physician-patient relationship is created, as that will dictate when the legal duties attach. A patient-physician relationship generally is established when a physician gives personalized medical advice to a patient. The relationship must be a consensual one where the patient knowingly sought the assistance of a physician and the physician knowingly accepted him as the same. Traditionally, this relationship would be created during the first initial hands-on, face-to-face meeting between the patient and the physician. Telemedicine substitutes these in-person consultations for evaluations made via video and audio conference systems. In evaluating liability for alleged telemedical malpractice, practitioners must understand that the relationship can be created during these initial “consultations,” regardless of whether or not they occur through a telecommunication medium or otherwise. Courts are beginning to coalesce around the tenet that the determination of whether a physician-patient relationship exists should be a question of fact for a jury to determine.

Practitioners also should be aware of the fact that the establishment of a physician-patient relationship often is dependent on the type of medical advice or treatment being provided to the patient. Using the authors’ home state as an example, a proper physician-patient relationship in the context of prescribing drugs requires the physician to: (1) personally perform and document an appropriate history and physical examination, make a diagnosis, and formulate a therapeutic plan; (2) discuss with the patient the diagnosis and the evidence for it, and the risks and benefits of various treatment options; and (3) ensure the availability of the licensee or coverage for the patient for appropriate follow-up care. S.C. Code Ann. § 40-47-113(A). No other South Carolina statute explicitly lays out the manner in which a patient-physician relationship is formed. Practitioners always should look to their state’s statutory code to see whether or not the elements for creating a physician-patient relationship already are defined.

The next question to consider is what standard of care applies. Is it the standard of care used in the physician’s state or the patient’s state? Is it the same as for a telemedicine

consultation as it is for in-person treatment? Most scholars believe that states eventually will hold telemedicine practitioners to the same standard applied in “traditional cases” where patients are treated in person, which in turn would allow the patient to sue in the state where he or she receives treatment. *See Hoffman, supra*. The scant case law mentioning standard of care in telemedicine matters tend to agree. *See United States v. Valdivieso Rodriguez*, 532 F. Supp. 2d 316, 327 (D.P.R. 2007)(“The best philosophy and approach to telemedicine is that the same standards of care and protocols applicable to more traditional forms of medicine exist with telemedicine. The physician-patient relationship and interaction are the same. The process should be the same as if the patient were in the room with the doctor.”). Other states, however, have argued that the practice of medicine over the internet should be considered a separate specialty with a separate standard of care, and that line of thinking logically could be applied to telemedicine. *See Lisa Rannefeld, The Doctor Will E-Mail You Now: Physicians' Use of Telemedicine to Treat Patients Over the Internet*, 19 J.L. & HEALTH 75, 100 (2004)(collecting cases). This fight will play out on the state level, whether through statutorily defined standards of care or by judicial fiat.

B. Jurisdictional and Choice of Law Concerns

Those defending medical malpractice actions in the telemedicine setting should be prepared to face new jurisdictional challenges. Because physicians who practice telemedicine arguably will have “minimum contacts” with the state where the patient is located, plaintiffs likely will have the choice to sue in their home state or the state where the physician practices. While plaintiffs usually have sought relief in the same jurisdiction that they received care, it can be foreseen that a plaintiff in a telemedicine malpractice case could “shop around” in search of a more favorable plaintiff’s forum. As is the case with determining the applicable standard of care, this issue already is being addressed by state legislatures. *See, e.g.,* La. Stat. Ann. § 37:1276.1 (“Any physician licensed to practice telemedicine in accordance with this Section shall be subject to the provisions of this Part, the jurisdiction of the board, applicable state law, and, with respect to providing medical services to state residents, to the jurisdiction of Louisiana courts.”); Ill. Comp. Stat. Ann. 60/49.5 (“An out-of-state person providing a service listed in Section 49 to a patient residing in Illinois through the practice of telemedicine submits himself or herself to the jurisdiction of the courts of this State.”).

II. REIMBURSEMENT

The absence of uniform and comprehensive reimbursement policies can be considered one of the largest obstacles to integrating telemedicine into healthcare practice. At present, Medicaid, Medicare, and private insurers are struggling to keep pace with technological advancements and the growing popularity of telemedicine. The needle, however, is trending toward coverage for an ever increasing amount of telemedicine services.

A. Medicare and Medicaid

The federal government at present does not limit or require states to reimburse for telemedicine services through Medicaid, electing instead to leave states to determine which services (if any) are eligible for reimbursement. *Schumacher, supra*. Federal law does,

however, restrict the types of telemedicine services eligible for reimbursement through Medicare as well as the geographic locations where those services can be provided.

Medicare only provides reimbursement for certain “real-time” interactive video and audio communications a Medicare beneficiary receives at an “eligible site.” 42 C.F.R. § 410.78(b)(3). Store-and-forward “asynchronous” telemedicine services are not fully reimbursed save for in Alaska and Hawaii, which are part of a special federal telemedicine demonstration program. Department of Health and Human Services, *Telehealth Services*, RURAL HEALTH SERIES (December 2015). Sites include a physician’s office, critical access hospitals, “rural health clinics,” hospitals, and federally qualified health centers. *Id.* These sites must be located in a “rural Health Professional Shortage Area” as defined by CMS. *Id.* According to one commentator, Medicare “treats tele[medicine] almost exclusively as a tool for rural areas” while failing to recognize coverage needs for other underserved populations such as inner-city communities. David Pratt, *Telehealth and Telemedicine in 2015*, 25 ALB. L.J. SCI. & TECH. 495, 496 (2015). While Medicare does limit reimbursement based upon geographic location, it has expanded the number of health professionals allowed to claim reimbursement for telemedicine services. The list now includes physicians, nurse practitioners, physician assistants, midwives, clinical psychologists, clinical social workers, and registered dietitians/nutrition professionals. American Telemedicine Association, *Telemedicine and Telehealth Services* (January 2013 news bulletin).

Generally, Medicaid allows states to establish their own specific eligibility standards, determine the type, duration, scope, and amount of services to reimburse, and set reimbursement rates. As of the time of writing, forty-eight state Medicaid programs now reimburse some form of real-time telemedicine services, and thirteen even offer reimbursement for remote patient-monitoring care. Center for Connected Health Policy: The National Telehealth Policy Resource Center, *State Telehealth Policies and Reimbursement Schedules* (available at: goo.gl/TvCmze). Federal regulations do, however, impose certain conditions on the states receiving federal funds. Medical practitioner must stay within the scope of their state’s “practice of medicine act” and must comply with federal requirements of efficiency, economy, and quality of care. Many state Medicaid programs also mandate that only certain providers – most often physicians – can be reimbursed for the provision of very limited services such as specialty consultations. *Id.*

B. Private Payors

Twenty-nine states and the District of Columbia now require that private insurers cover telemedicine in the same manner as in-person services. The laws do not mandate that the health plan provide “new” service lines or specialties, and the scope of services in the plan’s member benefit package remain unchanged in those states. See Nathaniel M. Lacktman, *Examining Payment Parity in Telehealth Laws*, HEALTHCARE LAW TODAY (August 13, 2015). Put simply, consumers in states with these parity laws now have the option of electing to see their doctor via telemedicine instead of in person. Telemedicine coverage is becoming increasingly popular among private payors; for example, Anthem Health Insurance Company estimates that it offers telemedicine coverage to at least 20 million of its members. As telemedicine grows in popularity, expect private coverage of those services to increase as well.

C. Fraud and Abuse Concerns

Providers must remember that the federal anti-kickback statute and Stark Law apply to telemedicine in the same manner as they do to in-person care. *See* 42 U.S.C. § 1395nn, et seq.; 42 U.S.C. § 1320a-7b, et seq. The anti-kickback statute is a criminal statute that prohibits the exchange (or offer to exchange) anything of value in an effort to induce or reward the referral of federal health care program business. 42 U.S.C. § 1320a-7b. A single violation of the anti-kickback statute can result in a fine of up to \$25,000 and imprisonment of up to 5 years. 42 U.S.C. § 1320a-7b(b). Convictions also result in mandatory exclusion from participation in federal health care programs. 42 U.S.C. § 1320a-7(a). The Stark Law, on the other hand, prohibits a physician from referring Medicare patients for designated health services to an entity with which the physician (or an immediate family member) has a financial relationship, subject to limited exceptions. 42 U.S.C. 1395nn. Violation of the Stark Law can result in False Claims Act liability and overpayment/refund obligations.

Several federal Office of the Inspector General (OIG) advisory opinions have explicitly examined telemedicine arrangements. Particularly informative is Advisory Opinion 99-14 (2000), wherein the OIG found that a proposed rural telemedicine network arrangement implicated the Anti-Kickback Statute in certain respects. In that opinion, the OIG addressed a telemedicine network formed by a health system with ten outlying rural health care facilities, with the stated network goal of providing better access to services for rural citizens. The health system was considered the “hub” of the telemedicine network, with the rural care facilities operating as “spokes.” The health system was to provide the spokes with technical communications capabilities, equipment, and technical assistance and training. The health system also would coordinate the network and pay transmission line charges. In return, the spokes would provide space for the equipment, site facilitators, data collection, and security. The spokes promoted the network to their respective medical staffs.

The health system was awarded supporting grants in 1994 and 1997, and those funds were used to purchase telemedicine equipment, install it in the spoke facilities, and to pay for transmission line charges. The grant also allowed the network to pay fees to the physicians providing the consultations in the event that no third-party payor could be billed for the visit. The network was providing telemedicine consultations in more than thirty specialties, and had agreements with more than one hundred physicians to provide those consultations. At the time, the only financial support the health system provided to the spokes was the equipment funded by the federal grants as well as some maintenance costs. The federal grants were set to expire in 2000. The health system proposed continuing to pay for the transmission line charges, as well as the equipment maintenance for the spokes through 2003. The spokes in turn would continue to provide their own space and staffing, while all new and existing spokes would be responsible for obtaining any new or replacement equipment.

The OIG found that the anti-kickback statute was implicated in the above arrangement because the health system conferred a benefit on two potential referral sources: the spoke facilities and the hub consulting physicians. The spokes were obtaining free equipment and subsidized line charges, while the consulting physicians were receiving additional opportunities to earn fees. Despite finding this finding, the OIG declined to impose sanctions against either the current or proposed arrangements. Practitioners should review each of the remaining OIG

advisory opinions (Nos. 98-18, 99-14, 04-07) for guidance as to permissible manners of structuring telemedicine affiliations.

III. PHYSICIAN LICENSURE

Like the law, medicine is a self-regulating profession where licensing and oversight powers are given to the states. Physician licensure laws came into existence in the early 20th century “when medicine was practiced at a local level.” *Schumacher, supra* at 8-9. Under this “traditional” model, an out-of-state practitioner could not consult, assess, or treat a patient in a state where the practitioner did not have a full license to practice medicine. *Id.* at 9. State medical boards continue to control the licensing process, but they have different rules, unique restrictions, and procedures that must be complied with if a physician wants to practice in a particular state.

Telemedicine directly challenges this traditional, state-based licensing model by enabling and promoting the practice of medicine across long distances and state boundaries. A physician seeking to practice telemedicine faces a complicated mélange of state-specific licensing requirements and schemes that must be followed before a physician can provide telemedicine services. Doctors and telemedicine companies need a legal counselor with knowledge of these distinct licensing models to guide them through the process, especially in light of the serious consequences a doctor can face if he or she does not fully comply with state licensing requirements. *See United States v. Valdivieso Rodriguez*, 532 F. Supp. 2d 316, 327 (D.P.R. 2007)(prosecution of physician under Controlled Substances Act for prescribing medication via telemedicine in states where he was not licensed to practice medicine).

Individual states address telemedicine licensing through four principle approaches: (1) the use of “special purpose” licenses; (2) requiring “full” state licensure; (3) state board “endorsement” and reciprocity statutes; and (4) “consulting exceptions.” A lawyer advising clients on telemedicine will be wise to understand the licensing requirements in the states their client seeks to practice, as criminal liability can await those physicians who engage in the practice of medicine without a proper license.² The respective approaches are best understood by an examination of the specific licensing requirements imposed by different states.

A. Special Purpose Licenses

As of the time of writing, 14 state medical boards issue special purpose licenses, often referred to as telemedicine licenses or certificates, which allow a physician to practice telemedicine in a state. Federation of State Medical Boards, *Telemedicine Policies: Board by Board Overview* (available at: goo.gl/8yP7Tf). The freedom afforded by these special purpose licenses vary widely from state to state and often come with significant strings attached. *See, generally*, Center for Connected Health Policy: the National Telehealth Policy Resource Center, *State Telehealth Policies and Reimbursement Schedules: A Comprehensive Plan of the 50 States and District of Columbia* (September 2014). For example, on one end of the spectrum is New Mexico, whose telemedicine regulatory favor simplicity. *See* N.M. Admin. Code § 16.10.2.

² Lynette A. Herscha, *Is There A Doctor in the House? Licensing and Malpractice Issues Involved in Telemedicine*, 2 B.U. J. Sci. & Tech. L. 8 (1996)

New Mexico statutory law defines a telemedicine license as a “limited medical license that allows a physician located outside New Mexico to practice medicine on patients located in New Mexico.” *Id.* at 16.10.2.8(B). To be eligible to receive one of these special purpose licenses, the applicant must have an unrestricted license to practice medicine in another state, undergo a comprehensive criminal background check, and pay a \$400 application fee. *Id.* at § 61-6-11.1. If you satisfy those requirements, you can practice telemedicine in New Mexico for three years before needing to renew your license.

Other states do not make it so simple, and clearly made it difficult to the practice. Louisiana is emblematic of states that impose more burdensome and intensive requirements both in terms of obtaining a special purpose license and in practicing under the same. *See* La. Admin Code, Title 46, § 408; La. Rev. Stat. Ann. § 37:1271; 1276 Those seeking a telemedicine license in Louisiana must hold a full and unrestricted license to practice medicine in another state and, most importantly, “shall establish a bona fide physician-patient relationship” with all people they treat in Louisiana. La. Rev. State. Ann. § 37:1276.1. This relationship is created by first conducting an “appropriate examination” of the patient, which involves ascertaining a diagnosis through the use of “accepted medical practices,” including but not limited to taking a patient history, determining mental status, and/or using “appropriate diagnostic and laboratory testing.” *Id.* The physician must then discuss with the patient any diagnoses as well as the risks and benefits of various treatment options. He or she also must ensure that the patient has access to appropriate follow up care. Those practicing telemedicine in Louisiana shall not utilize the practice for the treatment of “non-cancer related chronic or intractable pain” or the treatment of obesity. 46 La. Admin. Code Pt XLV, 7513. Further, prescriptions cannot be written by a telemedicine practitioner unless the physician has at least one in-person visit with the patient at a physical practice location in the state except in certain select circumstances. *Id.* Finally, those practicing telemedicine in Louisiana by virtue of a special purpose license cannot open an office in the state, meet with patients there without the company of an in-state treating physician, or receive telephone calls from Louisiana patients. *Id.* at (d).

Those counseling practitioners operating under special purpose telemedicine licenses must be well-versed in the physician regulatory system in the state where the patient is located, as the licensee will be subject to that state’s regulatory authority. This can become particularly problematic when and if the practitioner receives a special purpose license in multiple states. Legal advisers should ensure that the physician knows the time period for which the license is valid and any restrictions placed on the license that are unique to that state.

B. Full State Licensure

Most commentators view the model of requiring full state licensure before a physician can practice telemedicine in a certain state to be overly burdensome and outdated. However, at least five states require doctors to be fully licensed to practice medicine in the state where the patient is physically located – no exceptions. Practitioners should be wary that such states often place substantial restrictions on the practice of telemedicine even if one is fully licensed to practice in that state. For example, those practicing telemedicine in Georgia cannot have “ultimate authority over the care or primary diagnosis” of any patient that is located in the state. Ga. Code Ann. § 43-34-31. Physicians practicing in these jurisdictions must understand that receiving a full medical license in a state does not remove specific restrictions imposed by the state’s telemedicine statutes and regulations.

C. Reciprocity and Endorsement

To date, only a handful of states allow telemedicine licensure reciprocity: Maryland, New York, Virginia, and the District of Columbia. Latoya Thomas & Gary Capistrant, *State Telemedicine Gaps Analysis: Coverage & Reimbursement*, American Telemedicine Association (2015). Systems based on reciprocity do not require a physician to submit to new review of individual credentials, as states that are party to the reciprocity agreement automatically recognize each other's licenses. Even those states allowing for reciprocity limit the courtesy to bordering states. Endorsement, on the other hand, is a "process whereby a state issues an unrestricted license to practice medicine to an individual who holds a valid and unrestricted license in another state." Endorsement allows states to retain their traditional regulatory power to set and enforce standards that best meet the needs of their population, but it still shoulders physicians with the burden of complying with the requirements necessary to retain a license in places other than their home states.

Endorsement and reciprocity schemes are being recognized and recommended by various industry groups, including the American Bar Association. Indeed, in 2008 the ABA's House of Delegates adopted the Health Law Section's recommendation regarding proposed mutual telemedicine licensure recognition by all states. Specifically, the ABA's proposed solution to the telemedicine licensure morass was:

to institute a system of mutual licensure recognition whereby a physician with a current, valid and unencumbered license in any state could file a single application which would permit the physician to practice telemedicine in some or all other states subject to continuing compliance with those states' licensure fees, discipline, and other applicable laws and regulations, and adherence to professional standards of medical care.

A similar approach was advocated by the Federation of State Medical Boards (FSMB). Under the FSMB scheme, an expedited license by endorsement process would be provided to physicians who (1) held full and unrestricted licensure in all jurisdictions where a medical license is held; (2) were free of any state board disciplinary history; and (3) graduated from an approved medical school.

While many commentators assert that the only way to streamline and "fix" our current unwieldy telemedicine licensing system is through federal regulation and oversight, the "mutual recognition through endorsement" model is gaining traction. For example, a "Nurse Licensure Compact" (NLC) was created by industry groups in 1997 and currently has been adopted by 24 states. The NLC allows a nurse with a valid license to practice in other states who are a party to the compact – both in person and through telecommunications technology. *Schumacher, supra*. The question of whether a compact system could prove viable in the world of physician licensure remains a debated question.

D. Consultation Exceptions

Several states have a "consulting exception" to their state licensure laws under which a physician who is not licensed in one state can practice medicine at the request of and in

consultation with a referring in-state physician. Susan E. Volkert, *Telemedicine: Rx for the Future of Health Care*, 6 MICH. TELECOMM. & TECH. L. REV. 147, 168-69 (2000). The scope of these exceptions varies from state to state: most prohibit the physician from receiving calls or opening an office in the state, and many allow consultations only if the out-of-state physician is consulting with an in-state physician who shares his or her specialty. *Id.* The only commonality among these schemes is the prerequisite that the in-state physician is the treating physician. *Id.* Most “consultation regulations” allow a physician to act as a consultant in a particular state only a handful of times, and the vast majority prohibits the out-of-state physician from exercising “primary control” over the in-state patient.

CONCLUSION

Telemedicine is only growing more popular and accepted in the American healthcare system. As it continues its march towards ubiquity, the medical industry will be faced with evolving legal questions without clear answers. In the absence of federal regulation and guidance, legal practitioners must become well-versed in the law of individual states where their clients intend to practice or establish business. The law governing telemedicine is poised to grow and expand along with the industry, and we must be prepared to navigate clients through what will prove to be a complex and constantly changing body of law.



THURSDAY, MARCH 9, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

DRUG, DEVICE & BIOTECHNOLOGY

**Promotional Claims: Off-Label Promotion and Debunking the Theory
and Defending the Claim**

Drayton

Moderator:

Michael J. Hurvitz

Speakers:

Jon Kahan

Greg Jackson

Marisa Trasatti

Off-Label Drug and Device Promotion in the Wake of *Amarin*



By Marisa A. Trasatti and Marie Claire Langlois

Recent cases involving promotion to doctors have challenged off-label promotion enforcement actions based on due process and First Amendment grounds as well as physicians' need for scientific information.

Marisa A. Trasatti is general counsel of the California-based laser company, Sciton Inc. Prior to joining Sciton Inc., she was a principal at Semmes Bowen & Semmes in Baltimore, focusing her practice primarily on civil litigation with an emphasis on product liability litigation, including cases involving drugs and medical devices. As general counsel, she continues to maintain an office at Semmes Bowen & Semmes' Baltimore office. Ms. Trasatti is president-elect of the Maryland Defense Counsel (MDC). Marie Claire Langlois was a 2016 law clerk at Semmes Bowen and Semmes.

From 2010 to 2012, the federal government collected billions of dollars in settlement money from medical drug and device manufacturers from claims of misbranding under the Food, Drug, and Cosmetic Act (FDCA) and the False Claims Act (FCA). See Monica Marrero, *Off Label Promotion of Pharmaceutical Drugs Under the Caronia and Amarin Cases*, 43 J. of Health Care Fin. 1, 5–7 (2016). It is important to note that up to now, the U.S. Food and Drug Administration's focus has been on alleged oversteps in promotion involving drugs and devices

potentially implicating federally funded insurers, not purely aesthetic drugs and devices.

Additionally, the off-label promotion cases have focused on speech to physicians, not direct-to-consumer advertising. The recent string of cases and settlements have challenged such off-label promotion enforcement actions based on due process and First Amendment principles as well as the physician's need for such scientific information to facilitate innovation and patient care.

In the wake of *Amarin* and its progeny, industry and other stakeholders have asked the U.S. Food and Drug Administration (FDA) to promulgate uniform guidance relating to (1) the determination of truthful, non-misleading off-label communications; (2) the exchange of medical and scientific information between manufacturers and physicians; and (3) good reprint practices. And, though the FDA has repeatedly promised action, including an official statement regarding reexamination in 2014, it has yet to issue formal guidance. In December 2015, Janet Woodcock, Director of the FDA Center for Drug Evaluation and Research (CDER), announced that one of the CDER's "front burner priorities" for 2016 was to "[r]e-evaluate [the] regulation of drug advertising and promotion in light of current jurisprudence around the 1st Amendment." See David L. Rosen et al., *How Will FDA Regulate Off-Label Communications in the Post-Facteau World?*, Food and Drug Policy Forum (Sept. 26, 2016), available at <http://www.fdpi.org>. Representative Fred Upton (R-MI), Chairman of the House Committee on Energy and Commerce, wrote to the U.S. Department of Health & Human Services Secretary Sylvia Burwell on May 26, 2016, to express his dissatisfaction with the lack of progress, stating that he was "perplexed by the agency's unwillingness or inability to publicly clarify its current thinking on these issues in a coherent manner." See *id.*

Misbranding or Legitimate Off-Label Promotion?

The Federal Food, Drug, and Cosmetic Act (FDCA) prohibits the misbranding of drugs or medical devices or introduction of a misbranded drug or medical device into interstate commerce. 21 U.S.C. § 331(a). A drug or device is misbranded if its labeling does not contain adequate directions for use or if it contains false or misleading information. 21 U.S.C. §§ 352(a)–(n). Use instructions that are not approved by the FDA, as reflected in the drug or device’s labeling, are considered “off-label.” Because promotional statements can serve as proof of a drug’s intended use, 21 C.F.R. § 201.5, off-label promotional statements made by a manufacturer or its representatives may constitute evidence of an intended use that is not FDA approved, resulting in misbranding. *See Marrero, supra*, at 1, 5–7. Hence, off-label *promotion* is prohibited by law, but off-label *use* is not. In one case, *United States v. Vascular Solutions, Inc.*, the court explained the distinction when it instructed the jury as follows:

Doctors may use medical devices that have been approved or cleared for one use for a different use that has not been cleared or approved by the FDA. This is often referred to as unapproved use or off-label use. This is not illegal. It is also not a crime for a device company or its representatives to give doctors wholly truthful and non-misleading information about the unapproved use of a device. If you find that VSI’s promotional speech to doctors was solely truthful and not misleading, then you must find the Defendants not guilty of the misbranding offense.

Final Jury Instructions at 12, *United States v. Vascular Solutions, Inc.*, No. 14-cr-00926-RCL, 2016 WL 1743175 (W.D. Tex. Jan. 27, 2016), ECF No. 282.

The FDA has frequently prosecuted drug and device companies for misbranding based on off-label promotions even though using drugs for off-label purposes is generally common and widely approved of in the medical community. In the most comprehensive study of off-label

prescription use in the United States, conducted in 2001, it was found that 21 percent of prescriptions were given for off-label uses. Christopher M. Wittich et al., *Ten Common Questions (and Their Answers) About Off-label Drug Use*, Mayo Clinic Proceedings, Oct. 2012. For example, a drug only approved for adults may still be extremely beneficial to children in smaller doses. Healthcare professionals may also prescribe the same drug for two conditions that are pathologically or physiologically similar, even though the drug has only been approved for one.

The consequences of misbranding are criminal, and misbranding can be asserted against the company itself or its representatives. 21 U.S.C. § 333(a)(2). *See also United States v. Facticeau, et al.*, No. 15-10076-ADB, (D. Mass. 2016) (U.S. Department of Justice charged two former executive officers of Accelerant, Inc., a medical device manufacturer, with wire fraud, conspiracy, and FDCA violations based on off-label marketing of Accelerant's Relieva Stratus Microflow Spacer). While showing that a defendant had intent to deceive or defraud makes the offense a felony with a significantly larger penalty, a misdemeanor charge may be brought successfully with little to no evidence of intent. 21 U.S.C. § 333. Nevertheless, despite the widely accepted nature of off-label drug uses, it was not until recently that manufacturers had gained any traction in their defense against misbranding claims.

***Caronia*: A Shift for Off-Label Promotion and the Commercial "Free Speech" Defense (December 3, 2012)**

In 2012, *United States v. Caronia*, 703 F.3d 149 (2d Cir. 2012), the district court convicted a pharmaceutical sales representative of conspiracy to misbrand after he was caught on tape marketing to doctors an FDA-approved drug for unapproved uses. The drug involved was

Xyrem, a powerful central nervous system depressant with potentially hazardous side effects, also known as the “date rape drug.” The Second Circuit vacated the conviction, finding that the representative’s marketing tactics were constitutionally protected commercial speech as truthful promotion of an FDA-approved drug for un-approved uses.

While on appeal, the government tried to rebut the freedom of speech defense by stating that the charges were based on conduct, and Caronia’s speech was only used as “evidence of intent.” The court disagreed, stating that the government’s case made clear that Caronia’s prosecution was for his *verbal* promotion and marketing efforts. This failed distinction between conduct and speech is one that Caronia’s progeny continued to tout unsuccessfully in defense of off-label promotion claims.

In response to *Caronia*, the FDA issued updated draft guidance on the dissemination of scientific or medical journal articles, authorizing the distribution of articles pertaining to unapproved uses of approved drugs as long as the articles were accompanied by certain disclosures. Additionally, the FDA specifically denounced the distribution of such articles as promotional materials or along with other promotional materials. Throughout the draft guidance, the FDA consistently maintained that if sales representatives characterized such articles as definitively making the drug safe or effective for unapproved uses, that the agency could use such speech as evidence of intent to promote misbranding.

The FDA justified this seemingly direct contradiction to *Caronia* by narrowly construing *Caronia*’s ruling as particularly fact based and turning on the existence of specific circumstances.

Amarin Pharma, Inc. v. USFDA (May 7, 2015)

While the ruling in *Caronia* paved the way for multiple rulings in favor of the drug and device manufacturing community, the most widely cited and recognized is *Amarin Pharma, Inc. v. U.S. Food and Drug Administration*, 119 F. Supp. 3d 196 (S.D.N.Y. 2015).

On May 7, 2015, Amarin filed a complaint in the United States District Court for the Southern District of New York. Amarin was actively seeking a preliminary injunction to prohibit the FDA from bringing against it a misbranding action for what it claimed were truthful, accurate, and non-misleading statements made to doctors regarding the off-label use of its drug, Vascepa.

Vascepa is a drug comprised of solely omega-3 fatty acids, developed by Amarin to improve cardiovascular health. In 2012 Amarin had received FDA-approval for use of Vascepa by adult patients with “very high triglycerides,” but Amarin still sought approval for use by adult patients with “persistently high triglycerides.” It is undisputed that Vascepa is safe and effective in reducing triglyceride levels, as reflected by an FDA-approved study (the ANCHOR study), but the FDA contended that other recent scientific studies left it unclear whether reducing triglyceride levels in persons with persistently high triglycerides actually reduced the likelihood of cardiovascular-related incidents. For these reasons, the FDA denied approval of Amarin’s “special protocol assessment” (SPA) agreement, something that the FDA has done only 10 times out of approximately 1,000 such agreements. David C. Gibbons, *A Victory for Amarin Further Erodes FDA Regulation of Off-label Promotion*, FDA Law Blog: Hyman, Phelps & McNamara, P.C. (Aug. 10, 2015).

Amarin appealed the decision through three successive levels of FDA review with no success, and on April 27, 2015, the FDA issued a “complete response letter” (CRL) finalizing its

decision. In the CRL, the FDA acknowledged that Amarin had fulfilled all the negotiated requirements under the SPA agreement and that the ANCHOR study had successfully proved that Vascepa reduces triglyceride levels in patients with persistently high triglycerides, but Amarin had failed to show any correlation between the reduction of triglycerides and a reduction of risk for major adverse cardiovascular events. Although the FDA then continued, stating that the final results from another on-going trial may very well satisfy this deficiency, the FDA explained that if Vascepa in the meantime were to be marketed alongside the ANCHOR results, the FDA would pursue prosecution for misbranding.

The FDA's threat gave Amarin the ammunition necessary to proceed in court. In its complaint for preliminary injunction, Amarin sought approval to release 13 peer-reviewed scientific publications, a statement and summary of the FDA-approved ANCHOR study, three textual statements, and five textual disclosures supporting Vascepa's ability to reduce triglyceride levels in its promotion of Vascepa. This was exactly what the FDA had warned against. Most likely in an attempt to avoid imminent litigation, the FDA proposed a resolution to the dispute, by providing altered versions of the requested submissions. In good faith, Amarin replied with further revisions; however, the parties could not reach an agreement.

After briefly addressing whether Amarin had standing to bring the case in light of the responsive negotiations, Judge Engelmayer dove into the substance of the argument: the likelihood of success for Amarin's case in light of the decision in *Caronia*. Specifically, Judge Engelmayer analyzed the merits of the FDA's argument that *Caronia* was particularly fact based, conducting a close inspection of *Caronia*'s language and reasoning to reach its ultimate conclusion:

By its explicit terms and its clearly-articulated reasoning, *Caronia* simply cannot be read as the proverbial ‘ticket good for one day only.’ On the contrary, the Second Circuit, at the close of its *Caronia* analysis presented its holding as a definitive one of statutory construction[,] [. . .] ‘we construe the misbranding provisions of the FDCA as not prohibiting and criminalizing the truthful off-label promotion of FDA-approved prescription drugs [. . .] *we conclude simply that the government cannot prosecute pharmaceutical manufacturers and their representatives under the FDCA for speed promoting the lawful, off-label use of an FDA-approved drug.*’

Id. at 226 (quoting *United States v. Caronia*, 703 F.3d 149 (2nd Cir. 2012)) (other internal citations omitted) (emphasis added).

Additionally, the court emphasized that *Caronia*’s holding did not leave the FDA with a loophole to prosecute manufacturers for misbranding conduct with speech evidence. Conduct that is alleged to be illegal only because of the speech associated with still has some constitution protections. As explained by Judge Engelmayer, “*Caronia*’s holding was that the FDCA’s misbranding provisions cannot constitutionally criminalize, and therefore do not reach, the act of truthful and non-misleading speed promoting off-label use.” *Id.*

The court stated definitively that truthful, accurate, and non-misleading speech regarding the off-label promotion of a drug cannot be used to support a misbranding prosecution. For purposes of the preliminary injunction, not only did Amarin have a *likelihood* of succeeding on a subsequent claim, but it was almost definitive. The court ultimately analyzed each and every suggested piece of promotional language that Amarin wished to use, agreeing with no changes to the uncontested pieces, and altering and piecing back together the truthful and non-misleading language in the remaining contested pieces. On the condition that Amarin use this revised language, the court granted the injunction.

Not long after the ruling, on March 8, 2016, the judge entered a Stipulation and Order of Settlement. Through the settlement, Amarin could use the court’s finalized language, as well as any other language that was truthful, accurate, and non-misleading. Under the terms of the settlement, the parties agreed to establish a special procedure by which Amarin would obtain FDA clearance for off-label promotion of its drug Vascepa, before releasing such communications to the public. Moreover, the settlement agreement permits Amarin to submit promotional materials for feedback twice every calendar year through 2020, in addition to the FDA providing continued access to optional procedures for feedback made available to *all* drug applicants. The FDA agreed not to appeal the district court decision, binding both parties to the district court’s holding from August 2015, which stated that the FDA could not prosecute Amarin for any truthful and non-misleading statements made regarding the off-label use of Vascepa. The FDA has provided, and will continue to provide, as part of the settlement, guidance to Amarin regarding the future promotion of Vascepa and Amarin’s other products. In return, the injunction against the FDA is lifted.

Pacira Pharmaceuticals, Inc. v. USFDA (December 15, 2015)

Even before the holding in *Amarin*, manufacturers were starting to push back against the FDA. EXPAREL is a non-opioid pain drug used to produce postsurgical analgesia, created by the company Pacira Pharmaceuticals. Following two pivotal Phase 3 studies, the FDA approved EXPAREL on October 28, 2011 for “administration into the surgical site to produce postsurgical analgesia.” While the “Clinical Studies” section of the approved prescribing information described the two studies (one following hemorrhoidectomy surgeries and one following bunionectomy surgeries) and stated that “EXPAREL has not been demonstrated to be safe and

effective in other procedures,” the “Indications and Usage” section authorized general use without any limitations to bunionectomies and hemorrhoidectomies. Pacira marketed its product consistent with the broad indications.

Three years after approval, on September 22, 2014, Pacira received a warning letter from the FDA, which alleged that Pacira’s marketing of EXPAREL for use other than for bunionectomies and hemorrhoidectomies constituted unlawful off-label promotion. The letter also stated that Pacira’s advertising claims regarding pain control that lasts up to 72 hours were misleading and an overstatement. While Pacira disagreed with the FDA’s allegations, it agreed to cease distribution of any relevant promotional materials, in addition to issuing a corrective message to customer’s regarding its approved use in two specific types of studies.

After briefly consulting with legal counsel, Pacira received a subpoena from the U.S. Attorney’s Office for the District of New Jersey that requested a broad range of documents pertaining to the marketing and promotional practices related to EXPAREL. *Client Alert Commentary: Lessons from Latham & Watkins’ Representation of Pacira Pharmaceuticals In Ground-Breaking Settlement with FDA*, No. 1912, Latham & Watkins, Jan. 5, 2016. Pacira threatened suit under the Administrative Procedure Act (APA) and the First and Fifth Amendments to the Constitution, stating that the FDA was trying to revise the broad scope of EXPAREL’s original approval, ignoring the normal administrative procedures and exceeding the authority granted to the agency under the FDCA. When Pacira’s request to find an amicable solution failed to receive a response, on September 8, 2015, it filed a Complaint and Motion for Preliminary Injunction in the United States District Court for the Southern District of New York *Pacira Pharmaceuticals, Inc. v. U.S.F.D.A.*, 2015 WL 5256628, No. 1:15-cv-07055 (S.D.N.Y.). The same court had just a month earlier granted Amarin’s preliminary injunction.

Shortly after the lawsuit was filed, settlement discussions began, and in a decision announced on December 15, 2015, the FDA publicly renounced its warning letter along with conceding to Pacira's APA claim. In a resounding victory for Pacira, the FDA approved a labeling supplement stating that EXPAREL was never limited to bunionectomies and hemorrhoidectomies and providing clarity on the drug's durational effect.

United States v. Vascular Solutions, Inc. (February 26, 2016)

In an even more recent case, medical device manufacturing company Vascular Solutions, and its CEO, Howard Root, were acquitted by a jury in the United States District Court for the Western District of Texas. *U.S.A. v. Vascular Solutions, et al.*, Criminal No. 5:14-CR-00962 (W.D.TX. Feb. 26, 2016). Vascular Solutions launched its Vari-Lase device in June 2007, for the treatment of varicose veins. This "Vari-Lase" laser device was cleared by the FDA for "the treatment of varicose veins and varicosities associated with the Great Saphenous Vein, and for the treatment of incompetence and reflux of superficial veins in the lower extremity." *Unbroken: The Howard Root/Vascular Solutions Acquittal— An Off-label Case About an On-label Use*, Duval Client Alert: Passing on Tribal Knowledge of FDA Law, *available at* <http://www.duvalfdalaw.com>.

Soon after, Vascular Solutions designed a "short kit," a shorter version of the Vari-Lase procedure kit to be used specifically in treating "short vein segments." In an attempt to cover all its bases, Vascular Solutions sought clearance through a 510(k) to add the "perforator vein" (a type of short vein segment) to its labeling. The FDA reviewer demanded clinical work, which was not required of its competitor, so the 510(k) was withdrawn. Vascular Solutions continued to market the product, specifically for the use on perforator veins, because its original clearance covered treatment of all varicose veins.

The U.S. Department of Justice charged Vascular Solutions and Root personally with conspiracy to distribute misbranded and adulterated medical devices and with distributing misbranded and adulterated medical devices. While the government had plenty of evidence that the company engaged in various sales schemes for the treatment of perforator veins, the case turned less on whether the speech and promotions existed, and more on whether that speech was unlawful.

Though Vascular Solutions spent twenty-five million dollars defending its case, it never called one witness, resting its case after the government rested. Through cross-examination, many of the witnesses had all but conceded that promotions of the short kit were not only truthful, but they may have been covered by the original clearance language. Moreover, the defense successfully moved for a jury instruction stating, “[i]t is [. . .] not a crime for a device company or its representatives to give doctors wholly truthful and non-misleading information about the unapproved use of a device.” While the jury’s exact line of thought is unknown, the resulting acquittal showed that the manufacturing industry may finally hold the upper hand, at least regarding truthful promotions.

Reactions to *Amarin* and Its Progeny

Amarin and its progeny surely clarify that truthful, accurate, non-misleading speech, even when it is commercial in nature, is protected by the First Amendment. While the industry was eagerly awaiting updated draft guidance from the FDA, an article written for the Mayo Clinic Proceedings’ June 2016 issue suggested that *Amarin*’s holding “effectively shift[ed] the decision-making process of what is considered truthful off-label promotion to industry rather than the FDA by giving deference to manufacturers in making the initial decision.” Tim K.

Mackley & Bryan A. Liang, *After Amarin v. FDA: What Will the Future Hold for Off-label Promotion Regulation*, 91 Mayo Clinic Proc. 701, June 2016.

On July 27, 2016, the Pharmaceutical Research & Manufacturers of America (PhRMA) and the Biotechnology Innovation Organization (BIO) endorsed the “Principles on Responsible Sharing of Truthful and Non-Misleading Information about Medicines with Health Care Professionals and Payers.” Jeffrey Francer & Deborah Shelton, PhRMA, PhRMA & BIO Release Joint Principles on Communications with Health Care Professionals and Payers (July 22, 2016), *available at* <http://catalyst.phrma.org>. By issuing these nine principles, the two groups intended to “guide the establishment of responsible, science-based parameters for accurate and trusted information-sharing under a modernized regulatory framework.” *Id.* The principles call for many things, including, but not limited to, accurate and both scientifically and statistically sound information sharing, clear labeling of what is an off-label use, more disclosure of sophisticated scientific knowledge for prescribers including the use of disclaimers, and the public sharing of new drugs and devices in the regulatory pipeline to the medical community. Bexis, *Off-Label Marketing– Industry Groups Step into the Breach*, Drug & Device Law Blog (Aug. 8, 2016), *available at* <https://www.druganddevicelawblog.com>. Most poignantly, the sixth principle articulates that manufacturers should be able to communicate truthfully, publicly, and appropriately within the medical community about uses for their products which are outside the FDA-approved labeling.

While these principles are notably unprecedented in their distinguishable disregard for the FDA’s outdated regulatory scheme, they provided much-needed guidance for an industry that the FDA had left in the dark. With this action, the manufacturing industry reclaimed control over the dissemination of medical research, effectively asking the FDA to stay out of professional

scientific dialogues, and instead, stick to consumer protection. The FDA will always play an integral role in safeguarding public health by ensuring post-market communications do not misrepresent the benefits or risks of a particular treatment. But manufacturers are encouraging full, truthful disclosure regardless of the source, and they also seek authorization for responsible distribution of scientific knowledge, which ultimately may help accelerate medical innovation.

On August 31, 2016, the FDA issued a notification of a public hearing, asking for comment on communication of unapproved uses of approved or cleared medical products. *Manufacturer Communications Regarding Unapproved Uses of Approved or Cleared Medical Products*, 81 Fed. Reg. 60,299, (Sep. 1, 2016) (public hearing and request for comments regarding 21 C.F.R. § 15). The hearing was scheduled to take place on November 9 and 10, 2016, and the FDA will accept public comment, though electronic or written comments, until January 9, 2017.

Within the FDA's announcement, it conceded that "relevant, truthful, and non-misleading scientific or medical information about an unapproved use may help health care professionals make better individual patient decisions." *Id.* at 60301. Still, the FDA requested comment on how such truthful information should or should not be communicated by medical firms, considering that it is already available to medical professionals through scientific journals and clinical practice guidelines. It seems as if the FDA has recognized that there are First Amendment protections for truthful speech, though it is still concerned with promoting public safety. Joanne Hawana & Joseph Lipchitz, *FDA Announces Dates for Long-Awaited Public Hearing on Its Regulation of Off-Label Communications*, Mintz Levin: Health Law & Policy Matters (Sept. 1, 2016), *available at* <https://www.healthlawpolicymatters.com>. Striking a balance

between protecting consumers and encouraging scientific and medical innovation will be key for the FDA during the hearing and comment review.

Many critics are suggesting that due to the nature of the FDA's request, it may be long into 2017 (or later) before manufacturers receive updated guidance. Jeff Overley, *3 Takeaways From FDA's Off-Label Forum Plan*, Law360 (Aug. 31, 2016, 9:23 P.M.), available at www.Law360.com (requiring subscription registration). Others, including PhRMA, have stated that they are pleased and hopeful, given the FDA's open-mindedness to truthful, non-misleading speech and the weight of the recent litigation, which reasonably has left the FDA much to consider.

In the meantime, the fight for many companies is not yet over. For example, prior executives of the company Acclarent are currently appealing a jury's decision to convict on multiple misdemeanors. Brian Amaral, *Ex-Acclarent Execs Want Misdemeanor Convictions Tossed*, Law360 (Aug. 2, 2016, 1:49 P.M.), available at www.law360.com (requiring subscription registration). Former CEO William Facteau and former Vice President of Sales Patrick Fabian were brought to court under multiple charges involving the misbranding of a medical instrument, called the Stratus, which was used for clearing patients' sinuses. While the device had been cleared for public use, prosecutors contended that the FDA had approved the device only for use with a saline solution or salt water and that instead, sales representatives were encouraged to promote use of the Stratus with a liquid steroid.

While both Facteau and Fabian were acquitted of all felony charges, showing that the jury found no intent by either party to defraud medical professionals or mislead consumer usage, the strict-liability misdemeanor misbranding charges stuck. On appeal, in light of *Amarin's* wide publicity, Facteau and Fabian are likely to reargue their First Amendment claims. Yet, they may

also push the legality of misbranding misdemeanors under 21 U.S.C. § 333, which would officially ask the court to take a stance on the role intent in off-label promotion.

Conclusion

While the discussion seems far from settled, it appears that the industry and regulatory agencies are moving toward accepting recent court pronouncements that truthful, accurate, non-misleading speech regarding the off-label use of medical drugs and devices is protected by the First Amendment. Some industry members are lobbying the FDA to promulgate a regulatory scheme that promotes a free flow of medical and scientific information that is consistent with “the nine industry principles” proposed by PhRMA and BIO. The court pronouncements and lobbying efforts have driven the FDA to schedule a forum for the medical drug and device community to articulate its proposed changes to off-label standards and regulations. Changes to the guidance will likely carry over to drug and medical device litigation, during which the learned intermediary defense is commonly asserted.



Lighting the way to...

Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10



THURSDAY, MARCH 9, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

PREMISES AND SECURITY LIABILITY

Current Trends in Negligent Security Defense

Hampton

Speaker:

Michael C. Tyson

Trends In Negligent Security Defense: A Lawyer's Guide to Winning the Case

A. Introduction

In 2011, a Broward County jury awarded Yahtavian Bellamy, \$4,255,280 arising out of a shooting that occurred at *Boomers!*, a child entertainment and fun park, in Dania Beach, Florida. In the heat of an argument between patrons on the property, the gun holder, Angel Lopez, drove his vehicle up to the plaintiff in the parking lot and fired 15 shots through plaintiff's car door, striking the plaintiff in the legs. During the course of litigation, the plaintiff argued *Boomers!* knew or should have known that its park and parking lot were in a high crime area and should have provided security guards for the protection of its invitees. The plaintiff further argued that the shooting was foreseeable due a history of violent crime on the premises. The jury agreed, finding *Boomers!* 90% negligent and plaintiff 10% negligent for the underlying incident.

While not all shootings result in massive verdicts based on the negligence of the property owner and inadequacy of the owner's security, such results have become more common across the country. Therefore, as plaintiffs continue to file suit against apartment complexes, restaurants, hotels, movie theaters, and other commercial establishments, defense counsel must proactively strategize to defeat these claims. Accordingly, this article explains the underlying themes of negligent security defense and strategies to combat the plaintiff's case.

B. Foreseeability Experts

1. How They Can Help

Retention of a security expert to testify regarding the foreseeability of the underlying incident is critical to defending any negligent security case. Two types of experts are generally available to render a foreseeability opinion: criminologists and ex-law enforcement officers. Overall, criminologists tend to be more polished and are likely to appeal more to educated jurors, largely because of the long list of lettered credentials attached to their name. However, criminologists lack actual field experience regarding criminal behavior, which can reduce their effectiveness. Since the average juror is programmed to think police officers know about crime, it may be beneficial to skip the criminologist and opt for a seasoned veteran in the police force or one who retired from law enforcement.

A security expert's role is to connect the dots for the jury and provide a concrete analysis as to why the subject incident was entirely: (1) unanticipated; and (2) unpreventable. Foreseeability of a crime in a negligent security case is based on the knowledge of the property owner. This standard requires only that the general danger, not the exact sequence of events that produced the harm, be foreseeable. *Johnson v. Seagle Pizza, Inc.*, No. 2015-CA-000085-MR, 2016 WL 4410705, at *7 (Ky. Ct. App. Aug. 19, 2016). Foreseeability is generally couched in expert testimony as whether the premises owner had cause to anticipate the incident. "Cause to anticipate" the incident may arise from actual or constructive knowledge that an atmosphere of violence existed on the premises.

Evidence used to establish foreseeability includes: (1) evidence from the particular property in question; (2) evidence from the general vicinity neighborhood; and (3) evidence from

similar properties that are outside the specific neighborhood. *See, e.g., Smith v. Regal Entm't*, 36 N.Y.S.3d 50 (N.Y. Civ. Ct. 2016) (explaining “[t]o establish foreseeability, the criminal conduct at issue must be shown to be reasonably predictable based on the prior occurrence of the same or similar criminal activity at a location sufficiently proximate to the subject location.”); *Rivera v. Wilson*, No. CV-156026424S, 2016 WL 402318, at *5 (Conn. Super. Ct. Jan. 13, 2016) (denying defendant’s motion for summary judgment in negligent security case where the plaintiff presented evidence of other motor vehicle thefts in the surrounding area, as well as thefts involving motor vehicle parts at the defendant’s premises, which raised a question of fact as to whether the defendant’s business was located in a high crime area)

Successful testimony from foreseeability experts generally revolves around the following five factors: (1) proximity, (2) recency, (3) frequency, (4) similarity, and (5) publicity of other incidents on the subject property. Stated more succinctly, a foreseeability expert should evaluate whether any criminal conduct previously occurred on or near the property, how recently it occurred, how often it occurred, how similar the conduct was to the conduct on the property, and what publicity was given the occurrences to indicate that the landowner knew or should have known about them and distinguish the subject incident in any way possible. *Del Lado Partners, Inc. v. Smith*, 307 S.W.3d 762, 768 (Tex. 2010).

However, courts have generally excluded testimony of experts pertaining to the foreseeability of a specific person’s actions if the expert does not have a psychological background. *See, e.g., L.B. v. Naked Truth III, Inc.*, 117 So. 3d 1114, 1116 (Fla. 3d DCA 2012). In *L.B.*, the plaintiff, a sales clerk at an adult retail store, was working the overnight shift when a male customer entered the store, brandished his weapon, and ordered that she produce money from the store’s register and safe. The assailant ultimately raped the plaintiff.

The plaintiff sued the store under a theory of negligent security. Subsequent investigations revealed four prior armed robberies had occurred at the store during the overnight shift, the last one only two months before the events at issue. However, none of these incidents involved sexual assault. During the course of litigation, both parties retained experts to testify regarding the store’s security. Defendant’s expert testified that the attack was a “victim-targeted” crime that was unforeseeable and unpreventable despite security measures taken by Defendant. A jury ultimately awarded a defense verdict and the plaintiff appealed, arguing that the trial court erred in permitting defendant’s expert to testify pertaining to the assailant’s motive in choosing to attack the plaintiff. In holding the lower court erred in admitting the defense expert’s testimony, the appellate court opined:

The purpose of expert testimony is to assist the trier of fact in understanding the evidence, or in determining a fact issue but expert testimony is not admissible at all unless the witness has expertise in the area in which his opinion is sought. *The witness was qualified to render an opinion on security matters and on the defendant’s allegedly negligent security procedures, but not on the robbers’ motives for choosing (plaintiff) as their target. The reasoning behind the coconspirators’ conduct is a matter beyond the scope of his expertise.*

Id. at 1116 (internal citations and quotation marks omitted) (emphasis added).

Therefore, when seeking to introduce testimony regarding a third-party criminal's motives and the preventability of the subject crime, retention of a criminal behavioral analyst or another expert with a strong psychological background is recommended.

2. How to Undermine the Plaintiff's Security Expert

One effective strategy used to undermine the opponent's security expert is to obtain the crime grid for the expert's office—where the plaintiff's expert will presumably be deposed—and compare it to the crime grid where the incident took place. If more or the same amount of prior similar crimes exist in the vicinity of the expert's office as compared to the commercial establishment at issue, this can provide a highly effective line of questioning. Additionally, security experts are often caught off guard based when confronted with such inquiries.

C. Strategies for Getting Criminal Background and Lifestyle into Evidence

1. Criminal Background and Lifestyle Relevant To Damages

The criminal background and lifestyle of a victim in a negligent security case can be particularly impactful as many jurors have little or reduced sympathy for a party with a criminal past or a history of drug and/or alcohol abuse. Moreover, evidence the decedent has been shot before tends to resonate with jurors and can be very effective when arguing that the decedent engaged in a lifestyle that made the subject crime inevitable.

While evidence pertaining to past crimes and lifestyle choices of a decedent are typically excluded from evidence at trial—as prior bad acts or inappropriate character evidence—there are several ways that defense attorneys have managed to get this information in. The first is to argue evidence of a defendant's past crimes and lifestyle is highly relevant to the determination of future lost earnings or income of the decedent, damages recoverable under most wrongful death statutes. *See Botte v. Pomeroy*, 497 So. 2d 1275, 1278 (Fla. 4th DCA 1986) (finding evidence of prior drug use was permitted as it showed a track record of inability to carry on useful employment and, as such, was admissible to rebut a claim for future earning capacity); *Dembinski v. Thomas*, No. 96-C-3039V, 2000 WL 33251877, at 357-58 (Pa. Com. Pl. June 8, 2000) (finding evidence of decedent's heroin addiction “highly relevant to determining the decedent's life expectancy and future earning capacity, which the jury will be required to consider in evaluating plaintiff's damage claim” in wrongful death case). The factors generally considered in determining a proper award for lost future income include, *inter alia*, the decedent's physical condition before his death, the decedent's past work history and consistency thereof, the amount the decedent probably would have earned absent the death, and the probability that the decedent would have continued to earn wages over the remainder of his working life. *Brossett v. Howard*, 998 So. 2d 916, 932 (La. Ct. App. 2008).

Even in Florida, where evidence of prior drug and/or alcohol use has been held admissible, courts are cautious to admit evidence of prior drug and/or alcohol use and do so under “certain very limited circumstances,” which are highly fact specific. *Sabol v. Bennett*, 672 So. 2d 93, 94 (Fla. 3d DCA 1996); *Knight v. Robinson*, No. 09-23462-CIV, 2015 WL 11198781, at *3 (S.D. Fla. Jan. 16, 2015) (admitting some evidence of the plaintiff's prior drug use but also clarifying for the jury drug use could not be used to attack the plaintiff's credibility but only to

evaluate her ability to perceive and recall events); *Cf. Mount v. Camelot Care Ctr. of Dade, Inc.*, 816 So. 2d 669, 670 (Fla. 3d DCA 2002) (finding the probative value of the evidence regarding past drug and alcohol problem substantially outweighed by the danger of unfair prejudice).

Since individuals with a significant criminal history or history of drug/alcohol abuse are typically unable to provide for their families, one can effectively argue they would not been able to provide a steady stream of income had the incident not occurred. In a negligent security case involving a death, defense counsel must expeditiously ascertain any survivors and obtain a comprehensive background on the decedent—his or her criminal history, records pertaining to domestic abuse injunctions, autopsy photos, and a social media search to screenshot any posts/photos which may get taken down later in the case at the direction of the plaintiff's counsel. Autopsy photos are particularly informative because they reveal tattoos showing everything from gang affiliations to ex-paramours. Gang symbol tattoos can also support an argument the decedent did not have a stable stream of income in the past and would not have had one in the future, again negating an element of damages.

Courts around the country, while reluctant to do so, admit personal background evidence of the decedent for the purpose of the calculating damages. In *Basham v. Terry*, 102 S.E.2d 285 (Va.1958), the Supreme Court of Virginia allowed defense counsel in a wrongful death action to cross-examine decedent's daughters pertaining to decedent's habits of alcoholism when evidence was first introduced establishing decedent's sobriety. In that case, the court permitted evidence of decedent's "exemplary habits and that he was a considerate, devoted and hardworking husband and father." *Id.* at 289. Accordingly, the Court found that evidence of decedent's flagrant alcohol abuse was essentially determinative of damages and that it would be unreasonable to allow plaintiff to paint a picture of decedent that was grossly inaccurate.

Likewise, in *Stocki v. Nunn*, 351 P.3d 911, 929 (Wyo. 2015), the Wyoming Supreme Court allowed the introduction of evidence of the accident victim's drug and alcohol use, particularly that the victim smoked one pack of cigarettes a day and drank a six-pack of beer per day. The Court held that lifestyle evidence was relevant to life expectancy, and found that life expectancy of the victim is always relevant to the calculation of damages. Moreover, the Court recognized a general medical nexus between overall health and smoking, finding that a person's drinking habits may influence their life expectancy. As such, other courts have found that evidence of chronic drug and alcohol abuse is admissible because it "suggested that [the plaintiff's] life expectancy deviated from the average." *Kraus v. Taylor*, 710 A.2d 1142, 1144 (Pa. Super. Ct.1998).

2. Criminal Background and Lifestyle Relevant to Comparative Fault and Statutory Defenses.

Many states allow evidence of voluntary intoxication as a means to establish comparative fault or, in some cases, to serve as a complete bar to recovery. In New York, where an intoxicated individual may not recover for his or her injuries under New York's Dram Shop Act, it is also well established an individual's intoxication may comparatively reduce an award for injuries caused by another's negligence. *See Ali v. Connick*, No. 11-5297, 2016 U.S. Dist. LEXIS 67466 (E.D. N.Y. May 23, 2016). Utah's comparative fault statute bars recovery where the plaintiff is 50% or more at fault—and in most cases an intoxicated individual negligence will

likely exceed that of the premises owner. UTAH CODE § 78B-5-817 (2016).

In states like Washington and Florida, intoxication serves as a complete bar to recovery depending on the level of intoxication. For example, RCW 5.40.060(1) states in pertinent part:

[I]t is a complete defense to an action for damages for personal injury or wrongful death that the person injured or killed was under the influence of intoxicating liquor or any drug at the time of the occurrence causing the injury or death and that such condition was a proximate cause of the injury or death and the trier of fact finds such person to have been more than fifty percent at fault.

RCW 5.40.060(1) (2016). Similarly, Florida law provides a plaintiff in a civil action may not recover damages for loss or injury to his person or property if the trier of fact finds that he was:

[U]nder the influence of any alcoholic beverage or drug to the extent that the plaintiff's normal faculties were impaired or the plaintiff had a blood or breath level of 0.08 percent or higher; and as a result of such alcoholic beverage or drug, the plaintiff was more than 50 percent at fault for his or her own harm.

FLA. STAT. § 768.36 (2016). The intoxication affirmative defense available in Florida has long been applied to wrongful death actions against the claims of a personal representative brought on behalf of the decedent's survivors. *See Griffis v. Wheeler*, 18 So. 3d 2, 5 (Fla. 1st DCA 2009). This is significant as many negligent security cases involve the death of the alleged victim.

In Illinois, evidence of drinking is admissible if there is also evidence "of intoxication with impairment of physical or mental capabilities." *Smith v. Stone*, No. 5-11-0541 (Ill. 5th App. Mar. 23, 2013). As the *Stone* Court elucidated:

Evidence of a plaintiff's intoxication is relevant to the extent that it affects the care he takes for his own safety and is therefore admissible. Such evidence is only relevant if the defendant can show that the plaintiff's lack of due care was causally related in some way to the injury. It is improper to insinuate or imply that a party is intoxicated based solely on evidence of drinking. Instead, the evidence must show that the intoxication resulted in an impairment of mental or physical abilities and a corresponding diminution in the ability to act with ordinary care. This impairment may be shown either directly or by reasonable inference.

Id. at 7 (internal citations and quotation marks omitted). To establish entitlement to the intoxication affirmative defense as either a complete bar to recovery or a means to establish the plaintiff's comparative fault, defense counsel should utilize blood alcohol test results, testimony from an expert toxicologist, and external indicia of impairment from witnesses who observed the plaintiff and/or decedent prior to the event in question. Obviously, once the jury hears evidence of the plaintiff's intoxication, they are much more likely to return a favorable verdict to the defense.

D. Discovery of Community Knowledge of Crime

A highly effective tactic in defending against a claim of negligent security is the use of testimony by members of the community who are familiar with the property. For example, the testimony of a tenant that she feels safe in her apartment complex, and even occasionally leaves her front door unlocked, typically resonates with jurors. Similarly, testimony from an employee that he has worked at the same factory for twenty years and has never seen a crime take place will ultimately be persuasive in proving to the jury that the defendant's property was ultimately a safe one.

However, using this type of anecdotal evidence is only as effective as the information is true, as jurors tend to have well-established beliefs about different areas of town. Therefore, introducing testimony from a tenant who lives in a horrible neighborhood that she couldn't imagine a safer place to raise her kids will ultimately serve to annoy the jury and discredit the defense's position during trial. On the flip side, learning the community's negative perception of a property or place of business as an unsafe place is equally important. Speaking with community members—whether it be other tenants, neighbors, employees, etc.—who may have knowledge of crime in the area as soon as possible is vital to establishing a defense strategy. The individuals should be interviewed in person early in the case and counsel should not simply rely on statements contained in police reports to gauge the community's perception of crime.

E. Taking the Depositions of Local Police and Community Leaders

Traditionally, there was public trust in police officers regarding matters of safety and security, which has undoubtedly been diminished in recent times. Deciding whether to take the deposition of a police officer that was involved in investigating a shooting, rape, robbery or other crime from which a claim for negligent security arose is a strategy call. Many police officers make very good witnesses. They are generally confident in their testimonial responses, polite, appear to be honest and non-confrontational. Their demeanor will usually make their testimony compelling. Depositions of law enforcement officers should be succinct as these individuals are pressed for time and have competing demands on their time. If you anticipate the police officer's testimony will be adverse to the defense, request for the officer's internal investigations file in advance of the deposition so you are aware of any disciplinary issues and can have a means to potentially discredit the officer's testimony.

F. Verdicts and Settlements From Around the Country

(1) Whether the Criminal Assailant is on the Verdict Form

In most states, in a premises liability action based on negligent security, the criminal assailant is placed on the verdict form and can be apportioned fault. *See, e.g., Graves v. N. E. Services, Inc.*, 345 P.3d 619, 636 (Utah 2015) (allowing fault to be apportioned among business owner and intentional wrongdoer); *Rodenburg v. Fargo-Moorhead Young Men's Christian Ass'n*, 632 N.W.2d 407, 418 (N.D. 2001) (concluding the trial court did not err in determining the jury must compare the negligence, if any, of the YMCA with the intentional tort of the assailant); *GFI Mgmt. Svcs., Inc. v. Medina*, 733 S.E.2d 329, 330 (Ga. Ct. App. 2012) (holding unknown

criminal assailants could be on the verdict form for apportionment of fault); *Rosner v. Denim & Diamonds, Inc.*, 937 P.2d 353, 356 (Ariz. Ct. App. 1996) (holding the trial court did not abuse its discretion by permitting the jury to apportion fault on non-party assailants in negligent security action against a nightclub). However, in a minority of states, such as Florida and Mississippi, juries are not allowed to apportion fault among the criminal assailant/wrongdoer and the premises owner/operator. See, e.g., *Merrill Crossings Assocs. v. McDonald*, 705 So. 2d 560, 562 (Fla.1997); *Whitehead v. Food Max of Mississippi, Inc.*, 163 F.3d 265 (5th Cir. 1998) (applying Mississippi law and finding exclusion of assailants from verdict form and omission of their share of fault was appropriate).

In *Merrill Crossings*, the defendant unsuccessfully sought to have the jury apportion fault between itself and a tortfeasor who shot the plaintiff in a Wal-Mart parking lot. *Merrill Crossings*, 705 So. 2d at 562. Although the court in that case disallowed apportionment between the negligent defendant and the intentional tortfeasor, the court allowed apportionment of fault between two negligent parties—Wal-Mart and the property owner. *Id.* at 562-63. Because apportionment between the property owner and assailant can significantly impact the value of a negligent security case, knowing the law of your jurisdiction on this issue is critical to appropriately evaluating the case.

(2) Favorable Verdicts for Plaintiffs

For plaintiffs' attorneys, proving the foreseeability of various criminal acts can yield multi-million dollar verdicts, as illustrated below.

Crisp, et. al. v. The McDonald's Corporation et. al.

On July 30 2014, a jury in Brazos County, Texas awarded \$27 million in a lawsuit against McDonald's relating to the 2012 deaths of two Blinn College students. In the early morning of February 18, 2012, the decedents, Denton James W., 18, and Lauren Bailey C., 19, stopped with another couple at the College Station McDonalds near Texas A&M University. While walking through the McDonald's parking lot, Mr. W. was assaulted by a vicious mob of 15 to 20 attackers. Ms. C. loaded Mr. W. into an SUV with the help of their two friends, who raced them to the nearby hospital. However, the driver ran a red light en route, and collided with a pickup truck, resulting in a crash that killed Ms. C. The estate of Mr. W. subsequently asserted that he perished in the parking lot.

The families of both decedents filed suit in the 361st District Court of Brazos County, accusing The McDonalds Corporation of liability for the wrongful death of both deaths, based on the company's negligent security. The defendant maintained that because Mr. W. died in the car wreck that followed and not on defendant's property, the company wasn't responsible for the teens' safety. At trial, the decedents' families argued that defendant should have provided better security at the restaurant. College Station police officers testified that they regularly were called to the location to break up fights and disperse unsupervised crowds numbering in the hundreds, between 2 a.m. and 4 a.m. on weekends. Two former managers who were working the location that night testified that they were unaware of any problems.

The plaintiffs asserted the defendant's, having never hired any security personnel, and having never installed security cameras to protect customers, created a negligent state of security. After six days of trial, the jury returned a verdict for the plaintiff, and awarded \$27,000,000 in actual damages.

The Estate of Tanya Renee Wilson and the Estate of Latonya Sharon Brown v. Yvonne Hiller and U.S. Security Associates, Inc.

On March 31, 2015, a jury in Philadelphia awarded \$46,532,600 in a lawsuit against U.S. Security Associates, Inc., a company hired to provide security services at a Kraft Food Factory. Two women were shot and killed at the food factory when a disgruntled employee, Yvonne Hiller, gained access to the factory and shot the women who were in a break room at the plant.

On the night of the shooting, Hiller and a group of Kraft workers were waiting in line to get their hearing tested when Hiller started ranting about being sprayed with toxins. Several in the group reported the strange behavior to supervisors who listened to both sides of the story and decided to suspend Hiller. After the defendant was escorted out of the plant, she returned to a back entrance armed with a gun and ultimately shot the two Kraft employees. The plaintiffs maintained that the defendant security company was negligent in failing to properly escort Hiller to her vehicle immediately after she was suspended, and in failing to notify people in the building that Hiller had returned with a gun.

On February 26, 2015, the jury found in favor of the plaintiffs, and awarded compensatory damages of \$4,600,000 to the Brown Estate, and \$3,420,000 to the Wilson Estate. The jury found Hiller 70% liable, and the defendant security company 30% liable. The jury awarded punitive damages in favor of plaintiff, The Estate of Brown, and plaintiff, The Estate of Wilson, in the amount of \$38,512,600 against U.S. Security Associates only.

(3) Favorable Defense Verdicts

Business operators and landowners cannot be expected to serve as insurers for the general public and juries often return defense verdicts in recognition that crimes by third-parties are not always foreseeable or preventable.

Stora v. Volunteers of New York, et. al.

On November 3, 2014, a New York County jury awarded a defense verdict in a matter involving the purported negligent security of a homeless shelter. The plaintiff, a 21-year-old male and resident of the homeless shelter run by the defendant, contended that the defendant negligently failed to provide adequate security to the shelter which he claimed would have prevented the subject incident.

After an altercation between himself and another resident, the other resident fled the facility. The plaintiff asserted that because of negligent security, the other resident gained access without going through the metal detectors by climbing a fence near the shelter. The plaintiff contended that because of the alleged inadequate security, he was shot. The defendant

maintained that the security was appropriate. The defendant contended that, in addition to the metal detectors, it also employed cameras and guards and that the targeted shooting could not be prevented by additional security.

Perez v. Leany's Enterprise Inc. d/b/a Napoles

A 29-year-old male restaurant worker and painter, Juan Perez, reportedly suffered a stab wound causing a right lung pneumothorax, a torn lower lip requiring plastic surgery repair, a nasal bone fracture, and a right shoulder labral tear as he left a restaurant and bar operated by defendant Leany's Enterprise Inc. d/b/a Napoles. Mr. Perez was allegedly was attacked by several other patrons just outside the bar's entrance.

The plaintiff claimed after the initial attack, the defendant's security employees refused his request for assistance and directed him to leave the premises, and as a result, he was beaten again and stabbed by the same patrons in the parking lot. The plaintiff claimed the defendant was negligent for failing to contact the police or take other measures to protect him from the second attack and stabbing; for failing to properly train, instruct and supervise its employees in the protection of patrons; and failing to exercise reasonable care in the selection of its employees and/or contractors providing security services.

The defendant denied liability, and claimed that the assault occurred while the plaintiff was drinking in the bar's parking lot after it was closed and its employees were gone. On July 29, 2015, the Suffolk County jury found the defendant was not negligent in providing security to the plaintiff.

Garnicki v. Hialeah Fuels and Caraf IV

The plaintiff in this matter alleged that he was shot in the back due to the inadequate security provided by the defendants, the owner and operator of a gas station in Hialeah, Florida. The defendants maintained that the crime was neither foreseeable nor preventable and that the defendants were not responsible for the plaintiff's injuries. The plaintiff was shot during a robbery on the defendants' premises in front of his wife and four children.

The plaintiff, through his security expert, claimed that the defendants should have had a security guard on the premises. The plaintiff claimed that the station's two prior robberies, two aggravated assaults and multiple other crimes necessitated the guard. The two assailants, who were apprehended after the shooting, testified that they would not have committed the robbery if there had been a security guard present.

The plaintiff was diagnosed with a fractured spine, disc herniations, pancreatic damage, and nerve injury to his legs, as well as extensive scarring, as a result of the shooting. The defense did not present a security expert. The plaintiff asked the jury to award damages of seven-figures during closing arguments. On July 29, 2013, the Miami-Dade jury returned a verdict in favor of the defendants, finding no negligence which was a legal cause of injury to the plaintiff. Post-trial motions are pending.

Conclusion

Not surprisingly, jury verdicts for wrongful death cases alleging negligent security yield the highest jury verdicts. However, these cases can be defended and won if the proper foreseeability experts are retained; all avenues of introducing the victim's poor lifestyle choices, drug use, alcohol use, etc. are explored; and law enforcement officers are selectively deposed with full consideration of their impact on the case. Because community knowledge of crime can play a significant role in the foreseeability analysis, in cases where the knowledge of crime is detrimental to the defense, framing the contested issues narrowly generally will benefit the defense—i.e. whether the premises owner owed a specific affirmative duty to provide armed security guards rather than whether it had a general duty to act reasonably to prevent injury to its tenants (customers, invitees, etc.).



THURSDAY, MARCH 9, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

**INTELLECTUAL PROPERTY, COMMERCIAL LITIGATION and
ALTERNATIVE DISPUTE RESOLUTION SECTIONS**

“Can You Keep a Secret?” The Federal Courts Can Help

Cypress

Speakers:

Michael A. Walshe

Ashley D. Hayes

Jose I. Rojas

John C. Sciacotta

Neil A. Hartzell

Kevin Cain

DEFEND TRADE SECRETS ACT OF 2016

I. Overview of Statute

The “Defend Trade Secrets Act of 2016” (“DTSA”) was signed into law by President Obama on May 11, 2016. DTSA amends Chapter 90 of Title 18, United States Code (the “Economic Espionage Act” (“EEA”)), codified, as amended, at 18 U.S.C. §§ 1831-1839 and the Racketeer Influence and Corrupt Organizations Act, 18 U.S.C. §§ 1961-1968 (“RICO”). The most significant change to the EEA involved striking and rewriting the entirety of 18 U.S.C § 1836(b) to provide for a private civil Federal cause of action for owners of trade secrets for the misappropriation of trade secrets used in, or intended for use in, interstate or foreign commerce. The key provision is as follows:

“(1) IN GENERAL. – An owner of a trade secret that is misappropriated may bring a civil action under this subsection if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce.”

II. Key Amendments to the EEA

A. Private Civil Actions.

The most significant amendment to the EEA provides an owner of a trade secret that has been misappropriated with the right to bring a civil action in either a Federal district court or a state court when the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce. This is an entirely new Federal cause of action. Prior to the enactment of the DTSA, the EEA only provided for criminal prosecution of individuals and/or organizations alleged to have intentionally engaged in “economic espionage” or “theft of trade secrets.”

Prior to the DTSA, civil actions alleging misappropriation of trade secrets were based primarily on state law and often prosecuted in state courts. All but two states have adopted a form of the Uniform Trade Secrets Act (UTSA) and actions can still be brought under those state statutes. The DTSA does not preempt state laws. Therefore, if additional claims can be asserted under any other applicable statutory or common law theories they should be included in any Complaint which may be filed.

B. Civil Seizure Procedures.

The DTSA provides the owner of a trade secret that has been misappropriated with the right to seek an order to seize property necessary to prevent the propagation or dissemination of the trade secret. The statute specifically provides for an *ex parte* application procedure as follows:

“(i) APPLICATION.—Based on an affidavit or verified complaint satisfying the requirements of this paragraph, the court may, upon ex

parte application but only in extraordinary circumstances, issue an order providing for the seizure of property necessary to prevent the propagation or dissemination of the trade secret that is the subject of the action.”

While a seizure order may be obtained *ex parte* by submitting an affidavit or verified complaint, the moving party must show “extraordinary circumstances,” before the order may issue. The statute provides strict requirements to be met by the moving party before an *ex parte* order may issue, including the following:

“(ii) REQUIREMENTS FOR ISSUING ORDER.—The court may not grant an application under clause (i) unless the court finds that it clearly appears from specific facts that—

“(I) an order issued pursuant to Rule 65 of the Federal Rules of Civil Procedure or another form of equitable relief would be inadequate to achieve the purpose of this paragraph because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order;

“(II) an immediate and irreparable injury will occur if such seizure is not ordered.”

The DTSA imposes a heavy burden upon the applicant to establish to the court’s satisfaction that a balancing of interests favors the applicant. The court must find a likelihood of success on the merits and sufficient proof that the person against whom seizure would be ordered has actual possession of the property to be seized. The applicant must provide the court with a detailed description of the property and location of the property to be seized, an allegation that the accused would likely destroy, move, hide, or otherwise make such matter inaccessible to the court. And the applicant must aver that he has not publicized the requested seizure.

The DTSA requires the court to include the following elements in its order:

- (i) Findings of fact and conclusions of law required for the order;
- (ii) Provide for the narrowest seizure of property necessary to achieve the purpose of this paragraph and direct that the seizure be conducted in a manner that minimizes any interruption of the business operations of third parties and, to the extent possible, does not interrupt the legitimate business operations of the person accused of misappropriating the trade secret;
- (iii) Provisions to protect the seized property from disclosure and address how access may be granted;
- (iv) Provide guidance to Federal Law enforcement officials executing the seizure that clearly delineates the scope of the authority of the officials;
- (v) Notice of hearing not later than 7 days after the *ex parte* order has issued;

- (vi) Set an amount of security to be paid by the applicant adequate for the payment of the damages that any person may be entitled to recover as the result of a wrongful or excessive seizure or wrongful or excessive attempted seizure.

The statute specifically requires the court to consider protecting the accused's reputation as follows:

“(C) Protection from publicity. The court shall take appropriate action to protect the person against whom an order under this paragraph is directed from publicity, by or at the behest of the person obtaining the order, about such order and any seizure under such order.”

The materials seized are placed in the custody of the court. If the material is in a storage medium which can be connected to a network, the court will forbid network connection. The court is also required to protect the confidentiality of the seized materials that are unrelated to the trade secret information it ordered to be seized. The court is empowered to appoint a special master to locate and isolate all misappropriated trade secret information and to facilitate the return of unrelated property and data to the person from whom the property was seized. A party or a person who claims to have an interest in the subject matter seized may make a motion at any time to encrypt any material seized or to be seized to further protect the materials from disclosure.

The seizure order is carried out by a Federal law enforcement officer or a State or local law enforcement official if specifically designated in the order. Upon law enforcement request, the court may permit an unaffiliated technical expert to assist in the seizure provided the expert is bound by a court approved non-disclosure agreement and the court finds that the expert's participation will aid in the efficient execution of and minimize the burden of the seizure.

At the seizure hearing scheduled within 7 days of the issuance of the *ex parte* order, the applicant will have the burden of proof and if the burden is not met, the order must be dissolved. The party against whom the order has been issued or any other person harmed by the order may move at any time to dissolve or modify the *ex parte* order after giving notice to the party who obtained the order. The court may make such orders modifying the time limits for discovery under the Federal Rules as may be necessary to prevent the frustration of the purposes of a seizure hearing.

A person who suffers damage by reason of a wrongful or excessive seizure has a cause of action against the applicant for actual damages suffered and may be entitled to punitive damages and reasonable attorney fees under the same standards as provided under section 34(d)(11) of the Trademark Act of 1946 (15 U.S.C. 1116(d)(11)).

C. Remedies

In an action for misappropriation, a court may order injunctive relief to prevent actual or threatened misappropriation on such terms as the court deems reasonable, provided the order does not prevent a person from entering into an employment relationship or conflict with applicable State law prohibiting restraints on employment.

The DTSA expressly rejects the “inevitable disclosure doctrine” which might otherwise allow the court to assume that a former employee will disclose trade secrets if employed by a competitor. Instead, the DTSA requires that any injunctive relief that prevents or restricts a person’s employment must be “based on evidence of threatened misappropriation and not merely on the information the person knows.”

A court also may:

“(B) award—

“(i) (I) damages for actual loss caused by the misappropriation of the trade secret; and

“(II) damages for any unjust enrichment caused by the misappropriation of the trade secret that is not addressed in computing damages for actual loss; or

“(ii) in lieu of damages measured by any other methods, the damages caused by the misappropriation measured by imposition of liability for a reasonable royalty for the misappropriator’s unauthorized disclosure or use of the trade secret;

“(C) if the trade secret is willfully and maliciously misappropriated, award exemplary damages in an amount not more than 2 times the amount of the damages awarded under subparagraph (B); and

“(D) if a claim of the misappropriation is made in bad faith, which may be established by circumstantial evidence, a motion to terminate an injunction is made or opposed in bad faith, or the trade secret was willfully and maliciously misappropriated, award reasonable attorney’s fees to the prevailing party.”

These remedies are discussed in more detail in Section III, below.

D. Jurisdiction

The DTSA provides district courts of the United States with original jurisdiction of civil action brought under the statute. Similar to trademark cases, the Federal

claims can be asserted in a State court action but will be subject to possible removal by the defendant.

E. Limitations Period

The DTSA includes the following limitations language:

(d) Period of Limitations. A civil action under subsection (b) may not be commenced later than 3 years after the date on which the misappropriation with respect to which the action would relate is discovered or by the exercise of reasonable diligence should have been discovered. For purposes of this subsection, a continuing misappropriation constitutes a single claim of misappropriation.”

F. Key Definitions added to 18 U.S.C § 1839

The DTSA adds two key terms, “misappropriation” and “improper means”, to the definitional section of the EEA which are defined as follows:

*(5) the term “**misappropriation**” means—*

(A) acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means; or

(B) disclosure or use of a trade secret of another without express or implied consent by a person who—

(i) used improper means to acquire knowledge of the trade secret;

(ii) at the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was—

(I) derived from or through a person who had used improper means to acquire the trade secret;

(II) acquired under circumstances giving rise to a duty to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(III) derived from or through a person who owed a duty to the person seeking relief to maintain the secrecy of the trade secret or limit the use of the trade secret; or

(iii) before a material change of the position of the person, knew or had reason to know that—

(I) the trade secret was a trade secret; and

(II) knowledge of the trade secret had been acquired by accident or mistake;

(6) the term “improper means”—

(A) includes theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means; and

(B) does not include reverse engineering, independent derivation, or any other lawful means of acquisition

G. Increased Criminal Sanctions Against Organizations

The DTSA dramatically increased the potential criminal penalties against organizations found guilty of “Theft of Trade Secrets” as defined in 18 U.S.C § 1832(a). Individuals continue to face possible fines up to \$5,000,000 or imprisonment up to 10 years but the EEA was amended to increase the potential sanctions against organizations as follows:

(b) Any organization that commits any offense described in subsection (a) shall be fined not more than the greater of \$5,000,000 or 3 times the value of the stolen trade secret to the organization, including expenses for research and design and other costs of reproducing the trade secret that the organization has thereby avoided.

H. Procedural Protections Afforded Trade Secret Owners to Maintain Confidentiality

The DTSA provides that “[t]he court may not authorize or direct the disclosure of any information the owner asserts to be a trade secret unless the court allows the owner the opportunity to file a submission under seal that describes the interest of the owner in keeping the information confidential.” The submission does not waive any rights in the criminal prosecution nor does the submission act as a waiver of trade secret protection “unless the owner expressly consents to such waiver.”

I. Attorney General’s Reporting Requirements to Congress

The DTSA mandates that no later than May 11, 2017 and biannually thereafter, the Attorney General, in consultation with the Intellectual Property Enforcement

Coordinator, the Director, and the heads of other appropriate agencies, shall submit to the Committees on the Judiciary of the House of Representatives and the Senate, and make publicly available a report addressing such things as:

“(1) The scope and breadth of the theft of the trade secrets of United States companies occurring outside of the United States.

(2) The extent to which theft of trade secrets occurring outside of the United States is sponsored by foreign governments, foreign instrumentalities, or foreign agents.

(3) The threat posed by theft of trade secrets occurring outside of the United States.

(4) The ability and limitations of trade secret owners to prevent the misappropriation of trade secrets outside of the United States, to enforce any judgment against foreign entities for theft of trade secrets, and to prevent imports based on theft of trade secrets overseas.

(5) A breakdown of the trade secret protections afforded United States companies by each country that is a trading partner of the United States and enforcement efforts available and undertaken in each such country, including a list identifying specific countries where trade secret theft, laws, or enforcement is a significant problem for United States companies.

(6) Instances of the Federal Government working with foreign countries to investigate, arrest, and prosecute entities and individuals involved in the theft of trade secrets outside of the United States.

(7) Specific progress made under trade agreements and treaties, including any new remedies enacted by foreign countries, to protect against theft of trade secrets of United States companies outside of the United States.”

The stated purpose of this mandate is for the Attorney General to provide recommendations to congress to reduce the adverse economic impact caused by the theft of trade secrets of U.S. companies, educate those companies regarding the threats outside of the U.S. and provide assistance to U.S. companies to protect their trade secrets and provide a mechanism for U.S. companies to anonymously report the theft of their trade secrets occurring outside the United States.

J. Immunity for Whistleblowers and Employee Notice Requirements

The DTSA provides immunity from both civil and criminal sanctions under the EEA for disclosure of a trade secret made to Federal, State, or local government officials solely for the purpose of reporting or investigating a suspected violation

of law; or when made in a complaint or other document filed in a lawsuit or other proceeding, provide the filing is under seal.

An individual who may be an employee or former employee who files a suit alleging retaliation by his employer for reporting a suspected violation of law may disclose the trade secret to his attorney and to the court subject to certain restrictions. Any filing with the court must be under seal and no disclosure can be made without first obtaining a court order.

The DTSA also includes a requirement that all employers who subject their employees to any contract or agreement that governs the use of a trade secret or other confidential information must provide notice of the immunity afforded under the statute. Failure to comply with this notice requirement will prohibit the employer from an award of exemplary damages or attorney fees in an action against an employee to whom notice was not provided.

III. Amendments to Racketeer Influence and Corrupt Organizations Act

The DTSA also amends the Racketeer Influence and Corrupt Organizations Act, 18 U.S.C. §§ 1961-1968 (“RICO”) by adding 18 U.S.C. §§ 1831 and 1832 (relating to economic espionage and theft of trade secrets) to the definition of “racketeering activity” as defined in 18 U.S.C. § 1961(a).

IV. Detailed Analysis of Civil Remedies under the DTSA

A. Damages

As stated above, 18 U.S.C. §1836 (b)(3)(B)(i) provides for damages for actual loss caused by misappropriation of the trade secret and damages for any unjust enrichment that is not addressed in compensatory damages for actual loss.

In other words, if due to the nature of the trade secret, a claimant cannot prove actual damages based on, for example, diminished sales caused by a competing product, the DTSA provides for an alternative damages method.

This would of course require discovery of the amounts of product sold with the typical offsets of expenses, but would require detailed discovery of the misappropriating party’s (“MP”) sales and marketing costs. Such discovery could lead to claims by the MP of needed protection of their own trade secrets. Confidentiality orders - - some of which may be limited to attorneys and outside experts’ eyes only - - may be needed.

If damages by actual loss or unjust enrichment are too difficult to prove, the DTSA provides an alternative method: a reasonable royalty for the MP’s unauthorized disclosure or use of the trade secret. Note that this section of the DTSA provides a royalty remedy for disclosure or use. Virtually all damage calculations will require expert testimony by accountants and industry experts in the appropriate field for, among other things, development costs and standards for industry royalty fees.

1. Exemplary Damages

The DTSA provides that the court may award exemplary damages in an amount not more than two times the actual damages under Subparagraph B of the DTSA (described above) if the trade secret is willingly and maliciously misappropriated. While the DTSA does not define maliciously, the word itself is defined as having intent to harm others. Obviously, the circumstances of any such theft, time of loss, method and who committed the theft would all be significant factors in determining and proving a claim for exemplary damages. Cases construing state law tort claims on theft or misappropriation may prove valuable guides on what is needed to prove a willing and malicious theft in connection with a trade secret misappropriation claim.

2. Attorneys' Fees

If a claim is proved for exemplary damages, the court may award reasonable attorneys' fees to the prevailing party. The DTSA does not provide for an award of attorneys' fees to a claimant without a finding of entitlement to exemplary damages. Claimants under the DTSA should also consider state law counts that may provide for an award of attorneys' fees if a claimant prevails on a claim under the DTSA but is unable to prove exemplary damages. Attorneys' fees may also be awarded to a defendant who proves that a claim of misappropriation was made in bad faith. The DTSA states that a bad faith claim may be established by circumstantial evidence. While fact scenarios can vary widely, some issues that may arise could concern the economic disparity between parties, market share and the desire to inhibit or prevent competition by bringing such a claim. The DTSA provides for attorneys' fees if motions to terminate an injunction are made or opposed in bad faith. Counsel involved with such claims or motions are well advised to carefully scrutinize client statements and documents in connection with any such motion.

B. Injunctive Relief

The DTSA provides for injunctive relief in certain circumstances.

A court may grant an injunction under the DTSA "to prevent any actual or threatened misappropriation." A motion for an injunction will in many cases determine the outcome of the case. Careful preparation, including confirming whether the claim actually involves a trade secret is critical. The DTSA's definition of trade secret is borrowed from the Economic Espionage Act and is broad. To qualify as a trade secret: (1) the owner must have taken reasonable measures to keep such information secret and (2) the information has to derive independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through paper means by, another person who can obtain economic value from the disclosure or use of the information. 18 U.S.C. §1389(3)(A)(B).

In some cases expert testimony concerning the nature of the trade secret may be needed. Verification of claimant's statements concerning claims under the DTSA is also critical in preparing any injunction motion. It is not unheard of for plaintiffs to make claims of

trade secrets only to find that the so-called trade secret was never protected or is comprised of substantial publically available information, thus undermining such a claim.

1. Ex Parte Motions

The DTSA provides for ex parte seizure of property. Such awards may only be granted in “extraordinary circumstances” based on specific facts that must describe with “reasonable particularity” the matter to be seized. 18 U.S.C. §1836(b)(2)(A). The court may not grant such an order unless it clearly appears from specific facts that other forms of equitable relief would be inadequate because the party to which the order would be issued would evade, avoid, or otherwise not comply with such an order. The claimant must also show immediate and irreparable injury, and show that the harm of denying the application substantially outweighs the harm to third parties. The claimant must also demonstrate that it is likely to succeed in showing that the information is a trade secret and that the information was misappropriated by improper means or the defendant conspired to use improper means to misappropriate the trade secret. Other specific requirements for an ex parte order are set forth in 18 U.S.C. §1836(b)(2)(B), and discussed above in Section II B.

2. Limitations on Injunctive Relief

The DTSA places two restrictions on injunctions because of “the importance of employee mobility.” The injunction may not: (1) prevent anyone from entering into an employment relationship; or (2) conflict with applicable state laws regarding restraints on trade.

The DTSA does not provide a means for circumventing unfavorable state law, thus an injunction will not issue if state law prohibits restraints on the practice of a lawful profession, trade, or business. An injunction under the DTSA is meant to coexist with and not preempt, influence, or modify established state law. The DTSA also does not permit an injunction that prevents a person from entering into an employment relationship. However, in the event the facts of a particular case demonstrate that there is evidence of a threat or misappropriation of trade secrets, conditions may be placed on such employment (e.g. restrictions on work in a particular industry segment).

Any conditions in an injunction will not be based merely on the information the person knows from their previous employment. 18 U.S.C. §1836(b)(3)(A). This language specifically rejects the “inevitable disclosure doctrine.” That doctrine, recognized in some states, concerns situations where a defendant’s new employment would inevitably lead the defendant to rely on plaintiff’s trade secrets. Thus for an injunction to issue, there must be evidence of threatened or actual misappropriation of a trade secret, not just what a person knows from his or her prior employment. Thus, forum selection clauses in any employer agreements are very important, as some states recognize the inevitable disclosure doctrine (e.g. Delaware, Illinois,

Connecticut, New Jersey)¹ and others do not (e.g. California, Maryland, Virginia, Louisiana). However, if an action is in a state that recognizes inevitable disclosure such law may be beneficial in proving entitlement to injunctive relief, but the requirements for evidence of threatened or actual misappropriation must still be met in order to obtain an injunction.

V. Criminal Penalties

As set forth above in Section II-G, the DSTA increased criminal penalties for the theft of trade secrets. Although the increased penalties are new, fighting economic espionage and theft of trade secrets from U.S. based companies has been a top priority for the FBI's Counterintelligence Division for years. The FBI created the Economic Espionage Unit in 2010 to focus solely on prosecuting cases under the Economic Espionage Act.² Since its creation, the number of economic espionage cases and theft of trade secret cases overseen by the unit has increased more than 60%.³

In 2015, the FBI, in collaboration with the National Counterintelligence and Security Center, launched a nationwide public awareness campaign to combat the threat of economic espionage, which “costs the American economy billions of dollars annually and puts our national security at risk.”⁴ The FBI warns that while historically, economic espionage was targeted mainly at defense-related and high-tech industries, “recent FBI cases have shown that no industry, large or small, is immune to the threat.”⁵ Any company with a proprietary product, process, or idea can be a target; any unprotected trade secret is ripe for the taking by those who wish to illegally obtain innovations to increase their market share at a victim company's expense.”⁶

Economic espionage occurs when a trade secret is stolen for the benefit of a foreign government, foreign instrumentality, or foreign agent.⁷ Theft of trade secrets subject to criminal sanctions essentially occurs when someone knowingly steals or misappropriates a trade secret for the economic benefit of anyone other than the owner.⁸

In order to educate trade secret holders about these crimes and encourage them to report suspected threats of theft and economic espionage to the FBI, rather than attempt to

¹ The list of states recognizing the inevitable disclosure doctrine is not exhaustive.

² See Statement before the Senate Judiciary Committee, Subcommittee on Crime and Terrorism, Washington D.C., May 13, 2014 (<https://www.fbi.gov/news/testimony/combating-economic-espionage-and-trade-secret-theft>), p. 3.

³ *Id.*

⁴ See *FBI Announces Economic Espionage Awareness Campaign*, <https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-economic-espionage-awareness-campaign>.

⁵ See *Economic Espionage, FBI Announces Nationwide Awareness Campaign*, <https://www.fbi.gov/news/stories/economic-espionage>.

⁶ *Id.*

⁷ 18 U.S.C. §1831.

⁸ 18 U.S.C. §1832(a).

address the issue through private negotiations or civil litigation alone, the FBI has released a variety of materials, including:

- 1) A 37 minute film called The Company Man: Protecting America's Secrets.⁹ The film is based on an actual case and demonstrates how a particular company was targeted by foreign actors and then worked with the FBI to resolve the problem.¹⁰
- 2) Recommendations for being more vigilant in protecting against threats of economic espionage, including: (1) Recognizing the threat; (2) Identifying and valuing trade secrets; (3) Implementing a definable plan for safeguarding trade secrets; (4) Securing physical trade secrets and limiting access to trade secrets; (5) Providing ongoing security training to employees; (6) Developing an insider threat program; and (7) Proactively reporting suspicious incidents to the FBI before proprietary information is irreversibly compromised.¹¹
- 3) A "Checklist for Reporting an Economic Espionage or Theft of Trade Secrets Offense," which describes the information that a trade secret holder should gather and provide to the FBI in the event of an offense. This information includes that related to a description of the trade secret, its value, measures taken to protect it, the existence of confidentiality or non-disclosure agreements, its location/method of storage, employee controls, and a description of the theft.¹²

In the event a trade secret holder suspects theft of its trade secrets or economic espionage, it should gather the information set forth in the FBI's checklist and contact its local FBI office or report the suspected activity at <https://tips/fbi.gov>, in addition to evaluating any civil action it may choose to pursue.

VI. Recent Case Law

From enactment of the DTSA in May 2016 through December 2016, a number of Federal District Courts have issued decisions which address elements of the new statutory language set forth in 18 U.S.C. 1836 et seq. Some decisions address the Plaintiff's entitlement to injunctive relief. A few decisions address the ability to bring a claim where the misappropriation occurs both before and after the effective date of the statute. One decision involves a motion to dismiss based on a claim of whistleblower immunity under the statute. Immediately below are brief summaries of these recent decisions which address the statute. Each case summary provides an overview of the facts, the claims alleged, and the issues addressed by each court. As evident from the summaries below, where ownership of the trade secrets is clear, the cases typically find in favor of the trade secret owner. However, where the owner of the trade secret fails to adequately protect against disclosure or the acquisition or disclosure of the trade secret information

⁹ See *Economic Espionage, FBI Announces Nationwide Awareness Campaign*, <https://www.fbi.gov/news/stories/economic-espionage>.

¹⁰ *Id.*

¹¹ *Id.*

¹² *Id.* A copy of the checklist is also provided at the end of these materials.

was arguably authorized, courts appear reluctant to grant preliminary injunctive relief in favor of the trade secret owner.

A. California District Court Cases

Henry Schein, Inc. v. Cook, No. 16-CV-03166-JST, 2016 WL 3212457 (N.D. Cal. June 10, 2016). This appears to be the first decision issued since enactment of the DTSA. Plaintiff, a healthcare product sales company, alleged that Defendant, a former field sales consultant for Plaintiff, stole proprietary and trade secret information prior to going to work for a competitor. Defendant signed Confidentiality and Non-Solicitation Agreements with Plaintiff. Plaintiff alleged that prior to resigning, Defendant electronically transferred from her work account to her personal computer, customer practice reports generated with Plaintiff's proprietary software, inventory reports, price quotations for prospective customers, ongoing equipment proposals, and specific customer-related sales and ordering data from Plaintiff's proprietary computer program.

Plaintiff's Complaint alleged eight causes of action¹³ including misappropriation under the California Trade Secrets Act¹⁴, Cal. Civ. Code § 3426, et seq. Plaintiff sought and was granted, ex parte, a temporary restraining order requiring that Defendant preserve all documents and data related to the case, and prohibiting Defendant from: altering or destroying any evidence or other materials; accessing, using or sharing any of the information at issue; and from soliciting accounts assigned to Defendant while employed by Plaintiff. The Court held that the information at issue constituted trade secrets. The Court further held that Plaintiff's allegations that Defendant had emailed and downloaded to her personal computer confidential information before leaving her employment, along with the executed Confidentiality and Non-Solicitation Agreements were sufficient to establish a likelihood of success on the DTSA claim, including establishing "improper means" as defined under the statute.

Henry Schein, Inc. v. Cook, No. 16-CV-03166-JST, 2016 WL 3418537 (N.D. Cal. June 22, 2016). This is a second decision issued in connection with the above case. Here, the Court decided Plaintiff's motion for a preliminary injunction seeking the same relief as provided above, but for the pendency of the case. In opposition, Defendant claimed that much of the trade secret information was generally available through Plaintiff's website and that many of the customers at issue came from an identifiable pool of dental practices and labs and/or were prior customers of Defendant prior to her employment with Plaintiff. The Court determined that the alleged trade secret information went well beyond lists of customers and dental practices or inventory numbers, prices, and order histories, known and ascertainable by others in the business. The Court held that Plaintiff was likely to succeed on its DTSA claim based on evidence showing that: it had created

¹³ Plaintiff's remaining six causes of action were for breach of fiduciary duty and duty of loyalty, breach of contract, breach of implied covenant of good faith and fair dealing, tortious interference with prospective economic advantage, violation of California Unfair Competition Law, violation of California Penal Code § 502.

¹⁴ The Uniform Trade Secrets Act will be referred to through the remainder of this section as the "UTSA."

the information at issue through proprietary software; the information included extensive data, such as buying patterns, margins, profit percentages, credit profiles, preferences and markets; and the information had been obtained through improper means—conduct that at a minimum breached Defendant’s Confidentiality Agreement. The Court upheld all aspects of the prior temporary restraining order, other than that which had prohibited Defendant from contacting or accepting business from accounts assigned to Defendant while employed by Plaintiff. The Court held that Plaintiff was not entitled to the non-solicitation portion of the temporary restraining order on the basis that the non-solicitation clause on which it was based was invalid under Section 1600 of the California Business and Professional Code, and Plaintiff could not establish that the non-solicitation portion of the injunction was necessary to protect Plaintiff’s trade secrets.

Trulite Glass and Aluminum Sols., LLC v. Smith, et al., No. 2:16-01798-CV-JAM-CKD, 2016 WL 5858498 (E.D. Cal. Oct. 6, 2016). Plaintiff, a manufacturer and distributor of aluminum and glass products, alleged that Defendants, former employees in top operational and sales positions, stole proprietary and trade secret information from Plaintiff, which they used to set up a competing enterprise. Plaintiff alleged that Defendants emailed themselves Plaintiff’s trade secret materials, including highly confidential customer lists, pricing data, supplier information, and strategic plans, all of which Defendants used to compete with Plaintiff.

Plaintiff’s Complaint alleged four causes of action for misappropriation under the DTSA and California UTSA, breach of fiduciary duty and duty of loyalty, and the violation of California Penal Code § 502. Plaintiff sought a preliminary injunction that required: the return of all hard copy documents and derivatives; the provision of a certification that all such documents were returned; that Defendants refrain from initiating contact with any current customer of Plaintiff for six months; and use of a forensic expert to assist with the identification and destruction of Plaintiff’s information residing on the Defendant’s personal computers and electronic storage accounts. After full briefing and oral argument, the Court granted the preliminary injunction finding that Plaintiff was likely to succeed in showing that the information at issue constituted sensitive business data subject to reasonable measures to maintain its secrecy and deriving independent economic value from not being known to Plaintiff’s competitors, and that the trade secret information was acquired by improper means by sending confidential information to personal email accounts and to a former employee’s new employer.

B. Colorado District Court Cases

Engility Corp. v. Daniels, et al., No. 16-CV-2473-WJM-MEH, 2016 WL 7034976 (D. Colo. Dec. 2, 2016). Plaintiff, a supplier of military deployable communications equipment, sued two former employees and a company they formed, alleging that defendant Daniels, the former technical program manager, had access to all of Plaintiff’s most sensitive information and technology. Daniels was subject to a Confidentiality Agreement, which protected Plaintiff’s proprietary and confidential information and prohibited Daniels from taking, using, copying or disclosing the information in any manner, other than as necessary to perform his duties. Daniel’s last day with Plaintiff

was August 29, 2016, on which his access to Plaintiff's network was terminated. Plaintiff contends that sometime thereafter, Daniels returned a flash drive, which contained Plaintiff's trade secret and proprietary data including a proprietary product pricing tool, profitability information used to bid government jobs, customer needs and purchasing goals, contract opportunities, product designs, and equipment configuration. The flash drive indicated that most of the data showed a modified date of August 30, 2016, inferring that Daniels copied the data after his employment ended and prior to returning the flash drive.

Plaintiff's Complaint alleged seven causes of actions, including violations of the DTSA and Colorado's UTSA.¹⁵ Plaintiff sought a preliminary injunction precluding Plaintiff from disclosing or otherwise making use of Plaintiff's trade secrets and from competing for business from an identified third-party for a period of one year. After holding a preliminary injunction hearing, the Court determined that: the information at issue contained trade secrets; defendant Daniels was likely to still possess those trade secrets; irreparable harm presumptively existed under the DTSA and UTSA because Defendants had misused or were likely to misuse trade secrets; and the balance of equities and public interest favored the injunction. The Court required that Plaintiff post a one million dollar bond. The Court then engaged in a detailed analysis of whether it could issue the non-competition portion of the injunction in light of the DTSA's prohibition against the issuance of an injunction that prevents a person from entering into an employment relationship. The Court held that the restriction did not apply on the basis that the Defendants would be outside contractors to the company it would be prohibited from doing business with. The Court saw no indication that the term "employment relationship," as used in the DTSA, encompassed the role of an outside contractor.

C. Florida District Court Cases

M.C. Dean, Inc. v. City of Miami Beach, Florida, No. 16-21731-CIV-ALTONAGA/O'Sullivan, 2016 WL 4179807 (S.D. Fla. Aug. 8, 2016). Plaintiff, an electrical design-build and systems integration firm, was hired as a subcontractor on a renovation project for Defendant, the City of Miami Beach (the "City"). Plaintiff was contractually required to provide certain payroll information (the "Payroll Information") to the City's general contractor in connection with renovation project. This information included its employees' identities, addresses, social security numbers, fringe benefits, hours worked and other similar information. Plaintiff claimed the information had independent economic value and that it took measures to protect the information. Defendant, International Brotherhood of Electrical Workers, Local 349 ("Local 349"), requested the Payroll Information pursuant to the Florida Public Records Act. Plaintiff objected to the disclosure and the City agreed that it would only disclose redacted records to Local 349. However, the City inadvertently disclosed unredacted copies to Local 349. When Local 349 refused to destroy the hard copy information and delete the electronic information, Plaintiff filed a Complaint alleging violations of the DTSA and Florida

¹⁵ The remaining five causes of action were for breach of the duty of loyalty, tortious interference with contract and prospective economic advantage, unfair competition, and defamation.

UTSA. Defendants moved to dismiss the Complaint. The motion was granted on the basis that, regardless of any independent value the information may have had and steps Plaintiff typically takes to protect the information, Plaintiff took no steps to protect the information in the context of the renovation project. Rather, Plaintiff was required to disclose the information to the City's general contractor and agreed to do so without any limitations, restrictions on use, or protection. Thus, Plaintiff failed to take reasonable steps to protect the information, thereby failing to satisfy the definition of a trade secret under both the DTSA and UTSA.

Adams Arms, LLC v. Unified Weapon Systems, Inc., et al., No. 8:16-CV-1503-T-33AEP, 2016 WL 5391394 (M.D. Fla. Sept. 27, 2016). In 2014, Plaintiff, a manufacturer of small arms, entered into an agreement to work with Defendants on a bid to supply high-powered military rifles to the Peruvian military. As an inducement to Plaintiff, a Mutual Confidentiality and Non-Disclosure Agreement was executed, which prohibited the use of Plaintiff's confidential information for any purpose other than the commercial relationship between the parties. Plaintiff thereafter manufactured demonstration rifles for examination and testing by Defendants, and provided supplier pricing information for the rifles' component parts, as well as information about Plaintiff's manufacturing facility and equipment, revealing step-by-step details of its manufacturing process, machinery, and tooling. Defendants submitted and won the bid using Plaintiff's designs, procedures, and specifications, but thereafter cut Plaintiff out of negotiations and entered into a written agreement with the Peruvian government specifying that they would manufacture the rifles in a Peruvian facility.

Plaintiff's Complaint alleged eight causes of action¹⁶ including misappropriation under the DTSA and Florida UTSA. Defendants moved to dismiss the DTSA claim (among others) on the basis that the Act did not go into effect until after the relevant events at issue in the litigation. Defendants argued that the DTSA did not become effective until May 11, 2016, after the relevant events at issue. The Court evaluated whether a party may bring a DTSA claim where the misappropriation occurs both before and after the effective date of the statute. The Court held that such a claim could be brought based on Section 2(e), which specifies that the DTSA applies to "any misappropriation...for which any act occurs" after the effective date. The Court relied on the omission from the DTSA of language in Section 11 of the UTSA stating: "with respect to a continuing misappropriation that began prior to the effective date, the [Act] also does not apply to the continuing misappropriation that occurs after the effective date." Thus, the Court held that Plaintiff stated a plausible claim for relief by alleging a prohibited "act" occurring after May 11, 2016. Plaintiff alleged that Defendant UWS signed a contract with the Peruvian military in late May or early June 2016, which relied upon Plaintiff's proprietary designs, specification, and processes divulged under false pretenses, supporting an inference that Defendants disclosed Plaintiff's trade secrets after the effective date of the Act. However, the Court specified that to the extent Plaintiff's claim

¹⁶ Plaintiff's remaining six causes of action alleged breach of the Letter of Intent, breach of the Confidentiality and Non-Disclosure Agreements, breach of Consulting Services Agreement, unfair competition under the Lanham Act, and unjust enrichment.

was based on Defendants' acquisition (rather than disclosure) of the trade secret information, that portion of the claim was dismissed because Defendant's acquisition of Plaintiff's trade secrets would have occurred prior to the effective date of the Act.

D. Illinois District Court Cases

Mission Measurement Corp., et al. v. Blackbaud, Inc., et al., No. 16C6003, 2016 WL 6277496 (N.D. Ill. Oct. 27, 2016). Plaintiff created a proprietary database for the purpose of analyzing social outcomes of various programs aimed at addressing issues such as poverty and hunger. Defendant, MicroEdge, a provider of software solutions to automate charitable giving processes, sought Plaintiff's help in creating a software product to measure outcomes from philanthropic programs. The parties executed a Confidentiality and Non-Disclosure Agreement to protect Plaintiff's proprietary information during discussions regarding the venture and Letter of Intent. The parties also executed a Letter of Intent explicitly acknowledging the joint nature of the project but clearly stating that Plaintiff's existing proprietary database remained Plaintiff's sole property. While the parties circulated versions of a final agreement memorializing the joint venture, Plaintiff educated Defendant about Plaintiff's intellectual property and proprietary database, which would be integrated into the new, jointly owned software product. Defendant eventually ceased communication with Plaintiff without signing a final written agreement regarding the venture. Plaintiff was subsequently informed that Defendant MicroEdge had been purchased by Defendant Blackbaud for \$160 million, but that the sale would result in even greater success for the joint venture. Defendants later issued a press release that unveiled a "transformational outcomes solution," featuring "a first of its kind outcomes measurement taxonomy," which Plaintiff alleged was the joint product covered by the Confidentiality Agreement and Letter of Intent. In 2016, Defendant Blackbaud issued a press release regarding its new software program, which Plaintiff alleges embodies most if not all, of the joint product offering developed by Plaintiff between 2012 and 2014.

Plaintiff contends that beginning in May 2014, Defendants executed a plan to misappropriate Plaintiff's trade secrets and repackage them as their own. Plaintiff sued MicroEdge and Blackbaud alleging causes of action for violations of the DTSA and Illinois UTSA, promissory estoppel, unjust enrichment, and breach of contract. Defendants moved to dismiss the misappropriation claims on the basis that the allegations lacked sufficient particularity because Plaintiff failed to allege the exact trade secrets at issue. In denying the motion, the Court recognized precedent holding that, at the pleading stage, a plaintiff need only describe trade secret information and efforts to maintain its confidentiality in general terms, which it found particularly warranted because requiring a plaintiff to plead such information more specifically would necessarily result in the public disclosure of the trade secrets. The Court held Plaintiff had adequately alleged specifics regarding the misappropriated information, including that it contained methods for collecting standardized data and calculating grantee impact, software design specifications, impact reports and analytics, drawings, designs, mock-ups, and product development plans, among other items.

E. Massachusetts District Court Cases

Unum Group v. Loftus, No. 4:16-CV-40154-TSH, 2016 WL 7115967 (D. Mass. Dec. 6, 2016). Plaintiff sued its former employee for conversion and misappropriation of trade secrets in violation of the DTSA and Massachusetts Trade Secrets Act, asserting that the employee had removed numerous company documents from its facility without authorization and had refused to return them. Plaintiff sought a preliminary injunction: enjoining Defendant from copying the documents; compelling Defendant and his counsel to return all of the documents and any other trade secret or confidential information in their possession; and enjoining Defendant from receiving a mirrored copy of the hard drive of his company laptop until after Plaintiff's trade secrets and confidential information had been removed. Defendant did not deny that the documents he removed contained trade secrets, but moved to dismiss the DTSA claim on the basis that he had turned over the documents to his attorney to report and investigate a violation of the law by Plaintiff, and was thus immune from liability under the DTSA. Defendant moved to dismiss the remaining state law claims based on the absence of supplemental jurisdiction. The Court denied the motion to dismiss the DTSA claim on the basis that the Complaint itself did not establish the alleged defense, no discovery had been conducted to determine the significance of the documents that were taken or their contents, and Defendant had not filed any lawsuit allegedly supported by the withheld documents. The Court issued the requested injunction based on Plaintiff's likelihood of success on its conversion claim, and declined to evaluate Plaintiff's likelihood of success on the trade secret claims as unnecessary.

F. Missouri District Court Cases

Phyllis Schlafly Revocable Trust, et al. v. Cori, et al., No. 4:16CV01631JAR, 2016 WL 6611133 (E.D. Mo. Nov. 9, 2016). Plaintiffs, two Trust entities, alleged that two Trust employees misappropriated Plaintiffs' trade secrets consisting of a database of contact information used for direct mail and fundraising efforts, and were sharing that information with other Defendants. Plaintiff claimed ownership of the trade secret information based on an Assignment of Rights. Plaintiff alleged causes of action for violations of the DTSA and Missouri UTSA, among others.¹⁷ After full briefing and oral argument, the Court denied Plaintiffs' motion for a temporary restraining order and preliminary injunction, finding that Plaintiffs were not likely to succeed on the merits of their DTSA and UTSA claims because questions of fact existed regarding ownership of the database, as well as its contents. The Court also found Plaintiffs' claim of irreparable harm speculative given the questions surrounding the ownership and content of the database, and Defendants' assertion that they had been granted access to the database in another court action.

¹⁷ Plaintiffs' additional causes of action alleged violation of the Lanham Act, 15 USC §1114(1) and 1125(a) and Missouri Common Law, and sought a declaratory judgment under 28 USC § 2201.

G. New York District Court Cases

Syntel Sterling Best Shores Mauritius Ltd., et al. v. Trizetto Grp., Inc., et al., No. 15-CV-211(LGS)(RLE), 2016 WL 5338550 (S.D.N.Y. Sept. 23, 2016). Plaintiff, a provider of software-related consulting services, entered into a Master Services Agreement (“MSA”) with Defendant, a developer of software products in the healthcare industry. Under the MSA Plaintiff promised to supply Defendant with appropriately qualified personnel to assist with its software development, consulting and other projects. The MSA prohibited each party from using the other’s confidential information for its own benefit. Additionally, the MSA provided that in the event Defendant was acquired by one of Plaintiff’s competitors, Plaintiff could elect to terminate the MSA. Defendant was acquired by a competitor and Plaintiff provided notice of termination.

Plaintiff sued alleging breach of contract, intentional interference with contractual relations, and misappropriation of confidential information. Defendants counterclaimed alleging that after providing notice of termination, Plaintiff misappropriated Defendant’s confidential files in order to compete, including systematically downloading 1500 of Defendant’s confidential and proprietary documents. Defendant’s counterclaims alleged breach of contract, breach of implied covenant of good faith and fair dealing, misappropriation of confidential information, unfair competition, and tortious interference with prospective business relations. After a period of discovery and passage of the amendment deadline, Defendant moved to amend its counterclaims to expand its allegations of misappropriation under New York State Law, and to include a new cause of action for violation of the DSTA based on information produced during discovery. Defendant claimed the newly produced information demonstrated that Plaintiff had downloaded, used and copied key pieces of Defendant’s confidential information and data, which it then used to develop sophisticated software and libraries of code and documents to compete with Defendant.

The Court found that Defendant timely raised the amendment after the passage of the DTSA and production of documents giving rise to the claim, thus good cause existed for the amendment. The Court also found that Defendant adequately pleaded the elements for relief under DTSA. The intellectual property at issue fell within the scope of trade secrets protected by the Act. Defendant took reasonable measures to keep the information secret by making those who use it subject to confidentiality provisions and limitations. Defendant sufficiently proved that the information was valuable and crucial to its business functions and competitive position. Defendant also successfully proved that Plaintiff used Defendant’s intellectual property, without Defendant’s consent, for Plaintiff’s own use and financial gain. In opposition, Plaintiff argued that the DTSA claim was barred because the Act only applies to misappropriation that occurs on or after the date of enactment. The Court found that regardless of any pre-enactment conduct, the Defendant’s allegations that Plaintiff *continued to use* the misappropriated trade secrets after enactment, brought the claim within the Act, which defines misappropriation as including the disclosure *or use* of a trade secret.

H. Oregon District Court Cases

Allstate Ins. Co. v. Rote, No. 3:16-CV-01432-HZ, 2016 WL 4191015 (D. Ore. Aug. 7, 2016). Plaintiff sued Defendant, a former exclusive Allstate agent, for breach of a Non-Compete Agreement and misappropriation of trade secrets. Defendant had opened an Allstate insurance agency and sold Allstate insurance products and services, providing her with access to Allstate confidential information, including customer contact information, the type and value of the policies carried by the customers, and the location and description of the assets insured through Allstate. Defendant signed an agreement with Allstate, which provided that upon termination of the agreement, Defendant was to return all property belonging to Allstate, and that Allstate would be entitled to injunctive relief if any of the agreement's provisions were violated. After Defendant failed to comply with the terms of the agreement upon termination of the relationship, Plaintiff sued Defendant alleging causes of action for breach of contract and misappropriation under the DTSA and Oregon UTSA.

Plaintiff sought a preliminary injunction prohibiting Defendant from: using Plaintiff's confidential information and trade secrets; soliciting insurance products competitive to those sold by Plaintiff; and requiring Defendant to account for and return all of Plaintiff's confidential information and trade secrets. After full briefing and oral argument, the Court determined that customer information, such as sales history and customer needs and preferences, constituted trade secrets under the DTSA and Oregon UTSA. The Court further held that Oregon law, as well as the DTSA, provided for the issuance of injunctions to maintain the sanctity of trade secrets and that the agreement prohibited defendant from retaining Allstate's confidential information after termination. Defendant was not entitled to retain the confidential information merely because she was in a financial dispute with Plaintiff and the information might ultimately be produced during the course of discovery. Thus, the Court granted the motion to the extent that it required that Defendant immediately return all confidential information to Allstate and refrain from using or disclosing such information.¹⁸

I. Utah District Court Cases

HealthBanc Int'l, LLC, et al. v. Synergy Worldwide, Inc., et al., No. 2:16-CV-00135-JNP-PMW, 2016 WL 5255163 (D. Utah Sept. 22, 2016). Plaintiff, a product developer, entered into a Royalty Agreement with Defendant, a multi-level marketing company, granting it the exclusive right to distribute a nutritional supplement. The Agreement required Defendant to make royalty payments on its sales, provide royalty calculations, and make its sales records available to Plaintiff. Nine years after entering into the Agreement, Plaintiff sued Defendant based on its failure to pay royalties and make records available and its disclosure of Plaintiff's nutritional supplement formula on the packaging of the product. Plaintiff's Complaint alleged causes of action for breach of

¹⁸ Plaintiff also sought to enjoin Defendant from operating her competing business out of the same location where she had operated the Allstate business. The Court declined to award this portion of the injunctive relief because the harm to Defendant would be significant were the preliminary injunction erroneously entered, while the harm to Plaintiff would be minimal.

contract, breach of the covenant of good faith and fair dealing, constructive fraud, and violations of the DTSA and Utah UTSA. Defendant moved to dismiss the constructive fraud and trade secret claims. The Court granted the motion finding that under Utah law, Defendant did not owe a duty to Plaintiff independent of the contract, barring the constructive fraud claim under the economic loss rule. The Court similarly dismissed the trade secret claims on the basis that both the DTSA and UTSA require the Plaintiff to own the trade secrets at issue. Here, Plaintiff had transferred to Defendant all rights—including trade secret rights—to the nutritional supplement under the Royalty Agreement. Thus, as a matter of law, Defendant could not be found liable for misappropriating the trade secret rights “of another,” as required by both statutes.

J. Washington District Court Cases

Earthbound Corp., et al. v. MiTek USA, Inc., et al., No. C16-1150 RSM, 2016 WL 4418013 (W.D. Wash. Aug. 19, 2016). Defendants were former employees and a prospective purchaser of Plaintiff, Intact Structural Supply, Inc. (“ISS”), which marketed and sold Plaintiff Earthbound’s earthquake-related products, services, and systems. Earthbound entered into acquisition negotiations with Defendant MiTek. After executing a Non-Disclosure Agreement protecting its trade secret information, Earthbound shared information regarding its profit and loss, customers, projects, and key personnel. In 2015, Earthbound rejected MiTek’s offer. In June 2016, Earthbound’s key personnel resigned and disclosed that they were leaving for MiTek. Earthbound terminated their access to its server and email, but discovered that at least one employee had forwarded work-related emails to his wife’s email address. Plaintiffs hired a forensic expert who discovered communications between the former employees and MiTek months prior to their resignation, and that one employee had accessed a large number of files days before his resignation and connected a USB to his computer and accessed documents from his Dropbox account and Google drive.

Plaintiffs filed their Complaint alleging ten causes of action¹⁹ including misappropriation under the DTSA and Washington UTSA, and sought a temporary restraining order and preliminary injunction requiring that Defendants return all of Plaintiffs’ property and information, and enjoining them from soliciting or servicing Plaintiffs’ customers for any purpose pending a determination of the scope of the misappropriated information. Plaintiffs also sought a preliminary injunction by order to show cause, and expedited discovery prior to the preliminary injunction hearing. The Court granted the temporary restraining order finding that information about Earthbound’s current and prospective customers, pending projects, bids, pricing, product design, and other elements of its business constituted trade secrets under the law, and that there was strong circumstantial evidence that Defendants misappropriated the trade secrets in question under both the UTSA and the newly enacted DTSA, which it noted defined trade secrets even more

¹⁹ Plaintiff’s remaining causes of action were for violations of the Computer Fraud and Abuse Act, 18 U.S.C. §1030 et seq., unfair business practices and unfair competition, conversion and/or trespass of chattel, unjust enrichment, tortious interference, breach of fiduciary duty and duty of loyalty, civil conspiracy, and accounting.

broadly than the UTSA. The Court further ordered expedited discovery including depositions, prior to the preliminary injunction hearing.

VII. Recommendations to Clients

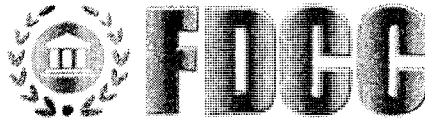
There are important employer notifications concerning the immunity provisions of the DTSA. The DTSA provides immunity to an individual who reports a trade secret to a government or law enforcement official or to an attorney solely for the purpose of reporting or investigating a suspected violation of law or is made in court documents filed under seal.

As discussed in Section II J above, the DTSA also provides immunity to an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of the DTSA to the attorney for the individual if the individual files any documents concerning the trade secret under seal and does not disclose it except pursuant to a court order.

The DTSA requires that an employer provide notice of the immunity provisions set forth in Section 1833(a)(b)(3). If an employer fails to do so, the employer cannot recover exemplary damages or attorneys' fees against an employee to whom notice was not provided.

The DTSA specifically applies to any individual performing work as a contractor or a consultant for an employer. The notice provisions apply to contracts or agreements (which presumably includes oral agreements) entered into after the DTSA took effect (May 2016).

Employers therefore need to update all contracts with employees to comply with these requirements. In addition, all employers need to update their current confidentiality, non-disclosure or any intellectual property agreements for the notice requirement and to ensure sufficient protection exists for their confidential and trade secret information. Care should also be taken to review forum selection clauses as certain state laws are more advantageous than others (i.e. statute of limitations and provisions for attorneys' fee awards). Employers should create or update employee termination procedures to include appropriate steps to help ensure that trade secret information is returned and has not been copied prior the employee leaving the work place. Finally, employers should consider contacting the FBI to investigate criminal charges for trade secret theft, and should certainly do so where the theft is suspected to be for the benefit of a foreign government, foreign instrumentality, or foreign agent.



DEFENSE LAWYERS. DEFENSE LEADERS.

Grant of Non-Exclusive Rights

This agreement is made on this 12 day of December 2016 by and between the Federation of Defense & Corporate Counsel (hereinafter referred to as "FDCC"), an Illinois Not-for-Profit Corporation having its principal place of business at 11812 North 56th Street, Tampa, Florida 33617, and A. Neil Hartzell (hereinafter referred to as "THE AUTHOR/SPEAKER").

THE AUTHOR/SPEAKER has created the following material(s):

(hereinafter referred to as "THE MATERIAL"). As a condition of publication, THE AUTHOR/SPEAKER grants to FDCC the following rights: (1) the non-exclusive right to publish, reprint, reproduce, display and distribute THE MATERIAL (in hard copy and/or electronic form) as it deems appropriate and to license use of THE MATERIAL, or any part thereof, in any medium or form of communication to others, including electronic distribution; (2) the right to use THE MATERIAL, or any part thereof, in other publications produced by FDCC; and (3) the right to copyright protection in any FDCC work that includes or incorporates THE MATERIAL. Under no circumstances will FDCC be required to compensate THE AUTHOR/SPEAKER for any use of THE MATERIAL as set forth herein.

THE AUTHOR/SPEAKER reserves all rights not specifically granted in this agreement by THE AUTHOR/SPEAKER to FDCC, including specifically the right to reprint or to grant others the right to reprint THE MATERIAL.

THE AUTHOR/SPEAKER warrants that publication of THE MATERIAL will not infringe on the rights of others and that THE AUTHOR/SPEAKER has full power to enter into this agreement. IF THE MATERIAL contains any material that requires written permission for inclusion in THE MATERIAL, THE AUTHOR/SPEAKER agrees to obtain such permission in writing from the copyright owner.

CONFIRMED AND AGREED:

THE AUTHOR/SPEAKER

Print Name

Signature:

Dated:

Federation of Defense & Corporate Counsel • 11812 N. 56th St., Tampa, FL 33617 • 813.983.0022 • Fax: 813.988.5837
www.thefederation.org • Executive Director, Marty Streeper mstreeper@thefederation.org



Ashley D. Hayes

Partner



P: (315) 565-4500 ext. 4526

F: (315) 565-4600

ahayes@hancocklaw.com

Ashley D. Hayes is the Co-Chair of the Litigation Department. She focuses her practice on complex commercial litigation matters, representing a variety of clients including publicly and privately-held corporations, municipalities, charitable organizations, and other small and large businesses. Ms. Hayes has litigated cases in federal and state courts and handled a wide range of alternative dispute resolution issues, including intellectual property claims, products liability claims, complex contractual disputes, and large-scale real property and water rights disputes.

Ms. Hayes also serves as local counsel to major law firms across the country and has assisted with the representation of a publicly traded sporting goods manufacturer, a global manufacturer of powered industrial trucks, a national lighting distributor, a national beer and wine distributor, a national housing manufacturer and a financing company, among other clients. Cases handled have involved patent, trademark, and copyright infringement claims, federal and state unfair competition claims, state deceptive and unfair business practices claims, federal Truth-in-Lending Act claims, claims relating to distribution agreement rights, and other statutory, tort and contract-related claims.

Ms. Hayes also prosecutes trademark applications in the United States and abroad and has been responsible for overseeing the management and maintenance of trademark portfolios for corporate clients.

PRACTICE AREAS

- Commercial Litigation
- Personal Injury Defense
- Products Liability Litigation
- Intellectual Property
- Appellate

REPRESENTATIVE MATTERS

- Obtained summary judgment on behalf of gun manufacturer resulting in dismissal of Federal Court action alleging strict products liability, negligence and warranty claims.
- Represented the Mohawk Valley Water Authority in an action to confirm its right to withdraw the maximum amount of water from Hinckley Reservoir as permitted under an agreement with the State of New York. The action was favorably settled giving the Authority the right to withdraw the maximum amount of water sought in the litigation, free from any compensation obligation.
- Assisted in extinguishing a temporary restraining order and defeating a motion for a preliminary injunction precluding termination of an agreement governing the sale and service of powered industrial trucks in an action removed from New York State Supreme Court to Federal District Court.

- Defeated a summary judgment motion brought against a small business in a multimillion-dollar trade secret theft case brought in Federal Court.
- Obtained summary judgment on behalf of an Upstate New York municipal water supply authority resulting in the dismissal of water rights, contract and tort claims brought by a northeastern energy supply corporation seeking damages, declaratory and injunctive relief. Assisted in successfully defending the summary judgment decision on appeal before the New York State Supreme Court Appellate Division, Fourth Department and on motion for leave to appeal to the New York State Court of Appeals.
- Successfully negotiated the resolution of a large-scale real property dispute involving the validity and enforceability of historic restrictive covenants running with real property surrounding an Upstate New York lake utilized as the water supply source for a nearby city.
- Obtained summary judgment on behalf of a charitable sports-related organization dismissing claimed violations of New York's Civil Rights Laws arising out of the promotion of a sporting event using a public figure's likeness and image.
- Assisted in obtaining a defense jury verdict for a medical device manufacturer on a \$26 million tortious interference action tried in Federal Court in the Western District of Pennsylvania.
- Assisted in obtaining summary judgment in the Western District of Pennsylvania, which dismissed millions of dollars in anti-trust claims. Assisted in defending the summary judgment decision on an appeal to the United States Court of Appeals for the Federal Circuit.
- Successfully opposed class action certification in an action brought against a leasing company arising out of an automatic renewal provision in an equipment lease.
- Obtained the reversal of the trial court's denial of summary judgment on behalf of a leasing company arising out of an automatic renewal provision in a mobile phone equipment lease, resulting in case dismissal (on appeal before the New York State Supreme Court Appellate Division, Second Department).
- Obtained an arbitration award on behalf of an owner and a corporate entity providing medical services dismissing breach of contract, unjust enrichment and labor law claims brought by a formerly employed doctor.
- Assisted in obtaining the dismissal of a contract and of tort claims brought by a state of Washington distributor against a New York manufacturer in Federal Court in the Western District of Washington.
- Negotiated the successful resolution on behalf of an automotive manufacturer on claims for damages arising out of an equipment manufacturer's failure to provide special-purpose machines meeting contract specifications, requirements and performance criteria.
- Negotiated the successful resolution on behalf of a national indoor air quality training organization for copyright infringement and tort claims arising out of the unauthorized use of its materials created to train and educate indoor air quality industry professionals.
- Obtained summary judgment entitling a commercial laundry equipment manufacturer to balance due on a commercial laundry system over counterclaims for a breach of warranty found, barred by the terms of the manufacturer's limited warranty, the validity and enforceability of which had been challenged by the defendant. Successfully defended the summary judgment decision on appeal to the New York State Supreme Court, Appellate Division, Fourth Department.
- Assisted in obtaining summary judgment of non-infringement on a patent infringement claim brought against a New York manufacturer by a German competitor.

REPORTED DECISIONS

- *Material Handling Products Corp. v. Nacco Materials Handling Group, Inc.*, 2011 WL 1205065 (NDNY 2011)
- *Camhi v. Ruckert, et al.*, 82 A.D.3d 1673 (4th Dept. 2011)
- *ERBE Electromedizin GmbH v. Canady Technology LLC*, 629 F.3d 1278 (Fed. Cir. 2010)
- *Frazier v. Turning Stone Casino*, 2008 WL 4834929 (NDNY 2008)
- *HSBC Bank USA v. Merrill*, 37 A.D.3d 899 (3d Dept. 2007)
- *Fortune Limousine Service, Inc. v. Nextel Communications et al.*, 35 A.D.3d 350 (2d Dept. 2006)

- *G.A. Braun, Inc. v. Tenney Laundry Systems, Inc.*, 26 A.D.3d 810 (4th Dept. 2006)
- *HSBC Bank USA v. Merrill*, 18 Misc.3d 1125(A) (Franklin Co. Sup. Ct. 2005)

RECOGNITIONS AND HONORS

- Recipient, 2011 Distinguished Young Alumnus Award, Syracuse University College of Law

PROFESSIONAL AND COMMUNITY ACTIVITIES

- Member, Federation of Defense & Corporate Counsel
- Member, New York State Bar Association
- Member, Northern District of New York Federal Bar Association
- Member, Central New York Women's Bar Association
- Member, New York State Academy of Trial Lawyers
- Member, Onondaga Historic Association
- Past President, Syracuse University Law Alumni Association
- Past Member, American Red Cross of Central New York
- Past Member, Onondaga County Bar Association
- Past Chair, Onondaga County Bar Association, CLE Committee
- Past Member, Children's Consortium

SPEAKING ENGAGEMENTS

- Second Annual Advisors to Small Business Symposium (June 2014)
- 2013 Elder Law Fair, "Estate Administration" (May 2013)
- Federal Court Bar Association, "Take It To The Limit? Effective Advocacy & The Ethical Boundaries of Witness Preparation"
- Onondaga County Bar Association, "Discovery in Civil Actions"
- Onondaga County Bar Association, "Federal Court Practice"

PRESS AND PUBLICATIONS

- "Protecting Your Brand: Federal Trademark Registrations Aren't Just for Big Business", *Hancock Estabrook Newsletter*, Spring 2014
- "The Right of Publicity and Protection of Personae: Preemption Not Required", *Syracuse L. Rev.* 1049, (2001)

EDUCATION

- Syracuse University College of Law, J.D., *summa cum laude*, 2001
 - Justinian Honorary Society
 - *Law Review*
 - Moot Court Honorary Society
 - National Trademark Team
 - Corpus Juris Secundum
 - Recipient, Outstanding Achievement Award

- Syracuse University, B.A., 1991

ADMISSIONS

- New York
- United States Court of Appeals (Federal Circuit)
- United States Court of Appeals (Second Circuit)
- United States District Court (EDNY)
- United States District Court (NDNY)
- United States District Court (SDNY)
- United States District Court (WDNY)
- United States Supreme Court



Biography

Mr. Hartzell is a shareholder with LeClairRyan. He works out of the LeClairRyan Boston, Massachusetts office and has extensive experience in a broad range of matters, representing parties in complex civil litigation including commercial disputes, eminent domain litigation, real estate, securities litigation and investigations, false claims act and state whistleblower, directors and officers, business torts, trade secrets, copyright, trademark, patent, civil RICO, insurance coverage, including environmental and bad faith claims, medical device litigation, class actions, contract actions, aviation, workplace and employment related matters, including discrimination claims, ERISA, construction, and environmental including Chapter 21E and CERCLA claims, banking litigation, creditors and debtors in bankruptcy proceedings, claims involving accountants, attorneys, design professionals as well as governmental investigations. He has represented parties in zoning and permitting matters, and parties in loan workouts, including forbearance agreements, loan sales, related litigation and bankruptcy.

Mr. Hartzell served as lead counsel in major cases involving environmental contamination, bank fraud, professional liability, securities, directors and officers, toxic tort, product liability, personal injury, class actions, and commercial disputes. He has appeared before state and municipal boards and agencies and represented witnesses before federal and state grand juries. He has tried more than 30 matters to verdict or arbitration award. Recent decisions include obtaining summary judgment in different cases involving federal qui tam litigation, professional liability, discrimination, employment, claims of interference with contractual relations, securities claims, and defense verdicts in professional liability, securities, and environmental cases. He has successfully mediated numerous disputes, including legal and accounting malpractice and professional liability claims. He also has extensive experience representing various entities, including the Program Manager, in connection with the Central Artery/Tunnel Project, one of the most complex construction projects in U.S. history.

He obtained his undergraduate degree from Boston College (cum laude) and his J.D. from Boston University School of Law where he was Topics Development Editor for the International Law Journal.

He is a member of the Rhode Island and Massachusetts Bars.

He is listed among *The Best Lawyers in America*® for Commercial Litigation, 2013 – 2017.

He has an "AV Preeminent" rating by Martindale Hubbell Peer Review Ratings System (Peer rating 5.0 out of 5.0) and has been recognized as a Massachusetts Super Lawyer by *Law & Politics* magazine in the areas of Employment & Labor Law (2015) and Environmental (2016).

He has been a member of the Federation of Defense & Corporate Counsel since 2015.



THURSDAY, MARCH 9, 2017

12:00 p.m. – 2:00 p.m.

Trial Technology Learning Laboratory
Jenkins

Moderator:
Thomas G. Oakes

USE OF TECHNOLOGY IN DEPOSITIONS

By: **Thomas G. Oakes**

THOMAS G. OAKES ASSOCIATES, LLC

With Special Thanks to: Francis J. Deasey, Esquire; Deasey, Mahoney & Valentini

INTRODUCTION

It goes without saying that the technological advantages of the last decade have changed the legal landscape dramatically. Applications of video technology have important implications for the future of the litigation process. Video depositions, almost universally permitted under Federal and State Rules of Civil Procedure, facilitate the transfer of information from pretrial events to the trial event. Traditionally, videotaped depositions were utilized for the depositions of testifying experts, particularly medical doctors. Today, most sophisticated plaintiff firms videotape every deposition. From the defense perspective this can create additional problems in preparing witnesses for depositions. Conversely, the savvy defense practitioner should make full use of the technology available to conduct video depositions.

In their formative years, most defense practitioners are taught that depositions are discovery tools designed to elicit facts. This way of thinking is obsolete. One of the major reasons most sophisticated plaintiff attorneys videotape depositions is to “Create a sound bite.” And, if permitted, this “sound bite” will be shown to a jury up to four times including:

- (a) During plaintiff counsel’s opening;
- (b) During plaintiff’s case-in-chief;
- (c) During cross-examination of the same witness (if called by the defense); and
- (d) During plaintiff counsel’s closing.

Every defense practitioner must understand how modern videotaped depositions work to prepare their witnesses for this experience. A video deposition brings to the forefront the concept of nonverbal communication, including concepts such as channeling, decoding,

encoding and rapport. All of these concepts impact how jurors will evaluate a witness' video deposition testimony,

However, it is important to remember that video deposition testimony is equally available to the defense and can be a tremendous weapon in defense counsel's arsenal when utilized effectively and professionally. This paper will explore the genesis of videotaped depositions up through and including interactive depositions, also known as smart depositions and will provide the defense practitioner with the tools to prepare their witnesses for video depositions and, at the same time, utilize videotaped depositions as part of their presentation.

GENESIS OF VIDEOTAPED DEPOSITIONS

In the early years of videotaping, the equipment was very antiquated. Cameras used VHS tapes only. Cameras were at least three times as large as today's cameras, bulky, heavy and the quality was not great. In fact, the lighting levels provided by the camera were so low, that additional lighting needed to be added. At times it resembled a mini movie set. Today, almost all videotaping is done digitally with digital cameras utilizing SD cards or directly to hard drives, and exporting the video to the format of counsel's choice, either Mpeg 1, 2 or 4.

In the early years, when the deposition was presented at trial and played to the jury, the videotaped deposition would not be edited, but any part of the deposition which was not to be shown to the jury would then be fast forwarded to the next part of the video to be played. The videographer would sit with a copy of the transcript with the portions not to be played X'd out. He/she would have a set of headphones on to listen and fast forward the VHS tape to the appropriate sections to be used.

While the process by which counsel and the court review objections or deposition designations has not changed, the ability to provide a more seamless edited file has made great strides in today's market. Years ago, the equipment used in the courtroom to play back the video was normally an old style television – not a flat panel – with a screen no more than 32 inches and the only audio came through the television. So that the audio could be heard better, one of the courtroom microphones would be placed close to the television audio output so it could be heard through the courtroom sound system. If we moved ahead a decade or two, we would find that

computers were fast enough, portable enough and software was developed for use in editing video. As a result, there was the advent of trial presentation software, such as Sanction and TrialDirector, which brought videotaped depositions to a new level. With this technology you could synchronize the audio, video and text file. The greatest part about having a video synched deposition is the ability to create clips or bites of the transcript. Delivery of videotaped depositions are now being made on CD, DVD, thumb drives and/or links. The video synched file that is received is a DVT file (digital video transcript). This portable DVT file allows the user to create their own clips of the deposition directly from the DVT and save the clips as either a PowerPoint file, MP4 file (iPad) or TrialDirector file to be imported into the full Trial Director Presentation software package.

SMART DEPOSITIONS – THE EARLY YEARS

First use of the smart deposition took place using an Elmo, which is a document camera. In the videotaped deposition, counsel would project onto a large screen a document to show the witness. Counsel would do the markings and/or have the witness make markings on a document or photo and capture this on videotape to be used later at trial. There are a number of issues using this type of technology. First, you needed to have multiple copies of the same document or photo for the witness or counsel to put markings on. Counsel would need to request the court reporter to put a sticker on each one of the files as they were made. You could not capture a digital copy of the document. You could only capture it on the video. The actual deposition was not being recorded to a hard drive and a video simultaneously. The video was the only recording. This could result in a very herky-jerky replay, since the video camera had to move its

focus from the witness to the document or the document camera and to the projection screen. However, this was a start and like any new technology, the bugs had to be worked out.

SMART INTERACTIVE OR SUPER DEPOSITIONS

If you intend to take a videotaped deposition of a witness using Smart, Interactive or Super Depositions, be sure that you take the time to either have your deposition exhibits pre-marked or numbered in such a way that the presenter (trial presenter) is able to offer up on the screen to the witness the document, x-ray or photo that you would like. A simple index of the documents with deposition exhibit numbers would work great. Also, even though the witness may using tools on the smart board or a monitor to do mark-ups on the exhibits, you will want to not only have this information recorded, but you will want to take screen shots of these documents for later use.

Screen shots can be used as a separate exhibit at trial. If you capture the document with its present markings, ask the presenter to capture the file for you. When asking that the file be captured, tell the presenter the number you want to give to the new exhibit. For example, if you offer the witness a photograph, which was pre-marked hypothetically Deposition Exhibit 3, the witness puts an X on the digital document denoting a location, etc., you would then tell the presenter to capture the new file, perhaps as Deposition Exhibit 3A. By capturing and numbering the exhibit at that time, you can then have that exhibit brought back at any time by just asking for 3A. You could also use this new exhibit with any other witness or in a PowerPoint presentation, etc. The file is captured as a PDF file.

A Smart/Interactive deposition provides you the ability to have a witness seen at trial exactly how the jury would see him/her on the witness stand, but you get the added benefit of being able to make clips of certain portions of the videotaped deposition to be used over and over again. You will also have the opportunity to have the witness pinpoint for you exactly what they are describing in words into a document, photograph, x-ray, etc. Thus, you create a picture which is “worth a thousand words.” Attached as Appendix A is information concerning terminology which will be helpful in understanding the intricacies of Smart depositions.

THE RULES

Federal Rule of Civil Procedure 30, provides impertinent part, as follows:

(3) Method of Recording.

(a) Method stated in the notice. The party who notices the deposition must state in the notice the method of recording the testimony. Unless the court orders otherwise, testimony may be recorded by audio, audio visual, or stenographic means. The noticing party bears the recording costs. Any party may arrange to transcribe a deposition.

(b) Additional Method. With prior notice to the deponent and other parties, any party may designate another method of recording the testimony and in addition to that specified in the original notice. That party bears the expense of the additional record or transcript unless the court orders otherwise.

(4) By Remote Means. The parties may stipulate – or the court may on motion order – that a deposition be taken by telephone or other remote means. For the purpose of this Rule and Rules 28(a), 37(a)(2) and 37(b)(1), the deposition takes place when the deponent answers the questions.

Many states have adopted verbatim or, in large measure, the Federal Rules of Civil Procedure including Rule 30. Before allowing your witness to be videotaped or noticing a

videotaped deposition, it is important to know the state's rules concerning videotaped depositions and, most importantly, restrictions on the use of videotaped depositions at trial.

NONVERBAL COMMUNICATION IN THE VIDEOTAPED DEPOSITION

Nonverbal communication is behavioral communication through facial expression, bodily movements and gestures, as well as vocal tone, hesitations, and pitch. Such communication is often subtle, uncontrollable and spontaneous. These cues are generally interpreted universally and cross-culturally. Thus, the advantage of allowing a jury to audio-visually perceive a witness' testimony through video tape means the jurors will be able to interpret nonverbal cues that they otherwise could not by simply hearing the testimony being read through a transcript. Another advantage is that the videotape is the most accurate way to relay the testimony, which alleviates concerns about objections that could be made regarding accuracy, inflection, tone, etc...when testimony simply is read from a transcript.

Of course, nonverbal communication can be controlled to achieve a purpose such as deception or impression management. This is a skill that some are better at than others. Actions such as nerves and anxiety can affect our ability to manage nonverbal communication. For example, a witness may attempt to project confidence, but the jury still might be able to sense nervousness from nonverbal cues, which may impact an assessment of the witness' credibility. Conversely, positive communication may establish mutual liking, empathy, rapport and most importantly, trust. A smile, direct gaze, forward lean, and warm vocal tone all convey interest and liking, when all are taken together. However, if you remove the smile or warm tone from that equation, the meaning could become entirely different. Nonverbal communication is imparted through a combination of these types of factors.

BASIC CHANNELS OF NONVERBAL COMMUNICATION

(a) Face

The face is the channel that is most easily controlled, and may be the most expressive channel of communication, particularly for emotions. Emotional expression occurs through movements of the mouth, eyebrows, cheek and eyes. Fear, surprise, anger, disgust, sadness and happiness are all conveyed in this matter, and have been observed universally in a variety of cultures. The direction and duration of a gaze is particularly important. We tend to associate direct eye contact with trustworthiness. Smiling and head nodding tend to be universal signs of empathy.

(b) Body

Bodily expression is less controllable than facial expression. Body orientation, positioning and postures are also key to emotional expression. Bodily expressions are also indicative of self-monitoring. High self-monitoring of one's behavior in relation to others and constant awareness of the social appropriateness of one's actions will likely be expressed through such cues. This is called postural mirroring and has been found to create empathy. Changes in posture can be indicative of aggression vs. passivity, as well as signs of emotions and/or mental conditions such as anxiety or depression. We tend to associate an erect posture with confidence and personal appearance.

(c) Gestures

Bodily expressions such as hand/arm gestures can have direct verbal meaning that replaces speech. The simplest example is a witness pointing to an object for

identification. Such movements can also be culture-specific, such as giving a “thumbs” up sign. The interpretation of these gestures can vary widely across cultures and serious misunderstandings can arise. Some gestures, such as crossing one’s arms, are universal signs of guardedness vs. openness. Hand wringing may be a sign of nervousness or anxiety.

(d) Voice

Voice is the least controllable channel of communication. Beyond the actual words spoken, a speaker’s voice, tone and inflection can mean expressions of emotion, mood, confidence and honesty. A harsh and loud vocal inflection such as a “command” voice will relay aggression, dominance and control. This is generally not the best way to establish empathy. A direct, warm and relaxed tone denotes confidence, genuineness and honesty.

IMPORTANCE OF NONVERBAL COMMUNICATION IN THE VIDEOTAPED
DEPOSITION

Studies have shown that jurors pick up nonverbal signs and cues unconsciously transmitted by the speaker. Up to 55% of the meaning of a speaker’s message is nonverbal. Nonverbal skill is the term used to describe individuals’ abilities to use nonverbal communication effectively and accurately. Nonverbal skills tend to be associated with enduring characteristics of people such as gender, personality and culture. Generally, nonverbal skills are conceptualized in terms of two separate sub skills: Encoding skills and decoding skills.

Encoding skills refer to the ability to communicate emotions, attitudes or other messages through nonverbal cues so that the observer (in this case the jury) can interpret the meaning of the message as the encoder intended. Thus, skilled encoders (the witness) tend to be judged as more empathic when they are being empathic and judged so purely from nonverbal channel such as the face or the voice. More-skilled encoders tend to be more popular, dominant and extraverted than less-skilled encoders.

Decoding skills refer to individuals' ability to interpret the nonverbal communication of other people. While the decoding skills of people vary all jurors will have decoding skills which will enable them, more or less, to interpret the nonverbal communications of witnesses. In general, women are more accurate encoders as well as decoders of nonverbal communication than men.

CREDIBILITY

Credibility is established in large part by the witness' confidence and rapport he/she is able to establish with his/her audience. Mutual involvement and interpretation of situations is key to establishing rapport. Witnesses who smile, nod their heads, lean forward, gaze directly at their subject, maintain direct body orientation, have an open as opposed to guarded posture, make few hand gestures, and speak with a warm and relaxed tone will most likely be able to establish a rapport with his/her audience and thus come across as more credible. Tone of voice, which is the most difficult channel to control, is important to establishing confidence. For example, a positive verbal message in a negative tone of voice may arouse suspicion, because we

generally expect a positive verbal message to be relayed in a positive tone. To the contrary, a negative verbal message in a positive tone of voice may communicate concern and acceptance.

DECEPTION

Deception occurs when one's behavioral expression is inconsistent with his/her true thoughts or feelings. Deception is not always considered unacceptable, as we often expect to mask non-verbal cues of our true feelings. The ability to mask these cues may vary from person to person. However, jurors can often times notice and react to deception. When lying, the witness tends to show more mismatch between the various channels of communication. More attention tends to be directed to managing facial expressions, which may not be synchronized with the bodily movement or voice inflection. People tend to move their face, hand and body more when lying. Also, facial expressions and eye contact can be quick and fleeting. While it is true that studies show that we tend to overrate our abilities to detect deception, it is also true that in the context of a witness' testimony, a jury's ability to detect deception is generally higher due to situational factors – primarily, the relationship of the witness to the parties and the motivation of that person to lie.

USES OF VIDEOTAPED DEPOSITIONS AT TRIAL

There are a number of reasons for using videotaped depositions at time of trial. Traditionally, testimony was preserved in case the deponent died, became too ill, fled or otherwise was unavailable to testify at trial. Deposition testimony was regularly used to impeach a witness if he/she changed his/her testimony at trial. Use of video depositions in these circumstances highlights the witness' inconsistencies. Seeing a witness make an unambiguously different statement on video than they did in court has much greater impact than simply reading the deposition transcript. Further, in the case of impeachment, particular segments are selected for presentation, which amounts to a mere fraction of the entire deposition. While these excerpts can be anticipated, they are only used when a witness unexpectedly alters his/her deposition testimony.

Today, the preservation of testimony via videotape is not only for provisional purposes but is used more and more to try to "catch the witness off guard." As an example, many skilled plaintiffs' attorneys do not begin a videotaped deposition in a traditional sense which would entail obtaining significant background information on the witness. Instead, the deposition may start with this question: "Isn't it true, sir, that your defective product has caused injuries to my client?" If your witness is not prepared for this style of questioning, then the normal response from the witness when asked a question like this is astonishment and his/her subsequent verbal and nonverbal communications can impart a lack of confidence, preparation and, worst of all, trustworthiness. The witness will typically look to counsel for help or an objection. But the video camera captures the witness' expression on his/her face. Thus, the defense practitioner

must be prepared and conduct research on their opponent. If possible, observe your opponent in action. Your opponent's use of videotaped depositions, whether clips, snippets or bites of your witness' testimony can provide your adversary with the ability to construct their case in a much more efficient and technologically advanced format.

EFFECTIVE PREPARATION OF YOUR WITNESS FOR THE VIDEOTAPED DEPOSITION

Traditionally, preparation for your client's deposition consisted of the standard instructions including:

- Tell the truth;
- Be concise;
- Don't guess;
- Speak clearly;
- Don't argue;
- Wait for the entire question before answering;
- Listen and understand the question before answering;
- Don't speculate; and
- Don't volunteer.

With the advent of videotaped depositions, preparation of your witness for a videotaped deposition must be taken to a much greater level. It is the general consensus of researchers that people do not see or hear themselves as others do. Most people have never been videotaped and, therefore, don't understand or appreciate how their nonverbal communication skills (or lack thereof) will affect how they are perceived by a jury. Therefore, it is important that as part of your deposition preparation your witness is videotaped both on direct and cross examination so that the witness can appreciate the strengths and weaknesses of his/her nonverbal communication skills. The weaknesses in your witness' testimony are magnified tremendously when their

testimony is videotaped. A dress rehearsal of the anticipated line of questioning by your adversary is essential for your witness to become comfortable “in their own skin” during videotaped deposition.

As the research described herein has shown, slouching, rapid eye movement, turning to the attorney for help, stammering, folding of the arms across the chest as well as other forms of body language impact the jury’s acceptance of your witness’ testimony much more than the words spoken by your witness. It is essential, therefore, for your witness to be prepared to develop the necessary rapport with the jurors by proper body language, voice control and inflection and body movement. Remember that the words spoken by your witness may become lost on the jury during the course of the trial but the jury’s perception of your witness as truthful or untrustworthy will remain.

Courts are split on whether videotaped deposition testimony can be utilized in openings. Therefore, it is important that you know the local rules of court for use of videotaped deposition during all phases of the trial. Alert your adversary well in advance of the trial that if he/she intends to utilize videotaped deposition testimony of your witnesses in his/her opening, they must provide you with the videotaped deposition well in advance of trial. While local court rules may permit use of videotaped depositions in openings objections can always be made on the grounds of relevancy or out of context.

EFFECTIVE USE OF VIDEOTAPED DEPOSITION AT TRIAL

The world we live in is moving faster and faster and, as a result, the attention span of most people is getting shorter and shorter. Consider, for example, why Superbowl ads are divided into 15 second segments. Effective advertisers can promote their product or message to the audience in as little as 15 seconds.

In the trial setting, jurors expect the attorneys will be polished, sophisticated and technologically savvy. Consider that almost 70% of today's jurors will be made up of GenX, GenY and Millennials. Many of your prospective jurors have grown up in our advanced technological age. T.V. shows and movies about lawyers show only snippets of courtroom drama. Your jurors will expect the same type of courtroom drama during your trial. Research over the past decade has demonstrated the following:

- Watching videotaped deposition testimony is much more boring than watching live testimony;
- If jurors are not engaged they are less likely to retain persuasive points;
- Jurors are most riveted by video clips that directly impeach or contain a dramatic nonverbal communication;
- Jurors are "turned off" by video clips that only marginally deviate from the testimony or where the contraindication was subtle.

Thus, when considering the use of videotaped deposition of your opponent consider the following:

- Important testimony should be broken down into “short clips” that can be repeated numerous times during openings, testimony and closing arguments;
- Avoid overuse of this valuable communication tool so that jurors will remain engaged and retain persuasive points;
- Combine videotaped deposition testimony with demonstrative evidence (exhibits, photos, x-rays, etcetera) to increase the jury’s understanding of your message;
- Use smart/super deposition techniques such as synchronized videotaped deposition so that the jury can see and hear the witnesses testimony.
- Follow the testimony through written word.
- Consider using your own “sound bites” during your opening and/or closing to emphasize your defense themes.
- If you have the ability to obtain the trial testimony of your adversary’s witnesses (daily copy) incorporate the written trial testimony into your cross-examination of the adversary’s witnesses highlighting the inconsistencies and/or contradictions between videotaped deposition testimony and trial testimony.
- Cue the jury during your opening to the importance of the videotaped deposition sound bites you will utilize to heighten the jury’s anticipation of your trial presentation.

Sophisticated use of videotaped deposition testimony using the most advanced technology methods available today can be one of the most persuasive elements of your trial presentation. Conversely, an ill prepared witness for a videotaped deposition can result in catastrophic consequences at time of trial. It is the responsibility of the defense practitioner to understand how technology, particularly with respect to videotaped depositions can impact their

case at trial either positively or negatively. Remember, in the final analysis the jury may not remember every word a witness said at trial or deposition. However, you can be assured that the jury will never forget the nonverbal communication expressed by a witness during their videotaped deposition or trial.

Appendix A

- Legal Videotaping – videotaping in the legal industry came about as a means to preserve for trial purposes the testimony of a witness who could not be at trial due to scheduling issues.
- Videotaped Deposition – The adjunct of videotaping the testimony provided by a witness at a deposition for preservation and presentation at trial.
- Video Synchronization – The result of combining the video, text and audio of a deposition into a searchable format which is synchronized by time, page and line number. Scrolling text can be turned on or off, in addition to linking exhibit files.
- DVT – Digital Video Transcript is the product that is produced as a video synched file. You can show the scrolling text under the witness if you would like – similar to closed captioning.
- Video Clips (depositions) – Individual portions of a deposition, such as a Question and Answer or multiple Questions and Answers in continuity, which can be as short or as long as necessary.
- Video Segments (depositions) – Portions or bytes of a deposition combined into one file to be played back to a finder of fact. This file would excise out portions not to be played, so that one complete stream is played without interruption.
- Smart Depositions (SuperDeps, Interactive Deps, iDeps) - Videotaped depositions with adjunct of trial presentation software, which allows the witness and/or counsel to interact with the document, photograph or X-ray applying mark ups and other iterations. All of the actions are recorded via video and also recorded digitally on the computer used by the

presenter, so that the final product shows the full video of the witness and the interaction of the witness with the documents. One important feature is that when viewing the video of the witness with the document offered to them, it can be in a split screen format or moving the witness into one of the four corners of the video, allowing the document to be shown almost full screen. After the witness is finished with the document, the document moves off the screen and the witness is then on the full screen.

- Smartboard – A computer monitor which allows the user to interact with anything presented on the monitor. An example is the weather person on your local newscast uses a Smartboard to draw arrows, circles, etc.
- Viewsonic Monitors – Touch Screen. Touch screen monitors are the newest generation of interactive monitors. Adding Windows 8 (Microsoft) provides the ability for you to use your fingers or a stylus to pinch open a file and markup a file.
- Videotaped Depositions – Linking Exhibits (split screen) - In post-production exhibits can be linked into the deposition to be shown to the jury. As an example, if you were discussing an animation with the witness, the way to present that to the jury would be when the exhibit is discussed, the screen would split into two so that the jury can see the witness testifying and the animation at the same time.
- Video Conferencing – The use of video conferencing for depositions and/or trial presentation is becoming more of a regular occurrence. Many times at trial the Court will allow a witness at an offsite location testify directly into the courtroom via video conference. The video conference is a two-way system, so that the video and audio is broadcast to both sides. You can also present documents to the witness in this situation for their view on the video conference screen.



Lighting the way to...

Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10



FRIDAY, MARCH 10, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

LAW PRACTICE MANAGEMENT

**Succession Planning: Protecting Your Firm and
Your Clients' Legal Interests in Times of Transition**
Jenkins

Moderator:

Michael Bonasso

Panelists:

John C. Trimble

Lewis Wagner

Thomas J. Welk

Alison R. Christian

SUCCESSION PLANNING: Protecting Your Firm and Client's
Legal Interests in Times of Transition

FDCC
Law Practice Management Committee
Charleston, S.C.
March 10, 2017

Panelists:

John C. Trimble
Thomas J. Welk
Alison R. Christian

Moderator: Michael Bonasso

[This paper was first presented at the DRI Women in Law Seminar in February, 2016. FDCC thanks DRI for the replication of this paper.]

Succession Planning: Protecting Your Firm & Clients' Legal Interests in Times of Transition

Gretchen Koehler Mote
Ohio Bar Liability Insurance Co.
1650 Lake Shore Drive
Columbus, Ohio 43204
(614) 488-7924
gmote@oblic.com

Debbie Riley
Quintairos, Prieto, Wood & Boyer, P.A.
Willis Tower
233 South Wacker Drive
70th Floor
Chicago, Illinois 60606 US
(312) 566-0040
driley@qpwbllaw.com

John C. Trimble
Lewis Wagner, LLP
501 Indiana Avenue, Suite 200
Indianapolis, IN 46202
(317) 237-0500
jtrimble@lewiswagner.com

Gretchen Koehler Mote, J.D. is Director of Loss Prevention for Ohio Bar Liability Insurance Company (OBLIC), a lawyers' professional liability insurance company, headquartered in Columbus, Ohio. She is a past President of the Ohio Association of Civil Trial Attorneys (the Ohio SLDO) and currently serves as the Chair of the OACTA Women in the Law Committee. She is an active DRI member who has served on the WITL Committee's Seminar planning and marketing subcommittees.

Debbie Riley is the General Counsel and Chicago Managing Partner for Quintairos, Prieto, Wood and Boyer, the nation's largest minority and woman owned law firm. She also serves as Chair of the Women Affinity group for QPWB. Previously, Ms. Riley was the Vice President of Claims at CNA where she managed the Health and Life Sciences claim department.

John C. Trimble defends catastrophic and complex litigation. He is the former managing partner of the 40-lawyer law firm of Lewis Wagner. He is the Immediate Past Chair of the Law Practice Management Committee of DRI and the Immediate Past President of the Indianapolis Bar Association.

Introduction

Lawyers as a group are fearless, ageless, and optimistic. We throw ourselves into our day-to-day work, and we prefer not to be bothered by anything that may distract us from our clients' cases. Many of us do not recognize the word *retirement*, and we assume that as long as our mind is intact, we can practice law as long as we want. Because we mostly practice in law firms, most law firms do not plan for the unexpected. Indeed, a recent study showed that less than 5 percent of law firms have any kind of succession plan in the event of the loss of firm leadership or firm rainmakers. (Sterling/Remsen, *Planning for the Future*, 2015.)

The reality is that every attorney can be sidelined by unexpected death, illness, or the death or illness of a spouse, child or parent. Life-changing events prompt lawyers to retire when retirement was not in the plan. Similarly, lawyers make life-changing decisions to leave private law practice to enter the judiciary, seek other public office, move in-house, or pursue personal business ventures. The reasons for succession planning are too numerous for this article, but the fact remains that all law firms and lawyers need to have a succession plan.

The first reason for succession planning is to protect the interests of our clients. The sudden and expected loss of a trusted advisor who understands the legal and business needs of a long-time client can be devastating and expensive for the client. Thus, clients should be concerned about the succession planning of their lawyers, and lawyers should be thinking about how their clients will be protected in the event that they are unable to continue representing the client.

A second reason for succession planning is to protect the interests of the law firm. The unexpected death or withdrawal of a law firm leader or significant rainmaker can be absolutely disastrous to a law firm. If the departing lawyer has been responsible for a significant percentage of the firm's revenues, then it is certainly possible (if not likely) that a law firm could have to lay off lawyers and personnel (or liquidate) in the event of the unplanned loss of a major player.

The younger, up-and-coming lawyers of a firm may be most vulnerable in the event that their supervisor or mentor is unable to continue practicing law. A comfortable and stable living can be turned into a short term or long term period of unemployment when lawyers and law firms have failed to plan for the unexpected.

This article seeks to address the array of fairly simple and sensible things that clients, law firms, and lawyers can do to plan for the expected and unexpected departure of a key leader or rainmaker.

General Challenges to Succession Planning

The first and most overriding barrier to succession planning is denial. Many lawyers and law firms simply do not contemplate the possibility of the sudden loss of a highly profitable lawyer, and for a variety of reasons, they do not anticipate a planned retirement of a senior lawyer. The lack of anticipation and planning means that lawyers and law firms frequently do not have *any* of the information they may need to react to a lawyer's death or departure.

Surprisingly, many law firms do not track or study the percentage of origination of revenue of their lawyers, so they may not understand the extent of the problem that may be faced by the loss of a lawyer's revenue. Depending upon the discipline of the firm, the firm may also lack clear information concerning the unbilled time, accounts receivable, and client fee agreements when the billing partner dies or leaves unexpectedly.

Conversely, a firm may be so origination driven that partners have been incentivized to hoard work to protect their client relationships from others. In those circumstances, the departing or departed lawyer may be the only person in the firm who has had a relationship with the client. It is an old and worn adage that "Clients hire lawyers, not law firms." If the departed or departing lawyer is the only person who had a relationship with the client, then it may be much more difficult for the client and the law firm to move forward with a new person handling the client relationship.

Financial considerations of a departing or deceased major rainmaker can be overwhelming to a firm. Frequently, partner agreements or state partnership laws may require immediate and long term payment to the departing partner or his or her beneficiaries. If the firm has not made provisions for the financial consequences of the death or departure of an attorney, the firm may be burdened beyond its means in pay-outs at the same time that the firm has lost the revenue of the attorney.

Factors That Bear Upon Client Relationships

In the defense business, there are many firms that have large institutional clients such as insurance companies and self-insured entities in which the firm has a "relationship partner" who oversees the account. In some instances, the relationship partner is the person who originally brought in the account and in other instances, they may be the person who has inherited the account and is doing the majority of the work for the account. Some firms will give all of the origination credit for the account to the relationship manager. Other firms encourage the account to call any lawyer in the firm who individual account representatives wish to use for a particular matter. In general, these types of large account relationships may be less impacted by a change in the relationship

partner. These larger accounts tend to be more metrics-driven, and their loyalty to the law firm may be based upon the firm's overall metrics score that is a product of the work of all of the attorneys who service the account. Firms may be able to be mildly less strategic in their planning for the change-over of relationship partners because the successor relationship partner may be readily apparent based upon the amount of work that the successor lawyer already has done for the account.

Whether an account is large or small, there are certain factors that almost always bear upon the relationship between the client and the law firm. These are factors that are inherent in the word "relationship" as it pertains to lawyer/client relationships. First and foremost, there is the issue of *trust*. The client will have developed trust in the subject matter knowledge, advice, predictability of outcomes, and billing practices of the firm. If a law firm has any hope of keeping a client after the death or departure of a senior attorney, then the firm will have to be positioned to continue to win the trust of the client.

Other factors that result in long term client relationships include excellent subject matter knowledge of the client's legal issues; knowledge of the client's business, needs, habits and decision-making protocols; a willingness and ability on the part of the law firm to be responsive, timely, and adherent to the client's billing and case handling guidelines; and, a history of successful outcomes and results.

The bottom line is that any successful succession planning needs to take into consideration most, if not all, of the above factors. In this competitive and changing legal environment, clients have many choices, and the glue to a long-lasting attorney/client relationship is all of the above.

Elements of Succession Planning

The Client's Perspective

Anyone on the client side of the attorney/client relationship has experienced the time and the cost associated with having to move a legal matter from one law firm to another. It is simply something that clients do not want to do. The challenge and cost of moving a matter is even more troubling when it occurs without much warning.

A clear starting point for attorney/client succession planning can certainly reside with the client. It is not only permissible, but it is perfectly reasonable for a client to inquire of its law firm's or attorney's succession plan in the event that lead counsel leaves, dies, or is incapacitated. All clients are concerned about the financial implication of "two-headed" handling of legal matters. They do not want to pay two or more lawyers to review or perform the same legal tasks on a matter. Nevertheless, the client is probably best represented by a *team* approach

to the handling of the client's matters. The client has great control over how the team will be constituted; the diversity of the team; the varying subject matter knowledge and talents of the team; and the client's guidelines as to how the team should bill and operate.

Ideally, a client will have a lead counsel who is responsible for the overall performance of the law firm's team, and there will be a second and slightly junior lawyer who may be available as backup in the event that the lead attorney is unavailable.

At a minimum, the client may wish to inquire as to whether the firm has other partner-level attorneys who would be available to handle the client's business on an interim basis in the event that a relationship partner is unavailable. Having another partner available then allows for the client and the firm to have the time to determine whether the firm will realign the client's team or whether the client will need to move the business to another, better qualified law firm.

As a part of the client's inquiries with the firm about succession planning, it is certainly within the right of the client to seek specific information about one or more of the following:

- Other substantively educated and experienced attorneys.
- The firm's billing policy with respect to the need for a new lawyer to get up to speed and take over a case.
- The firm's procedure with respect to appointment of new relationship partners.
- The question of whether the firm will allow the client to participate in the selection of replacement counsel within the firm.
- The financial wherewithal of the firm to carry on with the business in the absence of the departed partner.
- The diversity pool of potential successors

The Law Firm's Perspective

As a starting point, all firms of *any* size should engage in strategic planning every three to five years. That strategic planning process should include a short term and long term look at how the firm would respond to the expected and planned loss of attorneys and key law firm personnel. A good strategic plan that addresses predictable succession planning will address most of the concerns and fears presented by the possibility of the loss of firm leaders, firm rainmakers, and firm administrators.

As part of the management of any law firm, firm managers *must* understand the reality of "life cycles." All lawyers have life cycles that will vary from person to person depending upon their health, their family, their personality, their gender, and their background. Clearly, men and women may be

permanently or temporarily affected by the birth of a child, child rearing, special needs children, aging parents, accidents, other health issues, college tuition, personality, marriage/divorce, personal issues, career burnout, and work history. Enlightened law firms understand that the availability and productivity of lawyers will rise and fall depending upon life cycles, and good firm managers' account for those changes in life.

The following is a list of questions about issues that could impact a firm's client relationship in the event of the death or departure of a rainmaking or managing attorney:

- Does the firm track and understand the percentage of origination of revenue of each lawyer in the firm?
- Does the firm's partnership agreement (or other governing document) address how a partner's law firm share will be paid to a departing partner or the partner's beneficiaries?
- Does the partnership agreement provide a balance between the needs of the departing partner/partner's beneficiaries and the firm so that the firm is not strained or rendered insolvent by the departure?
- Does the firm have key-person life or disability insurance that may be available in the event of death or disability to bridge the financial needs of the firm and the departing partner or partner's beneficiaries?
- Does the firm have other attorneys who have the experience and subject matter knowledge to step in to handle client legal matters in the event of death or disability or departure of a lead attorney?
- Does the firm's compensation system incentivize rainmaking partners to share client relationships and origination with younger lawyers and successors?
- Does the firm have practice groups arranged around substantive practice areas so that a "team" approach to the subject matter litigation can be implemented?
- Are younger, up-and-coming lawyers encouraged and permitted to communicate directly with clients so that they become a part of the client relationship?
- Are clients advised of the names and contact information of lawyers other than the relationship partner so that the client can choose whether to reach out directly to other attorneys within the firm?
- Are younger lawyers mentored and trained to understand the array of factors that a relationship manager must know in order to establish the bond of trust and performance that will be suitable to maintain a client relationship?
- Are younger lawyers cultivated or encouraged to view themselves as successors to the firm's client relationships?
- Is the firm's structure of equity partners, non-equity partners, associates, counsel, and contract lawyers sufficiently balanced to allow for the right number of lawyers to rise within the firm to become successors?

- Has the firm engaged in conversations with the client concerning how the client relationship would transition in the event that the primary attorney was to die or be disabled or retired?
- Is the firm financially prepared to absorb the costs that may be necessary for successor attorneys to get up to speed on client matters so that the client does not bear the cost?
- Does the firm, in its hiring culture, give consideration to practice areas that may need to “grow” successors?
- Does the firm ask its more senior attorneys to advise the firm of the attorney’s retirement plans? If so, at what age does the firm begin asking, and how often does the firm ask?
- Has the firm studied the profitability of its client’s account so that it can determine whether it wishes to *keep* an account in the event that a partner dies, departs or retires?

The above list is anything but exhaustive, but these questions taken, as a whole, will enable the firm to study its succession issues in a way that allows for emergency or planned succession as the case may be. There is no ideal timetable for planning succession, but at least one expert has suggested that a firm allow at least five years for a planned retirement. (Sterling/Remsen, *Planning for the Future*, 2015.)

Individual Attorney Succession Planning

In the category of succession planning for individual attorneys, there are really two categories that bear discussion. First, there is the relationship/rainmaking partner who anticipates the day in the foreseeable future when he or she will want to slow down or retire. The other category is, of course, the up-and-coming attorney who hopes to step into the successor relationship.

Relationship/Rainmaking Attorney

The first and most pressing question for the relationship/rainmaking attorney is whether he or she has given *any* thought whatsoever about succession planning. If they have thought about it, then one would hope that a younger successor attorney is already being positioned to move into the relationship when the time arrives. Anyone grooming a successor needs to understand that it cannot occur over night. It is essential that the proposed successor be brought into the relationship with sufficient time to allow for trust to be established between the client and the attorney and to allow the successor attorney to understand the business needs of the client. It is a given that the successor attorney must have the subject matter knowledge and the skill to successfully handle the client’s work at a reasonable price with reasonable billings. Therefore, to the extent that a more senior attorney begins to anticipate retirement, some very open discussion and planning needs to take place between senior counsel and his or her successor. Once the timeline and planning for succession has been discussed, then it is

probably beneficial (if not essential) to bring the client into the discussion and to let the client know that a successor is on the horizon. Sometimes, the successor moves into the relationship seamlessly, and no discussion is even needed because the senior lawyer over time has allowed the younger lawyer enough contact with the client that the younger lawyer has become a defacto successor simply by progression of the relationship.

In firms in which origination credit discourages sharing of clients in successorship, then the retiring attorney and proposed successor are going to have to be involved in a conversation with the firm as to how the transition occurs. More times than not, the relationship partner is the one who is going to decide who the successor is going to be, but sometimes the firm will want to have some input, particularly if the selection of the successor will create controversy in the law firm. In instances where multiple potential successors exists, it may be imperative for the firm to be involved so that the retiring attorney is not burdened with choosing between one or more equally qualified candidates. In such a situation, the client should likely also be involved in the decision.

Proposed Successor Attorneys

A famous American politician, Oliver Wendell Holmes once said, “Destiny (opportunity) is a matter of choice not chance.” Not every law firm gives its younger lawyers the opportunity to craft a practice area or choose a client. However, it is well known in all walks of life that the persons who behave strategically in their career advancements will have a greater chance for success than those who let opportunities come their way.

If young lawyers aspire to be successors to a client relationship, then they must position themselves to be a successor. That means trying to be a part of the team that represents the client, and trying, in all ways possible, to develop client trust and respect and client awareness of the attorney’s involvement. Ideally, the opportunities to gain trust and respect are facilitated by the partner who controls the relationship. In those instances in which the relationship partner does not facilitate relationships among young lawyers, then younger lawyers simply have to credential themselves in the substantive area of practice, and they need to do all they can to be timely, responsive, and competent in the work they perform. They should take every opportunity that comes along for them to meet the client and make a good impression. In addition, they need to study all that they can in the public domain to learn as much as they can about the client’s business so that their representation of the client reflects the depth of understanding that they have of the client’s needs. With proper succession planning a client and firm may be able to place the successor candidate in-house for a period of time with the goal of learning the client’s business and people.

If given a choice between standing silent or letting the relationship partner know of the associate’s interests, it is likely best to error on the side of disclosing

long term interests in serving the client. One could hope that the relationship partner would already notice and recognize the potential successor's level of interest, but that is not always clear.

The bottom line is that no young lawyer is going to succeed to a client relationship unless they have done all of the things they can possibly do to demonstrate that they are worthy in all respects of moving into a closer client relationship role that could evolve into relationship partner.

Succession Challenges Unique to Women

A 2015 survey by the National Association of Women Lawyers (NAWL) demonstrated that over the last ten years, women lawyers have continued to lag behind male colleagues in being promoted to equity partnership and senior leadership roles within their law firms. They also continue to lag in compensation. This survey was taken of the top 200 AmLaw firms. This survey suggests that women will have a harder time gaining more senior relationship partner positions. The same challenges ring true for women who work in in-house positions. As women climb the proverbial "corporate ladder", the higher they climb the less diversity. Women continue to be left behind or be paid less than their male counterparts.

What does this mean for younger rising women in defense law firms? At a minimum, it demonstrates the need for women to be as strategic in their personal career plans as they can be. This is no time to sit on the sidelines or be shy. Women must clearly articulate to the rainmakers and relationship partners their career goals and seek feedback on their plans and results. Seeking feedback on progress along the way is critical. It may be uncomfortable on both sides of the fence; however, feedback is essential to development. Ask targeted questions. Instead of asking a colleague "how am I doing" a better question would be "can you suggest 2 – 3 things that may improve my results? Don't be defensive when feedback is delivered. Absorb, contemplate and remember, it's not whether the feedback is "right" or "wrong," it's the perception of others that matters most.

Much has been said and written about the differences between how men and women develop, cement, and maintain relationships. As the business and insurance world have become more metrics driven and more focused on diversity in the work place, there may be no better time than now for women who aspire to succeed to client relationships to position themselves. Long term, the quality of legal work, the consistency of responsiveness, and the demonstration of professional and substantive competence will earn the opportunity for younger female lawyers to gain successor client relationship opportunities.

It is going to be incumbent upon leaders, both women and men, to continue to push to lift up and mentor aspiring successors. Men should make note of the importance of gender diversity in law firm promotion and client succession. This will mean overcoming any lingering biases among male clients who prefer a

male relationship manager. It may require greater attention communication within the law firm and to communication with clients on client relationship matters. Above all else, it will certainly require a strategic approach to client development and client relationship succession.

It cannot be understated that women have the direct ability to positively influence the career growth of other women. But, it takes deliberate and thoughtful action. As you walk through your career you make choices daily that could impact others. Some examples include:

1. You are handling a matter for a client and you need to hire an arbitrator. Give thought to hiring a woman. Helping other women to generate revenue helps that person succeed.
2. You need a mediator: Make sure you are considering female mediators, especially those in a firm who are working on their own career development plan.
3. You need to retain local counsel for one of your files: look for a woman.
4. If you are an in-house corporate attorney with the ability to make hiring choices, make sure you have a diversity inclusion policy. As in-house counsel you literally hold the key to the success of several attorneys throughout the country. Use your key wisely! Even one assignment to a woman can be the grain that tips the scale.

In Summary

In summary, clients and law firms alike cannot afford to ignore the importance of succession in client relationships. With the disruptive innovation of the internet, competition for clients will increasingly be coming from new directions. Attorneys and law firms can no longer take client relationships for granted. They need to be pro-active within their law firms and their mentoring programs to bring a team approach to client management and to groom multiple successors for the inevitable day when the relationship/rainmaking partner will experience a life cycle change that will result in departure from the law firm or retirement. The lawyers who plan ahead and think strategically will be ready. Each one of us has the ability to positively impact the career of those around us. Take time to help others succeed in their careers. Developing succession plans can literally promote the career of individuals and ensure the financial longevity of a firm.



Lighting the way to...

Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10



FRIDAY, MARCH 10, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS INSURANCE COVERAGE

**When a Disaster Turns the Insured's Address into the Boulevard of Broken
Dreams, Does Business Interruption Coverage Become Contentious?**

Dogwood

Speakers:

Michael S. Knippen

Heather Sanderson

William J. Kautter

FDCC Winter Meeting
Charleston, S.C.
March, 2017

WHEN A DISASTER TURNS THE INSURED'S ADDRESS TO THE BOULEVARD
OF BROKEN DREAMS,

DULL BUSINESS INTERRUPTION COVERAGE BECOMES CONTENTIOUS

Heather A. Sanderson

Sanderson Law
Calgary, Alberta
Canada

James M. Eastham

(with the research assistance of Kyle Dickinson, Jason
Taylor, Jeremy Macklin, Julie Klein, Grant Peoples)

Traub Lieberman Straus & Shrewsberry,
Chicago, IL



James M. Eastham

Traub Lieberman Straus & Shrewsberry LLP
Chicago, IL
jeastham@traublieberman.com

James Eastham is a partner in the firm's Chicago office with over 20 years of experience in insurance coverage analysis and litigation. His practice entails counseling and representing insurance companies both nationally and locally in both the first and third party context. Over the course of his career, he has obtained extensive experience in all forms of third party matters as well as first party insurance coverage in actions brought in state and federal courts throughout the United States. Apart

from policy interpretation, Jim also has experience in policy drafting and has been called upon to prepare and refine a vast array of exclusionary provisions including those dealing with Chinese drywall, contracted persons, pesticides and lethal weapons. Drawing on this diverse experience counseling insurers, Jim frequently gives presentations to clients on established and emerging coverage issues.



Heather A. Sanderson

Sanderson Law
Calgary, Alberta
hasanderson@sanderson-law.com

Heather A. Sanderson, the principal with Sanderson Law in Calgary, Alberta, Canada, is a nationally recognized insurance coverage counsel and author who has provided expert evidence on CGL coverage issues to Canadian Courts and has appeared as counsel before the full range of the courts in Alberta as well as a full panel of the Supreme Court of Canada.

In addition to being a member of FDCC, Heather is a director of Canadian Defence Lawyers (CDL) and is extensively involved in the DRI Insurance Law sub-committee as an author, presenter and active committee member. Throughout her career, Heather has defended a multiplicity of first party property claims on all manner of policies. She is currently engaged in a number of such claims stemming from the devastating Fort McMurray wildfire of 2016.

I Introduction

The last twenty years has born witness to the frequent disruption of normal business operations by natural phenomenon, geo-political events, as well as human actions and errors. These interruptions are so wide-spread that no business in any country can consider itself immune from the risk that it will be unable to continue its operations in any given fiscal year. [See a report from Allianz Global Corporate & Specialty (“Allianz”), which analyzed more than 1,800 instances of large business losses totaling over \$3.2 billion from 68 countries from 2010 to 2014, titled RISK AND REPUTATION IN THE AGE OF DISRUPTION (2015) (hereinafter “RISK REPORT”). The 2014 Risk Report states that over 500 risk managers and corporate insurance experts found, for the third consecutive year, that business interruption loss is the number one risk for business worldwide.

This is not just a frequency issue. It is also a severity issue. The average business interruption insurance claim is now in excess of \$1 million. (See RISK REPORT, at 6.) As a result, business interruption insurance has become increasingly important part of business planning in all sectors of the commercial world.

Natural disasters like hurricane Katrina and Sandy illustrate this point. In 2005, hurricane Katrina caused an estimated \$10 billion in loss due to the interruption of business. (J. Wilier, M. Kok, & R.P. Nicolai, *Assessment of the losses due to business interruption caused by large-scale floods*, in SAFETY, RELIABILITY AND RISK ANALYSIS: BEYOND THE HORIZON 2415 (Steenbergen ed., 2014). Hurricane Sandy hit New York and New Jersey hard in 2012, resulting in an estimated \$20.6 to \$25.3 billion in business losses. *Id.* A recent article states that the frequency of insured business loss related to natural disasters worldwide has *tripled* since the 1980s. See Peter Hoeppe, *Trends in weather related disasters – Consequences for insurers and society*, 11 WEATHER & CLIMATE EXTREMES 70–79 (2016).

Despite their prevalence, perhaps increasingly so, natural disasters only account for a small percentage of lost business income. Rather, non-natural events, such as fires and explosions, machinery breakdown, and cyber security breaches, account for the majority of business interruption losses. (See *Risk Report*). In North America, the top causes of business interruption loss (by value) include fires and explosions (52%), storms (14%), cast loss (entertainment)¹ (8%), water damage (5%), and floods (4%).

The vehicle to cover these losses, business interruption coverage, is a first party coverage that was first written in England in the 1700’s as a separate form that covered income or profits, as distinct from property coverage. (See Lentz, Melton & Torpey, *The Business Interruption Book, Coverage, Claims and Recovery*, 2nd Edition, 2011. The National Underwriter Company, at p. 1). The coverage evolved to cover the profits of ship owners for lost ships and cargo. In the 1800’s ‘use

¹ “Cast loss” is a prevalent cause of business interruption loss in the entertainment industry. It refers to when a cast member or performer is unable to perform due to illness, injury, or death.

and occupancy” coverage was developed for landlords to cover loss of rents when insured buildings were destroyed. In the 1930’s, this type of coverage was extended to business generally and became known as ‘business interruption coverage’. In the 1980’s the term ‘business interruption coverage’ became cemented into insurance lexicon when the American Insurance Services Office issued a new policy form for business interruption insurance. (*Id.*, at p. 5)

In modern times and certainly since the 1980s, the various policy forms are clear that the purpose of the coverage is to ensure that as much as is possible, the insured’s revenue stream will continue following a covered loss, through to the point where the business is back up and running in repaired, restored or replacement premises with repaired, restored or replaced equipment and stock.

In the UK and the United States, there are two types of coverage: Gross earnings coverage and Business Income forms. The former extends coverage from the top down: What the insured would have earned had the covered loss not occurred (less the expenses that do not continue following the loss). Business income coverage forms calculate business interruption losses from the bottom up, which means the business interruption loss is the net income the policyholder would have earned if not for the interruption, plus the insured’s continuing fixed expenses such as payroll and taxes. In theory, the amount of a business interruption loss should be the same under the two policy forms. (See, generally: Roberts, Harry, *Riley on Business Interruption Coverage*, 9th Edition, Sweet & Maxwell, 2013, London; French, Christopher C., *The Aftermath of Catastrophe*, Georgia State University Law Review, Vol. 30:2, p. 461-520.)

From its modern inception as a recognized form of coverage in the 1980’s through to today, standard business interruption coverage is coverage that is added by endorsement to a first party property policy. As an ‘add-on’ to property coverage, it was intended to be read as an extension of that coverage.

Standard business interruption usually provides that during the “period of restoration,” which is usually the period of time required to repair, replace, or otherwise restore the physically damaged insured property, the insurer will pay the loss of business income sustained by the insured, usually defined as the net income that would have been earned by the insured had the physical damage not occurred, as well as covering the continuing normal operating expenses of that business that is caused by covered physical damage to the insured premises. A common and a now-basic add-on to the coverage also includes “extra expenses,” which is usually defined to include other “necessary expenses” that the business incurred as a result of the covered cause of loss.

The usual pre-requisite to coverage is proof that the loss of business income is caused by *covered physical* damage to the insured premises that has produced the loss, described in the attached property coverage. The coverage is specific to the business described in the declaration, and therefore, under standard wording, there is no coverage in the event that the insured sustains business loss at other separately insured premises owned by the insured but which were not physically damaged.

Standard business interruption coverage extends to only a small portion of the global business interruption risk; specialized variations have been developed and marketed to deal with the coverage gaps between this standard coverage and the financial risk arising from the rapid changes in the way that business is conducted world-wide. These variations that have developed overtime

demonstrate that business interruption coverage is a key component in the risk management plan of any business.

This paper discusses the international aspect to this coverage; the interpretation that has been placed on standard business interruption coverage by the American courts, a synopsis of the American judicial treatment of contingent business interruption coverage, comment on the issues surrounding the application of this coverage when a covered cause of loss effects an economic region and concludes with a discussion the evolving nature of business interruption coverage.

II Business Interruption Coverage is International

The interconnectivity of the commercial world means that even small and medium sized businesses deal with suppliers and customers outside of the United States or have branch offices outside of the United States. An event that causes damage to any of the foreign branch offices, customers or suppliers can cause a business interruption loss to the insured in the United States. Further, the American insured may be very involved in resolving the business interruption claim of a key supplier or its own branch office, causing the American home office to sustain a loss of business income. In either case, there may be claims for business interruption coverage in a jurisdiction outside and within the United States.

One cannot assume that the business interruption coverage that is commonly available in the United States is issued on identical terms in other countries. European insurers, as well as insurers operating in the United Kingdom, Canada and Australia do not use American forms. The wording of those forms is similar in that it incorporates some of the same concepts but similar does not mean identical and the differences, however subtle, can have a dramatic impact on the coverage that is available.

Some countries lack a well-developed body of case law that interprets their business interruption forms. In those instances, the American forms and judicial treatment of the wording contained in those forms, may be references by a foreign court to interpret the wording before them, particularly in the common law countries that share a British legal tradition.

For example, Canadian property insurers do not use a common business interruption form. Each insurer has its own form, the wording of which has been gleaned from policies issued in multiple jurisdictions. In some instances, the wording is similar to that used in the United Kingdom, others are influenced by American and Australian wording. In other cases, the wording is 'broker wording'; wording offered by an international broker which in turn was influenced by policies issued in multiple jurisdictions.

Consequently, the forms used by Canadian insurers have commonalities amongst each other, but the wording differences mean that one cannot assume that the same event will result in identical coverage across the board. Canadian Courts asked to interpret these wordings will use the well-known rules of insurance contract interpretation to provide meaning to the coverages and exclusions. If the wording is identical to, or similar to, American wording, Canadian Courts will consider American judicial authority where it does not conflict with existing Canadian case law.

For that reason, it is important to have an understanding as to how standard business interruption coverage is interpreted by American courts.

There is another reason for lawyers practicing outside of the United States to understand the American judicial treatment of business interruption coverage. Under some broker controlled insurance programs, where the insured is headquartered in the United States, the coverage will stipulate that it will be interpreted according the law of a certain American state. In that case, the private international conflict of law rules of the foreign jurisdiction where the litigation lies will determine whether the foreign court will recognize such a clause and apply the law of that state to a given dispute.

All of this is to say that American judicial treatment of standard business interruption coverage has implications beyond the jurisdiction of the American courts. For all of these reasons (in addition to assisting domestic American insurers and their counsel) we discuss how American Courts have dealt with the fundamental concepts of standard business interruption coverage.

III Salient Issues in the American Treatment of Standard Business Interruption Coverage

In our opinion, the most contentious issue regarding the interpretation of business interruption claims is determining when the insurer's obligation to indemnify the insured against a business loss terminates.

A. Duration of Business Interruption Coverage

i) Overview

When the insured premises are damaged by a covered cause of loss, the property coverages of the insured's commercial package policy respond to the repair and restoration of the physical damage to the property. If the damage causes a loss of business income, then the business interruption coverage (which again, is an endorsement to the property coverage) is triggered. The loss of business income is calculated. The insured requests that the insurer pay the insured for the sales / profit that the insured would have earned if the damage had not occurred. The insured bears the onus to prove the loss; and, since insurers often hear "We were having our best year yet ..." from their insureds, it's no surprise that business interruption claims are looked on with a measure of skepticism. (See Torpey, Daniel, *The Essential Equation: A Formula for Determining Business Interruption Loss*, February, 2004, <https://www.irmi.com/articles>.)

Once the loss is proven, then American standard business interruption coverage usually stipulates that the insurer is obligated to pay that loss until the insured property is repaired or restored to its pre-loss state or, when through the exercise of reasonable diligence and dispatch, the property ought to have been repaired or restored. This period of time which commences with the occurrence of the covered cause of loss and ends with restoration, or when restoration ought to have occurred, is called the "Period of Restoration." Some policies alternatively refer to it as the "Period of Liability" or "Period of Indemnity." In contrast, to the American wording, in the United Kingdom and in some Canadian policies, business interruption coverage is paid for a time limited period that is specified in the declarations to the policy, regardless as to when the premises are actually restored.

Seldom is there confusion or difficulty establishing when the Period of Restoration begins. Where the coverage is not time limited, there is much fact-based controversy and, therefore, litigation over when it ends.

Under older forms of standard business interruption coverage, once the Period of Restoration ends, no further amounts are payable. The loss of business income is deemed to terminate once the premises are restored. However, it is well-known that the loss of business income actually continues, as it is logical that there is a ‘ramping up’ phase that follows restoration, where income is lower than projected prior to the damage occurring and remains low while the insured’s ability to extend services or deliver production climbs to its pre-loss levels.

For that reason, brokers and underwriters agreed to add an optional second period of time during which the policy would respond to business income loss. This second time period is the “Extended Period of Indemnity.” For additional premium, the insured can extend its business interruption coverage from the time that the business has been physically restored to its pre-loss state through to the time when the insured’s business income is no longer affected by the damage that occurred.

In most cases, and, in those policies whose Period of Restoration is not time limited, the date upon which the period of restoration terminates is usually established by the date of issuance of the final occupancy permit for the premises that have been repaired or restored, or the actual completion date of the repair contracts. The controversial instances are those where the insured, in the opinion of the insurer, took far too long to determine when, where and whether to rebuild, or agree to the scope of repairs, or retain a contractor, or agree to a deficiency list. In those instances, negotiations will ensue to determine if the insurer should receive a time credit on the business interruption loss.

Once the termination date of the period of restoration is established, then, if available, the optional extended period of indemnity begins. The termination of the optional extended period of indemnity is even a grayer area than the termination of the period of restoration.

Unlike the initial Period of Restoration, the Extended Period of Indemnity is tied to the restoration of the insured’s *business due to a covered cause of loss*, not the restoration of the insured’s *property due to a covered cause of loss*. This is largely because the Extended Period of Indemnity does not begin until the damaged property has or should have been restored. Under most policy forms, the language mandates that in order for coverage to continue, there must be proof of a causal connection between the physical loss that occurred and the ongoing business loss.

In those policies where there is language permitting closure of the period of restoration at a time when the property should have been restored, then the extended period of indemnity will begin at the earliest of the actual or theoretical restoration dates. For the most part the extended period of indemnity has a capped end date (specified in the declarations or in the wording itself) but it will close earlier if there is a break in the causal relationship between the physical loss that was sustained and the reported loss of business income. However, the absence of a significant body of reported cases on the issue speak to the fact that for the most part, although litigated, these issues are negotiated short of the court house, or determined, with the agreement of the parties, by private arbitration.

ii) The Property Must be Restored with “Reasonable Speed”

It is important to review a few cases on the factual matrix that determines the termination of the

period of restoration where: (a) the policy does not apply a time limit on the payment of the business interruption loss and (b) there is an argument that the insured acted unreasonably during the repairs and restoration of the premises, delaying the time period during which the insured could not operate at capacity.

The reasonableness of the insured's speed in making repairs was the main issue considered in *G&S Metal Consultants v. Continental Casualty Company*, 2016 U.S. Dist. LEXIS 100851 (N.D. Ind. Aug. 2, 2016). In that case, an explosion caused extensive property damage to the insured's aluminum processing and recycling facility. *Id.* at *4. The damage eventually necessitated a complete shutdown of the facility's operations. *Id.* at **4-5. After the explosion, it took the insured nearly eleven months to find a contractor to make the necessary repairs. *Id.* at *5. After the insured hired a contractor, it took another five months to make the agreed-upon repairs to the facility. *Id.* at *5.

The insurer took a coverage position that the Period of Restoration only included the five months that it took the contractor to repair the facility. *Id.* at *5. The insurer contended that it took the insured far longer than it should have to find a contractor, and so the eleven months between the date of explosion and the hiring of the contractor should be excluded from the Period of Indemnity. *Id.* at **25-26. The insured filed a bad faith breach of contract action to challenge the coverage position. *Id.* at *2. It argued that its eleven-month search for a contractor was reasonable under the circumstances because it had reached out during that time to the insurer and the local government for assistance in locating a contractor, but received no bids. *Id.* at *26.

On the insurer's motion for summary judgment, the court held that the calculation of the period of indemnity must be resolved by a trier of fact. *Id.* at *28. The court recognized that "reasonable speed" provisions require the insured to act "as quickly as possible" in the repair of damaged property. *Id.* at 23-24. The court further recognized that certain evidence in the record suggested that the insured did not act in the most diligent fashion. *Id.* at *27. The court took issue, however, with the insurer's position that the Period of Restoration did not include *any* time to locate a contractor and held that finding a contractor is an essential part of the rebuilding process. *Id.* at 25-26. The period of restoration, should have included the amount of time it would have taken an insured acting "as quickly as possible" to locate a contractor. *Id.* at *26. The determination of the actual length of that period of time was reserved for the jury. *Id.* at *28.

The court further held that the period of restoration could have been extended by the insurer's actions in handling the claim if those actions frustrated the insured's efforts to make repairs. *Id.* at *30. The insured presented evidence that after the contractor completed the agreed-upon repairs, the facility's roof still leaked and created a safety hazard. *Id.* at *5. Additional repairs were necessary, but by that point, the insured was facing severe financial hardship due to business interruption and could not afford to front the cash for those repairs. *Id.* at *6. The insured submitted a claim to the insurer for the additional repair work under the policy's building and personal property coverage. *Id.* at *6. The insurer internally authorized the additional repair work, but took two months thereafter to actually fund the repairs. *Id.* at 6. The insured argued that the period of restoration should include the time necessary to make the additional repairs, including any delay caused by the insurer's processing of the claim. *Id.* at *28. The court agreed, reasoning that "it is reasonable to presume that an insured requires assistance from the insurer before it is able to make repairs." *Id.* at *31. Thus, "...[I]f an insurer drags its feet in assisting the insured, regardless of whether it technically breaches the policy, that can slow restoration and increase the

insured's losses." *Id.* at *30.

The *Continental* case demonstrates that the Period of Restoration can be affected by the actions of *both* the insured and the insurer. "Reasonable speed" and "due diligence" requirements impose a duty on the insured to mitigate its losses by acting "as quickly as possible" to restore its property. The insurer, however, can extend the restoration period if it fails to promptly assist its insured.

iii) Restored Property must be of "Similar Quality"

Those policies that do not have a time limited period of restoration mandate that the Period of Restoration is subject to a "similar quality" prong. Under most forms of standard business interruption coverage, the insured is entitled to indemnity against business loss until the damaged property is "made ready for operations under the same or equivalent physical operating conditions that existed prior to the damage." When repair of the property is not feasible, courts hold that these provisions entitle the insured to recover its lost profits until it can build a reasonably equivalent facility in a reasonably equivalent location. *Duane Reade, Inc. v. St. Paul Fire & Marine Ins. Co.*, 411 F.3d 384, 393 (2nd Cir. 2005).

For business interruption losses arising from the destruction of owned or specifically-insured property, the insured is generally entitled to rebuild the same facilities on the same location as the property that was destroyed. *See, e.g. Anchor Toy Corp. v. American Eagle Fire Ins. Co.*, 155 N.Y.S.2d 600, 603 (N.Y. Sup. Ct. 1956); *Omaha Paper Stock Co. v. Harbor Ins. Co.*, 596 F.2d 283, 285 (8th Cir. 1979); *Beautytuft, Inc. v. Factory Ins. Asso.*, 431 F.2d 1122 (6th Cir. 1970); *Steel Prods. Co. v. Millers Nat. Ins. Co.*, 209 N.W.2d 32, 33-34 (Iowa 1973). The insured, however, is not required to reuse available architectural drawings for the destroyed property and may update the restored facilities to modern standards. *Anchor Toy*, 155 N.Y.S.2d at 603.

iv) Applying these Concepts to Business Losses Generated by Damage Caused by a Regional Disaster

The applications of these requirement becomes very, very problematic in a regional disaster scenario such as when the economy of an entire region is decimated by a hurricane or a wildfire.

There are worldwide examples of this level of disaster – particularly disasters caused by wildfire. In Australia, one cannot forget the Black Saturday bushfires of 2009. These fires killed 173 people, destroyed around 2000 homes and burnt out 4,500 km² of land, leading to insured losses of \$1.09 billion (See www.cgu.com.au.) In addition to the perennial California wildfires, the United States experienced the 2013 Black Forest Fire and the 2012 Waldo Canyon Fire in Colorado which caused \$292.82m and \$453.7m of damage respectively. (See Maynard, Trevor et al., *Wildfire, A Burning Issue for Insurers?*, 2013, www.lloyds.com at p. 20.) In May, 2016 the Fort McMurray wildfire in Alberta, Canada, burned 2,400 structures in the City of Fort McMurray and decimated 590,000 hectares (1.5 million acres). This fire achieved the status of the largest wildfire in Canadian history – as this paper is being written, that fire still smolders.

Landlords operating office and retail space may decide that the economy in which it operated prior to the destruction of the owned property will be too slow to return and elect not to rebuild, invoking the *force majeure* clause in the leases, (or argue that the lease is now frustrated); or elect to rebuild, but the rebuild is slow as the disaster has resulted in a building boom and there is a shortage of materials and trades; or, the upgrades necessary to comply with evolving building codes requires

a building very different than what existed prior to the disaster. Similarly, the tenants must research their markets and determine if it is feasible to re-establish in the same area and if so, where; or, move to another locale. Both the landlord and the tenant have business interruption claims.

The leading source of case law that deals with these issues arises from the destruction of the twin towers as a result of the 9/11 terror attacks, which litigation is ably summarized in Johnson, Scott G., *Ten Years After 9/11: Property Insurance Lessons Learned*, 686 Tort Trial & Insurance Practice Law Journal, Spring-Summer 2011, particularly at pp. 691-702.

The shocking facts that spawned this litigation are so well-known, they almost do not bear repeating. However, to be complete, on September 11, 2001, terrorists hijacked and flew two commercial aircraft into the twin towers of the World Trade Center (WTC), destroying both of them, damaging or destroying a number of other surrounding buildings, and killing nearly three thousand people. This event (together with the attack on the Pentagon and the downing of United Flight 93 into a field near Shanksville, Pennsylvania) resulted in the largest insured claim in American history, a title that was held until 2005 when Hurricane Katrina blew through Louisiana. Nearly two thirds of the losses paid as a result of the hijacking of the four planes were property losses. (*Id.*, at p. 686)

The WTC policies typically defined the period of restoration as beginning on “the date and time of direct physical loss or damage” and ending on “[t]he date when the property should be repaired, rebuilt or replaced with reasonable speed and similar quality.” (*Id.*, at pp. 691-2). Although an arbitration panel determined the period of restoration for the landlord group, the courts issued several noteworthy rulings to guide the arbitrators under the style, *SR Int’l Bus. Ins. Co., Ltd. v. World Trade Center Properties LLC*.

In a decision under that style and reported at 2005 U.S. Dist. LEXIS 13001 (S.D.N.Y. 2005), the court found that the insureds were in the business of providing facilities services to the WTC. Its businesses were entirely dependent on the existence of the WTC, and there was no dispute that the end of the actual Period of Restoration would coincide with the reconstruction of the WTC. However, given the policy language “...when the property should be repaired, rebuilt or replaced with reasonable speed ...”, what was the termination date of the period of restoration under the business interruption coverage?

The insurers argued that the period of restoration was eight years as appraisers had calculated the time that was theoretically reasonably necessary to replace the WTC to be eight years from the destruction of the towers in 2001. *Id.* at 4. The insureds did not contest this calculation but argued that the Period of Restoration was the amount of time it would actually take to replace the WTC, and that the Period could not be calculated until reconstruction of the WTC was actually complete. *Id.*

The Court sided with the insurers on the basis of precedent and the policy’s plain language. Specifically, the policy provided that the Period of Restoration ended on “the date when the property *should* be repaired, rebuilt, or replaced with reasonable speed and similar quality.” *Id.* at 11. The subjunctive use of “should” in the definition mandated a theoretical measure. *Id.* at 19. Nothing in the policy suggested that an actual measure was intended. *Id.* The court then cited

extensively from precedent applying theoretical measures, and considered whether an “actual measure” would be preferable. It dismissed any concerns about the reliability of theoretical measures, and arrived at the following conclusion:

Where an insured rebuilds with ‘reasonable speed’ and ‘similar quality’ . . . the actual period should coincide with the theoretical period. [. . .] It is only where an insured party fails to comply with such policy terms, or in the rare case where an insured rebuilds more quickly than anticipated, that a gap between the actual and theoretical periods will arise. In such cases, it is the theoretical, not the actual, period of restoration that governs. *Id.* at 25-26.

With the benefit of hindsight, we now know that the court and appraisers were overly optimistic as the WTC’s replacement, One World Trade Center, was actually completed in July 2013, nearly four years after the theoretical restoration period terminated. Nonetheless, the theoretical measure is considered preferable because it allows the insured and insurer to calculate the restoration period without waiting for the actual completion of reconstruction, enabling both parties to resolve the issue sooner and make corresponding adjustments to their financial planning. *See Id.* at 28. Although the theoretical measure turned out to work against the insured in *SR International*, the theoretical measure can also create the possibility of a windfall to the insured if it is able to resume operations before the theoretical restoration period ends. To avoid such a windfall, some policies will adjust the amount of available business interruption coverage if the insured is able to resume operations sooner than expected. *See Beautytuft, Inc. v. Factory Ins. Asso.*, 431 F.2d 1122 (6th Cir. 1970).

In summary and to emphasize, the Period of Restoration in the landlords’ policy was declared to be a theoretical measure, not an actual measure. It is based upon the hypothetical time it *should* take to replace the damaged property and is not subject to proof of the time it actually takes to restore the property.

The Courts also dealt with the date of termination of the period of restoration for the displaced tenants of the towers. The leading case on the tenants’ side is *Duane Reade, Inc. v. St. Paul Fire & Marine Insurance Company*, 411 F.3d 384, 387 (2nd Cir. 2005). Duane Reade held a commercial package policy containing business interruption coverage that insured more than 200 Duane Reade drug stores in and around New York City. Duane Reade’s busiest and most profitable store was located in the WTC which was destroyed on 9/11. *Id.* The WTC location was not specifically identified in the policy, but Duane Reade nonetheless argued that the Period of Restoration was site-specific and the period of restoration lasted until Duane Reade could reopen a store in the replacement for the WTC. *Id.* The trial court agreed, holding that the restoration period would end “once Duane Reade could resume functionally equivalent operations in the location where its WTC store once stood.” *Id.* at 388.

The Second Circuit reversed. The court reasoned that the policy made no reference to the WTC store, and so the physical premises of the WTC building were not the subject of the policy. *Id.* at 395. The court further opined that it would be unreasonable to tie the duration of business interruption coverage to the reconstruction of the WTC because such rebuilding would “be a herculean undertaking far exceeding the rebuilding of a Duane Reade store . . . and involving numerous and complex contingencies over which neither Duane Reade nor [the insurer] has any control.” *Id.* at 396.

Instead, the court held that when destroyed business premises were leased and not specifically identified in the policy, the Period of Restoration extended only to the hypothetical time that it would reasonably take Duane Reade to rebuild or replace its personal property at another suitable location. The policy made no reference to the WTC store and therefore there was no basis to argue that the policy provided site-specific coverage. Any losses caused by the inferiority of the new location would be covered by another endorsement to the Duane Reade policy called 'leasehold interest' coverage that covered the actual loss sustained due to the fact that the leasehold premises were not usable.

Subsequent to the Second Circuit's decision in *Duane Reade*, the Southern District of New York reached a similar conclusion in another WTC case, *Retail Brand Alliance, Inc. v. Factory Mutual Insurance Company*, 489 F. Supp. 2d 326 (S.D.N.Y. 2007). Retail Brand Alliance (RBA) operated three retail women's clothing stores in the underground mall in the WTC complex as part of a chain of 600 stores across the country. After the WTC was destroyed, RBA sought recovery of business interruption losses for the theoretical period of time reasonably necessary to replace its three WTC stores "at a location with a sales environment that is comparable to the one which existed at the WTC" or, if none, the hypothetical period of time to rebuild the WTC stores with reasonably equivalent stores . . . in a reasonably equivalent location." (Johnson, *supra.*, at p. 694)

The court rejected RBA's claim that the attributes that led to large sales volumes at the WTC location, "increased foot traffic, entrenched customer base, or superior location" was protected by the business interruption endorsement. As in *Duane Reade*, the court found that the policy did not tie coverage to the site-specific restoration of each of RBA's more than 600 stores.

Duane Reade and *Retail Brand Alliance* show that the Period of Restoration cannot be read in isolation from the rest of the policy and the circumstances of the loss. Instead, all facts and circumstances must be considered in determining whether potential replacement property is of "similar quality" to its predecessor. What is key to these findings is that in the case of a disaster which renders it impossible to rebuild on the pre-loss location, the period of restoration for tenants is unlikely to be extended due to an inability to rebuild on the same site that was destroyed. The period of restoration will be calculated on the basis of the time it reasonably takes to replace the insured's property at a reasonably suitable location, even if the new location lacks the attributes that rendered the destroyed location profitable.

The WTC litigation establishes that for landlords and tenants alike, where the policy contains wording that stipulates that the period of restoration terminates "when the property *should* be repaired, rebuilt, or replaced with reasonable speed and similar quality", then the period of restoration will be a theoretical period determined by the trier of fact. If the premises can actually be repaired or restored, with reasonable diligence, then the theoretical period of restoration will coincide with the actual period of restoration.

Regional disasters often result in unique issues regarding the calculation of the loss that is payable under business interruption coverage. Business interruption forms do not contain a formula as to how the loss is to be calculated – the absence of a formula results in uncertainty in all cases but particularly in a regional disaster scenario.

A regional disaster can cause populations shifts; residents leave due to housing or job loss; as a portion of the population leaves, contractors move in, creating a mini building boom.

Those insureds who are in the building trades, those in the hospitality sector that operate hotels and restaurants to house and feed the workers, or those that sell furniture, large appliances and building supplies who are able to get back to business to take advantage of the reconstruction effort, will experience an increase in income over pre-disaster projections (particularly if the disaster eliminates their pre-loss competitors) which will taper once the boom ends. In that environment, does an appliance dealer, initially crippled by covered physical damage but who is able to get back into business fairly quickly and increase its pre-loss sales due the unforeseen post-loss demand, have a business interruption claim? Based on what?

Can the insureds who would have profited from the reconstruction, but are so crippled by the disaster that they are unable to participate in the reconstruction, able to argue that they are entitled to claim the profits that they would have earned if they were up and running?

In addition to the effects that the reconstruction bubble can have on business income, the disaster can wipe out the market of a business that thrived pre-disaster. The case in point is that of a minimally damaged insured that can get back to business fairly quickly, only to find that the disaster has eliminated its customer base and revenue plummets. Can the insurer argue that this insured has not suffered a business interruption loss on the basis that if their premises had not been damaged, the surrounding disaster would have eliminated the market for their goods and services and they would have lost business regardless?

In short, taking into account the actual impact that the disaster has had on the regional economy can work for and against insureds. In these scenarios, how are the claims calculated? The answer lies in determining whether it is appropriate to utilize the post-loss actual earnings and losses to calculate the loss or whether the loss is calculated solely on the basis of pre-disaster projections.

There is divided authority in the United States as to whether losses are to be calculated solely on the basis of pre-loss projections and not on the basis of actual earnings. (One of the leading cases stating that only historical projections can be used is *Finger Furniture Co. v. Commonwealth Ins. Co.*, 404 F.3d 312 (5th Cir. 2005). A leading case stating that actual post-loss earnings may be taken into account is *Sher v. Lafayette Insurance Co.*, 973 So. 2d at 47.). There are fewer appellate decisions stating that actual post-loss earnings are to be taken into consideration than there are in the camp that maintains that only historical projections may be analyzed. Further the cases that use actual results are largely out of Louisiana. The balance of American authority appears to favour the sole use of pre-loss and historical projections to calculate the loss, however, the actual policy language will trump in all cases. In that regard, some business interruption policies stipulate that post loss profits caused by the disaster are not to be taken into account when calculating the loss. In the result, there appears to be an argument that losses are to be valued solely upon the use of pre-loss actual earnings and historical projections. Policies that bear that prohibition, in addition to language stating that the insured is entitled to the actual loss sustained, will be calculated premised upon the difference between what the insured would have been earned during the period of restoration (had no loss occurred), and what actually was earned.

However, the issue of negative post-loss changes in the economy produced by the disaster is not completely settled by the case law and policy wording that determines the basis upon which the amount of the claim is to be calculated. If there is a post-loss change in customer sentiment regarding the insured's goods or services, or if there are less people in the vicinity of the insured's business to purchase its goods or services, insurers have argued that the "loss of market" exclusion

serves to bar coverage for the financial impact caused by these circumstances. In short, even though the loss is calculated based upon the insured's pre-loss projections without taking into account the impact that the regional disaster has had on the insured's actual income; the "loss of market" exclusion may permit the insurer to reduce the amount payable by the negative impact of the post disaster economy, if that negative impact can be said to be a "loss of market".

The meaning of 'the loss of market' exclusion in a regional disaster scenario was considered in the *Duane Reade* case where the court held that "...The loss of market exclusion relates to losses resulting from economic changes occasioned by, e.g., competition, shifts in demand, or the like; it does not bar recovery for loss of ordinary business caused by physical destruction or other covered peril. (*Id.* at 240). Time will tell whether the *Duane Reade* case has firmly settled the issue of the meaning of the "loss of market" exclusion as it applies to a regional disaster. (For a general pro-policy holder discussion on the application of this exclusion, see Daar, Henry R., ABA Section of Litigation Insurance Coverage Litigation Committee CLE Seminar, March 3-5, 2011: *The Misadventures of the Loss of Market Exclusion: The Calculation of "Actual Loss Sustained" Has No Relationship to the Exclusion*, unpublished paper, <https://apps.americanbar.org/litigation/committees/insurance/docs/2011-cle-materials/21-BusinessInterruptionConundrum/21aLossMarketReport.pdf>)

In the event the 'loss of market' exclusion applies, the insured may find relief against its losses if the insured carries contingent business interruption coverage; the loss is due to a loss of "a supplier"; or a "recipient location" due to damage to a "dependent property" which is defined as a property that accepts the insured's products or services.

IV. CONTINGENT BUSINESS INTERRUPTION COVERAGE

A limitation of standard business interruption coverage is the requirement that the business loss must emanate from the same premises that were physically damaged.

Business income losses caused by "off-premises" fires, explosions, flooding and connectivity issues are growing in frequency and severity. As businesses move away from vertical integration and have increased supply chain interdependencies, failure of a link in the supply chain makes contingent losses more and more likely. (See Kaliner, Bruce R., *The Expanding Role of Contingent Business Interruption Insurance*, § 17 Mealey's Business Interruption Ins. (Volume 3, 1st ed.) (2003)). These factors are particularly prevalent in the energy sector, as oil and gas companies have complex and heavily concentrated supply chains. *Id.*; also see Chris Dye, *Cost of Oil and Gas Insurance Claims Continues to Rise*, OIL & GAS FIN. J., Dec. 16, 2014. Further, energy companies often have several facilities (such as oil fields) feeding into a single processing location, meaning that a covered loss at a drill site can cause a loss of income at a refinery, thousands of miles away.

"Contingent business interruption" was designed as a partial answer to this off-premises problem, as it protects an insured's business income when it sustains loss caused by damage to property owned or managed by a "supplier" or a "customer" (both of which are tightly defined terms). Usually, "a supplier" is only defined to include direct suppliers; however, additional coverage is available for indirect suppliers, *i.e.*, the supplier of the insured's direct supplier. Similarly,

coverage is available for “contingent extra expenses.” This coverage will also include the necessary extra expenses incurred due to damage at the premises of a “dependent property,” as that term is described in the schedule of insurance. Depending upon the wording, “dependent property” can include losses of business income that the insured sustained at a facility that it owns due to covered physical damage that occurred at another.

Contingent business interruption (“CBI”) insurance provides coverage for losses sustained by an insured when its supplier is unable to deliver to the insured with parts or resources, or when the insured’s customer is unable to take delivery of the insured’s product, because of damage to the supplier or customer’s property. See, e.g., *Park Electrochemical Corp. v. Cont’l Cas. Co.*, No. 04-CV-4916 (ENV) (ARL), 2011 U.S. Dist. LEXIS 16344 (E.D.N.Y. Feb. 16, 2011); *Children’s Place Retail Stores, Inc. v. Fed. Ins. Co.*, 37 A.D.3d 243 (App. Div. 2007).

Closely associated with “Contingent Business Interruption Coverage is another form of business interruption coverage called “Leader property”. This refers to an endorsement that provides coverage for business interruption losses incurred as a result of damage to a nearby property not owned by the insured, within a stated distance, and which attracts business to the insured. For example, if a Disney World location closed due to a covered occurrence, such as a hurricane, this endorsement may apply to the loss of business income sustained by a nearby hotel, owned by an insured independent of Disney World, that was dependent upon traffic attending Disney World.

While the particular provisions of CBI coverage forms vary, an example of a typical CBI coverage in a first-party property policy is as follows:

2. Dependent Locations – Coverage for earnings and/or extra expense is extended to loss of earnings or extra expenses that “you” incur during the “restoration period” when “your” “business” is interrupted by direct physical loss of or damage, caused by a covered peril, to property at a “dependent location”.

“Dependent location,” or often “dependent property,” is typically defined as property operated by others upon which the insured depends to deliver material or services to the insured (a “contributing” location), property that accepts the insured’s products or services (a “recipient” location), property that manufactures products for delivery to the insured’s customers (a “manufacturing” location), or property that attracts customers to the insured’s business (a “leader” location).

Few courts have interpreted CBI coverage in the context of natural disasters. Given the vast differences in the nature of businesses and how businesses operate, the particular language of a CBI provision and the terms of the “dependent location” or “dependent property” definition can lead to disparate outcomes.

A. Initial Grant of Coverage

As noted above, CBI coverage may apply in a variety of circumstances involving damage to property other than the insured’s own property. A threshold matter is whether the cause of property damage to the contributing, recipient, manufacturing or leader property is a covered cause of loss. For CBI coverage to be triggered, the peril causing property damage sustained by the dependent, supplier, or recipient property must be of the type that is covered under the insured’s own policy.

In the context of hurricane or flooding, for example, CBI provisions may not be triggered in a situation where a dependent, supplier, or recipient location is damaged by wind or flood, but wind or flood is not a covered cause of loss under the insured's policy. In *Pel Hughes Printing, LLC v. Hanover Ins. Group, Inc.*, No. 07-4044, 2008 U.S. Dist. LEXIS 31224 (E.D. La. Apr. 16, 2008), the issue was whether a loss of business income and extra expense caused by off-premises power failures in the wake of Hurricane Katrina was covered under contingent income provisions of the policy. Windstorms and "water damage" were specified causes of loss covered by the policy. "Water damage" was defined as an "accidental discharge or leakage of water or steam as the direct result of the breaking or cracking of any part of a system or appliance containing water or steam." *Id.* at *17.

The insured argued that breaking of levees in New Orleans resulted in a "water damage" loss. The court denied the insured's summary judgment motion, however, on the basis that the insured failed to provide any evidence as to what caused the damage to the off-premises structure. It held instead that there was a question of fact as to whether wind or water damage caused the loss. *Id.* at 19. Also see *Wms Indus. v. Fed. Ins. Co.*, Civil Action No. 1:06CV977-LG-JMR, 2009 U.S. Dist. LEXIS 68678, n. 9 (S.D. Miss. Aug. 4, 2009) (noting that although flood damage was excluded from a CBI coverage, where it was estimated that hurricane winds accounting for approximately 20% of the loss at the dependent property, and 20% of the damages were still in excess of CBI limits, the distinction was moot).

Similarly, in *Southern Hospitality, Inc. v. Zurich American Insurance Co.*, No. Civ. 02-923-C, 2003 WL 2341 23416117 (W.D. Okla. Sept. 30, 2003), the insured managed a number of hotels. It claimed that losses sustained as a result of the Federal Aviation Administration's grounding of all airplane flights in the United States following the September 11, 2001 terrorist attacks were covered under the "dependent property" provisions of its policy. The CBI coverage was premised on physical loss or damage at the premises of a "dependent property." *Id.* at *12. The court rejected the insured's claim on the basis that the insured could not identify a contributing property which was damaged by a covered cause of loss, nor any dependent property which sustained physical damage from a covered cause of loss. *Id.* at *13.

In addition to requiring a covered cause of loss to dependent property, there must also be a causal connection between the physical loss or damage to the property of the direct supplier or key customer and the interruption of the insured's operation. (Kaliner, *supra.*, citing *Archer-Daniels-Midland Co. v. Phoenix Assurance Co. of New York*, 936 F. Supp. 534 (S.D. Ill. 1996), *aff'd* sub nom. *Archer-Daniels-Midland Co. v. Aon Risk Servs., Inc. of Minn.*, 356 F.3d 850, 854-57 (8th Cir. 2004)). In *Archer-Daniels-Midland Co.*, the insured, ADM, processed farm products for domestic and international consumption. Widespread flooding in the Midwest in the summer of 1993 increased ADM's costs to obtain raw materials and caused increased transportation costs. ADM sought coverage for these added expenses. The court agreed that ADM was entitled to coverage. Inherent in the court's rationale was that flooding caused physical damage to the insured's downstream farm suppliers. Flooding was a covered cause of loss under ADM's policy.

Thus as an initial matter, to trigger coverage, the peril causing property damage sustained by the supplier must be of the type that is covered under the insured's own policy. Further, there must be a causal connection between the physical loss or damage to the dependent property or location and the interruption of an insured's business.

B. The Scope of Coverage for Contributing, Recipient, Leader, and Manufacturing Locations

Assuming the CBI coverage is triggered, the scope of CBI coverage available to the insured depends in large part on how “dependent property” or “dependent location” is defined.

1. Suppliers or “Dependent Locations”

One type of “dependent location” or “dependent property” is property operated by others upon which the insured depends to deliver material or services to the insured, i.e. the insured’s “supplier”. A typical CBI provision may define “supplier” as:

- a. Contributing locations, these are “your” suppliers’ locations or locations of suppliers that deliver services or materials to others for “your” account. Contributing locations do not include suppliers of: 1) water; 2) telecommunications, including but not limited to internet service providers; or 3) power [damage to suppliers is dependent property];

The seminal case interpreting a CBI coverage definition of “supplier” is the case of *Archer-Daniels-Midland Co. v. Phoenix Assurance Co. of New York (supra)* where the policy at issue covered against “loss of earnings and necessary extra expenses resulting from necessary interruption of business . . . of any supplier of goods or services which results in the inability of such supplier to supply an insured locations [*sic*].” *Id.* at 540.

ADM argued that Midwest farmers affected by the floods and the Army Corps of Engineers, which operated and maintained the Mississippi River system, were “suppliers of goods and services” under the policies. *Id.* Citing the dictionary definition of “any” and “supplier,” the court read the policy phrase “any supplier of goods or services” to include the Army Corps of Engineers because the Corps “supplied” “services” by constructing improvements on the Mississippi River. *Id.* at 541. It also held that the Midwest farmers who grew the crops that ADM processed were also “suppliers of goods and services,” even though the farmers were not in direct contractual privity with ADM. *Id.* at 544. Notably, the Archer-Daniels-Midland policy did not define “supplier.” The Archer-Daniels-Midland holding is favorable to insured’s affected by natural disasters in asserting CBI claims because it supports a broad reading of the definition of “supplier,” and because it holds that no contractual privity is required between the insured and its suppliers to support a CBI claim.

ADM brought an additional case against its insurance broker in *Archer-Daniels-Midland Co. v. Aon Risk Servs., Inc. of Minn.*, 356 F.3d 850, 854-57 (8th Cir. 2004). In that case, a federal court in Minnesota concluded that ADM did not have to identify each particular grain supplier who was unable to supply grain to ADM. Since the language of the CBI provision referred to “any” supplier, the court defined “any” supplier to include those farmers in the Midwest who supplied or could have supplied grain to ADM. *Id.* Such an expansive reading of the CBI provision may have the effect of relieving a CBI claimant of “individually identifying each supplier or customer who sustained property damage.” (See Mascali Jr., Arnold. *Contingent Business Interruption Coverage*, 41 Tort & Ins. L.J. 843 (2006)).

The case of *Pentair, Inc. v. American Guaranty & Liability Insurance Co.*, 400 F.3d 613 (8th Cir. 2005), provides a more restrictive and recent interpretation of the term “supplier” in a CBI policy. In *Pentair*, an earthquake struck Taiwan in 1999, disabling a substation that provided electric power to two Taiwanese factories. The factories could not manufacture products they were

supplying to the insured, Pentair, Inc. in Minnesota. Taiwanese production resumed several weeks later, and Pentair had their orders shipped from Taiwan via airfreight to make up for lost time in anticipation of Christmas, resulting in additional costs. Pentair filed a claim for loss under its contingent business interruption coverage, which extended business interruption to include losses incurred by Pentair as the result of damage to “property of a supplier of goods and/or services to the insured” that is caused by a covered peril. *Id.* at 614.

The court held that the electric substation, though physically damaged by the earthquake, was not a Pentair supplier for purposes of coverage. *Id.* at 615. The court distinguished the *Archer-Daniels-Midland* case, reasoning that in that case, each farmer supplied a product – grain – that a dealer then resold to the insured. *Id.* By contrast, the Taiwanese power company did not supply a product or service ultimately used by Pentair, and therefore, the power company did not supply a good or services to Pentair. *Id.* The Court did not address the possibility that the power company was a supplier of services to Pentair in the same manner that the *Archer-Daniels-Midland* court found that the Army Corps of Engineers was a supplier of services.

Policies that define “supplier” or “contributing property” more narrowly may reduce the scope of coverage available to the insured. In *Millennium Inorganic Chems. Ltd. v. Nat’l Union Fire Ins. Co. of Pittsburgh*, 744 F.3d 279 (4th Cir. 2014), for example, the policy at issue explicitly limited coverage to apply only to a “direct contributing property” of the insured. Specifically, the policy at issue stated that covered locations “must be direct suppliers of materials to [Millennium’s] locations.” *Id.* at n. 2.

In *Millennium Inorganic*, the insured was a titanium dioxide processor that received natural gas from its producers via pipeline. An explosion occurred at a producer’s facility, causing production to cease, and Millennium was forced to shut down its titanium dioxide manufacturing operations for a number of months. Millennium filed a claim for CBI coverage with its insurers. Although the policy at issue did not define “direct,” the Fourth Circuit held that the producer was not a direct supplier to the insured because it merely injected the gas into the pipeline, where the gas was commingled with other suppliers’ product, before it reached the insured. *Id.* at 286. The court further noted that Millennium had “no legal relationship, direct or otherwise, with Apache [the producer].” *Id.*

Imagine, for example, a hypothetical insured, “Fully Covered.” Fully Covered is a fashion retailer that designs and sells t-shirts at storefronts that it leases in shopping malls across the country. Fully Covered purchases cotton and dyes from various suppliers in Mexico. It designs the t-shirts and contracts with a manufacturer to dye, sew, and package the t-shirts. Depending on the definition of “dependent property,” the cotton and dye suppliers in Mexico may be considered a “contributing location.” The shopping mall storefronts may be considered a “recipient location” or a “leader location.” The manufacturer that dyes, sews, and packages the t-shirts may be considered a “manufacturing location”. A disaster at any of these locations may interrupt Fully Covered’s supply chain and distribution to its customers, resulting in loss of income and high exposure to its CBI carrier.

3. “Leader” Locations

Dependent locations typically include property upon which the insured relies to attract customers to the insured’s business (a “leader” location). In the example of Fully Covered, the commercial

shopping malls in which the fashion retailer sells Fully Covered's products may be considered a leader location. A typical "leader location" provision may state:

- c. leader locations, these are locations that attract customers to "your" "business"; or [property damage to attraction properties located in the vicinity of the insured's property is attraction or leader property].

In *Zurich Am. Ins. Co. v. ABM Indus.*, 397 F.3d 158 (2nd Cir. 2005), the Second Circuit considered whether CBI coverage was available to an engineering and janitorial service contractor in connection with losses suffered as a result of the September 11, 2001 terrorist attack at the World Trade Center ("WTC") complex. The insured, ABM, provided janitorial, lighting, and engineering services at the World Trade Center. It serviced the common areas of the complex pursuant to contract with the owners of the facility and the Port Authority of New York and New Jersey. In addition to other business income claims, ABM asserted that losses of business income from the destruction of the WTC were covered by the "Leader Property" provision of its coverage, which applied to losses to "property not owned or operated by the Insured, located in the same vicinity as the Insured, which attracts business to the insured. *Id.* at 171.

The trial court held that WTC was not a "leader property" in the "vicinity" of ABM which "attracts business" to ABM, but instead that the WTC is itself the site and source of the ABM business at issue. *Id.* The Second Circuit rejected this, holding instead that a property can attract business to another entity at the same site, or adjacent to it. The court noted that the "interconnectedness of the WTC complex that 'attracted' its tenants to ABM's services by providing an opportunity for ABM to exploit economies of scale." *Id.* Nevertheless, the Second Circuit found that because ABM "operated" the infrastructure of the complex, there was no CBI coverage, as the policy only covered properties not owned or operated by the insured.

While the Second Circuit denied coverage under the leader property provisions on the basis that ABM operated WTC infrastructure, its rationale suggests a willingness to recognize coverage for leader locations where businesses are "interconnected." This expansive reading may be cited by policyholders in future CBI claims caused by natural and man-made disasters. In the hypothetical example of Fully Covered, leader locations are those locations that attract customers to purchase Fully Covered's t-shirts. This likely includes the shopping malls in which Fully Covered has retail storefronts. Fully Covered could argue for a more expansive reading of "leader location," though. If Fully Covered has retail store in New York City, nearly any property in the metro area is in the "vicinity" of the Fully Covered's property that attracts customers. Again, the extent of what qualifies as a leader location is virtually limitless.

4. "Manufacturing" Locations

Finally, dependent property or location can be property upon which the insured relies to manufacture products for delivery to the insured's customers. The CBI provisions may define manufacturing locations as:

- d. manufacturing locations, these are locations that make products for delivery to "your" customers under contract of sale.

It appears that there are no cases interpreting the manufacturing location provision in any American jurisdiction. A court would likely interpret this language in a similar manner as courts interpreting

the meaning of other dependent location and in accordance with the limits and specificity required by the particular policy language. For example, if the policy is silent regarding whether the insured and the manufacturing location is required to be in privity of contract, courts might read the policy expansively and find coverage. On the other hand, if the policy requires the manufacturer to be a “direct” manufacturer, a court might deny coverage for manufacturers that are further attenuated from the insured’s business operations.

2. Customers or Recipient Locations as “Dependent Locations”

A dependent location or property can also include property that accepts the insured’s products or services, i.e. customers or recipient locations. In the hypothetical case of Fully Covered, the fashion retailer which purchases Fully Covered’s t-shirts may be considered a customer or recipient location. A typical CBI coverage may describe a “recipient location” as:

- b. recipient locations, these are locations that receive “your” products [property damage to customers is recipient property];

There are few cases interpreting customer or recipient locations in the context of a disaster. In *Wms Indus. v. Fed. Ins. Co.*, Civil Action No. 1:06CV977-LG-JMR, 2009 U.S. Dist. LEXIS 68678 (S.D. Miss. Aug. 4, 2009), the insured, WMS, was manufacturer of electronic slot machines. WMS operated a sales and distribution facility called Premises 24 in Gulfport, Mississippi, which sold, serviced, leased, and installed slot machines to WMS’s Mississippi and Louisiana casino customers. Hurricane Katrina caused damage to dependent casino customers, and WMS filed a claim under the BI and CBI portions of its policy. The CBI portion of the policy provided coverage for “dependent business premises,” which was undefined by the policy. *Id.* at n. 3.

In an attempt to argue that the BI provisions applied to the loss rather than the CBI coverage (which had higher limits), WMS argued that the casinos were not dependent business premises but, instead, were “online access providers,” and therefore, the dependent business premises coverage did not apply. *Id.* at n. 8. WMS withdrew this argument at the end of trial, however, and agreed that the dependent business premises coverage applied to the damaged casinos. *Id.* The court held that the casinos were dependent business premises by definition. *Id.* at *20.

Outside the context of disasters, the case of *CII Carbon, LLC v. National Union Fire Insurance Co. of Louisiana, Inc.*, 918 So. 2d 1060 (La. Ct. App. 2005), provides an example of one court’s interpretation of the recipient locations provision. In that case, the insured owned and operated an industrial facility that processed coke by heat-treating petroleum coke for use in the aluminum smelting industry. It sold the heat-treated coke to customers. It also sold the steam generated in that process to customers who used it to generate electricity, including to the Kaiser Bayer plant. An explosion occurred at the Kaiser Bayer plant in 1999, and the insured was unable to sell its steam to the customer until the plant resumed full operations in 2000. According to the court, this loss was “exactly the type of loss that contingent business interruption insurance is designed to cover,” and it upheld the trial court’s finding that CBI coverage applied to the loss when the Bayer plant could not accept steam from the insured. *Id.* at 1067-68.

In the hypothetical case of Fully Covered, a flood or other covered cause of property damage to the shopping malls where Fully Covered sells its goods would likely be considered a recipient property pursuant to *CII Carbon, LLC*. Depending on the definition of recipient property, there

may be an argument that if the policy defines a recipient location as “locations that receive ‘your’ products [property damage to customers is recipient property],” a post office or warehouse that is involved in the process of shipping arguably receives Fully Covered’s products, and could be considered a recipient location. Similarly, if recipient property is defined as “premises operated by others on whom you depend to accept your products or services,” the warehouse or post office could be considered a recipient property. Such definitions do not clearly define the parameters of what and what is not a recipient location, because nearly any location that the insured’s product travels through (e.g. a warehouse, semi-truck, or post office) may be considered a recipient property.

C. Conclusions

Interpretation of contingent business provisions largely depend on the language of the policy at issue. Whether a particular claim is covered often turns on whether the insurance contract requires privity with a supplier, manufacturer, or customer. Where the policy is silent, some courts have held that no privity is required. See, e.g., *Archer-Daniels-Midland Co.*, 936 F. Supp. 534, *supra*. On the other hand, CBI provisions that reference a “direct” supplier or customer of the insured have interpreted more restrictively. Some courts have read in the requirement that the “direct” language calls for privity of contract before coverage is triggered. See, e.g., *Millennium Inorganic Chems. Ltd.*, 744 F.3d 279, *supra*. Given that very few courts have interpreted CBI provisions in the context of disaster, the potential to argue for expansive coverage, especially where a policy is silent or vague in its definition of dependent location or property seem nearly limitless.

In the hypothetical case of Fully Covered, whether a court would consider the cotton and dye suppliers as contributing locations would depend on the language of the policy. Under the rationale of the *Archer-Daniels-Midland* case, the suppliers’ properties would likely be considered contributing locations, and potentially, farmers that supply dye or cotton to those suppliers. The farmers would not be considered Fully Covered’s suppliers under the reasoning used by the *Millennium Inorganic Chems.* or *Pentair, Inc.* courts, because the farmers do not directly supply Fully Covered. Further, a court likely would not consider the farmers to be Fully Covered’s suppliers based on the policy language discussed above – “these are ‘your’ suppliers’ locations or locations of suppliers that deliver services or materials to others for ‘your’ account” – because the farmers are not necessarily delivering materials to service Fully Covered’s account, exclusively.

V The Evolving Nature of Business Interruption Insurance

Over the last twenty years, loss scenarios have proven standard business interruption coverage to be inadequate and out-of-step with the needs of modern business.

A The Limitation Imposed by the Physical Damage Requirement

The physical damage requirement means that standard business interruption coverage does not apply to a growing number of scenarios, such as where a business has been interrupted by a loss of computer systems, utilities (electricity, internet or gas), strikes, industrial action or infectious disease outbreaks. (See Denise Johnson, *The Changing Landscape of Business Interruption Claims*, Claims J. (June 3, 2015)).

Further, a lack of physical damage also means that business loss caused by an evacuation order issued by government preventing access to insured property would not be covered. To fill that gap, “Interruption by civil or military authority” coverage is available by endorsement, to cover that type of business loss on a strict time limited and geographical basis. Under most forms extending this protection, coverage is triggered when access to the premises is prohibited by an order of civil authority that was issued as a direct result of a covered cause of loss. This type of coverage is sometimes included with an “ingress/egress” endorsement, that extends coverage to a loss of business income caused by a covered cause of loss that blocks access to the insured property but does not damage it.

Finally, a lack of physical damage means that a loss of business income caused by a loss of a key individual for a project or event is not covered under standard business interruption coverage. This is the case even if the key individual is killed or injured by a covered cause of loss. To deal with the financial impact of such a loss, the business must purchase ‘key man’ life insurance and ‘key man’ disability coverage.

The loss of key personnel is a particularly common cause of business income loss in the entertainment sector which sees significant losses -- a whopping 72 percent of business interruption claims by value in the entertainment sector -- due to business interruption caused by the loss of a cast member. The impact of cast loss was highlighted in November 2016, when the producers of Broadway musical “Shuffle Along” sued their insurer for \$12 million, claiming that they should be able to get coverage for business interruption loss after the musical’s star, Audra McDonald, announced she was pregnant and unable to perform. The insurers denied the claim on the ground that the loss wasn’t caused by an “accident” or “illness” as defined in the policy. (*See* Kat Sieniuc, *Broadway Show Seeks \$12M Coverage For Star Dropping Out*, LAW360 (Nov. 4, 2016)). Although that case has yet to be resolved, it highlights the costly impact of cast loss. According to an entertainment claims specialist, some productions can have a \$200 million budget with daily operating costs running between \$400,000 and \$500,000. *See* RISK REPORT, *supra*. In other words, any interruption on the production set is costly. Specialized endorsements have been developed to apply to ‘cast loss’ scenarios.

B The Limitation Imposed by the Damage to Insured Premises Requirement

Another increasingly common scenario is where an insured has suffered a loss of business income because of an event that did not cause damage at the insured’s place of business and does not qualify for contingent business interruption coverage. To meet that type of coverage gap, brokers and underwriters have developed various forms of business interruption coverage to address the off-premises risk which have reduced, but not eliminated the exposure that business faces from loss caused by damage occurring away from its premises.

“Off premises power coverage” which applies to loss of business income due to the lack of incoming electricity caused by a covered cause of loss is widely available as an endorsement to commercial property policies. These endorsements are sometimes extended to include coverage for business losses caused by a loss of other utilities such as water, gas and sewer.

A further variation of this endorsement, which is sometimes endorsed on to the property coverage or forms part of a cyber security policy, warrants its own discussion and applies to losses caused

by a loss of computer systems, telephones and internet connectivity due to an event away from the insured premises, or on the insured premises.

Business interruption exposures are becoming more significant in the cyber world, with a number of recent incidents impacting sectors such as telecoms, manufacturing, transport, media and logistics. For example, in April of 2015, hackers took a French broadcast off air, affecting eleven TV stations, social media, websites and e-mail. Two months later, in June 2015, hackers struck again, this time grounding ten planes belonging to a Polish airline after the attack blocked ground control from sending flight plans to the planes. (*See Risk Report, supra*, at 33). In addition to safety and logistical concerns, these types of events can result in significant lost revenues and business interruptions.

Not all cyber-related business interruption loss is caused by hackers; business interruption can also be caused by technical failure or human error. For example, in July 2015, trading of all securities on the New York Stock Exchange was suspended for over three hours caused by an internal technical glitch. In that same week, United Airlines was forced to ground its fleet of airlines due to what it called a “network connectivity issue.” The two-plus hour outage affected approximately 4,900 flights.

It is seldom the case that this cyber risk is covered under standard business interruption coverage as the loss is not due to physical damage and therefore is outside the realm of standard business interruption coverage. Further, in most cases, the loss occurs away from the insured premises.

To meet this coverage gap, a “network business interruption” endorsement has been created. This endorsement covers income loss and expenses incurred during the period of interruption following a computer system failure or breach of network security. This extension can also cover business interruption caused by the outage of a service provider, when caused by a computer failure or network security. (Guy Carpenter, Marsh & McLennan Co., *Ahead of the Curve: Understanding Emerging Risks*, unpublished paper (Sept. 2014)). These endorsements are necessary to deal with an increasingly expensive part of a loss of computer systems and connectivity.

In certain circumstances, it is possible to insure against contingent business interruption in the cyber context, such as insuring against the failure of IT or operational technology belonging to a third party. However, insurance companies generally only offer limited coverage for contingent business interruption due to cyber exposure. (*See Risk Report*).

C Broker Liability in the Business Interruption Context

The frequency and severity of business income loss has generated a secondary source of coverage for business interruption losses: Broker’s errors and omissions policies.

One of the biggest sources of coverage gaps with business interruption insurance is insufficient limits caused by undervaluing the amount of insurance required. The broker may be at risk to respond to loss in excess of limits to the extent that the broker advised the insured as to the limits and deductible that they ought to purchase and such coverage would have been available had it been requested and the insured would have opted for the higher limits. According to one survey, 40 percent of declarations were deemed too low by about 45 percent. *See Johnson, The Changing Landscape of Business Interruption Claims, supra*. This discrepancy is particularly evident in the

cyber insurance world, where businesses acknowledge that the threat to cyber security is one of the biggest risks necessary to insure, yet they are consistently under insured for this risk. *See CYBER RISK REPORT, supra.*

Another issue spawning lawsuits against brokers is their alleged failure to properly analyze the insured's supply chains in order to prepare for business interruption at the insured facility in the event a supplier's business is damaged or otherwise 'off-line'. *See, e.g., Johnson, The Changing Landscape of Business Interruption Claims, supra.* Again, there must be evidence that coverage was available at the time the inadequate policy was placed that would have extended to the loss that the insured in fact sustained and would have been purchased by the insured had it been offered.

Trends such as the increase in interdependency, climate change, technology, and geo-political risk, are all growing concerns for businesses. Despite the many uncertainties in the future of this area of insurance, one thing is certain: Business interruption loss, that is increasing in frequency and severity, will be met with an ongoing array of forms created by brokers and underwriters to deal with emerging coverage gaps which reality will test over time.

VI Conclusion

The increasing incidence of severe weather-related disaster as well as accidents, explosions and fires will continue to test the business interruption coverage that businesses of all stripes must have in place in today's marketplace. The variety and severity of these claims as well as the unique issues that apply when the loss occurs in the context of a regional disaster means that legal practitioners in the area will no longer complain that business interruption coverage is dull when the insured's address changes to the Boulevard of Broken Dreams.



Lighting the way to...

Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10



FRIDAY, MARCH 10, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

TOXIC TORTS AND ENVIRONMENTAL LAW

A Tsunami of Rising Water Litigation

Cyprus

Speakers:

William K. Koska

James E. Smith

Gary E. Hokkanen

A Tsunami of Rising Water Litigation

Speakers: William K. Koska, James Smith, Gary E. Hokkanen

**2017 FDCC Winter Meeting
Charleston, South Carolina
March 6-10, 2017**

Water Litigation

- Too Little Water
- Too Much Water
- Contaminated Water

Too Little Water



Too Little Water



Too Much Water



Contaminated Water





Daubert v. Merrell Dow Pharmaceuticals, Inc. 509 U.S. 579 (1993)

Correct Pronunciation “Dow-Burt”

Hartwell v Superior Ct, (2002) 27 Ca. 4th, 256 and In re Groundwater Cases, (2007) 154 Cal App 4th 659.

Safe Harbor

- Following the Brockovich case, which my former firm defended, the same attorneys sued several water purveyors in CA whose adjudicated/designated pumping area included Superfund sites. The polluters were not sued initially, as plaintiff's attorneys wanted the water purveyors to sue the polluters on cross-complaints and spend a fortune proving the polluters liability. The legal theory was that the EPA standards for the water pumped from these sites were inadequate. After 10 years of litigation and 3 published decisions including the latter two, the court in 2007's decision, found a safe harbor for companies that comply with all federal and state clean water regulations.
- Ohio, Arizona and possibly North Carolina have passed “ **Safe Harbor** ” **legislation**. Cases where Federal and State EPA standards are challenged have become very rare because the body of scientific knowledge against liability theories is substantial.

Emerging Contaminants

- MTBE
- 1,4- Dioxane
- PFCs
 - Perflourinated Chemicals
- PPCPs
 - Pharmaceuticals and Personal Care Products





BEWARE

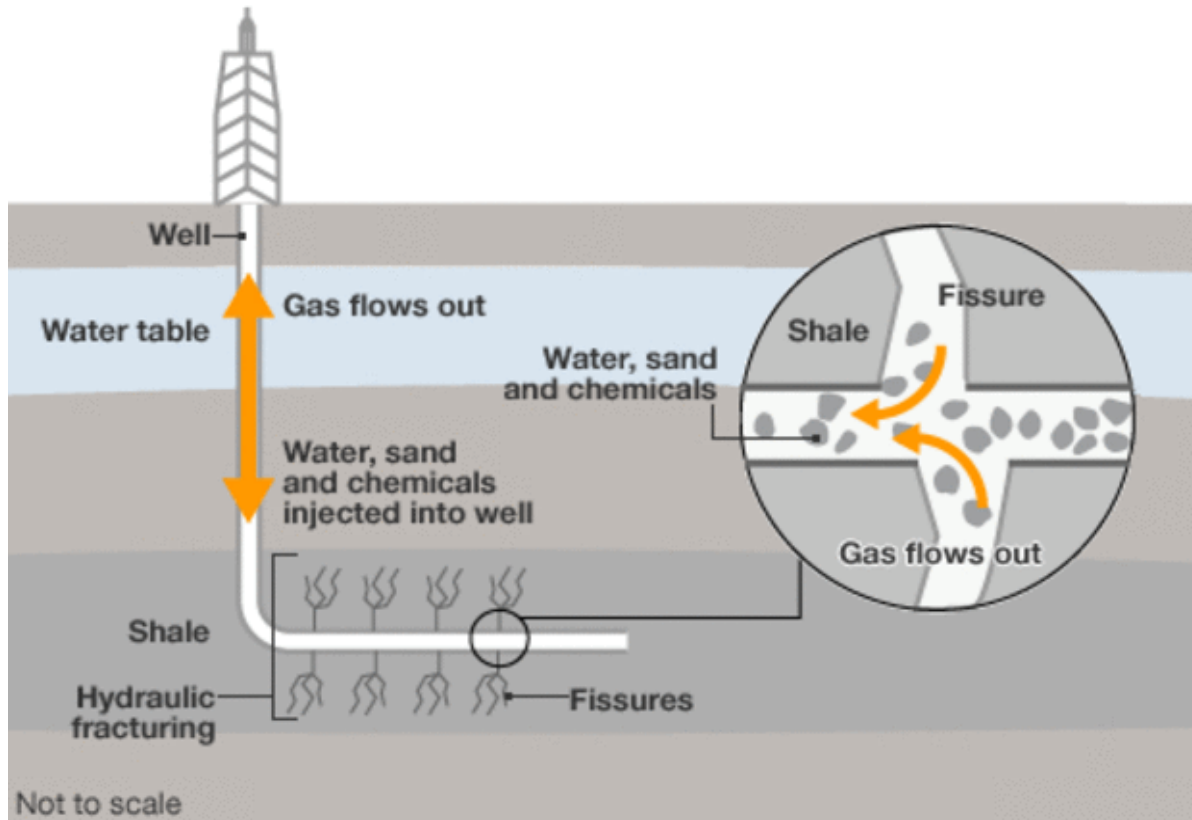
- When you are the only good defendant
- When your counter parties ignore your advice
- Of informal government “approvals”

HYDRAULIC FRACTURING OR “FRACKING”

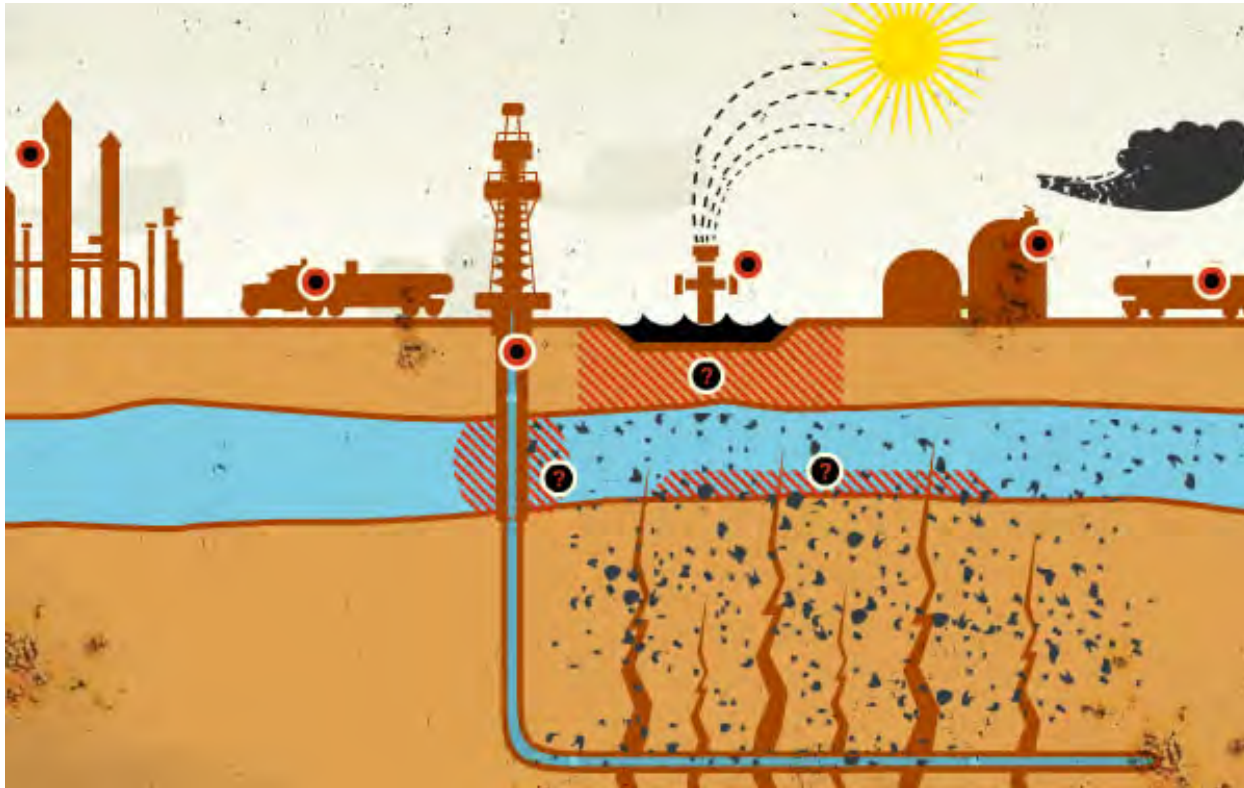
Fracking, or hydraulic fracturing is a process in which rock is fractured by a pressurized liquid. Fracking fluid is injected under high pressure into a wellbore to create cracks in deep rock formations that contain natural gas and petroleum. The fracturing allows the natural gas and petroleum to flow more freely into the borehole.

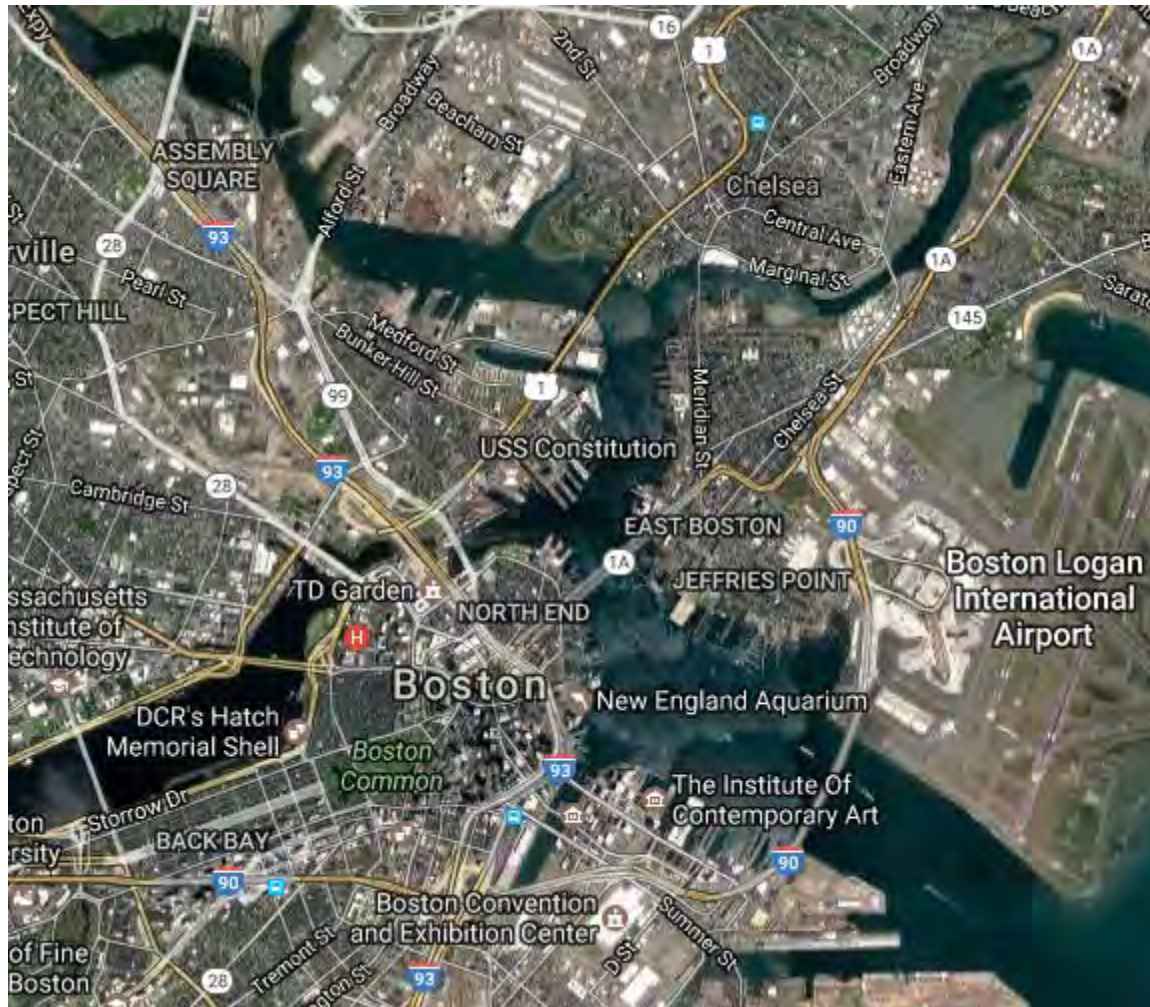
Hydraulic Fracturing

Shale gas extraction



Hydraulic Fracturing





Climate Change

- Eight children in Seattle, WA, November 2016, asked a judge to find WA in contempt for failing to adequately protect them and future generations from the harmful effects of climate change. Petitioners requested that the State Dept. of Ecology come up with “ science-based “ numeric emissions reductions. Though the appeal was denied because WA was already working on meeting its obligations by writing new rules for greenhouse gas emission, the court agreed with the premise that WA had an obligation to protect/hold natural resources in trust for future generations.
- In December 2016, a federal court in Eugene, Ore. allowed a similar case against the Obama administration to proceed, premised on the the theory that the government has violated its obligation to hold certain natural resources in trust for future generations.
- Both cases are a part of the nationwide effort led by the Oregon-based non-profit “ Our Children’s Trust “.

California's solution to its water crisis: GROUNDWATER MANAGEMENT ACT OF 2014

CA has 515 basins of which 127 supply roughly 90 % of all groundwater (GW) produced. CA has divided basins into high, medium, low and very low priority in terms of management necessity. Act requires that all the basins rated as high or medium (127) have a management agency in place by July 1, 2017 and a sustainability plan in place by January 31, 2022.

A “few” of the problems in the Act

- Public utilities and mutual water companies provide water to over 6.8 million people. However, since both types of companies are organized as private corporations, neither type can serve as a part of/or a sustainability agency. So millions of water users are excluded from the process.
- A portion of the Act allows agencies to adopt GW extraction allocations, limiting GW production, but does NOT spell out any basis for establishing the allocation.
- The Act states several times that it does not impact existing GW rights, but this claim is impossible to square with the powers granted in other portions of the Act.

Speaker Bio:

William K. Koska, Of Counsel Fredrickson, Mazeika & Grant, LLP



For over three decades, Bill has repeatedly produced favorable results in contentious trial work and litigation. He has prosecuted landmark condemnation litigation against state agencies for their failure to properly supervise and implement an effective cleanup plan at a CERCLA site, and prosecuted the contaminator of the site without becoming involved in the then-pending CERCLA litigation. In this action, Bill's clients obtained settlements valued at 100 Million Dollars.

Email: wkoska@fmglegal.com
wkoska@koskalaw.com

Speaker Bio:

James Smith, Senior Counsel **Schirrmeister, Diaz-Arrastia, Brem, LLP**



Jim's first chair environmental experience includes civil and criminal jury trials, arbitrations, administrative hearings, and support of complex transactions. He has argued precedent setting environmental cases before the Supreme Court of Texas and the U. S. Court of Appeals for the Fifth Circuit. His first chair trial experience also includes intellectual property, construction, breach of fiduciary duty, and engineering design cases.

Email: jsmith@sdablaw.com

Speaker Bio:

Gary E. Hokkanen, Principal Hydrogeologist Farallon Consulting



Gary has more than 36 years of experience in the investigation and remediation of contaminated property, with a focus on soil and groundwater contamination. He has extensive experience in litigation support as a technical expert in Allocation, Remedial Investigation/Feasibility Studies (RI/FS), National Contingency Plan compliance, and contaminant source identification. Gary manages Farallon's California offices.

Email: ghokkanen@farallonconsulting.com

Water litigation years ago meant some occasional cases about water that was contaminated by some chemical or foreign object that caused human beings to be injured in some fashion. It has evolved into far more than object/material contamination issues. As we are seeing across the country, water is a very valuable commodity and the legal battles are escalating at all levels of human activity.

This presentation by both lawyers and a hydrogeologist paints a picture of the current types of litigation involving water and many of the additional issues that surround its usage, cost, scarcity and potential for harm. The legal issues for anyone practicing in this area of the law are plentiful and can be deceptive. We hope this paper assists and alerts the watchful attorney.

- **Central Valley (California) groundwater over-withdrawal**
 - Groundwater has been used in the Central Valley for decades. As groundwater is withdrawn through wells, the land consolidates and sinks, generally termed subsidence. Figures one and two on the attached exhibit list graphically illustrate the effects of subsidence. The process is **irreversible**.
 - California's "solution" to this problem and the larger problem of a continuing 5 year drought was to pass the "Sustainable Groundwater Management Act in 2014. More on that "solution" later in this presentation.
- **General principles of water litigation and damages**
 - **Proof**
 - For damage that can be repaired or remediated, claimants can recover the remediation costs plus any lost rental value prior to completion of the remediation.
 - For damage that cannot be repaired, or if the repair costs significantly exceed the property value, the lost market value due to the injury.
 - In some instances, the most economical approach may be a mix of remediation and compensation for residual lost market value, if the remediation removes some but not all of the contamination.
 - **Stigma**
 - Stigma is a residual loss in market value based on perception, which lingers even after the property is remediated or contamination has subsided.
 - Some courts reject any stigma recovery absent ongoing permanent physical injury. *Bradley v. Armstrong Rubber Co.*, 130 F.3d 168, 176 (5th Cir.1997).
 - Some courts have allowed for stigma recovery despite the physical injury being only temporary. *Walker Drug Co., Inc. v. La Sal Oil Co.*, 972 P.2d 1238, 1246 (Utah 1998).
 - Texas Supreme Court has stated that it has not decided if stigma damages are recoverable, but that before it will decide, it must see evidence of properties showing diminution of value that cannot be attributed to ongoing contamination. That is, unless and until claimants can present legally admissible proof that the market has devalued properties even after the physical injury has

been removed, the Court will not decide if it will recognize stigma damages. *Houston Unlimited, Inc. Metal Processing v. Mel Acres Ranch*, 443 S.W. 3d 820, 827 (Tex. 2014)

- West Virginia Supreme Court of Appeals has stated that in an extraordinary situation, residential homeowners can recover:
 - Repair costs, even if greater than market value, but not it unreasonably greater; and
 - Lost market value even after full repair.
 - *Brooks v. City of Huntington*, 234 W. Va. 607, 768 S.E.2d 97 (2014): case involved negligence by the City that caused homes to encounter flooding and to enter the 100 year flood plain. Court upheld repair cost to raise homes above the flood plain, and remanded for determination of the extent, if any, of ongoing market value even after completion of the repairs.

- **Water contamination and personal injury**

- **Proof**

- General causation and specific causation
 - In exposure cases, courts generally require two steps to establish causation. First, plaintiffs must establish general causation, by showing that the type of exposures that the plaintiff encountered could result in the disease contracted by the plaintiff. Second, plaintiffs must establish specific causation, by showing that the disease suffered by the plaintiff was indeed caused by the particular exposure, as opposed to other potential causes.
 - **Practice Note: A rigorous exposure assessment should be part of the “general causation” analysis. (“In terms of general causation, accurate exposure assessment is important...” Reference Manual on Scientific Evidence [3rd Ed.] Page 657, footnote 67.) Merely submitting information to support that some exposures to the constituents at issue can cause the claimant’s injury does not establish general causation. Rather, the actual exposures of the claimant must be demonstrated and must be adequate to cause the claimed injury, in order to establish general causation.**
 - Even if general causation is established, plaintiff must reasonably negate alternative possible causes in order to show specific causation.
 - **Medical monitoring-substantial differences throughout individual states.**
 - Available without proof of some physical injury; or
 - Available, but only with proof of physical injury; or
 - Generally unavailable for future injuries.

- **Proof of disease/personal injury from water contamination** can be difficult depending on the chemical/s involved, and the length and degree of exposure.
- **Hartwell v Superior Ct.; cases in LA, and Sacramento, CA.**
 - Following the Brockovich case, the same attorneys sued several water purveyors in CA, whose adjudicated/designated pumping area included Super Fund sites. The polluters were not sued, as plaintiffs' attorneys wanted the water purveyors to sue the polluters on cross-complaints and spend a fortune proving the polluters liability. The legal "idea" was that the EPA standards for the water pumped from these sites were inadequate. One CA Appellate court decision and one Supreme Court opinion later in *Hartwell v Superior Court*, (2002) 27 Cal 4th, 256, and a second later Court of Appeal decision, *In re Groundwater Cases*, (2007) 154 Cal App. 4th 659, established the law in California: as long as drinking water provided by the purveyors meets all state and federal safe drinking water standards, the water purveyors are/were, for all intent and purposes, immune from liability.
 - Ohio, Arizona and possibly North Carolina have passed "Safe Harbor" legislation. It is a fairly simple process in most states. Cases where Federal and State EPA standards are challenged have become very rare because the body of scientific knowledge against liability theories is substantial.
- **Safe Harbor issues**
 - Will meeting regulatory standards protect companies from tort claims? Generally yes.
 - Can state and federal legislatures pass laws to give safe harbors for companies that meet regulatory standards? Yes.
 - **Practice note: If your clients are water utilities, public or private, alert them to the "safe harbor" theory, and make sure the clients' record keeping is precise, especially concerning violations.**
 - **Practice note: If your client is faced with potential litigation, it may be cheaper to pay lobbyists to pass safe harbor legislation than to fight legal battles for decades.**
- **Emerging Contaminants**
 - Newly recognized contaminants have been the source of new litigation for decades. The discovery of MTBE in gasoline which created groundwater contamination led to numerous cases across the country. The latest contaminant De Jour is a group of compounds known as Perfluorinated chemicals (PFSs). The two most well-known are PFOA and PFOS.
 - These chemicals are used in waterproof/stainproof fabrics and carpets, non-stick cookware, leak-proof coating on packaging materials and on a type of fire-fighting foam. The contamination from PFC's can be found at manufacturing facilities, commercial and military airports, fire-fighting training facilities, oil refineries, landfills and agricultural

sites receiving bio-solids and wastewater. Testing for these chemicals is increasing and litigation will follow.

- **Key issues from Flint, Michigan experience**

- Engineering/Environmental Firms named in class actions (seeking recovery for bodily injuries and property damages) and in suit filed by Michigan Attorney General against LAN and Veolia entities. These paragraphs focus on the claims against LAN.
- Prior to Flint controversy, even many water supply experts may not have appreciated the extent to which older water systems can be susceptible to leaching lead into drinking water, due to old lead pipes contacting water with elevated chlorides due to runoff from salt used on roads.
- In the summer of 2011, when Flint was considering the change to river water, LAN recommended that the system have full water softening and corrosion control. City chose to have only partial water softening, because the Michigan Department of Environmental Quality (MDEQ) said that was all that was necessary.
- In the summer of 2013, the City hired LAN to design certain components of the Flint Water Treatment Plant (FWTP), in order for Flint to use river water. The City did not hire LAN to advise the City on water quality or operation of the FWTP. LAN provided engineering drawings as requested by the City.
- In the summer of 2013, LAN recommended that the city operate its water system on a test run basis for 60-90 days prior to full operation. The City did **not** follow this recommendation. In April 2014, the City switched to river water.
- State of Michigan, in its suit against LAN, says that LAN was negligent in providing the engineering services and drawings, because LAN knew or should have known that the FWTP was not safe. The State claims it was professional negligence for LAN to have engineered the components of a system that was unsafe, even when system safety does not appear to have been within the scope of LAN's contract.
- At the time, the City was in receivership. LAN should have realized that it was a private party and the other actors were a city in receivership and a state agency, so that LAN would be the target of any litigation.
- While LAN recommended a more robust corrosion and water softening approach, LAN apparently did not put in writing to the City that the failure to do so could result in high levels of lead in Flint's drinking water, or that the failure could increase the risk of Legionnaire's disease
- In October 2014, the City hired LAN to study the issue of trihalomethane formation in the city's water. LAN provided a report based on the limited scope of trihalomethane formation. The state's suit and the private suit against LAN allege that LAN made recommendations for reducing the potential for trihalomethane formation, but did not look for or find indications of high lead in the city's water. Further, the suits allege that one of LAN's recommendations, to add ferric chloride to reduce trihalomethane formation, may have increased corrosion and made the lead problem worse.

Apparently, LAN's recommendations on trihalomethanes did not include a statement that LAN had not considered general corrosion issues; that the City had chosen not to install a full water softening and corrosion program, and that the issue of potential lead in the water due to corrosion had not been resolved. It is possible that LAN thought that between the City and MDEQ, adequate testing for lead had been done, and had shown no problem.

- **Practice notes:**

- **Especially when costly third party claims are possible, private parties must remember that they are the first, and often last, targets for claims.**
- **If a counter party refuses to follow your entity's recommendations or practices on a safety issue, reconsider your ongoing work with that entity, especially if that entity is in financial distress or otherwise unable to make good on potential claims;**
- **Informal "approvals" or directives by governmental agencies provide no safe harbor. MDEQ now admits that it was wrong not to require that Flint follow LAN's advice on corrosion control and water softening, but the State sued LAN, anyway. (Another example: a fire marshal's inspection that results in no citation does not guarantee fire code compliance, nor preclude a claim based on failure to comply with the fire code.)**

- **Hydraulic Fracturing-clear definition with pictures**

- Fracking, or hydraulic fracturing is a process in which rock is fractured by a pressurized liquid. Fracking fluid is injected under high pressure into a wellbore to create cracks in deep rock formation that contain natural gas and petroleum. The fracturing allows the natural gas and petroleum to flow more freely into the borehole.
- Why Hydraulic fracturing is not a threat to water supplies generally: the primary water concern is the loss of fracking fluid into groundwater, either from losses at the surface, breaks in the casing, and upward movement from the deep rock formations. Although much controversy is associated with fracking, the actual incidences of groundwater contamination and litigation has been less than expected, to date.
- See *Fiorentino v Cabot Oil & Gas Corp*, 750 F. Supp. 2nd, 506 (2010) and
- *Antero Resources Corp. v. Strudley*, 347 P.2d 149 (Colo. 2015), which held that Colorado procedural rules do not allow for *Lone Pine* orders, and remanded to the trial court for further proceedings in this case alleging injuries from hydraulic fracturing. See figures three and four on the attached exhibit list.

- **Regulatory actions including the use of programs to discourage oil and gas development**

- Monterey County California voters passed measure Z, characterized as an anti-fracking measure.
- Measure Z bans hydraulic fracturing, even though that technique is not really used in this county. The measure bans certain well stimulation activity, bans new wells, and places restrictions on re-injection of wastewater.

- Denton, Texas passed a ban on hydraulic fracturing, only to see the Texas legislature enact a statute prohibiting such bans.

- **Climate Change**

- Eight children in Seattle, WA in November 2016, asked a judge to find the state in contempt for failing to adequately protect them and future generations from the harmful effects of climate change. The petitioners requested that the State Department of Ecology come up with science-based numeric emissions reductions. Though the judge denied the appeal because the State was already working on meeting their obligation by writing new rules for greenhouse gas emission, the court agreed with the case's premise that the state had an obligation to protect/hold natural resources in trust for future generations.
- In December 2016, a federal judge in Eugene, Ore., allowed a similar case against the Obama administration to proceed, premised on the theory that the government has violated its obligation to hold certain natural resources in trust for future generations.
- Both cases are a part of the nationwide effort led by the Oregon-based nonprofit "Our Children's Trust."
- **Practice note to attorneys who represent public entities/agencies: you can expect to hear the "hold natural resources in trust" argument used repeatedly. Public entities/ private companies that have any use of water or land, and/or that manufacture hard goods, need to be prepared to make sure they are in compliance with state and federal regulations on climate change, whether the regulations concern air, water or land. The real argument that environmentalists will use is whether the state has fulfilled its constitutional/statutory duties to protect the public from hazards of climate change.**
- **Practice note: Will shareholders/stakeholders claim that those with asset management responsibility failed to increase asset protection that was necessary due to climate change, and therefore file litigation against the officers/directors of public and private organizations.**
- **Oil company litigation in Mass.:**
 - **Conservation Law Foundation v ExxonMobil Corporation, Case No. 1:16-cv-11950-MLW**; suit seeks civil penalties, injunctive relief and attorneys' fees based on the citizen suit provisions of the Clean Water Act and the Resource Conservation and Recovery Act. Among the claims, CLF alleges that ExxonMobil must update its Storm Water Pollution Prevention Plan (SWPPP) for its petroleum storage terminal in Everett, Massachusetts, to reflect increased potential for pollution incidents due to climate change related risks, such as sea level rise and greater storm severity. ExxonMobil has filed a motion to dismiss for failure to state a claim and lack of standing; CLF filed a response on December 20, 2016.
 - Lawyers for CLF include Kanner & Whiteley, LLC in New Orleans, which has represented the State of Louisiana against BP in the Deepwater Horizon Litigation
 - Ruling could affect SWPPP requirements for thousands of facilities

- **Water Rights litigation:**

- Maryland and West Virginia have had long-running disputes over water rights to the Potomac River. The latest dispute was on November 2, 2016 when West Virginia told Maryland that Maryland had no authority to issue permits or deny access to West Virginia to withdraw water from the Potomac River. Maryland officials wrote to West Virginia officials telling them that their state has no management program for withdrawals from the river and the state has not taken an active role in the management of the river. (Sounds like some of the issues in California) Maryland backed down and agreed to cease reviewing and issuing water appropriation and use permits for West Virginia users on the Potomac.

- **Water Rights litigation: California's Sustainable Groundwater Management Act of 2014.**

- California has been in a drought since 2011. The states' water law is a hybrid of riparian rights and prior appropriation doctrine. Because of the drought's effects, surface water supplies and surface storage reservoirs were unable to meet the needs of users. Much more groundwater began to be pumped from groundwater wells. Groundwater levels were already declining in many parts of the state and had been for some time. Most groundwater rights tend to be owned and used by individuals, unlike surface water rights.
- The Act establishes "Groundwater Sustainability Agencies." The state has tabulated that there are 515 basins in the state, but only 127 basins supply the source for roughly 90 % of all groundwater produced. The state has further divided the basins into high, medium, low or very low priority in terms of management necessity. Some 15 agencies statewide have already been designated as sustainability agencies because of the role they presently play within their boundaries. The plan for critical basins must be in place by July 1, 2017, or the state may adopt a probationary plan of their choosing.
- Public utilities and mutual water companies provide water service to 5.5 million and 1.3 million respectively in California. Public utilities are governed by the California Public Utilities Commission and their rights are circumscribed by that agency. However, because both types of companies are organized as private corporations, neither can be eligible to serve as a sustainability agency. Some 6.8 million Californians are not going to be part of the sustainability process.
- At least one section of the Act allows the agencies to adopt groundwater extraction allocations, and to limit the production of groundwater. However, the Act does NOT spell out any basis for establishing the allocation.
- Though the Act states in several provisions that it does not impact existing groundwater rights, this is just impossible to "square" with the powers granted in other language found in the Act.
- There are plenty of places where the Act can be challenged, from due process issues at the very beginning in terms of how a "sustainability agency" is established, to due process challenging the actions of the agency once established, on both due process

grounds as well as inverse condemnation issues, and a whole panoply of other ideas in between. See *City of Barstow v. Mojave Water Agency*, 23 Cal. 4th 1224 (2000).

- There is nothing in the Act which even mentions climate change as a part of the evaluation criteria to be applied to sustainability plans. This is particularly ironic because of California's boasting by its politicians as being "the leading edge" or "first" in climate change legislation. Challenges to the Act on that basis are also likely.

EXHIBITS



EXHIBIT 1



EXHIBIT 2

Shale gas extraction

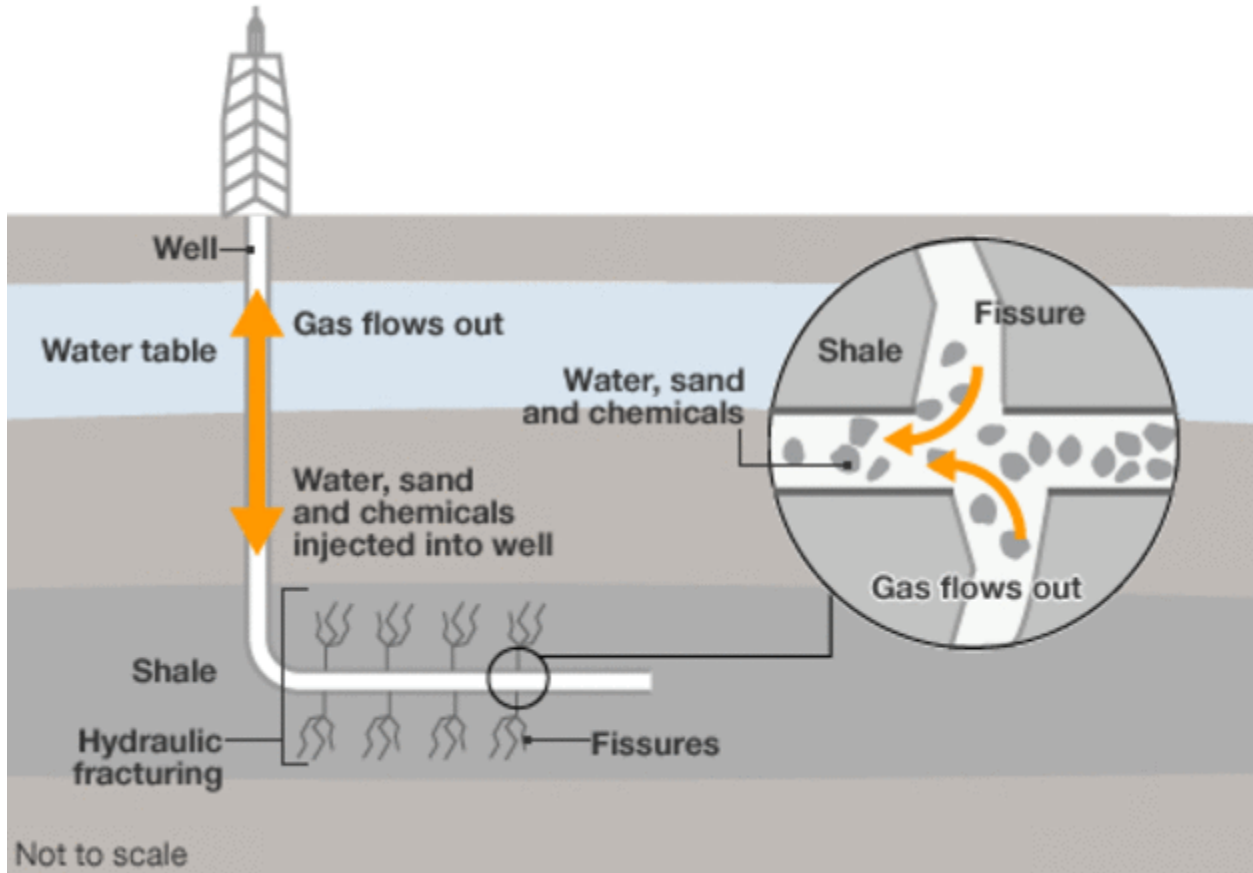


EXHIBIT 3

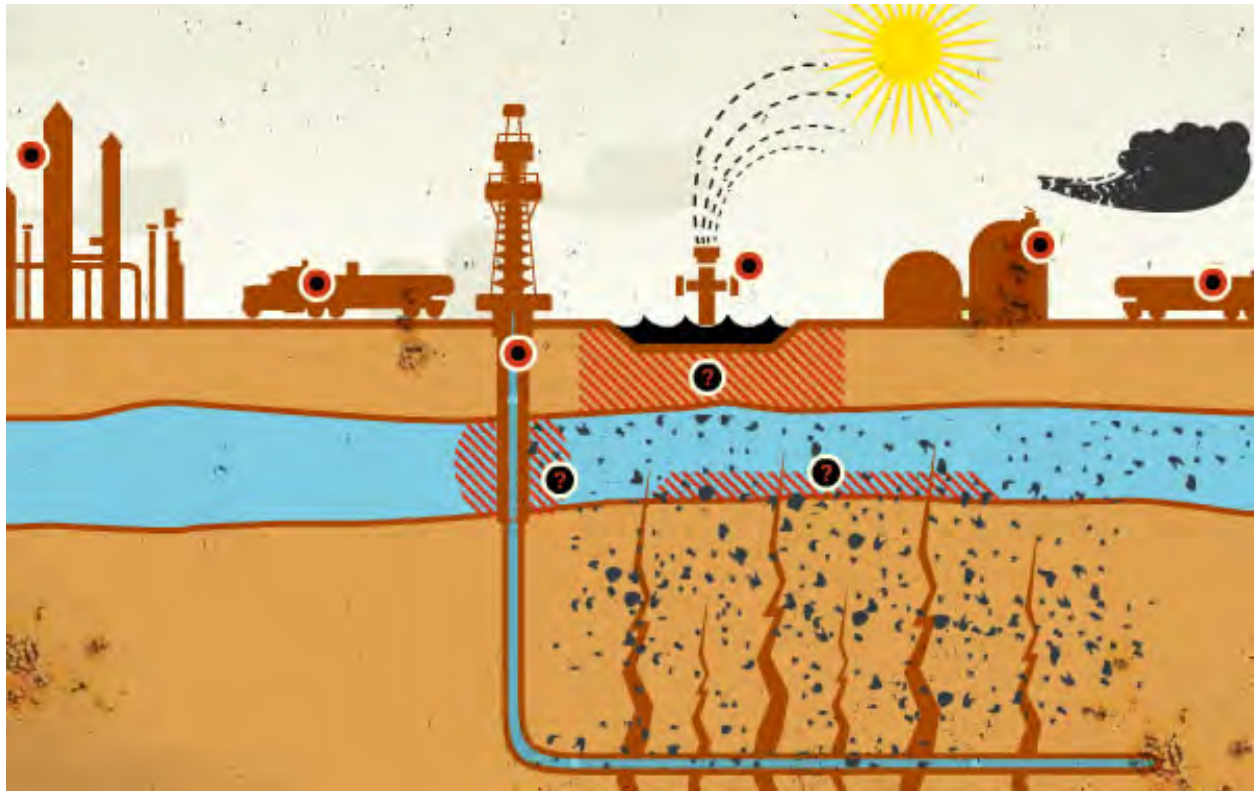


EXHIBIT 4



Lighting the way to...

Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10



FRIDAY, MARCH 10, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

APPELLATE LAW

Legal Writing in the Electronic Age

Drayton

Moderator:

Charles T. Frazier

Speakers:

Michael F. Aylward

Robert A. Olson

The Honorable Justice John C. Few;
South Carolina Supreme Court

Legal Writing in the Electronic Age

**FDCC Winter Meeting
Charleston, South Carolina
March 6 - 10, 2017**

Paper author and moderator:

Charlie Frazier
*Alexander Dubose Jefferson & Townsend LLP
(Dallas, TX)*

Panel members:

Honorable John Cannon Few
*Justice, South Carolina Supreme Court
(Greenville, S.C.)*

Michael Aylward
*Morrison Mahoney
(Boston, MA)*

Bob Olson
*Greines, Martin, Stein & Richland LLP
(Los Angeles, CA)*

Table of Contents

Table of Contents	i
I. Introduction: the judiciary is going electronic	1
II. How screens have changed reading.....	2
A. Screen reading occurs in a different environment than paper reading.....	2
1. Our electronic devices create an environment of distraction.....	3
2. Readers expect information instantly.	3
3. Because screen reading is more challenging, readers tend to skim screen text.	4
4. Multiple Window screens fosters multitasking.	4
B. Studies reveal that screen readers read differently—and in some cases comprehend less—than print readers.....	5
1. The low “physicality” of screens makes navigating long texts more difficult.	5
2. Screen readers skim over text—they don’t read it.	6
3. Screen readers have lower attention spans and want information quickly.	8
III. Suggestions for structuring an effective and persuasive legal argument to the screen reader.....	9
A. Use visible structures.	9
B. Use summaries.	11
C. Use white space.....	12
D. “Chunk” complex information.	13
E. Write visually.	14
F. Simplify the presentation.....	16

G.	Utilize available electronic navigating tools.	18
1.	Bookmarks.	18
2.	Internal hyperlinking.	19
3.	External hyperlinking.	20
IV.	Conclusion	22

Charlie Frazier

Charlie Frazier is a partner in the Dallas office of the appellate law firm of Alexander Dubose Jefferson & Townsend, LLP, with offices also in Austin and Houston. Charlie has been board certified in civil appellate law by the Texas Board of Legal Specialization since 1994. For over 27 years, his appellate and litigation-support practice has covered many areas of civil law, including substantial experience in complex commercial and contractual disputes, insurance-coverage and bad-faith disputes, and professional-liability claims.

Charlie successfully argued before the Supreme Court of the United States on behalf of ten psychiatrists who were sued by a former patient under RICO, claiming that a pattern of racketeering activity existed to keep him under hospitalization. *Rotella v. Wood*, 528 U.S. 549 (2000). The Court rejected the patient's argument that accrual of a civil RICO claim is postponed until the pattern was or should have been discovered, thereby holding that the patient's claim was time-barred.

Charlie received his B.A., magna cum laude, from Baylor University and his J.D. from the Baylor School of Law, where he was published in the *Baylor Law Review*, on which he held various editorial positions. In between college and law school, Charlie received the M.A. in International Relations from the University of Kent, in Canterbury, England, on a Rotary International Scholarship. He has been listed since 2009 in *Best Lawyers in America* in Appellate Law. Charlie is a Vice Chair of the Appellate Section of the FDCC, and has participated on panel presentations at the 2015 and 2016 Winter Meetings. He currently holds, and has held, several leadership positions in the Appellate Advocacy Committee of the DRI.

Michael Aylward

Michael Aylward is a senior partner in the Boston office of Morrison Mahoney LLP where he chairs the firm's complex insurance claims resolution group. For nearly thirty years, Michael has represented insurers and reinsurers in coverage disputes around the country concerning the application of liability insurance policies to commercial claims involving intellectual property disputes, environmental and mass tort claims and construction defect litigation. He also consults frequently on bad faith and ethics disputes and has served as an arbitrator and testified as an expert in various matters involving coverage and reinsurance issues arising out of such claims.

In addition to his trial and appellate practice, Michael often testifies as an expert on insurance-related issues. He is also an AAA-certified neutral and has served as a party-appointed arbitrator in a number of large insurance disputes.

Michael is a prolific author and speaker on insurance coverage issues. He is a contributing author to several leading insurance treatises, including two chapters in the New Appleman Insurance Law Practice Guide (2008) and a chapter in the 2012 ABA treatise on environmental liability and insurance coverage disputes. He also publishes an e-newsletter that is sent each week to over a thousand claims professional and in-house counsel. For the past five years, he has also served as one of the contributing editors of the Insurance Law Forum, a leading insurance coverage blog.

Michael has chaired the FDCC Reinsurance, Excess and Surplus Lines Committee, and has held leadership positions in the DRI, International Association of Defense Counsel, and the Insurance Committee of the ABA Litigation Section.

Bob Olson

Bob Olson is a partner in Greines, Martin, Stein & Richland, LLP, in Los Angeles. Both he and his firm specialize in appellate proceedings in state and federal courts, including appeals, petitions for extraordinary writs, amicus briefs, and petitions for review and certiorari, as well as related law and motion in trial courts. The firm devotes its practice exclusively to appellate law and is one of the nation's leading appellate law firms.

In addition to being a member of the FDCC, Robert is a past president of the Association of Southern California Defense Counsel, a fellow of the American Academy of Appellate Lawyers, a past president of the California Academy of Appellate Lawyers, a member of the Claims Litigation Management Alliance. He is certified as an Appellate Law Specialist by the State Bar of California Board of Legal Specialization.

Robert has taught Appellate Advocacy as an adjunct professor at Loyola Law School. He has been repeatedly named to the "Best Lawyers in America" and Southern California "Superlawyers" lists. He obtained his law degree from Stanford University where he was elected to Order of the Coif. After receiving his law degree, he clerked for United States Court of Appeals for the Ninth Circuit Judge, now United States Supreme Court Justice, Anthony M. Kennedy.

The Honorable John Cannon Few

Justice John Cannon Few is a Justice of the South Carolina Supreme Court. He was elected on February 3, 2016, and sworn in on February 9, 2016. Born in Anderson, South Carolina, Justice Few grew up in Greenwood, South Carolina. After earning a Bachelor of Arts degree in English and Economics at Duke University, he earned his J.D. degree from the University of South Carolina School of Law, where he was a member of

The Order of Wig and Robe and The Order of the Coif, and served as Student Works Editor of the *South Carolina Law Review*. Justice Few is admitted to practice in South Carolina, the United States District Court for the District of South Carolina, the United States Court of Appeals for the Fourth Circuit, and the United States Supreme Court.

Justice Few began his legal career as law clerk to The Honorable G. Ross Anderson, Jr., United States District Judge. He practiced law in Greenville from 1989 to 2000, and then served as a judge on the Circuit Court of South Carolina for almost ten years. On February 3, 2010, he became Chief Judge of the South Carolina Court of Appeals, a position he held until February 2016, when he was elected to the South Carolina Supreme Court.

Justice Few is a frequent public speaker. In 1996, he gave a speech entitled "Citizen Participation in the Legal System," for which he was awarded first place in the ABA's nationwide Edward R. Finch Law Day speech contest. He has given numerous speeches to bar associations and civic groups throughout the country, and has delivered commencement addresses to the graduates of Lander University and the Charleston School of Law, where he delivered "What it Means to be a Lawyer." His most frequent speech is entitled "The Courage of a Lawyer," which he has delivered to legal associations in South Carolina, North Carolina, Georgia, Florida, Arizona, and California, and which was published in the 2013 Winter edition of the ABA's *Litigation* journal.

Justice Few has served on the faculty of the National Judicial College in Reno, Nevada, as Adjunct Professor of Law and later a Distinguished Visiting Professor at the Charleston School of Law, and most recently as Adjunct Professor of Law at the University of South Carolina School of Law. He has also given or moderated over 125 continuing legal education seminars in South Carolina and numerous other states.

Justice Few is a Fellow in Liberty Fellowship, and as a part of Liberty Fellowship is currently undergoing moderator training through The Aspen Institute. He completed the Diversity Leaders Initiative through The Riley Institute at Furman University in 2010. In December 2012, the Charleston School of Law awarded him the degree Doctor of Laws, honoris causa.

Justice Few is the proud father of daughters Reed and Anna, and son Cannon.

I. Introduction: the judiciary is going electronic

Over the past 20 years, a shift from paper filing to electronic filing has occurred in appellate courts across the United States, and the rate is increasing. From 2010 to 2014, the number of state appellate courts requiring or allowing e-filing increased from 15 to 33. ABA Council of Appellate Lawyers, *The Leap from E-Filing to E-Briefing* at 3 (2017) (“CAL Rpt.”), http://www.americanbar.org/content/dam/aba/administrative/appellate_lawyers/2017_cal_ebrief_report.authcheckdam.pdf. It is not a stretch to expect that “all or nearly all jurisdictions will have appellate e-filing within the decade.” *Id.*

With the advent of e-filing has been the introduction of electronic-document management, allowing judges and court staff to access documents by computer instead of paper files. Currently, every federal circuit court of appeals issues iPads to their judges (judges in the D.C. Circuit may choose the tablet type), and over 50% of state appellate courts do the same (usually iPad or Surface). CAL Rpt. at 8-11. See [App. A](#). However, not every appellate judge uses them to read briefs. Surveys show judges often read on a PC screen and in print when in the office. But the number of judges reading on paper decreases each year. It seems likely that nearly all judges and court staff will eventually read arguments on screens, not paper.

What effect, if any, will the change in the way judges read legal arguments have on the way attorneys present arguments in appellate briefs and motions? Will legal writing have to change along with the medium that is used to read it? Yes: If attorneys wish to effectively communicate to the electronic reader, they must reassess how they write and consider additional ways of communicating their arguments.

To support this conclusion, this article summarizes the results of various studies by cognitive scientists, educators, and website designers showing that screen readers read and retain differently than paper readers. The article then proposes ways attorneys can structure legal arguments and present them more effectively and persuasively to the screen reader, and how to utilize the electronic tools available to them.¹

¹ The author wishes to thank Robert Dubose, partner in the Houston office of Alexander Dubose Jefferson & Townsend, LLP, for his permission to use as a source for this paper his book, *LEGAL WRITING FOR THE REWIRED BRAIN: PERSUADING READERS IN A PAPERLESS WORLD* (ALM 2010) (cited as “Dubose”).

II. How screens have changed reading

Research has revealed that people read and retain information differently when reading electronic texts because there are material differences between the reading environment of digital and print media.

Because we literally and physiologically can read in multiple ways, how we read—and what we absorb from our reading—will be influenced by both the content of our reading and the medium we use.

Maryanne Wolf, *Our “Deep Reading” Brain: Its Digital Evolution Poses Questions*, Nieman Reports (Summer 2010), *quoted in* Anne Niccoli, *Paper or Tablet? Reading Recall and Comprehension*, Educause Review at 3 (Sept. 28, 2015), <http://er.educause.edu/articles/2015/9/paper-or-tablet-reading-recall-and-comprehension/>.

A. Screen reading occurs in a different environment than paper reading.

I recently observed readers at a large bookstore across from a mall, and then later that day readers at a Starbucks next door to a university. The readers in the bookstore read in an open lounge area between the book displays and a Starbucks counter. They were quietly engrossed in their books, sipping their coffee or tea as they casually flipped the pages. Some were listening to something on their earphones, but most weren't. There was little distraction.

In contrast, the readers at the other Starbucks were reading from a screen; nearly all had earphones tapped into the reading device or a phone. While not knowing the screen content (I couldn't read it if I wanted to), I noticed the screens changing at a fairly quick pace. Between scrolling through screens, constantly checking their phones, and encountered occasional interruptions by other patrons, I couldn't imagine the readers being able to concentrate on the screen content. There was one brave paper reader who, despite the activity surrounding him, appeared as engrossed in his book as the bookstore readers. The age of the readers at the two venues were surprisingly similar.

Admittedly, a busy Starbucks and a placid bookstore reading area present two contrasting *external* environments. But the differences I noticed between the paper and screen readers likely were an accurate reflection of the different *internal* reading environments between the two media. Below are several material differences between paper and screen environment.

1. Our electronic devices create an environment of distraction.

Back when lawyers read on paper at their office desk, they had a limited amount of information immediately available to them: their papers, client files, a few books, periodicals, and journals.

The amount of information lawyers now available in their offices is virtually unlimited. As Mitch Kapor, the founder of Lotus, once said, “Getting information off the Internet is like taking a drink from a fire hydrant.” When we sit at a computer, or carry a smart phone, tablet, or laptop, we have a limitless supply of information.

And not only is the available information unlimited, it is *always* available—the ever-present siren call leading us to us “check in.” We are never without our smart phones, and a tablet, laptop, or PC is almost always within reach. These devices not only wake us up and tell us our schedule for the day, they constantly communicate with us, distracting us from our reading. Unless the “notifications” function is turned off, we can potentially receive interruptions from (1) social media (Twitter, Facebook, Instagram, Snapchat, GroupMe, SoundCloud, Houseparty), (2) subscriptions (newsmagazines, bank and credit-card activity, weather updates, Uber and Lyft, news alerts), and (3) other messages (calendar alters, Amber alerts, software updates). The distractions are endless.

The result? Our electronic readers do not have the same focus and sustained attention as our readers had 25 years ago. As technology writer John Freeman concludes, our readers “work in the most distraction-prone workplace in the history of mankind.” JOHN FREEMAN, *THE TYRANNY OF E-MAIL: THE FOUR-THOUSAND-YEAR JOURNEY TO YOUR INBOX* 140 (2009).

2. Readers expect information instantly.

Like our paper readers in the bookstore lounge, reading in the past was a process of discovery that required time (and quietness) to find information. Now, search engines like Google, Yahoo, Safari, Westlaw, and LEXIS have trained readers to expect information quickly. Searching is relatively easy—it requires very little thinking or time to find information. See Nicholas Carr, *Is Google Making Us Stupid?*, *The Atlantic* (July/August 2008), <http://www.theatlantic.com/doc/200807/google>.

Because readers have become so accustomed to quickly obtaining information electronically, many now also expect to extract information from written documents, including legal filings, with the same ease and speed. When readers now approach a document, they expect to locate the necessary information in it as quickly and easily as they locate information through an Internet search. ROBERT DUBOSE, *LEGAL WRITING FOR THE REWIRED Brain: PERSUADING READERS IN A PAPERLESS WORLD* 22 (2010).

3. Because screen reading is more challenging, readers tend to skim screen text.

Studies have shown that screens are more difficult to read than paper. See *infra* Section B.1. When we read word-for-word, we read 10 to 30 percent more slowly on screens than paper. Sri H. Kurniawan & Panayiotis Zaphiris, Reading Online or on Paper: Which is Faster? (Aug. 2001), http://users.soe.ucsc.edu/~srikur/files/HCI_reading.pdf.

Why is this so? Technology writer John Freeman suggests the difference has to do with *light*. Freeman at 15. He notes that the human eye evolved to see the world by *reflected* light—it is not designed to look directly at a light source. Thus, we see most of the world using reflected light. An electronic device presents a relatively new exception. A computer screen shines light directly into our eyes. *Id.* It dries the eyes, increases blink rate, and creates headaches. *Id.*

It is therefore unsurprising that readers compensate for this more challenging reading environment by skimming screen text to more quickly gather information. Dubose at 40-41.

4. Multiple Window screens fosters multitasking.

The Windows-type operating system of course enables users to run more than one program at one time. *Id.* at 24-26. Today, most computer devices enable multitasking, turning readers into multitaskers as they move from one window to another. This ability is further enhanced by large screens or the use of multiple monitors at the office.

Yet, as with the constant electronic notifications, multiple windows compete for our attention and disrupt our concentration.

Freeman says multitaskers are capable of rote, mechanical tasks, but their performance declines in higher areas of thought, such as memory and learning. Freeman at 141. A Stanford University study found that people who are regularly bombarded with several streams of electronic information have a lower attention span, less memory control, or cannot switch between jobs as well as those who tackle one task at a time. Adam Gorlick, *Media Multitaskers Pay Mental Price, Stanford Study Shows*, *Stanford University News* (Aug. 24, 2009), [http://news.stanford.edu/\(search for “media multitaskers”; then follow hyperlink to “Media Multitaskers Pay Mental Price”\)](http://news.stanford.edu/(search+for+%22media+multitaskers%22);+then+follow+hyperlink+to+%22Media+Multitaskers+Pay+Mental+Price%22)).

Multitasking actually slows our thinking because it “forces us to chop competing tasks into pieces, set them in different piles, then hunt for the pile we’re interested in, pick up its pieces, review the rules for putting the pieces back together, and then attempt to do so, often quite awkwardly.” Walter Kirn, *The Autumn of the Multitaskers*, *The Atlantic* (November

2007), <http://www.theatlantic.com/> (search for “autumn multitaskers”; then follow hyperlink to “The Autumn of the Multitaskers”).

These distractions present a challenge for legal writers. Electronic readers of our legal documents will most likely be bombarded with these distractions as they attempt to absorb and understand what we have written. Dubose at 26-28. The challenge to communicate complex legal information to the screen reader is therefore higher than ever.

B. Studies reveal that screen readers read differently—and in some cases comprehend less—than print readers.

1. The low “physicality” of screens makes navigating long texts more difficult.

Studies show that “[t]here is physicality in reading.” Ferris Jabr, *The Reading Brain in the Digital Age: The Science of Paper versus Screens*, SCIENTIFIC AMERICAN at 3 (Apr. 11, 2013) (quoting Maryanne Wolf), <https://www.scientificamerican.com/> (search for “the reading brain”; in the black box click on “The Reading Brain in the Digital Age: The Science of Paper versus Screens”; scroll down to the paragraph immediately preceding the heading “Navigating textual landscapes”).

The brain perceives the entirety of a text “as kind of physical landscape,” and readers often locate particular information that they have read by recalling where it was located in the text. *Id.* at 4-5. It not unlike remembering the location of a certain productive pool in a trout stream by recalling it was located directly opposite a large buffalo jump.

Paper readers, especially when reading books, are reading in a clear, physical domain: two pages, eight corners, and a “feel” for the paper, which the reader leaves for a new vista by turning the page. *Id.* at 5. Paper readers read left-to-right, down the page, concentrating on one text at a time, doing only one task: reading. *Id.*

Screens, on the other hand, “interfere with intuitive navigation of a text and inhibit people from mapping the journey in their minds.” *Id.* The screen only displays one virtual page, disappearing as the reader clicks for the next screen, or scrolls or jumps to another part of the text. Even with page numbers and headers, “it is difficult to see any one passage in the context of the entire text.” *Id.*

The relative ease in navigating paper texts enables better absorption and therefore higher comprehension than reading screen texts. Studies have shown that the “spatio-temporal markers” that paper provides—touching paper and turning pages—“aids the memory, making it easier to remember where you read something.” Caroline Myrberg & Ninna Wiberg, *Screen vs. paper: what is the difference for reading and*

learning?, Insights, 28(2) at 49-54 (2015), <http://insights.uksg.org/articles/10.1629/uksg.236/>. The necessity of scrolling on a computer screen makes it more difficult to recall the substance of the text. *Id.*

In addition to Freeman's study on the effect of light from a screen, other studies have suggested that the low "physicality" of the screen increases the effort required to read screen text, especially if it is long. For example, one Swedish study revealed that screen readers reported higher levels of stress and tiredness, resulting in lower comprehension. Jabr at 8. Another study found that readers who had to scroll through continuous text recalled less than readers who flipped pages. *Id.* at 9. Again, researchers reasoned that scrolling requires more mental reserves because scrolling demands that the reader focus on the text and how she is moving it; in contrast, turning or clicking a page "are simpler and more automatic gestures." *Id.*

Why would the physical qualities of paper matter? Some researchers have concluded that qualities of words on a physical page help readers remember and find their location and content better. The four corners of a page "make it easier to form a coherent mental map of the text." *Id.* And others who read on a Kindle found that "people who read on paper were much better at reconstructing the plot of the story." Annie Sneed, *Everything Science Knows about Reading On Screens*, Fast Company, at 6 (July 8, 2015), <https://www.fastcodesign.com/3048297/evidence/everything-science-knows-about-reading-on-screens>. The researcher who conducted the study hypothesized that the tactile feedback of paper may help people process certain information when they read.

2. Screen readers skim over text—they don't read it.

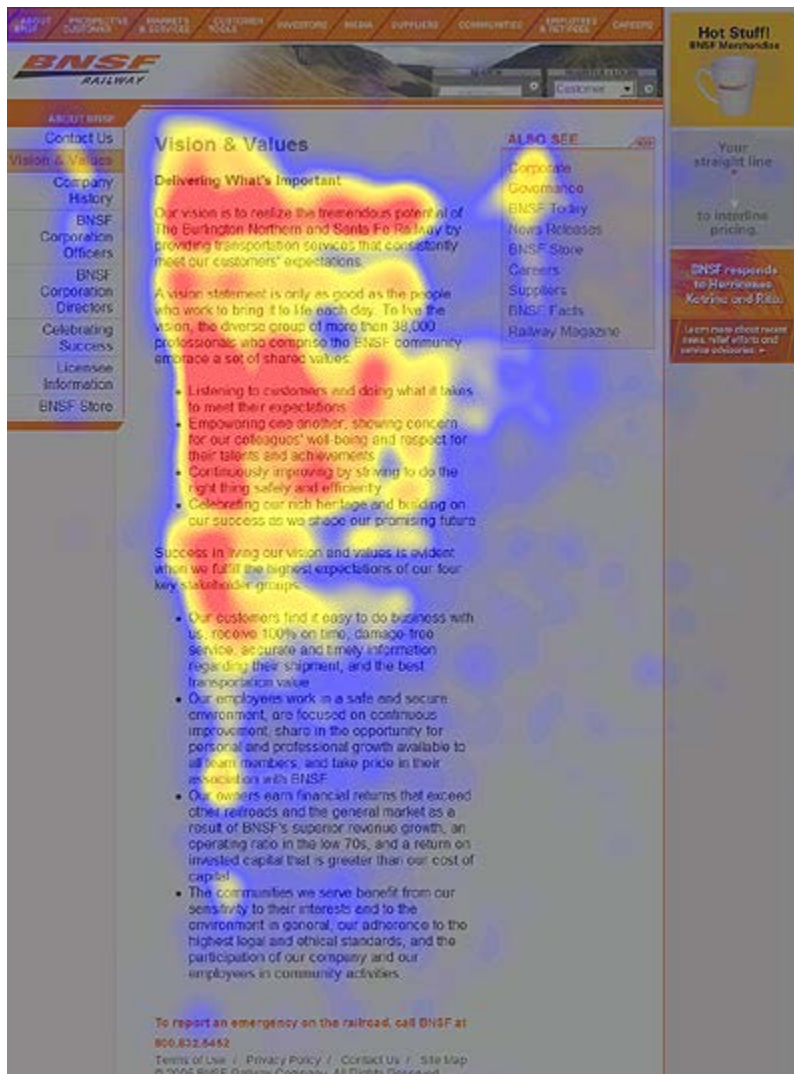
Studies have shown that reading from a screen has changed the very mechanics of reading. Screen readers spend more time "browsing and scanning, keyword spotting, one-time reading, non-linear reading, and reading more selectively." Sneed at 1. They don't read every word; they *skim* the text, focusing on only a portion of the page to gather what they want. Dubose at 40-41.

Eye-tracking studies have shown that screen readers are more likely to focus on certain portions of the page—typically:

- the top of the page,
- headings,
- the first line or two of paragraphs, and

- the text in a narrow band on the left side of the page running from top to bottom.

Because this reading pattern is shaped like an “E” or an “F,” web designers refer to it as the “F-Pattern,” which is demonstrated below:



Jakob Nielsen, *F-Shaped Pattern For Reading Web Content*, Nielsen Norman Group (Apr. 17, 2006), <https://www.nngroup.com/articles/f-shaped-pattern-reading-web-content/>.

The red and yellow areas of the page around the top left are the portions that test subjects looked at most. Blue areas had fewer views. Some words on the page were not read by any subjects. Studies have found the same sort of pattern not only in the way people read websites, but also in the way they read other types of online texts, such as newsletters.

Web designers have learned that a visible text structure takes advantage of these patterns and enables rapid-information gathering. For legal writers, the lesson is that visible structure is crucial for our readers to understand our primary arguments and quickly see the structure of an argument's logic

The F-pattern suggests that screen readers are more likely to:

- **Look for headings and summaries** of content;
- **Read the first paragraph** of a text more thoroughly than the rest of the text;
- **Read the first sentence** of a paragraph, but skim the rest of the paragraph; and
- **Look for structural cues** down the left side of the page.

See *id.*

Another lesson of the F-pattern is that screen readers usually do not read thoroughly. In the study, almost none of the readers read all of the words on the screen. When words are located toward the end of a paragraph, further down the page, or further to the right, they are less likely to be read. *Id.*

This switch to skimming results from the nature of the computer reading environment. Computer readers are in a hurry. STEVE KRUG, DON'T MAKE ME THINK 22 (2d ed., 2006). As discussed, the Internet provides an unlimited amount of information at a click, and readers simply do not have enough time to read it all. Skimming is not caused by laziness. It is a necessary adaptation to handle the information explosion and the demands of screen reading. Dubose at 41.

3. Screen readers have lower attention spans and want information quickly.

Because of the massive amount of available information on a screen and the lack of sufficient time to actually see it, “[w]eb users are impatient and insist on instant gratification.” Vitally Friedman, *10 Principles of Effective Web Design*, Smashing Magazine (Jan. 31, 2008), <http://www.smashingmagazine.com/> (search “effective web design”; then follow hyperlink under “Principles of Effective Web Design”).

Steve Krug’s landmark book on web design is named for the key principle for writing to the new reader: “Don’t Make Me Think”. Krug explains that when a user looks at a web page:

[I]t should be self-evident. Obvious. Self-explanatory. I should be able to “get it”—what it is and how to use it—without expending any effort thinking about it.

Krug at 11. Rather than an attack on the intelligence of screen readers (which is generally high), this statement recognizes that they are simply busy, bombarded with multiple sources of information, and therefore eager to get the crux of the text without significant effort. Their reading method is on the other side of the spectrum from the method of “deep” reading.

So it is with this impatient screen reader, in a non-physical, distracting screen environment that legal writers must more than ever communicate. But persuasively conveying a complex legal argument is a daunting challenge for the legal writer—that is, if the manner in which the message is conveyed does not change.

III. Suggestions for structuring an effective and persuasive legal argument to the screen reader.

The foregoing studies reveal that traditional legal writing may not be compatible with screen reading and rapid-information gathering. From law school and through years of practice, we have traditionally written in long paragraphs, using long sentences and lengthy argument development with little visible structure. This method of communicating demands more effort and focus than the new reader is able, or wants, to give.

So how can we better communicate complex legal concepts and arguments in a more screen-friendly format? Thankfully, a large body of research exists on how to write for the new style of reading. This research comes from the school of web design known as “usability.” As Dubose explains:

Usability tools are web design tools that have proven effective for making programs and websites easier to use. Many of these tools are as useful in legal writing as they are in web design. They help readers locate information. And they help readers to get the point quickly.

Dubose at 52. The following is a summary of several usability principles that Dubose recommends legal writers employ to more effectively communicate with the new screen reader, which also enhances communication with the paper reader. See *id.* at 51-52.

A. Use visible structures.

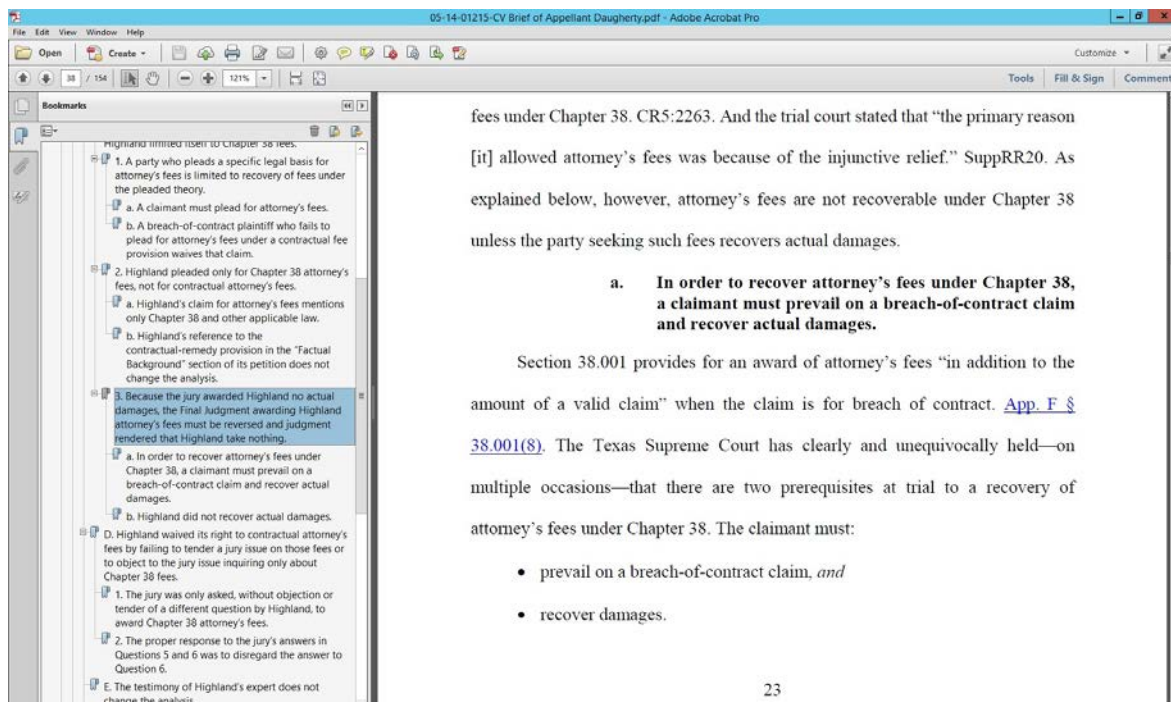
As the F-pattern demonstrates, screen readers need structure to process information rapidly. Recall that the study revealed that screen readers spend as much time looking up and down the left-hand side of the

screen as they do reading text from left to right. Therefore, they look for signs of structure.

Dubose recommends using the following structural tools:

- **Frequent headings.** Headings enable the screen (and paper) reader to see the overall structure of the argument, serve as sign posts to help him recall where he is in the argument, and enable comprehension by skimming. The smaller the screen, the more necessary headings are.
- **Outlines.** Outlines help show the overall structure of the argument.
- **Topic sentences.** The F-pattern shows that screen readers are more likely to read the *first sentence* of paragraphs. Thus, the first sentence should persuasively summarize the topic of the paragraph.
- **Lists.** Lists can effectively delineate separate arguments. They also concisely reveal how many points support an argument and where each new point begins and ends.
- **Bullets.** Like lists, bullets delineate examples or support where the number of points is not important.

See *id.* at 61-64, 72-76, 78-79, 92. The following section of an appellate brief, taken from a PC screen, demonstrates how the legal writer can employ some of these structural tools to provide the reader a roadmap of the argument: using an outline in the bookmark pane on the left side of the screen, and headings and bullet points in the text:



Utilizing bookmarks that state or summarize headings and other “road markers” greatly help the screen reader to navigate long documents. See *infra* Section G.1.

B. Use summaries.

Summaries are not new to the legal writer, and most appellate courts require them. They are essential for writing to the screen reader. Dubose notes that summaries at the beginning of a document more quickly convey the main points of an argument, which in turn assist readers to recall and absorb each point as they read. If your best argument does not appear until the end, screen readers will likely miss it because they read less carefully as they progress through a long document, as paper readers often do. Dubose at 87.

Thus, an effective summary of a legal document does three things:

- (1) provides a roadmap of the document;
- (2) gives the most persuasive details; and
- (3) does it quickly.

Id. at 88. Most of our summaries fulfill only the first point. But the second and third points are essential in communicating with the screen reader, who wants the information now, and reads more text at the beginning of a document and skims the remainder.

To persuade readers, Dubose recommend a concise summary that provides two or three specific, persuasive reasons supporting the primary proposition. If possible, the summary should include the most important facts and legal points of the argument, rather than just general concepts or conclusions. *Id.* at 89.

C. Use white space.

White space is any blank part of a page. It is a break in the text that provides the reader a brief rest. Thoughtful use of white space enhances readability. Note the difference between these two versions of the same table of contents.

Compare:

Argument.....	17
I. The court of appeals did not render a contract judgment in violation of the statute of frauds; it found sufficient evidence to support the jury's quantum-meruit verdict.....	17
A. Hill's statute-of-frauds theory is based on a misperception.....	17
1. Hill's statute-of-frauds argument is based on a misunderstanding of what occurred at trial.....	18
2. Hill's statute-of-frauds argument misunderstands the court of appeals' opinion.....	21
B. The relevant standard of review informs the validity of the court of appeals' result.....	22
1. Review of the statute of frauds issues.....	24
2. Review of the jury findings.....	24
3. Review of the judgment.....	25

With:

Argument.....	17
I. The court of appeals did not render a contract judgment in violation of the statute of frauds; it found sufficient evidence to support the jury's quantum-meruit verdict.....	17
A. Hill's statute-of-frauds theory is based on a misperception.....	17
1. Hill's statute-of-frauds argument is based on a misunderstanding of what occurred at trial.....	18
2. Hill's statute-of-frauds argument misunderstands the court of appeals' opinion.....	21
B. The relevant standard of review informs the validity of the court of appeals' result.....	22

1.	Review of the statute of frauds issues.....	22
2.	Review of the jury findings.....	24
3.	Review of the judgment.....	25

As the foregoing shows, white space gives the eyes and brain a break, a pause, without which the reader tires more quickly. The CAL Report addresses the effect of “text density,” and recommends line spacing and margin settings that provide more white space. CAL Rpt. at 25-28.

We have already seen why screen reading is more taxing than paper reading. So the use of white space is essential for communicating with the screen reader, particularly those reading from a small tablet screen.

D. “Chunk” complex information.

Another usability tool is “chunking.” Chunking is a memory-enhancement strategy that organizes “pieces of information into a smaller number of meaningful units (or chunks)—a process that frees up space in working memory.” <https://psychlopedia.wikispaces.com/Chunking>. This is most commonly done by breaking a long list of numbers, such as 4409275553040, into chunks, (44) (0) 927-555-3040.

Chunking can also be used to break down a long sentence full of information into separate, short points. Compare the ability to read and recall the elements of the following equitable doctrine:

Under the doctrine of virtual representation, a party not named in the trial court is deemed a party in the appellate proceeding where that party is bound by the judgment, its privity of interest appears from the record, there is an identity of interest between the litigant and a named party to the judgment, and if equitable considerations do not weigh against allowing [the movant] to participate on appeal.

Under the doctrine of virtual representation, a party not named in the trial court is deemed a party in the appellate proceeding where –

1. that party is bound by the judgment,
2. its privity of interest appears from the record,
3. there is an identity of interest between the litigant and a named party to the judgment, and

4. if equitable considerations do not weigh against allowing [the movant] to participate on appeal.

The “chunked” explanation is easier to remember because our brains find it much easier to process multiple bits of information when they are broken into these distinct chunks. No wonder our phone numbers, social security numbers, and credit card numbers are separated by hyphens.

E. Write visually.

Visuals convey information in ways that words cannot. They can often be recalled more easily than words. Although frequently used in jury trials, lawyers rarely use visuals in written documents. In 2007, Dubose surveyed briefs filed with the Texas Supreme Court during a six-month period. Only five percent of the briefs used any visuals—mostly charts—and none used photos. Dubose at 123. Thus, 95% of the briefs presented the entire argument with only words. This soon may change: The CAL Report recommends that courts “[a]dopt rules or guidelines for embedding visual images in briefs, such as videos, photos, and maps. CAL Rpt. at 22.

Yet inserting or creating visuals in legal documents is easier than most of us think it is. It usually involves only copying a photo or graph and pasting it into the body of the document. “[M]ost fixed images (such as photos) display reliably across different reading platforms.” *Id.* at 23. And most word-processing packages provide the ability to create tables, graphs, and other images in documents.

Consider how the photograph below—a trial exhibit that was included in the appellate record—adds clarity to the following text:

The sidewalk outside Crew’s Burgers & Shakes and the other establishments is a common area, and belongs to and is operated, managed, and maintained by landlord ABC Property, L.P. The sidewalk faces the park, is wide, and has tables and chairs down the sidewalk. The tables are open to the general public and any patron of the establishments in Maple Town Square, not just Crew’s. Crew’s owns the tables and chairs located in front of the restaurant, and had joint responsibility with ABC Property to keep the area clean, but it did not serve its patrons on the sidewalk area and had no right of control over it. Nearly all of the people that crowded the sidewalk area to listen to the concert at the park were not patrons of Crew’s.



One of the issues in that case was whether or not Crew's was liable for injuries that occurred in this sidewalk area caused by a fight initiated by an intoxicated man during a concert. The photograph helps explain that the incident occurred in a common area.

Visuals also help can readers comprehend complex information. For instance, in a recent brief, I explained the insurance packages under which the insured operator was seeking coverage after a storm damaged its oil and gas production facilities. The written explanation was less than clear:

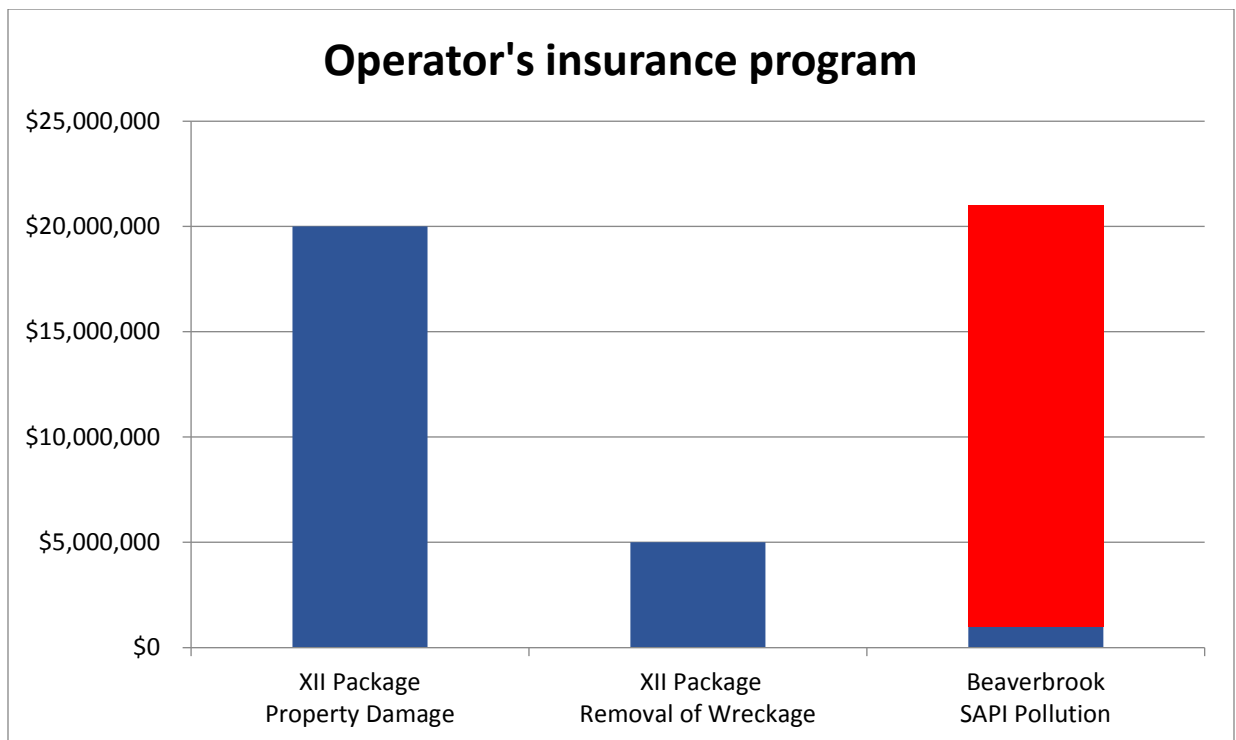
Operator had an Energy Package Policy from XII Insurance Company that included \$20 million in coverage for property damage and \$5 million for removal of wreckage.

Operator also had two insurance policies issued by Beaverbrook Insurance Company—a Commercial General Liability policy ("primary") and an Umbrella Excess Liability ("excess") policy. The primary policy provided \$1 million in coverage for "covered pollution clean-up costs that result from a sudden and accidental pollution incident," as defined in the policy. The excess policy provided \$20 million of coverage above the primary policy limits for pollution clean-up costs that "would have been

covered by the primary policy but are not because the primary limit is exhausted.” The primary policy responds to covered pollution clean-up costs that Operator “voluntarily incur[s]” or “is legally required to pay.” The excess policy only responds to covered pollution clean-up costs that Operator “is legally required to pay.”

The Beaverbrook policies were liability policies that included a narrow grant of coverage for certain pollution clean-up costs, as described more fully in the next section.

This insurance program is much more easily explained with a visual:



Visuals are common on the Internet. They often communicate information more quickly, and with less work for the reader, than the same information in paragraph form.

F. Simplify the presentation.

One of the best lessons from Internet usability is the success of the most widely used web page ever—Google. It continues to dominate the search-engine market.

Dubose notes that the key to Google’s success is simplicity. Google’s homepage has few words. Dubose at 103. No sentences. Most of the screen is white. Users find any information they want by typing a few words into a box and pressing “Search.”

The executive responsible for keeping Google's home page simple for many years was Marissa Mayer. She explained why the page is so effective:

Google has the functionality of a really complicated Swiss Army knife, but the home page is our way of approaching it closed. It's simple, it's elegant, you can slip it in your pocket, but it's got the great doodad when you need it. A lot of our competitors are like a Swiss Army knife open – and that can be intimidating and occasionally harmful.

Quoted in RICKY W. GRIFFIN, FUNDAMENTALS OF MANAGEMENT 1 (5th ed. 2007).

Similarly, the electronic writer must design legal documents with the same goal as Google's design to make the document useful to the screen reader. A brief usually addresses a complex subject. It may involve technical or scientific information. It may need to be long. It may seek alternative relief. Nevertheless, the brief must be approachable to the electronic reader such that he can navigate it without requiring too much thought about how to locate key information in the document.

Dubose suggests the following to make a document simpler:

- **Follow conventions.** Some documents, such as letters, memoranda, most appellate briefs, have certain formats and order of content. Stick to these ingrained conventions.
- **Use parallel structures.** For instance, when a series of sentences repeats the same words, readers can follow the structure more easily if those words appear in the same location in each sentence.
- **Avoid unusual fonts or fancy formatting. THEY ONLY DISTRACT**

YOUR

READERS.

See CAL Rpt. at 29-30 (recommending font sizes and types).

- **Use ordinary capitalization; avoid underlining.** Sentences, including headings, are harder to read when a writer USES ALL CAPS, Capitalizes The First Letter Of Every Word, or UNDERLINES THE ENTIRE SENTENCE. See *id.* at 33-35.

- **Use simple sentence structure.** A long sentence with a simple structure is harder to read than a short sentence with an easy structure.
- **Avoid unnecessary words.** When readers have to read unnecessary words—and they *will* recognize them—they resent having to work harder to understand your point.

See Dubose at 103-115. Knowing that screens readers do not want to work hard to get your point, and want to get it quickly, the simpler we make our documents, the more persuasive they will be.

G. Utilize available electronic navigating tools.

Electronic writers should periodically investigate new tools and programs that will enhance the reading experience for the screen reader. Remember, the easier and quicker it is for a screen reader to “use” our legal documents, the more likely the reader will understand our arguments and be persuaded by them. Multiple programs and apps exist to assist with electronic writing and editing, and more are created seemingly every month. Those features are beyond the scope of this paper.

Three tools facilitate navigation of an electronic document. Those tools are bookmarks, internal hyperlinking, and external hyperlinking.

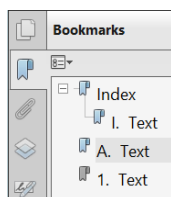
1. Bookmarks.

A bookmark is a text link that appears in the Bookmarks Panel of Adobe Reader and Adobe Acrobat on the left side of the screen. The content of the bookmark in a brief or motion usually consists of the headings—or a summary of the headings—in the document and a concise description of items included in an appendix attached to the document.

Readers use bookmarks to quickly navigate to different sections of the document and the appendix. See *supra* Section III.A (photo of screen showing bookmark panel). In some jurisdictions, like California and Texas, bookmarks are required for any items contained in an appendix. CAL. R. CT. 3.1110(f)(4); TEX. R. APP. P. 9.4(h). California also requires bookmarking of all exhibits in e-filed motion papers in the trial courts. CAL. R. CT. 3.1110(f)(4). Unsurprisingly, the ABA Council of Appellate Lawyers recommends that courts encourage or require bookmarks “so that readers may see an outline of the brief in a side panel and jump to a particular section.” See CAL Rpt. at 38-40.

The following provide the steps to set up a bookmark in Adobe Reader or Adobe Acrobat PDF that is not created using Word Styles:

- Select the heading in the text to bookmark.
- Click on the bookmark symbol .
- Edit the heading by typing in the bookmark box, if necessary.
- To create a hierarchy, click and drag bookmarks under headings.



2. Internal hyperlinking.

A hyperlink is a word, phrase, or image that the screen reader can click to jump to a new section within the document or to another document. Virtually all web pages contain hyperlinks, which is how you can jump to other portions of the Internet link that you are on or to a completely different web page. This discussion addresses hyperlinking to documents attached to a brief or motion, such as cases, key portions of the appellate record, or summary-judgment evidence.

Unlike bookmarks, which appear on the left margin of the screen, a hyperlink appears in the text, and is marked in a way that informs the screen reader that it is a hyperlink. Briefs filed in Texas appellate courts usually mark the hyperlink like [this](#) (blue custom color number 255 really stands out).

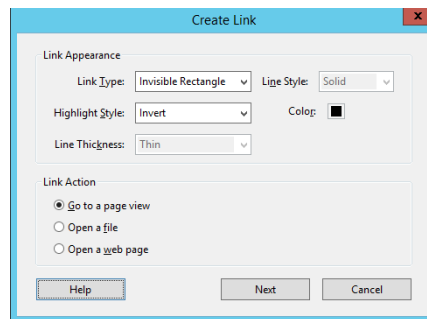
This document contains an Appendix, which the curious reader may already have accessed by clicking on the hyperlink on page 1: [App. A](#) (or by clicking on “Appendix” in the Bookmarks or on “A” in the dropdown). Appendix A contains the chart from the ABA Counsel of Appellate Lawyers article on electronic filing that is addressed in the Introduction. So if you are wondering whether the state in which you practice issues tablets to the appellate judges or justices of the state, clicking on [App. A](#) immediately takes you there.

Many states require appellate briefs to contain an appendix with certain documents, such as judgment of the lower court(s), jury verdict, findings of fact, the text of statutes at issue in the appeal, and the text of contracts or other documents that are critical to the argument. *E.g.*; TEX. R. APP. P. 38.1(k), 53.2(k); MASS. R. APP. P. 18. If the rules permit optional materials, then the advocate should also include—and hyperlink to—seminal cases, excerpts of key testimony that is too long to quote in the brief, “smoking gun” exhibits, etc.

Hyperlinking is a fabulous tool to bring the screen reader immediately (and easily) to the very piece of information that may persuade the reader to agree with your argument. Judges and court staff have frequently commented that they like hyperlinked briefs. And the CAL Report recommends that courts “[e]ncourage internal hyperlinking within briefs.” CAL Rpt. at 40.

To create hyperlinks from the main document to a document in the appendix (you must have Adobe Acrobat installed):

- Open the Bookmarks panel.
- Highlight and change the color (see above) of the word or citation you want to hyperlink.
- Right click and choose *Create Link*.
- In the Create Link dialogue box, choose how you want the link to look:



- Press *Next*
- Navigate to the target view
- Press *Set Link*

3. External hyperlinking.

As its name provides, an external hyperlink takes the reader out of the document to an outside Internet site. Please note that some courts do not allow, or disapprove of, external hyperlinks out of concern for potential malicious websites. In fact, the CAL Report recommends that courts prohibit hyperlinking briefs to the Internet, or require that a copy of the cited material be included in an appendix to the brief. CAL Rpt. at 50.

To hyperlink to an external Internet site, the reader of course must be connected to the Internet. Because most homes, business establishments, and now airplanes have WiFi available, the Internet is

almost always available. Most smart phones can become WiFi “hot spots,” enabling access to the Internet. Several cell phone providers sell personal portable WiFi devices through which the purchaser can set up her own secure WiFi network.

The most practical use of external hyperlinking in appellate documents is hyperlinking to every legal authority cited in the brief. That enables the judge and court staff to instantly read the specific portion of the case cited in the brief without having to separately log on to Westlaw or LEXIS. The CAL Report recommends that courts encourage brief filers to hyperlink to legal citations on Westlaw or LEXIS. CAL Rpt. at 41-45.

This paper contains several external hyperlinks to cited studies on screen reading that are available on the Internet. As the balloon states when your cursor hovers over the link cite, just simultaneously hit the “Control” key and click your mouse or pad, and the article will appear in a separate window on the Internet.

Here is how to create an external hyperlink:

1. Go to the website to which you want to hyperlink from the document.
2. Highlight and copy the website address in the url bar at the top of the page.
3. Return to the document and go to the place where you want the website address to appear.
4. Paste the address there.
5. Then hit the “Enter” key.
6. The website address will turn a light blue, indicating the hyperlink has been created.

The use of bookmarks and hyperlinking are extremely helpful to the electronic reader. Although they are not difficult to set up, your brief will likely stand out from others, as many advocates choose not to utilize them.

While not a “tool,” another way to enhance navigation of an e-brief that is converted to a PDF (as most courts require) is to begin pagination with the first page of the document, so that the pagination of the brief corresponds to the pagination of the PDF. See CAL Rpt. at 36-37. Most California appellate courts require that all e-filed briefs require this matching pagination. CAL. R. CT. 3.1110(c).

IV. Conclusion

The reading habits of our audience have been changing over the past 25 years, and will continue to change at a higher rate as the legal community moves toward a completely electronic environment. So we advocates must change the way we write. The first step is to develop a better understanding of *how* our audience is now reading. Then we must become aware of *methods of communicating* more effectively and persuasively to the electronic reader. And then we should learn to use *electronic tools* to create a more navigable legal document. It is then that we will have adapted to make legal writing usable for the screen (and paper) reader.

The following are additional resources for creating electronic appellate briefs:

- ABA Council of Appellate Lawyers, *The Leap from E-Filing to E-Briefing* (2017), http://www.americanbar.org/content/dam/aba/administrative/appellate_lawyers/2017_cal_ebrief_report.authcheckdam.pdf.
- *Guide to Creating Electronic Appellate Briefs, Appendices, and Hyperlinking* (2016), <http://www.courts.ca.gov/documents/DCA-Guide-To-Electronic-Appellate-Documents.pdf>.
- Blake A. Hawthorne, *Guide to Creating Electronic Appellate Briefs* (2014), <http://www.txcourts.gov/media/124903/guidetocreatingelectronicappellatebriefs.pdf>.
- *How to Build Electronic Briefs* (ABA 2010), http://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/solo_lawyer_acrobat_electronic_brief.html.
- *Attorney Guide to Hyperlinking in the Federal Courts*, <http://federalcourthyperlinking.org/attorney-guide-to-hyperlinking/>
- *Electronic Filing at the Appeals Court*, <http://www.mass.gov/courts/court-info/appealscourt/efiling-appeals-faq-gen.html>

INDEX

- A. ABA Council of Appellate Lawyers, *The Leap from E-Filing to E-Briefing* at 8-11 (2017), http://www.americanbar.org/content/dam/aba/administrative/appellate_lawyers/2017_cal_ebrief_report.authcheckdam.pdf

APPENDIX A

Tablets and annotation software issued to judges in federal and state appellate courts, 2016

<i>Federal Appellate Courts</i>		
	Standard Tablet	Standard Software
First Circuit	iPad	Documents by Readdle PDF Expert
Second Circuit	iPad	PDF Expert iAnnotate PDF
Third Circuit	iPad	Good Reader
Fourth Circuit	iPad	Good Reader
Fifth Circuit	iPad	Adobe Acrobat Reader iAnnotate PDF
Sixth Circuit	iPad	Good Reader
Seventh Circuit	none	none
Eighth Circuit	iPad	Adobe Acrobat Reader
Ninth Circuit	iPad (most common) Surface	GoodReader (preferred) Adobe Acrobat Reader
Tenth Circuit	iPad (most common) Surface	GoodReader WPD Reader
Eleventh Circuit	iPad	Adobe Acrobat Reader GoodReader PDF Reader
D.C. Circuit	judge's choice	unknown
Federal Circuit	iPad	Adobe Acrobat Reader
Armed Forces	none	none
<i>State Appellate Courts</i>		
	Standard Tablet	Standard Software
Alabama	none	none
Alaska	none	none

Arizona	iPad Android Surface	Adobe Acrobat Reader iAnnotate PDF GoodReader
Arkansas	unknown	unknown
California	iPad Surface	Adobe Acrobat Reader Adobe Acrobat Pro iAnnotate PDF GoodReader
Colorado	iPad	GoodReader
Connecticut	none	none
Delaware	judge's choice	unknown
District of Columbia	none	none
Florida	iPad	Adobe Acrobat Reader
Georgia	none	none
Hawaii	none	none
Idaho	none	none
Illinois	iPad	Adobe Acrobat Reader
Indiana	Revolve iPad Pro	Adobe Acrobat Reader
Iowa	judge's choice	unknown
Kansas	none	none
Kentucky	none (coming soon)	none
Louisiana	none	none
Maine	none	none
Maryland	iPad	Adobe Acrobat Reader PDF Reader GoodReader
Massachusetts	Surface	Adobe Acrobat Reader PDF Reader
Michigan	Surface	Adobe Acrobat Reader iAnnotate PDF GoodReader

Minnesota	Surface Pro iPad Pro	Adobe Acrobat Reader iAnnotate PDF GoodReader
Mississippi	iPad	none
Missouri	iPad	Adobe Acrobat Reader EzPDF Reader iAnnotate PDF PDF Reader
Montana	Surface	unknown
Nebraska	iPad	unknown
Nevada	none	none
New Hampshire	none	none
New Jersey	none	none
New Mexico	none	none
New York	none	none
North Carolina	Helix	Adobe Acrobat Reader iAnnotate PDF PDF Reader
North Dakota	iPad	Adobe Acrobat Reader iAnnotate GoodReader PDF Reader
Ohio	none	none
Oklahoma	none	none
Oregon	iPad	Good Reader iAnnotate PDF PDF Expert Acronis Access (future)
Pennsylvania	iPad	Acronis Editor
Rhode Island	none	none
South Carolina	iPad	GoodReader
South Dakota	iPad	West Drafting Assistant Adobe Acrobat Reader

Tennessee	iPad	Adobe Acrobat Reader iAnnotate PDF
Texas	iPad	Adobe Acrobat Reader iAnnotate PDF GoodReader
Utah	iPad	none
Vermont	none	none
Virgin Islands	iPad	Adobe Acrobat Reader
Virginia	Surface	Adobe Acrobat Reader GoodReader
Washington	iPad Surface (pilot)	Adobe Acrobat Reader
West Virginia	none	none
Wisconsin	none	none
Wyoming	iPad	unknown



FRIDAY, MARCH 10, 2017

7:30 a.m. – 8:30 a.m.

SECTION MEETINGS

DATA BREACH, PRIVACY AND CYBER INSURANCE LAW

What's Hot and the Impact of Technology Competence

Comment 8 to the ABA Model Rules

Colleton

Speakers:

John W. Sinnott

Christopher A. Holecek

F. Marshall Wall

Stephen E. Embry

Can a Refrigerator Invade Your Privacy? Data Privacy in a Digitally Connected World

Christopher A. Holecek

Wegman, Hessler & Vanderburg

6055 Rockside Woods Blvd., Suite 200

Cleveland, OH 44131

Writer's Biographical Information

Mr. Holecek is a partner at Wegman, Hessler & Vanderburg in Cleveland, OH. He is the Co-Chair of the firm's litigation and cyber security practice groups. Mr. Holecek handles product liability, commercial and employment litigation. He is board-certified by The National Board of Trial Advocacy and has been elected to "Ohio Super Lawyers" every year since 2012.

Introduction

In the 1998 movie *Enemy of the State*, Will Smith starred as a labor lawyer whose career was upended by an out-of-control government surveillance program. *Enemy of the State* (Touchstone Pictures 1998). In the movie, Gene Hackman appeared as a paranoid privacy nut who believed the government was watching everyone. As the movie developed, it turned out that Gene Hackman's character actually was not paranoid and that the government had been tracking the lawyer's movements and purchases. In the end, the paranoid privacy nut was actually right! While the scope of the government's surveillance program in *Enemy of the State* seemed hard to believe when the movie was released in 1998, it no longer seems far-fetched today. And regardless of one's position on Edward Snowden, his 2013 revelations of the government's collection of telephone data, paired with continuing technological breakthroughs, indicate that perhaps the government really can see and hear almost everything. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, The Guardian, June 6, 2013. Indeed, even the FBI Director, James Comey, recently admitted that he puts tape over his laptop's webcam as a "common sense" precaution and recommends others do the same. Julian Hattem, *FBI Director: Cover Up Your Webcam*, The Hill, Aug. 14, 2016.

But even outside of the government's sphere, potential intrusions on privacy are evident. Most of us engage in e-commerce on a regular basis. We hand over personal identifying information about ourselves, including

our names, date of birth, Social Security and credit card numbers to complete strangers in exchange for a product or a service. We also allow large internet companies, such as Google and Facebook, to collect our data so that they can generate personalized ads for us. See Privacy, *Your Data: We Want You to Understand what Data we Collect and Use*, Google.com, available at <https://privacy.google.com/your-data.html>. Despite revelations of potential privacy intrusion, e-commerce continues to flourish. Why? Because consumers trust that companies will safeguard their personal information. But when this trust is breached, privacy lawsuits follow.

Protecting private data is obviously a challenging and daunting task. Not only are potential hackers, including their equipment, becoming more sophisticated, but the sheer amount of personal data that is collected and stored is staggering. Hayley Tsukayama, *Hackers are Getting Better at Offense. Companies Aren't Getting Better at Defense*. The Washington Post, Apr. 22. A Federal Trade Commission ("FTC") Staff Report estimates that fewer than 10,000 households using devices connected to the Internet can generate 150 million discreet data points each day. *Federal Trade Commission Staff Report on the November 2013 Workshop Entitled: The Internet of Things: Privacy Security in a Connected World*, FTC, Jan. 27, 2015, at p. 14. When you multiply that number by the 286,942,362 people in the United States who are internet users, the number of data points per day is astronomical. Internet World Stats, *North America*, available at <http://www.internetworldstats.com/america.htm#us>. At the same time, three out of four Americans say that it is "very important" that they be in control of *who* can get information about them. Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW Research Center, Sept. 21, 2016.

Not surprising, the law regarding privacy concerns created through the new Internet Age is unsettled. And it will certainly evolve as technology changes. Congress, states and courts will create new, or expand old, causes of action. As a result, attorneys who handle privacy suits will need to understand and be conversant in the language of cyber technology. To that end, when privacy lawsuits arise attorneys will need to recognize that they are defending a different type of tort, one predicated not on a tangible bodily injury but upon a breach of trust: a consumer handed over personal information with the expectation that it would be safeguarded and it wasn't. It is not surprising, therefore, that privacy plaintiffs feel betrayed when their data is either misused or falls into the hands of cyber criminals. Ignoring the emotional component of the case is risky and may interfere with your client's ability to resolve the case early and on favorable terms. Very simply, if

consumer trust is the lifeblood of our retail clients, then we must assist our clients in repairing that trust during all phases of the litigation.

1. The Internet of Things: Will there still be privacy?

One of the more interesting areas of technological advancement and privacy concerns relate to the “Internet of Things.” The “Internet of Things” is a term that describes the ability for everyday devices such as refrigerators, thermostats, and cars to connect to the Internet. Nicole Kobie, *What is the Internet of Things?*, The Guardian, May 6, 2015. The 2015 FTC Report cited estimates that 26 billion connected devices will be available by 2020. *Federal Trade Commission Staff Report on the November 2013 Workshop Entitled: The Internet of Things: Privacy Security in a Connected World*, FTC, Jan. 27, 2015, at p. 14. But even today, many common household devices connect to the Internet. For example, washing machines from General Electric can be started and monitored via cell phones, refrigerators from LG are equipped with cameras that can text a picture of what’s inside while the owner is grocery shopping, Fitbit devices monitor your health by tracking your heart rate, sleeping patterns, and blood pressure, and thermostats, light switches, and door locks can be managed through apps. And that is just the beginning! See, Keith Barry and Mike Roorda, *Text this LG Fridge, and it Will Send You a Selfie: Use Your Phone to Check What’s In Your Fridge*, Reviewed.com, Sept. 4, 2014; General Electric, *GE Wifi Connect Homepage*, available at <http://www.geappliances.com/ge/connected-appliances/>.

Advancements in the Internet of Things will continue to grow and make our lives more convenient. But these devices can also create an exponential number of entry points for cyber criminals. In the past, hackers could only access your information through computers. Now, sophisticated hackers can gain access to an entire network through poorly protected smart devices. For example, the much publicized Target data breach that impacted millions of Target’s customers in 2015 was not an “inside” job. Danny Yadron and Paul Ziobro, *Before Target, They Hacked the Heating Guy*, The Wall Street Journal, Feb. 5, 2014. Instead, the intrusion occurred through an HVAC subcontractor who had worked at various Target stores. *Id.* Because Target’s subcontractor system was connected to the Internet, cyber criminals were able to use that system as an entry point into Target’s entire network.

2. Other Privacy Concerns with the Internet of Things

Despite their convenience, connected devices also create public profiles containing their owner's personal information. For instance, the "Smart Refrigerator" collects data about the type and amount of food purchased and consumed, and the Fitbit collects data on one's heart rate, weight, and exercise information. Hunter Walker, *Senator Warns Fitbit Is A 'Privacy Nightmare' And Could Be 'Tracking' Your Movements*, Business Insider, Aug. 10, 2014. Further, a connected car tracks how fast one drives, when and how much one drives, and the number of "hard brakes" one makes. See *Frequently Asked Questions About Snapshot*, Progressive.com, available at <https://www.progressive.com/auto/snapshot-common-questions/>.

But who owns all the data collected by these connected devices? It would seem that the owner of the device owns the data. Manufacturers and sellers, however, believe they own the data from and about the consumer. Manufacturers utilize the data to better market their products and have monetized this data by selling it to advertisers. Yet the desires of the manufacturers is at odds with the wishes of consumers. A recent PEW survey, for instance, found that most Americans struggle to understand the nature and scope of the data collected about them and three out of four Americans say it is "very important" to control what type of information is collected about them. *The State of Privacy in Post-Snowden America*, PEW Research Center, Sept. 21, 2016. Despite confusion as to what data is being collected, most people recognize that the data collected from and about them has the potential to be misused.

For example, private data collected from connected or "smart" devices can be used for both beneficial and harmful purposes. A conscientious person who exercises and eats well could be a good candidate for employment, and a good driver should be entitled to better insurance rates. But what happens if an employment, credit, or insurance decision is made using the consumer's data without that person's consent and/or without the decision maker taking steps to ensure that the data is accurate?

At first blush it would seem that the Fair Credit Reporting Act ("FCRA") would govern the use of data collected from "smart" devices. The FCRA imposes obligations on employers, lenders, and insurers to take measures to ensure maximum possible accuracy of consumer data and gives consumers an opportunity to correct erroneous data. 15 USC § 1681 et seq. But the FCRA safeguards do not seem to cover instances where manufacturers *directly* collect the data from the consumer. Therefore, it would seem that when companies make employment, credit and insurance

decisions from data collected directly from connected devices, they do not need to give consumers access to the information they rely on, or give consumers an opportunity to correct errors in the data as required by the FCRA.

A majority of Americans, according to a recent PEW survey, favor additional legal protections against abuses of their private data. *The State of Privacy in Post-Snowden America*, PEW Research Center, Sept. 21, 2016. Therefore, it seems the public will eventually demand that laws be enacted offering similar FCRA type protections when a consumer's private data is collected from connected devices and is then used for employment, credit and insurance purposes.

3. Recent Decisions on Privacy Litigation

In addition to new legislation, courts have been interpreting current law to cover privacy violations that were previously not allowed. For example, the Sixth Circuit has recently given aggrieved consumers a potential way to sue companies for losing customer data. *Galleria v. Nationwide Mut. Ins. Co.*, No. 15-3386/3387, 2016 U.S. App. LEXIS 16840 (6th Cir. Sept. 12, 2016). In 2012, cyber criminals accessed Nationwide's network obtaining private information of 1.1 million Nationwide customers and potential customers. *Id.* These cyber criminals obtained names, Social Security and drivers' license numbers, dates of birth and other private information. *Id.* The customers whose information had been stolen brought suit against Nationwide as a class action in *Galleria v. Nationwide*. *Id.* In that case, the U.S. District Court for the Northern District of Ohio dismissed the suit finding that there was no Article III standing because the Plaintiffs could not establish a concrete injury under *Clapper* to support their invasion of privacy claims. *Id.*

But on appeal, the Sixth Circuit, in a 2 to 1 decision, reversed the district court, holding that it would be unreasonable to expect the Plaintiffs to wait for third parties to actually misuse their data before bringing suit. *Id.* After all, why would cyber criminals steal the data unless they were going to use it? *Id.* The Sixth Circuit, thus, held that Plaintiffs could maintain an action against Nationwide before the stolen data had actually been misused. *Id.*

Galleria seems to demonstrate how privacy plaintiffs can make a "substantial risk of harm" showing even where the full potential of a data breach had not yet been realized. It is too early to tell, however, what impact (if any) this decision will have on data breach litigation. Presently, the case has not been scheduled for trial so the ultimate outcome against Nationwide remains unknown. However, this case is certainly worth monitoring.

4. Defending Privacy Suits

As defense lawyers, it is important to recognize that data privacy law is, as reflected in the *Galaria* decision, constantly evolving. As indicated, we must recognize that a privacy lawsuit concerns a breach of trust. A plaintiff feels betrayed because his or her private information was handed over to a company believing that it would be safeguarded at all times. The plaintiff is also upset because he or she lost control over their private information.

In assessing damages in a privacy lawsuit, we need to be mindful that unlike bodily injury cases, quantifying the harm is more challenging. Because we are dealing with litigants who are angry, hurt, or even embarrassed that their trust has been violated, we cannot underestimate the emotional component of the claim. And we cannot assume a settlement will be low just because there is no direct financial harm to the plaintiff. We must also be mindful of the reputational damage to our clients, especially in a publicized data breach.

Moreover, taking privacy suits to trial poses risks regardless of the plaintiff. Counsel must not assume juries will take it “easy” on a defendant if the invasion of privacy concerns “bad” people or “sleazy” behavior. For instance, Terry G. Bollea, commonly known as “Hulk Hogan”, was awarded \$115 million by a jury after Gawker.com published a 2012 sex tape involving Bollea and the wife of one of his associates. Gawker’s founder ultimately filed for Chapter 11 Bankruptcy protection after the crippling verdict. Sydney Ember, *Gawker, Filing for Bankruptcy After Hulk Hogan Suit, Is for Sale*, The New York Times, June 10, 2016.

5. Conclusion.

Privacy law is unsettled. In a connected world, it is generally understood that the “right to be left alone” is impractical. But most Americans view privacy as the right to control their identity and any information about them. *The State of Privacy in Post-Snowden America*, PEW Research Center, Sept. 21, 2016. Undoubtedly, new and different forms of harm will evolve and be created. Counsel who defend privacy suits, and companies who process consumers’ private information, need to understand and be conversant in cyber technology and the laws regulating this area.

CYBER INSURANCE: THE WILD, WILD WEST

**FDCC Winter Meeting
Charleston, South Carolina
March 6-10, 2017**

Presented by:

**John W. Sinnott
IRWIN FRITCHIE URQUHART & MOORE LLC
New Orleans**

About the Author:

John W. Sinnott

John is an experienced products liability, insurance coverage, and construction litigator. He has defended product manufacturers in litigation involving pharmaceutical and over-the-counter medications, medical devices, industrial machinery, synthetic stucco, and tankless water heaters. In the insurance coverage field, he advises and defends insurers in coverage litigation and direct action cases. John has also defended premises liability claims, environmental and toxic tort actions, and claims against medical laboratories and termite/pest control companies.

In addition to his involvement with the FDCC, John is an active Fellow in the American College of Coverage and Extracontractual Counsel. He has spoken at the organization's Annual Meeting and serves as Co-Chair of the Website and Social Media Committee. He is also involved in the Defense Research Institute and other defense groups. He is his firm's partner in charge of pro bono service.

John is a frequent author and speaker. He has spoken and written about topics such as cyber insurance, cy pres distributions in class action settlements, social media discovery and admissibility, the recent amendments to the Federal Rules of Civil Procedure, traumatic brain injury litigation, insurance coverage for mold and mildew claims, ethics for insurance defense counsel, insurance coverage settlements, UM/UIM coverage, and claims handling. He recently wrote three chapters for the ACCEC's First-Party Property Insurance Appraisal Law Compendium. You can follow John on Twitter at @JohnWSinnott.

John graduated from Dartmouth College and Tulane Law School. He is a former Captain in the United States Marine Corps. He is the Vice President for the Dartmouth Club of the Gulf South, the Cubmaster for his sons' Cub Scout pack, and a coach for his sons' baseball and soccer teams.

CYBER INSURANCE: THE WILD, WILD WEST

I. THE EXPLODING CYBER SECURITY PROBLEM

Data breach and other cyber security incidents have generated increased attention in recent years. Perhaps the most well-known incident involved hackers who obtained credit card data and debit card PIN numbers from Target's online customers. After the announcement, consumers filed multiple lawsuits, financial institutions sought to recover the cost of issuing new credit and debit cards to affected customers, the government instituted regulatory actions, and Target lost a lot of money.

What was initially viewed as a problem primarily for online retailers who maintain consumers' credit and debit card information has grown and impacted businesses in widely varying industries, including financial institutions, health care providers, insurers, the U.S. government, and online dating sites (Ashley Madison). Law firms have also been targeted. The most prominent example is referred to as the "Panama Papers"—an online leak targeting a Panamanian law firm that allegedly structured the finances of prominent politicians and their friends and relatives in such a way as to minimize taxes.

Companies store more personal information than ever—financial, health, etc.—electronically, but the protection of customer and employee data is far from the only problem. Companies' important competitive data, trade secrets, operational controls, emails, and other sensitive and confidential information are all vulnerable to attack and disclosure.

Emerging technologies compound the problem. The internet of things, driverless cars, home appliances connected to the internet, connected medical devices (smart pacemakers, insulin pumps), cloud computing, mobile devices, drones, and other products are susceptible to hacking. Ironically, technology that was once intended to provide increased protection over traditional measures is now vulnerable. For example, auto manufacturers abandoned standard metal keys for remote entry and other features that now allow a hacker to use technology to gain access to a car, take over its electronic ignition system, and steal the car.

Attacks can cause losses to all types and sizes of businesses. Larger companies may have greater overall exposure than small and midsize companies but may also have greater technological and financial

resources which make them better able to respond to an attack than smaller companies.

Attacks exert pressure on companies to increase their protection of personal information and company data. Some have extended that pressure “downstream,” i.e., by requiring vendors and suppliers to increase their security and to buy insurance that protects the upstream company from liability in the event of vendor or supplier fault in causing a breach. Corporate and insurer RFPs to law firms now frequently ask about firms’ cyber security protections.

Attackers have become more sophisticated and include hackers, criminals, insiders, foreign governments, and activists. Many if not most attacks can go undetected and unreported.

There are many potential cyber risks. The most obvious example is the theft or disclosure of personal information from customers or employees (social security numbers, credit cards, PINs, etc.) that may result in identity theft. A typical response to this type of breach may include: (a) a forensic investigation to determine the cause of the breach; (b) restoration of the data damaged by the attack; (c) notification to people whose data may have been compromised; and (d) credit monitoring services for those people. Other cyber risks include, but are not limited to, reputational harm (which is never covered by insurance), business interruption from a hacked website, malware, cyber extortion, the theft of intellectual property or trade secrets, and inadvertent or intentional disclosure of data or information by an employee. Hackers have successfully run what are called business email compromise scams, or CEO fraud. In these instances, a hacker accesses a company’s email system and sends an email appearing to be from the company CEO asking the accounting department to transfer money to another company, but the money is actually sent to the cyber criminal’s account.

As cyber risks increase, liability is a significant concern for our clients. The legal environment includes data breach liability, class actions, insurance coverage disputes, and state and federal government regulatory actions. Companies are, not surprisingly, increasingly looking to insurers to help manage their risk and to help them prevent and respond to attacks.

II. THE BIRTH OF CYBER INSURANCE

Traditional commercial general liability insurance policies do not afford coverage for most, if not all, cyber risks. Insurance Services Office's Exclusion P excludes "damages arising out of the loss of, loss of use of, damage to, corruption of, inability to access, or inability to manipulate electronic data." Policies may also carve out damage or disruption to electronic data from the definition of the term "property damage." A typical CGL policy may afford coverage for personal and advertising injury resulting from publication of material that violates a person's right of privacy; insurers may exclude data breach from this coverage and, instead, afford such coverage in separate cyber policies.

Cyber liability is a rapidly evolving risk, and standalone cyber insurance is still in its infancy. Policies can be difficult to price due to the lack of historical data available to underwriters. Underwriters have lots of data and insured loss history on things like earthquakes, floods, car accidents, and life expectancies. However, there is little or no such data available for the complex and emerging risk of cyber security. During the underwriting process, insurers may require applicants to assess their vulnerability to attack and help the applicants structure their defenses.

III. CYBER INSURANCE COVERAGE

Cyber insurance policies do not have standard policy forms and do not even have standard names. Generally, the policy provisions are negotiated individually with each applicant. While a number of insurers offer cyber coverage, not all of them insure every type of cyber risk.

Cyber policies may provide both first party and third party insurance, meaning they afford coverage for claims by third parties against the insured and for losses sustained by the insured. Policies may afford coverage in the following areas:

- Lawsuits
- Privacy liability coverage (insured's liability to third parties for disclosure of private information and, in some cases, for the insured's failure to notify affected parties regarding a breach)
- Notification to affected parties (expense associated with notifying third parties that their personal information may have been compromised)

- Call centers
- Credit/identity monitoring
- Regulatory and government actions
- Directors and Officers (D&O) liability
- Transmission of viruses
- Media liability (intellectual property, copyright, trademark, defamation)
- Cyber extortion/ransom (“settlement” with an attacker in exchange for the return of stolen data and hiring a security firm to track down the blackmailer)
- Theft and fraud coverage
- Forensic investigation (to figure out what happened, how to correct it, and how to prevent it in the future)
- Data loss, corruption, and restoration
- Business interruption
- Crisis management (public relations response)

There are a number of issues to be aware of with cyber insurance. Cyber policies typically have different policy limits for the different types of coverage afforded, as well as different deductibles and/or self-insured retentions. There may be, for example, a higher policy limit for data breach liability with lower sublimits for regulatory actions and business interruption. The extortion/ransom coverage may have alternative sublimits in both U.S. dollars and bitcoins.

The policies have other important terms and conditions. For example, notification cost coverage, which affords coverage for notifying third parties that their personal information may have been compromised, often have limits on the number of people to be notified and the method(s) for such notification. Call center coverage may limit the number of people who can use the call center, the hours and location of the call center, and the services the call center will provide. Credit/identity monitoring coverage may limit the number of people for whom service will be provided and may require the insured to use a vendor approved by the insurer. Similarly, crisis management coverage may include a predetermined list of vendors to select from for public relations assistance.

Selection of outside defense counsel is extremely important in the event of an attack. Some policies require that the insurer and insured mutually agree on outside counsel and provide that absent such an

agreement, the insured can choose outside counsel subject to any rate limitations in the policy.

Cyber policies preclude coverage for things that took place prior to the retroactive date, which can in some instances be the inception date of the policy. Since breaches may go undetected for some time, this is an important issue.

Policy language addressing when a policy is triggered is also important. Consider a typical data breach incident. The insured's customers may not know that their information has been breached until the company notifies them. Therefore, the insured may not receive a written demand or lawsuit regarding the breach until after it conducts its forensic investigation and notifies its customers. Some policies are triggered when a loss occurs and others are triggered when a claim is made against the insured. Similarly, policy provisions may specify whether regulatory and other governmental actions must be initiated via a formal "suit" in order to trigger the policy or whether the policy is triggered during the investigative period of such actions. There may be other terms and conditions that determine when a policy applies. For example, business interruption coverage may not kick in until after a network is impaired for a specified period of time.

Coverage may be afforded for the acts or omissions of third parties. This may apply if a company outsources data processing or storage to a third party vendor.

Cyber policies may contain a condition regarding the insured's failure to use reasonable means to avoid security problems. They may also address the location of a security failure by limiting coverage to theft of data from company premises as opposed to theft of, for example, a laptop outside the premises.

Other potential issues include the extent to which coverage is afforded for loss of data on portable and/or unencrypted devices, late notice, and whether the policy excludes coverage for intentional acts of an employee.

Policies may cover some but not all cyber risks. It is fairly standard to include coverage for data breach. It is less common to find coverage for risks such as business email compromise scams, or CEO fraud, in which

a hacker impersonates (electronically) the company CEO and asks that money be transferred to an account controlled by the hacker. Policies may specify the causes of loss to which they apply. For example, a business owners policy may afford coverage for the loss of electronic data damaged or destroyed by a covered cause of loss, which may include a computer virus, malware (harmful code), etc. but may exclude loss or damage caused by the actions of a company employee.

IV. THE FUTURE OF CYBER INSURANCE

Cyber insurance is a rapidly evolving field, with new developments expected in a number of areas. Look for it to be a hot topic for many years.

Policy language will likely become more standardized and could be included within a traditional CGL policy rather than sold as standalone coverage. An increasing number of insurers will likely offer policies that cover a full range of cyber risks rather than focusing more narrowly on data breach. Traditional insurers run the risk that a new “disrupter” will enter the market and control it—this is an area in which a tech startup could potentially excel.

On the underwriting side, expect insurers to continue to help insureds evaluate and improve their cyber security. Insurers may turn to third parties to help determine premiums. For example, QuadMetrics, now owned by FICO, provides an “enterprise security score” for companies analogous to a FICO score that judges a person’s creditworthiness. This helps underwriters set premiums for cyber policies based on a predictive risk analysis. At the same time, it will be interesting to see what litigation arises over the policy condition regarding the insured’s failure to use reasonable means to avoid security problems.

Cyber coverage is often thought of in terms of data breach and other purely “cyber” liabilities. What are the insurance coverage implications, however, if a cyber attack causes bodily injury or property damage traditionally covered by a CGL policy? Consider potential attacks against infrastructure elements such as pipelines, electric grids, or utility safety monitoring systems. Companies will want to make sure they manage risk for bodily injury or property damage caused by a cyber attack.

Individuals may start buying cyber insurance to protect against the personal cyber risks. This coverage could be added to homeowners policies.

Data Breach Bootcamp
F. Marshall Wall
Cranfill Sumner & Hartzog LLP
5420 Wade Park Blvd., Suite 300
Raleigh, NC 27607

The headlines scream at us weekly about the latest data breach at a well-known company. Target, Home Depot, Yahoo, Sony, ChoicePoint, DSW, Anthem – the names are familiar even if the specifics of the events are foggy in our memories. Litigation against the companies whose data was compromised has also made headlines but in many situations has not resulted in victories for the plaintiff's attorneys bringing suit. The tide may be turning, however.

Since an individual consumer's claims will have limited value, most cases involving large-scale data breaches have been filed as class actions and these cases have almost invariably ended up in federal court based on jurisdiction allowed by the Class Action Fairness Act. This paper will examine typical causes of action set forth in these lawsuits and two of the defenses most often asserted against them, as well as the relative success of each. It will also include examples of several recent data breach cases. Most of the issues raised by data breach litigation are state-specific, however, and it is beyond the scope of this paper to address each state's laws.

I. Plaintiffs' Causes of Action

A. Negligence

The elements of negligence are well known: duty, breach, causation and damages. Plaintiffs have typically been successful in pleading a duty owed and breach of that duty. Often the allegation is that the defendant had an obligation to safeguard the plaintiff's personal information and failed to do so. These allegations are rarely challenged.

Most data breach litigation has focused on the last two elements, specifically whether the plaintiffs have sufficiently alleged a causal connection and whether they have pled actual damages.

Standing is a common, and often successful, defense to data breach claims and it is discussed in more detail below. The economic loss rule, also discussed below, has also proven successful as a defense against these claims in some circumstances.

B. Breach of Express Contract

When plaintiffs are cardholders of the named defendant, for example those with a store credit account, patients of a medical practice, or policyholders of a health insurer, plaintiffs will include a claim for breach of express contract. These typically focus on the terms of the cardholder agreement, insurance contract, or privacy notices and any representations made about the way data will be handled. Others rely on pronouncements contained on a company's website, including within its privacy policies, to support a breach of contract claim.

For example, in the *Target* litigation the plaintiffs argued that a statement in their debit card agreement promised that Target would "use security measures that comply with federal law" but failed to do so, resulting in harm to them. *In re Target Corporation Customer Data Security Breach Litigation*, 66 F.Supp.3d 1154, 1177 (D. Minn. 2014). The plaintiffs failed to cite to any federal law with which Target failed to comply, however, and so the claim was dismissed without prejudice, allowing plaintiffs' counsel to attempt to correct this flaw.

General allegations of a breach of contract will not be enough to satisfy pleading requirements under *Twombly* and *Iqbal*; plaintiffs must point to specific contract provisions that were not adhered to and also allege the damages that resulted. Some allegation of the timing of the alleged contract is also required and so, for example, a plaintiff must allege that he received the defendant's privacy notice before the breach occurred.

C. Breach of Implied Contract

Where no express contract exists, a plaintiff may allege an implied contract with the defendant that entitles her to some relief. Conversely when an express contract does exist, by definition there cannot be an implied one and the implied contract claim should be dismissed. Plaintiffs must allege sufficient facts about the implied contract to allow a trier of fact to determine whether in fact the agreement existed and whether it was breached. Contracts may be implied in fact or implied in law.

In the data breach context, plaintiffs typically claim that the breached company impliedly promised to keep their information secure but failed to do so. There must be an offer and acceptance, as well as consideration, and the plaintiffs must allege each element of the purported contract with specificity. Failure to do so has resulted in dismissal of implied contract claims. See *Krottner v. Starbucks Corp.*, 406 Fed.Appx. 129 (9th Cir. 2010).

D. Unjust Enrichment

Unjust enrichment claims typically require that a plaintiff show: “1) the plaintiff has conferred a benefit on the defendant; 2) the defendant has knowledge of the benefit; 3) the defendant has accepted or retained the benefit conferred; and 4) the circumstances are such that it would be inequitable for the defendant to retain the benefit without paying fair value for it.” *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1328 (11th Cir. 2012).

To support an unjust enrichment claim, plaintiffs may argue that they were overcharged for merchandise purchased from retail defendants (“overcharge theory”), that they would not have patronized the retailer at all (“would-not-shop theory”) or that the subscription they purchased did not have the value it would have if their data had been properly protected.

An unjust enrichment claim was asserted against Target relying on the first two theories. The overcharge theory claim was dismissed with prejudice, since Target charged all of its customers the same regardless of whether they used a stored branded card or not. The would-not-shop theory claim survived Target’s motion to dismiss, however, with the court holding that “a reasonable jury could conclude that the money Plaintiffs spent at Target is money ... which Target ‘in equity and good conscience’ should not have received.” *Id.* at 1178.

E. Violation of State Data Breach Notification Statutes

No national data breach notification law exists yet, but 47 states have their own schemes and so larger class actions involving residents of multiple jurisdictions require analysis of the states of residence of the claimants. For example, some states require notification of a breach within a short period after it is discovered, but many mandate notice “without unreasonable delay.” Where a specific deadline is set, the failure to meet it is obviously more likely to provide support for a claim.

Other statutes require proof of some economic harm before a claimant can pursue relief. In a few states, no private right of action is allowed and only the attorney general or other government agency can bring an action. For instance, plaintiffs’ claims premised on a negligence theory for failure to follow the requirements of Indiana’s data breach law were dismissed when the court determined only that state’s Attorney General could enforce the statute. *In re Anthem, Inc. Data Breach Litigation*, 162 F.Supp.3d 953, 977 (N.D. Cal. 2016)

Most state statutes require acquisition of unencrypted data before a security breach is considered to have occurred and notification to

consumers is required. In those states, if data is only viewed but not obtained by a third party, or only encrypted data is obtained by a hacker (and the encryption key is not lost with it), then no notice need be sent and plaintiffs will not have a remedy under the statute.

F. Violation of State Consumer Protection Statutes

Most states have a consumer protection statute prohibiting unfair or deceptive trade practices, often modeled on Section 5 of the Federal Trade Commission Act. Since these statutes often allow exemplary damages and attorneys' fees, they are a popular vehicle for plaintiffs' attorneys to put settlement pressure on defendants.

These statutes often require "actual damages" and this requirement can bar a plaintiff whose claims focus on potential future harm, however likely. See *Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 968-969 (2016) (applying Illinois law).

G. Bailment

Bailment claims have had little success. For example, *In re Target* included a claim based on a bailment theory. After reciting that "[a] bailment is 'the delivery of property for some purpose upon a contract, express or implied, that after the purpose has been fulfilled, the property shall be redelivered to the bailor or otherwise dealt with according to his directions'", the court dismissed this claim as to all plaintiffs with prejudice. *Id.* at 1177 (quoting *Indemnity Ins. Co. of N. Am. v. Hanjin Shipping Co.*, 348 F.3d 628, 637 (7th Cir. 2003)).

The court questioned whether intangible information could qualify for protection under bailment case law but reached its decision based on the fact that the plaintiffs "have not – and cannot – allege that they and Target agreed that Target would return the property to them." *Id.* (citing *Richardson v. DSW, Inc.*, 2005 WL 2978755, at *4 (N.D. Ill. Nov. 3, 2005)). Further, the information in question was stolen by third parties and not unreasonably retained by Target.

II. Defenses

A. Lack of Standing

In many cases the class representatives have difficulty proving damages and their cases have been subject to dismissal due to a lack of Article III standing. This defense was very successful in the early days of data breach litigation and it still remains a potent weapon for defendants,

but its effectiveness seems to be waning. Once a standing defense is asserted, the plaintiff has the burden of showing that standing exists before a case can survive a motion to dismiss.

To have standing, a plaintiff must show that: “(1) it has suffered an ‘injury in fact’ that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.” *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, 528 U.S. 167, 180–81 (2000).

In *Clapper v. Amnesty International USA*, 133 S.Ct. 1138 (2013), the Supreme Court, in a 5-4 decision, gave some clarity to Article III standing issues. It found that the plaintiffs, a group of organizations and individuals working to support human rights around the world, did not have standing to challenge the use of the Foreign Intelligence Surveillance Act to surveil persons outside the United States.

The Court noted that it had “repeatedly reiterated that ‘threatened injury must be certainly impending to constitute injury in fact,’ and that ‘[a]llegations of possible future injury’ are not sufficient.” *Id.* (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)). The plaintiffs’ claims did not meet this standard, focused as they were on the *possibility* that the US intelligence community might intercept their communications in the future. Further, plaintiffs could not sufficiently show that any alleged, potential injury was “fairly traceable” to FISA. Plaintiffs argued that they had incurred expenses in an effort to avoid surveillance of their communications, but the Court also found this insufficient, pointing out that “an enterprising plaintiff would be able to secure a lower standard for Article III standing simply by making an expenditure based on a nonparanoid fear.” *Id.* at 1151.

Circuits have split in analyzing standing issues in data breach cases. For instance, the Ninth Circuit found that a group of plaintiffs had established standing in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (2010). Those plaintiffs were employees of Starbucks whose personal information, including Social Security numbers, names and addresses, were on a laptop that was stolen. While it was apparently undisputed that the personal information was taken, there was no allegation that it had been misused when suit was filed. Since the plaintiffs were at increased risk of harm in the form of future identity theft, however, both the District Court and Ninth Circuit found that standing was present.

No standing existed for a customer of Michael's, the arts and crafts retailer, in a lawsuit resulting from a malware intrusion into the company's computer system. *Whalen v. Michael Stores Inc.*, 153 F.Supp.3d 577 (E.D.N.Y. 2015). The plaintiff made purchases using a credit card at a Michael's store in New York within 30 days before the breach was publicly announced. After the breach was announced, someone in Ecuador tried to use her credit card information to complete two separate transactions, but both were declined and so she suffered no actual loss. The court found that she had suffered no harm by the time the action was filed and the risk of future economic loss was too remote and insufficient to confer standing. *Remijas* was distinguished on the basis that many of the plaintiffs in that action could show that they had suffered fraudulent charges. At the time of this writing, the *Whalen* case was on appeal.

One important issue for standing defenses is when the court will consider them. While most do so by way of a motion to dismiss, others hold that a challenge to standing will only be considered at the class certification stage. Since that often is much farther into the litigation, defendants need to anticipate whether their court will rule on this issue early in the case or withhold its ruling until later.

Where there was evidence that software licensees and subscribers' data was taken, including addresses, credit card numbers and expiration dates was accessed by hackers and subsequently located on the Internet, the plaintiffs had alleged sufficient injury to survive a motion to dismiss for lack of standing. *In re Adobe Systems, Inc. Privacy Litigation*, 66 F.Supp.3d 1197 (N.D. Cal. 2014).

The Third Circuit affirmed dismissal based on a lack of standing in *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011), where the plaintiffs were law firm employees who alleged that the firm's payroll processing firm had suffered a breach. Crucially, however, it was unclear whether their data had been "read, copied, or understood" by the hacker, despite the potential that the information accessed included Social Security numbers and dates of birth. *Id.* at 40. Plaintiffs could point to no misuse of their data before suit was filed. "In data breach cases where no misuse is alleged, however, there has been no injury – indeed, no change in the status quo." *Id.* at 45.

B. Economic Loss Rule

"Under the economic loss doctrine, a plaintiff's tort recovery of economic damages is barred unless such damages are accompanied by some form of physical harm (i.e., personal injury or property damage). Thus, in actions for negligence, liability is limited to damages for physical

injuries and recovery of economic loss is not allowed.” *In re Sony Gaming Networks and Customer Data Security Class Action*, 903 F.Supp.2d 942 (S.D. Cal. 2012).

Also, when the relationship between parties and the duties owed are defined by a contract, then that contract defines their rights and precludes a negligence claim. Generally, a breach of contract does not allow for recovery in tort and so when plaintiffs bring alternative claims for breach of contract and negligence, the latter claims are subject to dismissal.

Several exceptions to the economic loss rule exist, including damage to physical property, but only the “special relationship” between the parties is likely apply in a data breach lawsuit. *In re Sony Gaming*, 903 F.Supp.2d at 961. Six factors determine whether a special relationship exists. These are: “(1) the extent to which the transaction was intended to affect the plaintiff; (2) the foreseeability of harm to the plaintiff; (3) the degree of certainty that the plaintiff suffered injury; (4) the closeness of the connection between the defendant's conduct and the injury suffered; (5) the moral blame attached to the defendant's conduct; and (6) the policy of preventing future harm.” *Id.* (citations omitted). The factors are considered together; none is determinative.

The economic loss defense garnered attention in the consumer class action against Target. *In re Target*, 66 F.Supp.3d 1154 (D. Minn. 2014). Plaintiffs argued that there was an “independent duty” owed by Target or that the case fell within the special relationship exception to the economic loss rule based on their status as cardholders. Since the plaintiffs came from many different jurisdictions, the court assessed the state law applicable to their claims where the parties disagreed about whether that state’s economic loss rule. Ultimately the court dismissed claims made by the plaintiffs from several states but allowed those from others, depending on whether the applicable jurisdiction had case law addressing application of the economic loss rule to a data breach lawsuit. For example, claims of negligence by California, Illinois, and Massachusetts plaintiffs were dismissed while those by plaintiffs from Georgia, New York, and the District of Columbia survived.

III. Recent Case Examples

A consumer class action against Target as a result of its well-publicized data breach in 2013 was countered with a motion to dismiss based on standing. *In re Target Corporation Customer Data Security Breach Litigation*, 66 F.Supp.3d 1154 (D. Minn. 2014). Various customer class actions were filed across the country after the Target breach

became public. These were consolidated by the Judicial Panel on Multidistrict Litigation and assigned to the District Court in Minnesota, the state where Target's headquarters is located. Since the combined case included plaintiffs from many jurisdictions, the court had to sort through various state laws.

Ultimately it dismissed all claims based on a bailment theory, since the plaintiffs could not plausibly allege that Target had taken something from them that would be returned, but allowed most other claims to go forward, although reserving ruling on the standing issue until some discovery had been completed. Those included claims for negligence, breach of express or implied contract, breach of state data breach notification statutes, and violation of state consumer protection statutes.

Among the allegations for breach of these consumer statutes, the plaintiffs claimed that Target had an obligation to disclose that it did not have adequate systems in place to safeguard consumers' personal information. The court found the various allegations of statutory violations sufficient, including this one. This seems to show the court's lack of understanding of the issues in the case. Would consumers have been safer if Target had publicly disclosed deficiencies in its cybersecurity before the breach occurred? Hardly. The contention that Target should have notified customers more quickly after the breach was discovered likely carried more weight, since allegedly Target continued to accept new card applications after the hack was discovered but before it had been fully addressed and contained.

Injunctive relief was sought, including a request that the court require Target to use chip technology and ensure that customers' data was encrypted. Yet again, the court found that the plaintiffs had stated a plausible cause of action for this relief.

A negligence count was also pled. The duty alleged was that Target had an obligation to "timely and accurately disclose" that the plaintiffs' personal information had been or might have been obtained by third parties as a result of the breach. Target did not contest that this duty allegation was sufficient. Arguing against plaintiffs' negligence claim, Target contended first that plaintiffs had alleged no cognizable damages and second that any claims were barred by the economic loss rule. Citing to its discussion of the alleged damages related to other causes of action, the court quickly decided that the damages claimed in the negligence count were also sufficient.

Since many of the plaintiffs were not Target REDCard holders, their allegation was that Target breached an implied contract. Specifically,

these plaintiffs claimed that, in exchange for using their credit or debit cards to purchase merchandise, Target made an implied promise to safeguard their personal information. A similar claim failed in another class action filed against Zappos, the online shoe retailer. *In re Zappos.com, Inc.*, 2013 WL 4830497 at *3 (D.Nev. Sept. 9, 2013). Here, however, the court determined that the existence and terms of any implied contract were for a jury to determine and denied the defendant's motion to dismiss.

In *Galaria v. Nationwide Mutual Ins. Co.*, 2016 WL 4728027 (September 12, 2016 6th Cir.) the plaintiffs claimed that sensitive personal information about them and more than 1,000,000 other Nationwide customers was access during an October 2012 hack of the insurer. The information included individuals' Social Security and driver's license numbers, dates of birth, marital status information, and occupations. Nationwide sent notice to the affected people and offered to provide one year of credit monitoring and identity theft protection of up to \$1,000,000 per individual. The plaintiffs alleged that there existed an international market for personal information about individuals and they were far more likely to be the victims of identity theft than if the Nationwide breach had not occurred. They incurred a loss of time and out-of-pocket expenses in trying to determine whether they suffered identity theft and in trying to minimize the risk of harm.

Plaintiffs asserted four causes of action in *Galaria*: negligence, bailment, violation of the Fair Credit Reporting Act, and invasion of privacy. Nationwide pled a lack of Article III standing and the District Court agreed, dismissing the plaintiffs' claims of negligence and bailment on this basis. The Sixth Circuit reversed, however, finding that the plaintiffs had stated claims for relief. The court noted that "[w]here a data breach targets personal information, a reasonable inference can be drawn that the hackers will use the victims' data for the fraudulent purposes alleged in Plaintiffs' complaints."

The Seventh Circuit has taken a similar tack, allowing a consumer class action against a major retailer to move forward to discovery. In *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015), it reversed dismissal of the case, finding that the plaintiffs had shown sufficient likelihood of harm to survive a motion to dismiss. The plaintiffs held Neiman Marcus store credit or debit cards. In 2013 a hacker infiltrated Neiman Marcus's system and obtained the plaintiff's card numbers. The hack was discovered in December 2013 and notification was sent in January 2014. While payment card data was taken, Neiman Marcus claimed that other personal identifying information, such as Social Security Numbers, was not.

Various causes of action were asserted, including violations of state laws governing data breaches, breach of an implied contract, negligence, unfair business practices, and invasion of privacy. Neiman Marcus moved to dismiss for lack of standing, arguing that it had reimbursed the plaintiffs for any fraudulent charges incurred and so they lack standing since they sustained no other damages. Plaintiffs claimed additional costs, however, as well as the value of lost time addressing the breach. Significant to the Court's decision was that the named plaintiffs were in the group of people whose information had been used by the hackers and they had incurred "identifiable costs associated with the process of sorting things out" *Id.* at 692.

The Court recognized that the more time that passes between the hack and any alleged damage, the more tenuous the causal link. There is an "objectively reasonable" probability that miscreants would use the plaintiffs' data and so they should not have to wait until identity theft was confirmed. Interestingly, the Court presumed that, since the hackers targeted the Neiman Marcus system seeking credit card information, it could be inferred that they planned to use the information for illicit reasons and so harm to the plaintiffs could be inferred. Citing to a report by the GAO, the Court recited that stolen personal information might be used years after its acquisition. "The injuries associated with resolving fraudulent charges and protecting oneself against future identity theft" were enough to satisfy Article III standing, although various other claimed damages were not. *Id.* at 696.

"It is enough at this stage of the litigation that Neiman Marcus admitted that 350,000 cards might have been exposed and that it contacted members of the class to tell them they were at risk. Those admissions and actions by the store adequately raise the plaintiffs' right to relief above the speculative level." *Id.* at 696. By this rationale, any plaintiff who can show that his or her data was exfiltrated or accessed in a hack or other security breach incident is likely to have standing to sue the holder of that data.

IV. Conclusion

After struggling for many years to get data breach class actions past motions to dismiss, plaintiff's attorneys have found greater success recently. Courts have been more receptive to arguments that plaintiffs have suffered injury even without evidence that their identities have been stolen or fraudulent credit card charges have been made.

We can expect this trend to continue as members of the plaintiff's bar uses the "roadmap" provided by cases like *Remijas* to successfully plead this claims. We can also expect to see further Circuit court opinions and perhaps a Supreme Court case further clarifying the standing issues that have provided a key defense to defendants.

Can a Refrigerator Invade Your Privacy? Data Privacy in a Digitally Connected World

Christopher A. Holecek

Wegman, Hessler & Vanderburg

6055 Rockside Woods Blvd., Suite 200

Cleveland, OH 44131

Writer's Biographical Information

Mr. Holecek is a partner at Wegman, Hessler & Vanderburg in Cleveland, OH. He is the Co-Chair of the firm's litigation and cyber security practice groups. Mr. Holecek handles product liability, commercial and employment litigation. He is board-certified by The National Board of Trial Advocacy and has been elected to "Ohio Super Lawyers" every year since 2012.

Introduction

In the 1998 movie *Enemy of the State*, Will Smith starred as a labor lawyer whose career was upended by an out-of-control government surveillance program. *Enemy of the State* (Touchstone Pictures 1998). In the movie, Gene Hackman appeared as a paranoid privacy nut who believed the government was watching everyone. As the movie developed, it turned out that Gene Hackman's character actually was not paranoid and that the government had been tracking the lawyer's movements and purchases. In the end, the paranoid privacy nut was actually right! While the scope of the government's surveillance program in *Enemy of the State* seemed hard to believe when the movie was released in 1998, it no longer seems far-fetched today. And regardless of one's position on Edward Snowden, his 2013 revelations of the government's collection of telephone data, paired with continuing technological breakthroughs, indicate that perhaps the government really can see and hear almost everything. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, The Guardian, June 6, 2013. Indeed, even the FBI Director, James Comey, recently admitted that he puts tape over his laptop's webcam as a "common sense" precaution and recommends others do the same. Julian Hattem, *FBI Director: Cover Up Your Webcam*, The Hill, Aug. 14, 2016.

But even outside of the government's sphere, potential intrusions on privacy are evident. Most of us engage in e-commerce on a regular basis. We hand over personal identifying information about ourselves, including

our names, date of birth, Social Security and credit card numbers to complete strangers in exchange for a product or a service. We also allow large internet companies, such as Google and Facebook, to collect our data so that they can generate personalized ads for us. See Privacy, *Your Data: We Want You to Understand what Data we Collect and Use*, Google.com, available at <https://privacy.google.com/your-data.html>. Despite revelations of potential privacy intrusion, e-commerce continues to flourish. Why? Because consumers trust that companies will safeguard their personal information. But when this trust is breached, privacy lawsuits follow.

Protecting private data is obviously a challenging and daunting task. Not only are potential hackers, including their equipment, becoming more sophisticated, but the sheer amount of personal data that is collected and stored is staggering. Hayley Tsukayama, *Hackers are Getting Better at Offense. Companies Aren't Getting Better at Defense*. The Washington Post, Apr. 22. A Federal Trade Commission ("FTC") Staff Report estimates that fewer than 10,000 households using devices connected to the Internet can generate 150 million discreet data points each day. *Federal Trade Commission Staff Report on the November 2013 Workshop Entitled: The Internet of Things: Privacy Security in a Connected World*, FTC, Jan. 27, 2015, at p. 14. When you multiply that number by the 286,942,362 people in the United States who are internet users, the number of data points per day is astronomical. Internet World Stats, *North America*, available at <http://www.internetworldstats.com/america.htm#us>. At the same time, three out of four Americans say that it is "very important" that they be in control of *who* can get information about them. Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW Research Center, Sept. 21, 2016.

Not surprising, the law regarding privacy concerns created through the new Internet Age is unsettled. And it will certainly evolve as technology changes. Congress, states and courts will create new, or expand old, causes of action. As a result, attorneys who handle privacy suits will need to understand and be conversant in the language of cyber technology. To that end, when privacy lawsuits arise attorneys will need to recognize that they are defending a different type of tort, one predicated not on a tangible bodily injury but upon a breach of trust: a consumer handed over personal information with the expectation that it would be safeguarded and it wasn't. It is not surprising, therefore, that privacy plaintiffs feel betrayed when their data is either misused or falls into the hands of cyber criminals. Ignoring the emotional component of the case is risky and may interfere with your client's ability to resolve the case early and on favorable terms. Very simply, if

consumer trust is the lifeblood of our retail clients, then we must assist our clients in repairing that trust during all phases of the litigation.

1. The Internet of Things: Will there still be privacy?

One of the more interesting areas of technological advancement and privacy concerns relate to the “Internet of Things.” The “Internet of Things” is a term that describes the ability for everyday devices such as refrigerators, thermostats, and cars to connect to the Internet. Nicole Kobie, *What is the Internet of Things?*, The Guardian, May 6, 2015. The 2015 FTC Report cited estimates that 26 billion connected devices will be available by 2020. *Federal Trade Commission Staff Report on the November 2013 Workshop Entitled: The Internet of Things: Privacy Security in a Connected World*, FTC, Jan. 27, 2015, at p. 14. But even today, many common household devices connect to the Internet. For example, washing machines from General Electric can be started and monitored via cell phones, refrigerators from LG are equipped with cameras that can text a picture of what’s inside while the owner is grocery shopping, Fitbit devices monitor your health by tracking your heart rate, sleeping patterns, and blood pressure, and thermostats, light switches, and door locks can be managed through apps. And that is just the beginning! See, Keith Barry and Mike Roorda, *Text this LG Fridge, and it Will Send You a Selfie: Use Your Phone to Check What’s In Your Fridge*, Reviewed.com, Sept. 4, 2014; General Electric, *GE Wifi Connect Homepage*, available at <http://www.geappliances.com/ge/connected-appliances/>.

Advancements in the Internet of Things will continue to grow and make our lives more convenient. But these devices can also create an exponential number of entry points for cyber criminals. In the past, hackers could only access your information through computers. Now, sophisticated hackers can gain access to an entire network through poorly protected smart devices. For example, the much publicized Target data breach that impacted millions of Target’s customers in 2015 was not an “inside” job. Danny Yadron and Paul Ziobro, *Before Target, They Hacked the Heating Guy*, The Wall Street Journal, Feb. 5, 2014. Instead, the intrusion occurred through an HVAC subcontractor who had worked at various Target stores. *Id.* Because Target’s subcontractor system was connected to the Internet, cyber criminals were able to use that system as an entry point into Target’s entire network.

2. Other Privacy Concerns with the Internet of Things

Despite their convenience, connected devices also create public profiles containing their owner's personal information. For instance, the "Smart Refrigerator" collects data about the type and amount of food purchased and consumed, and the Fitbit collects data on one's heart rate, weight, and exercise information. Hunter Walker, *Senator Warns Fitbit Is A 'Privacy Nightmare' And Could Be 'Tracking' Your Movements*, Business Insider, Aug. 10, 2014. Further, a connected car tracks how fast one drives, when and how much one drives, and the number of "hard brakes" one makes. See *Frequently Asked Questions About Snapshot*, Progressive.com, available at <https://www.progressive.com/auto/snapshot-common-questions/>.

But who owns all the data collected by these connected devices? It would seem that the owner of the device owns the data. Manufacturers and sellers, however, believe they own the data from and about the consumer. Manufacturers utilize the data to better market their products and have monetized this data by selling it to advertisers. Yet the desires of the manufacturers is at odds with the wishes of consumers. A recent PEW survey, for instance, found that most Americans struggle to understand the nature and scope of the data collected about them and three out of four Americans say it is "very important" to control what type of information is collected about them. *The State of Privacy in Post-Snowden America*, PEW Research Center, Sept. 21, 2016. Despite confusion as to what data is being collected, most people recognize that the data collected from and about them has the potential to be misused.

For example, private data collected from connected or "smart" devices can be used for both beneficial and harmful purposes. A conscientious person who exercises and eats well could be a good candidate for employment, and a good driver should be entitled to better insurance rates. But what happens if an employment, credit, or insurance decision is made using the consumer's data without that person's consent and/or without the decision maker taking steps to ensure that the data is accurate?

At first blush it would seem that the Fair Credit Reporting Act ("FCRA") would govern the use of data collected from "smart" devices. The FCRA imposes obligations on employers, lenders, and insurers to take measures to ensure maximum possible accuracy of consumer data and gives consumers an opportunity to correct erroneous data. 15 USC § 1681 et seq. But the FCRA safeguards do not seem to cover instances where manufacturers *directly* collect the data from the consumer. Therefore, it would seem that when companies make employment, credit and insurance

decisions from data collected directly from connected devices, they do not need to give consumers access to the information they rely on, or give consumers an opportunity to correct errors in the data as required by the FCRA.

A majority of Americans, according to a recent PEW survey, favor additional legal protections against abuses of their private data. *The State of Privacy in Post-Snowden America*, PEW Research Center, Sept. 21, 2016. Therefore, it seems the public will eventually demand that laws be enacted offering similar FCRA type protections when a consumer's private data is collected from connected devices and is then used for employment, credit and insurance purposes.

3. Recent Decisions on Privacy Litigation

In addition to new legislation, courts have been interpreting current law to cover privacy violations that were previously not allowed. For example, the Sixth Circuit has recently given aggrieved consumers a potential way to sue companies for losing customer data. *Galleria v. Nationwide Mut. Ins. Co.*, No. 15-3386/3387, 2016 U.S. App. LEXIS 16840 (6th Cir. Sept. 12, 2016). In 2012, cyber criminals accessed Nationwide's network obtaining private information of 1.1 million Nationwide customers and potential customers. *Id.* These cyber criminals obtained names, Social Security and drivers' license numbers, dates of birth and other private information. *Id.* The customers whose information had been stolen brought suit against Nationwide as a class action in *Galleria v. Nationwide*. *Id.* In that case, the U.S. District Court for the Northern District of Ohio dismissed the suit finding that there was no Article III standing because the Plaintiffs could not establish a concrete injury under *Clapper* to support their invasion of privacy claims. *Id.*

But on appeal, the Sixth Circuit, in a 2 to 1 decision, reversed the district court, holding that it would be unreasonable to expect the Plaintiffs to wait for third parties to actually misuse their data before bringing suit. *Id.* After all, why would cyber criminals steal the data unless they were going to use it? *Id.* The Sixth Circuit, thus, held that Plaintiffs could maintain an action against Nationwide before the stolen data had actually been misused. *Id.*

Galleria seems to demonstrate how privacy plaintiffs can make a "substantial risk of harm" showing even where the full potential of a data breach had not yet been realized. It is too early to tell, however, what impact (if any) this decision will have on data breach litigation. Presently, the case has not been scheduled for trial so the ultimate outcome against Nationwide remains unknown. However, this case is certainly worth monitoring.

4. Defending Privacy Suits

As defense lawyers, it is important to recognize that data privacy law is, as reflected in the *Galaria* decision, constantly evolving. As indicated, we must recognize that a privacy lawsuit concerns a breach of trust. A plaintiff feels betrayed because his or her private information was handed over to a company believing that it would be safeguarded at all times. The plaintiff is also upset because he or she lost control over their private information.

In assessing damages in a privacy lawsuit, we need to be mindful that unlike bodily injury cases, quantifying the harm is more challenging. Because we are dealing with litigants who are angry, hurt, or even embarrassed that their trust has been violated, we cannot underestimate the emotional component of the claim. And we cannot assume a settlement will be low just because there is no direct financial harm to the plaintiff. We must also be mindful of the reputational damage to our clients, especially in a publicized data breach.

Moreover, taking privacy suits to trial poses risks regardless of the plaintiff. Counsel must not assume juries will take it “easy” on a defendant if the invasion of privacy concerns “bad” people or “sleazy” behavior. For instance, Terry G. Bollea, commonly known as “Hulk Hogan”, was awarded \$115 million by a jury after Gawker.com published a 2012 sex tape involving Bollea and the wife of one of his associates. Gawker’s founder ultimately filed for Chapter 11 Bankruptcy protection after the crippling verdict. Sydney Ember, *Gawker, Filing for Bankruptcy After Hulk Hogan Suit, Is for Sale*, The New York Times, June 10, 2016.

5. Conclusion.

Privacy law is unsettled. In a connected world, it is generally understood that the “right to be left alone” is impractical. But most Americans view privacy as the right to control their identity and any information about them. *The State of Privacy in Post-Snowden America*, PEW Research Center, Sept. 21, 2016. Undoubtedly, new and different forms of harm will evolve and be created. Counsel who defend privacy suits, and companies who process consumers’ private information, need to understand and be conversant in cyber technology and the laws regulating this area.

Technology for Lawyers: What is my Ethical Duty and What Do I Need to Know?

Stephen E. Embry
Frost Brown Todd LLC
400 West Market Street, Suite 3200
Louisville, Kentucky 40202-3363

Stephen is a member of Frost Brown Todd LLC and is a member of the firm's Class action, Privacy and Mass Tort groups. He frequently defends participants in consumer class actions and mass tort litigation. Stephen is a national litigator and advisor who is experienced in developing solutions to complex litigation and corporate problems. He is the former chair of Frost Brown Todd's mass tort practice group. Stephen is also a member of fbtTECH, the firm's technology industry group that focuses on the future and anticipating the ways in which technology will impact the legal system and the issues facing clients. He writes frequently on issues of technology and its impact on the practice of law.

Introduction

Much has been written about the need for lawyers to have at least core competency in technology. While many lawyers prefer to adopt the ostrich approach and stick their heads in the proverbial sand ("I have people that know about that. I don't need to know anything"), such an approach is likely to lead to trouble and may not satisfy ethical obligations.

Like it or not, technology is a part of our everyday practice. Email. E-discovery. The cloud. Practice management. Social media and discovery, and its use and impact on such things as jury selection. The dangers that some forms of particular technologies and their use pose for our duty to maintain confidences. The list goes on and on.

Technology plays an ever-expanding role in our daily life and practice and we have to be able to at least spot issues. One only must consider the [recent hack](#) at a Panamanian law firm to see there are significant threats to clients' privacy and confidences on an ongoing basis.

And like it or not, our clients and the public more and more expect and demand some knowledge of technology risks and benefits from their lawyers. Failure to be knowledgeable enough to at least see issues and pitfalls and adequately supervise projects and cases where technology is being used or is in issue could lead to some unwelcome results and frustrations.

And finally, perhaps to state the obvious given the above, fundamental technological proficiency is something you likely owe your client: both generally, morally and ethically. Technology issues are so ingrained in everything we all do that in most matters they just can't be completely delegated to others. It's a matter of competence, protecting your client and living up to expectations. While you may not have to be tech geek, lawyers do need some working knowledge of technology to be able to ask the right questions and spot issues. And this duty is more and more being recognized by State Bar Associations.

Comment 8 to Model Rule 1.1

In 2009, the American Bar Association created the [Ethics 20/20 Commission](#) to examine in depth how changes in technology might affect the ABA Model Rules of Professional Conduct. The Commission made many recommendations; most notably, it provided additional comments to Rule 1.1 regarding lawyer competence.

In August, 2012, the ABA House of Delegates passed several amendments to the Model Rules of Professional Conduct recommended by the [Commission](#) including [Comment 8 to Rule 1.1](#).

Rule 1.1 provides:

Client-Lawyer Relationship **Rule 1.1 Competence**

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment 8 provides:

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Id. Emphasis added.

Certainly, the Model Rules are just that — a model. By design, they provide guidance to the states in formulating their own rules of

professional conduct: each state is free to adopt, reject, ignore or modify the Model Rules. **Almost all states** have adopted the Model Rule 1.1, however.

To date, some 26 states have also adopted Comment 8. They are:

- o Arizona, **effective Jan. 1, 2015**.
- o Arkansas, **approved June 26, 2014**, effective immediately.
- o Colorado, **approved April 6, 2016**.
- o Connecticut, **approved June 14, 2013**, effective Jan 2014.
- o Delaware, **approved Jan. 15, 2013**, effective March 1, 2013.
- o Florida, **approved Sept. 29, 2016**, effective Jan. 1, 2017.
- o Idaho, **approved March 17, 2014**, effective July 1, 2014.
- o Illinois, **approved Oct. 15, 2015**, effective Jan. 1, 2016.
- o Iowa, **approved Oct. 15, 2015**, effective Oct. 15, 2015.
- o Kansas, **approved Jan. 29, 2014**, effective March 1, 2014.
- o Massachusetts, **approved March 27, 2015**, effective July 1, 2015.
- o Minnesota, **approved Feb. 24, 2015**.
- o New Hampshire, **approved Nov. 10, 2015**, effective Jan. 1, 2016.
- o New Mexico, **approved Nov. 1, 2013 (text of approved rules)**, effective Dec. 31, 2013.
- o New York, **adopted on March 28, 2015**, by the New York State Bar Association.
- o North Carolina, **approved July 25, 2014**. Note that the phrase adopted by N.C. varies slightly from the Model Rule: "... including the benefits and risks associated with the technology relevant to the lawyer's practice."
- o **North Dakota**, approved Dec. 9, 2015, effective March 1, 2016.
- o Ohio, **approved Feb. 14, 2015**, effective April 1, 2015.
- o Oklahoma, **approved Sept. 19, 2016**, effective immediately.
- o Pennsylvania, **approved Oct. 22, 2013 (text of approved rules)**, effective 30 days later.
- o Utah, **adopted March 3, 2015**, effective May 1, 2015.
- o Virginia, **approved Dec. 17, 2015**, effective March 1, 2016.
- o Washington, **approved June 2, 2016**, effective Sept. 1, 2016.
- o West Virginia, **approved Sept. 29, 2014**, effective Jan. 1, 2015.
- o Wisconsin, **approved July 21, 2016**, effective Jan. 1, 2017.
- o Wyoming, **approved Aug. 5, 2014**, effective Oct. 6, 2014.

Florida has not only adopted the Comment but now requires attorneys to participate in at least 3 hours of CLE devoted to technology

competence and issues annually. [According to the Florida Supreme Court](#), members of the Florida bar are now required to take 3 CLE credit hours per year on technology-related topics. Significantly, some [ethical commentators](#) believe the requirement appears to put attorneys on notice that they risk malpractice if they fail to competently navigate technology-related issues, such as properly safeguarding confidential electronic communications or not engaging technical advisers when necessary. (Indeed the well known tech and class action plaintiffs firm [Edelson PC](#), filed [a class action](#) against a large Chicago law firm alleging that the firm was negligent and engaged in malpractice by allowing security vulnerabilities to develop that posed security risks to clients).

Some other states, while not having formally adopted the change to their rules of professional conduct, have nonetheless acknowledged a duty of lawyers to be competent in technology. For example, the New Hampshire Bar Association, in [Advisory Opinion #2012-13/4](#) concerning cloud computing, [said](#) in language similar to Comment 8:

Competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes.”

In Delaware, the Supreme Court set up its own [Commission on Law & Technology](#) in 2013 for the purpose of issuing guidance on the use of technology in the practice of law. The guidance issued so far includes Leading Practice papers on multiple computing subjects, including “Basic Skills.” The Commission makes the rather obvious and yet extremely important comment in the Basic Skills paper that “it is impossible to practice law in Delaware today, or even to become a lawyer, without a basic understanding of how to use technology.”

That is exactly the point. A lawyer must have some basic skills on technology in order to get by.

Other states have also codified rules regarding the protection of client data and electronic communications stored on law firm servers. [Connecticut, for example](#), considers a number of factors in determining whether a lawyer has made reasonable efforts to prevent unauthorized access to client documents and communications, such as the nature, complexity and cost of various technical safeguards the attorney and his or her firm used. This requirement, at the very least, demands that attorneys have knowledge of the kinds of software appropriate for encrypting and protecting client data, and be able to either implement this software or find an expert who can.

Even jurisdictions that have not adopted technical competency requirements have also cautioned attorneys to focus on eDiscovery and client data protection best practices. While the [District of Columbia's Bar Association](#), for example, has only addressed technological competency issues involving metadata, it has also stated that attorneys should be able to sufficiently understand whatever software their firms use to properly protect client data.

The California Opinion

Perhaps one of the best and thorough opinions concerning the need for lawyers to have baseline technology competency came recently from the California Bar Association. Although California has not adopted Comment 8 and the Opinion did not directly focus on the Comment, the Opinion clearly articulates that technological competence is an expectation and what the parameters of that expectations are. See [Formal Opinion No. 2015-193](#).

Citing Comment 8, the Californai Bar Association stated

Legal rules and procedures, when placed alongside ever-changing technology, produce professional challenges that attorneys must meet to remain competent. Maintaining learning and skill consistent with an attorney's duty of competence includes keeping "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, . . ." ABA Model Rule 1.1, Comment [8]...

Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI")."

Not every litigated case involves e-discovery. Yet, in today's technological world, almost every litigation matter *potentially* does.

And:

Depending on the factual circumstances, a lack of technological knowledge in handling e-discovery may render an attorney ethically incompetent to handle certain litigation matters involving e-discovery, absent curative assistance under rule 3-110(C), even where the attorney may otherwise be highly experienced. It also may result in violations of the duty of confidentiality, notwithstanding a lack of bad faith conduct.

The Opinion recognizes that where an attorney lacks sufficient capability, they can effectively “contract out” the necessary competence to someone else. That someone else could be another attorney in a firm, an outside attorney, a vendor or even your client, the opinion says, provided the person has the necessary expertise. Not surprisingly, according to the Opinion, lawyer cannot, however, contract out the duty to supervise the case and protect client confidentiality. The lead lawyer remains the captain of the ship.

According to the California Association, the specific tasks that attorneys need to either possess an understanding of, or retain an experienced lawyer or non-lawyer technology expert who does, include:

- Initially assessing e-discovery needs and issues,
- Implementing or causing to implement appropriate ESI preservation procedures,
- Analyzing and understanding a client’s ESI systems and storage,
- Advising the client on available options for the collection and preservation of ESI,
- Identifying custodians of potentially relevant ESI,
- Adequately conferring with opposing counsel on managing eDiscovery plans,
- Performing data searches,
- Collecting responsive ESI in a manner that preserves the integrity of that ESI, and producing non-privileged ESI in a recognized and appropriate manner.

The opinion also recognizes “Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney’s duty of confidentiality.”

So perhaps the biggest take away from this Opinion may be that even in a state that has not formally adopted Comment 8, there is ethical support for requiring some technological competence by lawyers.

For a good analysis of the Opinion see recent [Redgrave Analysis](#).

What Does the Comment Really Do?

Comment 8 certainly reflects the ABA’s view and desire to give lawyers a subtle push when it comes to technology; according to the [Report](#) accompanying the proposal:

The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain

aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.

In other words, the **ABA's position** seems to be that Rule 1.1 does not actually impose any new obligations on lawyers but simply reiterates the obvious: in order for lawyers to adequately practice and be competent under the Rules in today's world, they need to understand the technological tools by which they can zealously advocate for and protect their clients. *Id.*

It should also be noted that the ABA used the word "should" in its revised language, rather than the words "shall" or "will," which are normally used to express a duty. Furthermore, the rule does not outline what technology skills a lawyer should actually know in order to provide competent representation.

Finally, the Comment requires nothing in specific and is directed toward technology that is "relevant". If you don't have a practice that touches Twitter, for example, the Comment does not necessarily require you to know much about it. But where technology touches an attorney's practice, that attorney needs to have some level of competence.

Putting all this together, it seems clear that the Model Comment does not appear to contemplate attorneys getting the technical proficiency of a software engineer or any place close. Instead, somewhat like the California Bar Association concluded, it seems to contemplate that lawyers should at least be able to spot potential issues—the benefits and risks—of the technology that impacts attorneys every day. The **ABA** wants basic understanding: we need not know everything. We do need to know some things.

So on the one hand, it's easy to conclude that nothing has really changed and the Comment adds little duties that already exist. On the other hand, **some commentators** have concluded that by merely having the recommendations/duty in writing a sea change has occurred. Either way, I don't think lawyers can safely ignore technology and be ignorant.

What Can I Do?

Exactly *what* technology do lawyers need to understand? If a lawyer lacks a solid grounding in technology to begin with, how can he or she be expected to know which topics are important? How do lawyers interested in learning more about technology filter out the geek hype,

vendor sales pitches and general misinformation to get to the real information they need?

Courtesy of [Josh Poje of the American Bar Association's Law Practice Division](#), below are five simple strategies to help lawyers develop and maintain the expected and minimum understanding of relevant technology.

First, it's easy to get overwhelmed by the technology and technology information that's out there. And the constant development of new technology happens at an dizzying pace and can quickly cause lawyers to turn away under the theory that they can never master the issues so why try? Instead, I Josh believes lawyers should ask some fundamental questions about any technology they come in contact with:

When scanning through the latest technology news, always ask yourself: *Is this relevant to my practice?* Or perhaps more directly: *Can this technology help me be a better lawyer?* In the end, your objective is to provide exceptional representation to your clients or employer, and the technology you'll want to explore and understand is the technology that will help you achieve that goal.

Id.

Second, make it a point to pick out a good technology blog or other source of information and scan at least the headlines. This will at least keep you conversant with major trends and issues. Some good sources are [Bob Ambrogi's LawSites blog](#), [the Kennedy-Mighell Podcast](#), [Ars Technica](#), [ZDNet](#), [The Verge](#), [David Pogue](#), [Wired](#).

Third, we all know lawyers or other legal professionals that are tech geeks. Talk to them: you can learn a lot just by chatting with those who have an interest in the subject and is keeping relatively up-to-date. Don't be afraid to ask the stupid question-its probably not as stupid as you think. (And unless you are truly a geek yourself, the geeks will probably think whatever question you ask is stupid, anyway). Use more formal means to engage your peers to share knowledge about software, hardware and other technology tools. Get involved in email discussion lists, bar networking events, alumni meetings, and even simple conversations in the hallways outside the courtroom.

Fourth, discuss issues with experts. Most consultants are all too happy to share their thoughts, opinions and predictions. Often, if you or

your firm has an expert it uses for technology related issues, they will talk to you for free. If not, buying an hour or two of their time to talk about the trends, risks and opportunities he or she sees in the tech world is a good investment. These kinds of discussions may not make you a tech expert, but it will help you understand the landscape.

Fifth, contact your state Bar Association and the ABA. Many state Bars offer guidance on practice management issues, including the use of technology. This guidance is often easy to obtain and tends to be free. It also is more neutral and free of the vendor bias. It's often written specifically for lawyers, in many cases *by* lawyers. And some state and bars have practice management advisers available to answer technology questions. The ABA also has excellent guides and helpful information. See the ABA Legal Technology Resource Center, the [Law Technology Today](#) blog, the [ABA Law Practice Management Section](#), and [ABA TECHSHOW](#).

Conclusion: What's the So What?

So you may ask, what's all this mean to me? As my friend and one of the most astute observers of the legal landscape, [Bob Ambrogi](#), so well put it:

What does all this mean to you? It is simple. You cannot assess the benefits and risks associated with various kinds of technology if you know nothing about the technology. Even if your state has yet to adopt this change, it is only a matter of time before it does. Don't be a Luddite who fears or resists technology. Neither do you have to become a geek. Make an effort to understand the basics of the technology you use. Get on social media, if you're not already. Ask questions. Learn. When it comes to technology, there is no more burying your head in the sand.

Technology for Lawyers: What is my Ethical Duty and What Do I Need to Know?

Stephen E. Embry
Frost Brown Todd LLC
400 West Market Street, Suite 3200
Louisville, Kentucky 40202-3363

Stephen is a member of Frost Brown Todd LLC and is a member of the firm's Class action, Privacy and Mass Tort groups. He frequently defends participants in consumer class actions and mass tort litigation. Stephen is a national litigator and advisor who is experienced in developing solutions to complex litigation and corporate problems. He is the former chair of Frost Brown Todd's mass tort practice group. Stephen is also a member of fbtTECH, the firm's technology industry group that focuses on the future and anticipating the ways in which technology will impact the legal system and the issues facing clients. He writes frequently on issues of technology and its impact on the practice of law.

Introduction

Much has been written about the need for lawyers to have at least core competency in technology. While many lawyers prefer to adopt the ostrich approach and stick their heads in the proverbial sand ("I have people that know about that. I don't need to know anything"), such an approach is likely to lead to trouble and may not satisfy ethical obligations.

Like it or not, technology is a part of our everyday practice. Email. E-discovery. The cloud. Practice management. Social media and discovery, and its use and impact on such things as jury selection. The dangers that some forms of particular technologies and their use pose for our duty to maintain confidences. The list goes on and on.

Technology plays an ever-expanding role in our daily life and practice and we have to be able to at least spot issues. One only must consider the [recent hack](#) at a Panamanian law firm to see there are significant threats to clients' privacy and confidences on an ongoing basis.

And like it or not, our clients and the public more and more expect and demand some knowledge of technology risks and benefits from their lawyers. Failure to be knowledgeable enough to at least see issues and pitfalls and adequately supervise projects and cases where technology is being used or is in issue could lead to some unwelcome results and frustrations.

And finally, perhaps to state the obvious given the above, fundamental technological proficiency is something you likely owe your client: both generally, morally and ethically. Technology issues are so ingrained in everything we all do that in most matters they just can't be completely delegated to others. It's a matter of competence, protecting your client and living up to expectations. While you may not have to be tech geek, lawyers do need some working knowledge of technology to be able to ask the right questions and spot issues. And this duty is more and more being recognized by State Bar Associations.

Comment 8 to Model Rule 1.1

In 2009, the American Bar Association created the [Ethics 20/20 Commission](#) to examine in depth how changes in technology might affect the ABA Model Rules of Professional Conduct. The Commission made many recommendations; most notably, it provided additional comments to Rule 1.1 regarding lawyer competence.

In August, 2012, the ABA House of Delegates passed several amendments to the Model Rules of Professional Conduct recommended by the [Commission](#) including [Comment 8 to Rule 1.1](#).

Rule 1.1 provides:

Client-Lawyer Relationship **Rule 1.1 Competence**

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment 8 provides:

Maintaining Competence

[8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, **including the benefits and risks associated with relevant technology**, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

Id. Emphasis added.

Certainly, the Model Rules are just that — a model. By design, they provide guidance to the states in formulating their own rules of

professional conduct: each state is free to adopt, reject, ignore or modify the Model Rules. **Almost all states** have adopted the Model Rule 1.1, however.

To date, some 26 states have also adopted Comment 8. They are:

- o Arizona, **effective Jan. 1, 2015**.
- o Arkansas, **approved June 26, 2014**, effective immediately.
- o Colorado, **approved April 6, 2016**.
- o Connecticut, **approved June 14, 2013**, effective Jan 2014.
- o Delaware, **approved Jan. 15, 2013**, effective March 1, 2013.
- o Florida, **approved Sept. 29, 2016**, effective Jan. 1, 2017.
- o Idaho, **approved March 17, 2014**, effective July 1, 2014.
- o Illinois, **approved Oct. 15, 2015**, effective Jan. 1, 2016.
- o Iowa, **approved Oct. 15, 2015**, effective Oct. 15, 2015.
- o Kansas, **approved Jan. 29, 2014**, effective March 1, 2014.
- o Massachusetts, **approved March 27, 2015**, effective July 1, 2015.
- o Minnesota, **approved Feb. 24, 2015**.
- o New Hampshire, **approved Nov. 10, 2015**, effective Jan. 1, 2016.
- o New Mexico, **approved Nov. 1, 2013 (text of approved rules)**, effective Dec. 31, 2013.
- o New York, **adopted on March 28, 2015**, by the New York State Bar Association.
- o North Carolina, **approved July 25, 2014**. Note that the phrase adopted by N.C. varies slightly from the Model Rule: "... including the benefits and risks associated with the technology relevant to the lawyer's practice."
- o **North Dakota**, approved Dec. 9, 2015, effective March 1, 2016.
- o Ohio, **approved Feb. 14, 2015**, effective April 1, 2015.
- o Oklahoma, **approved Sept. 19, 2016**, effective immediately.
- o Pennsylvania, **approved Oct. 22, 2013 (text of approved rules)**, effective 30 days later.
- o Utah, **adopted March 3, 2015**, effective May 1, 2015.
- o Virginia, **approved Dec. 17, 2015**, effective March 1, 2016.
- o Washington, **approved June 2, 2016**, effective Sept. 1, 2016.
- o West Virginia, **approved Sept. 29, 2014**, effective Jan. 1, 2015.
- o Wisconsin, **approved July 21, 2016**, effective Jan. 1, 2017.
- o Wyoming, **approved Aug. 5, 2014**, effective Oct. 6, 2014.

Florida has not only adopted the Comment but now requires attorneys to participate in at least 3 hours of CLE devoted to technology

competence and issues annually. [According to the Florida Supreme Court](#), members of the Florida bar are now required to take 3 CLE credit hours per year on technology-related topics. Significantly, some [ethical commentators](#) believe the requirement appears to put attorneys on notice that they risk malpractice if they fail to competently navigate technology-related issues, such as properly safeguarding confidential electronic communications or not engaging technical advisers when necessary. (Indeed the well known tech and class action plaintiffs firm [Edelson PC](#), filed [a class action](#) against a large Chicago law firm alleging that the firm was negligent and engaged in malpractice by allowing security vulnerabilities to develop that posed security risks to clients).

Some other states, while not having formally adopted the change to their rules of professional conduct, have nonetheless acknowledged a duty of lawyers to be competent in technology. For example, the New Hampshire Bar Association, in [Advisory Opinion #2012-13/4](#) concerning cloud computing, [said](#) in language similar to Comment 8:

Competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes.”

In Delaware, the Supreme Court set up its own [Commission on Law & Technology](#) in 2013 for the purpose of issuing guidance on the use of technology in the practice of law. The guidance issued so far includes Leading Practice papers on multiple computing subjects, including “Basic Skills.” The Commission makes the rather obvious and yet extremely important comment in the Basic Skills paper that “it is impossible to practice law in Delaware today, or even to become a lawyer, without a basic understanding of how to use technology.”

That is exactly the point. A lawyer must have some basic skills on technology in order to get by.

Other states have also codified rules regarding the protection of client data and electronic communications stored on law firm servers. [Connecticut, for example](#), considers a number of factors in determining whether a lawyer has made reasonable efforts to prevent unauthorized access to client documents and communications, such as the nature, complexity and cost of various technical safeguards the attorney and his or her firm used. This requirement, at the very least, demands that attorneys have knowledge of the kinds of software appropriate for encrypting and protecting client data, and be able to either implement this software or find an expert who can.

Even jurisdictions that have not adopted technical competency requirements have also cautioned attorneys to focus on eDiscovery and client data protection best practices. While the [District of Columbia's Bar Association](#), for example, has only addressed technological competency issues involving metadata, it has also stated that attorneys should be able to sufficiently understand whatever software their firms use to properly protect client data.

The California Opinion

Perhaps one of the best and thorough opinions concerning the need for lawyers to have baseline technology competency came recently from the California Bar Association. Although California has not adopted Comment 8 and the Opinion did not directly focus on the Comment, the Opinion clearly articulates that technological competence is an expectation and what the parameters of that expectations are. See [Formal Opinion No. 2015-193](#).

Citing Comment 8, the Californai Bar Association stated

Legal rules and procedures, when placed alongside ever-changing technology, produce professional challenges that attorneys must meet to remain competent. Maintaining learning and skill consistent with an attorney's duty of competence includes keeping "abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, . . ." ABA Model Rule 1.1, Comment [8]...

Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI")."

Not every litigated case involves e-discovery. Yet, in today's technological world, almost every litigation matter *potentially* does.

And:

Depending on the factual circumstances, a lack of technological knowledge in handling e-discovery may render an attorney ethically incompetent to handle certain litigation matters involving e-discovery, absent curative assistance under rule 3-110(C), even where the attorney may otherwise be highly experienced. It also may result in violations of the duty of confidentiality, notwithstanding a lack of bad faith conduct.

The Opinion recognizes that where an attorney lacks sufficient capability, they can effectively “contract out” the necessary competence to someone else. That someone else could be another attorney in a firm, an outside attorney, a vendor or even your client, the opinion says, provided the person has the necessary expertise. Not surprisingly, according to the Opinion, lawyer cannot, however, contract out the duty to supervise the case and protect client confidentiality. The lead lawyer remains the captain of the ship.

According to the California Association, the specific tasks that attorneys need to either possess an understanding of, or retain an experienced lawyer or non-lawyer technology expert who does, include:

- Initially assessing e-discovery needs and issues,
- Implementing or causing to implement appropriate ESI preservation procedures,
- Analyzing and understanding a client’s ESI systems and storage,
- Advising the client on available options for the collection and preservation of ESI,
- Identifying custodians of potentially relevant ESI,
- Adequately conferring with opposing counsel on managing eDiscovery plans,
- Performing data searches,
- Collecting responsive ESI in a manner that preserves the integrity of that ESI, and producing non-privileged ESI in a recognized and appropriate manner.

The opinion also recognizes “Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney’s duty of confidentiality.”

So perhaps the biggest take away from this Opinion may be that even in a state that has not formally adopted Comment 8, there is ethical support for requiring some technological competence by lawyers.

For a good analysis of the Opinion see recent [Redgrave Analysis](#).

What Does the Comment Really Do?

Comment 8 certainly reflects the ABA’s view and desire to give lawyers a subtle push when it comes to technology; according to the [Report](#) accompanying the proposal:

The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain

aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.

In other words, the **ABA's position** seems to be that Rule 1.1 does not actually impose any new obligations on lawyers but simply reiterates the obvious: in order for lawyers to adequately practice and be competent under the Rules in today's world, they need to understand the technological tools by which they can zealously advocate for and protect their clients. *Id.*

It should also be noted that the ABA used the word "should" in its revised language, rather than the words "shall" or "will," which are normally used to express a duty. Furthermore, the rule does not outline what technology skills a lawyer should actually know in order to provide competent representation.

Finally, the Comment requires nothing in specific and is directed toward technology that is "relevant". If you don't have a practice that touches Twitter, for example, the Comment does not necessarily require you to know much about it. But where technology touches an attorney's practice, that attorney needs to have some level of competence.

Putting all this together, it seems clear that the Model Comment does not appear to contemplate attorneys getting the technical proficiency of a software engineer or any place close. Instead, somewhat like the California Bar Association concluded, it seems to contemplate that lawyers should at least be able to spot potential issues—the benefits and risks—of the technology that impacts attorneys every day. The **ABA** wants basic understanding: we need not know everything. We do need to know some things.

So on the one hand, it's easy to conclude that nothing has really changed and the Comment adds little duties that already exist. On the other hand, **some commentators** have concluded that by merely having the recommendations/duty in writing a sea change has occurred. Either way, I don't think lawyers can safely ignore technology and be ignorant.

What Can I Do?

Exactly *what* technology do lawyers need to understand? If a lawyer lacks a solid grounding in technology to begin with, how can he or she be expected to know which topics are important? How do lawyers interested in learning more about technology filter out the geek hype,

vendor sales pitches and general misinformation to get to the real information they need?

Courtesy of [Josh Poje of the American Bar Association's Law Practice Division](#), below are five simple strategies to help lawyers develop and maintain the expected and minimum understanding of relevant technology.

First, it's easy to get overwhelmed by the technology and technology information that's out there. And the constant development of new technology happens at an dizzying pace and can quickly cause lawyers to turn away under the theory that they can never master the issues so why try? Instead, I Josh believes lawyers should ask some fundamental questions about any technology they come in contact with:

When scanning through the latest technology news, always ask yourself: *Is this relevant to my practice?* Or perhaps more directly: *Can this technology help me be a better lawyer?* In the end, your objective is to provide exceptional representation to your clients or employer, and the technology you'll want to explore and understand is the technology that will help you achieve that goal.

Id.

Second, make it a point to pick out a good technology blog or other source of information and scan at least the headlines. This will at least keep you conversant with major trends and issues. Some good sources are [Bob Ambrogi's LawSites blog](#), [the Kennedy-Mighell Podcast](#), [Ars Technica](#), [ZDNet](#), [The Verge](#), [David Pogue](#), [Wired](#).

Third, we all know lawyers or other legal professionals that are tech geeks. Talk to them: you can learn a lot just by chatting with those who have an interest in the subject and is keeping relatively up-to-date. Don't be afraid to ask the stupid question-its probably not as stupid as you think. (And unless you are truly a geek yourself, the geeks will probably think whatever question you ask is stupid, anyway). Use more formal means to engage your peers to share knowledge about software, hardware and other technology tools. Get involved in email discussion lists, bar networking events, alumni meetings, and even simple conversations in the hallways outside the courtroom.

Fourth, discuss issues with experts. Most consultants are all too happy to share their thoughts, opinions and predictions. Often, if you or

your firm has an expert it uses for technology related issues, they will talk to you for free. If not, buying an hour or two of their time to talk about the trends, risks and opportunities he or she sees in the tech world is a good investment. These kinds of discussions may not make you a tech expert, but it will help you understand the landscape.

Fifth, contact your state Bar Association and the ABA. Many state Bars offer guidance on practice management issues, including the use of technology. This guidance is often easy to obtain and tends to be free. It also is more neutral and free of the vendor bias. It's often written specifically for lawyers, in many cases *by* lawyers. And some state and bars have practice management advisers available to answer technology questions. The ABA also has excellent guides and helpful information. See the ABA Legal Technology Resource Center, the [Law Technology Today](#) blog, the [ABA Law Practice Management Section](#), and [ABA TECHSHOW](#).

Conclusion: What's the So What?

So you may ask, what's all this mean to me? As my friend and one of the most astute observers of the legal landscape, [Bob Ambrogi](#), so well put it:

What does all this mean to you? It is simple. You cannot assess the benefits and risks associated with various kinds of technology if you know nothing about the technology. Even if your state has yet to adopt this change, it is only a matter of time before it does. Don't be a Luddite who fears or resists technology. Neither do you have to become a geek. Make an effort to understand the basics of the technology you use. Get on social media, if you're not already. Ask questions. Learn. When it comes to technology, there is no more burying your head in the sand.



Lighting the way to...

Charleston

South Carolina

2017 FDCC Winter Meeting – March 6-10



FRIDAY, MARCH 10, 2017

8:30 a.m. - 9:30 a.m.

PLENARY PROGRAM

Part I - Cool Kids Go International

Magnolia Ballroom

Moderators:

Debra Tedeschi Varner

Lauren S. Curtis

Panelists:

Michael F. Aylward

Kathleen B. Browne

Heather Sanderson

Richard K. Traub

250 Summer Street
Boston, MA 02210

+1 (617) 439-7500

www.morrisonmahoney.com

COVERAGE IN REAL TIME

How the Internet of Things Is Changing Insurance Underwriting

I. INTRODUCTION

Since the early Twentieth Century, insurers have assessed risk and quoted premiums based on actuarial data reflecting large pools of similarly-situated insureds. This traditional view of underwriting is now being upended by a confluence of market conditions, big data and the new technological capabilities created by the Internet of Things that threaten to shift this paradigm towards an entirely uncertain future in which underwriting practices may be utterly transformed.

In the United States, most general liability policies are rated based on code classifications developed by the Insurance Services Office that reflect the historical loss experience of property and casualty insurers. As described in ISO's *Commercial Lines Manual*, the purpose of the classification system is "to group insureds into classifications so that the *rate* for each classification reflects the *hazards common* to those insureds." The ISO classification system starts with a 5-digit code that describes the industry of the insured—Manufacturing or Processing (Codes 50000 to 59999), Contracting or Servicing (90000 to 99999), Mercantile (10000 to 19999), Building or Premises—office or space leased to others (60000 to 69999), and Miscellaneous (40000 to 49999). A more specific code and classification is then assigned taking into account the specific business of the insured and related factors, such as gross sales (*e.g.* 51370 Bicycle Mfg.—Not Motorized—\$10 Million Gross Sales).

Apart from considerations based on the gross risk experience of large groups of insured, underwriting has in the past also taken into account factors specific to the insured's own situation, as might be revealed by a detailed inspection of the insured's premises or an analysis of the information supplied in a policy application. In a soft insurance market, as has prevailed in the United States in recent years, there is great pressure on insurers to reduce the cost associated with such time-consuming inspections and evaluations. As a result, insurers are increasingly looking to technological fixes to facilitate underwriting.

At the same time, new technologies are giving insurers the ability to underwrite risk in real time. Rather than assessing the risk presented by a twenty-five year old single driver in Chicago, an automobile insurer now has the capability to place a tracking device in that

policyholder's car to assess risk factors such as speeding, attention to traffic signals and even drunk driving.

Newcomers to the insurance industry such as Lemonade have expressed a desire to "Uberize" the insurance industry by way of innovative business plans employ big data, smartphones, and machine learning along with artificial intelligence bots to assess risk, manage claims and enhance customer service.

All this comes at a time when a soft insurance market, poor investment results and a brutally competitive business environment are placing much more emphasis on better underwriting.

What does all this mean for the future of insurance? Are we moving away from the idea of pooling risk? Does a focus on individualized risk pose a renewed risk of insurers discriminating against certain groups of individuals? If insurers are able to discriminate on the basis of tools like this, will poor risks be deprived of the ability to purchase insurance and instead be relegated to assigned risk pools?

II. THE IMPACT OF TECHNOLOGY AND BIG DATA

In 2013, IBM Global Services released a white paper¹ entitled "Integrating the value of data in the underwriting process." In this report, IBM found that

Some carriers are forging ahead with telematics and complex algorithms, while others are underwriting each risk based on the underwriters' experience and intuition. Even when data is modeled, insurers struggle with how to integrate the derived insights within the underwriting process and align them across enterprise objectives.

Last year, IBM issued a follow up study entitled "Rethinking Insurance: How cognitive computing enhances engagement and efficiency." In contrast to its 2013 study, IBM found in this June 2016 report that:

The insurance industry is awakening to the potential of cognitive technologies. Thirty-eight percent of our survey respondents said they have adopted cognitive computing, almost three times the adoption rate of their peers in the banking industry. Outperforming insurers are even

¹ <https://www.the-digital-insurer.com/wp-content/uploads/2013/12/54-Integrating-data-into-Underwriting.pdf>

further ahead —an impressive 71 percent of this group has already started working with cognitive technologies.

Similarly, a 2016 Willis Towers Watson report found that

More than half of insurers surveyed (54%) currently use predictive models for underwriting and risk selection, but many additional uses are planned. Two years from now, carriers expect to significantly ramp up model use in important areas. Several top future uses cited by survey respondents (such as evaluation of fraud potential, claim triage and evaluation of litigation potential) reflect the importance of effectively managing bottom-line results as carriers continue to compete aggressively on price. Other top uses (e.g., report ordering) are directed at expense control, another key to managing profitability in an intensely competitive marketplace. To help improve top-line growth, carriers are also using modeling to inform their marketing and advertising strategies.

III. THE INTERNET OF THINGS

Even as tracking devices such as FitBit and Nest are changing our personal lives, the Internet of Things is also allowing third parties to assess risk in relation to our physical movements.

Private employers are already using global positioning devices (GPS) to track the movements of their employees. A December 2016 survey² of 1000 employees commissioned by T-Sheets determined that nearly a third of the respondents were being tracked by their employers and half of those were being tracked 24/7.

This kind of monitoring has obvious applications to insurance. To use only one example, the risk that trucking insurers underwrite can be dramatically impacted by the failure of long-haul drivers to comply with company requirements with respect to taking breaks and limiting driving hours. A GPS monitor creates a read means of ensuring that such rules are complied with and weeding out drivers that break the rules.

There may be legal limitations on the use of this technology, however. In California, a woman sued her employer in 2015 claiming that her discharge for disabling a GPS app on her company-issued phone violated Section 637.7 of the state Penal Code, which prohibits the use

² <https://blog.tsheets.com/2016/inside-tsheets/employees-gps-tracking-workplace>

of “an electronic tracking device to determine the location or movement of a person.” The case settled without a decision.

Unlike California, it appears that most states permit employers to monitor the movements of their employees. Indeed, the Xora app that was involved in the California litigation is now being marketed across the country by a Massachusetts company known as ClickSoftware. According to ClickSoftware’s website, its Xora StreetSmart produces allows clients to “drill down into the map and see specifically what is happening at each stop. Review how long a mobile worker has been there, the address, what actions they are taking and the status of the mobile app.”

While the Xora device has an Orwellian tinge to it, insureds are now being asked to provide this kind of reporting data voluntarily in return for cheaper insurance. A recent article in Forbes³ reports that some U.S. auto insurers are now offering telemetry-based packages that feed a motorist’s driving behavior to a computer, where a highly “personalized, highly accurate profile of an individual customer’s behavior” can be developed. The data is derived from a black box that is installed, with the insured’s consent, in a vehicle and that tracks its movements via a sensor in the car or the insured’s smartphone.

According to Boston-based insurance consultants Strategy Meets Action (SMA) nearly a third of all U.S. auto insurers are now deployed “usage-based insurance” programs that track a driver’s behavior. SMA predicts that this figure will rise to 70% by 2020.

Both Nationwide’s “Smart Ride” and Progressive Insurance’s “Snapshot”⁴ programs invite policyholders to share data with them to confirm that they are good drivers. Nationwide’s “Smart Ride” program⁵ promises insureds an immediate 5% discount for installing a tracking device in their cars and further discounts up to 40% depending on the insured’s driving over the course of the year. The Smart Ride recording device tracks data in four categories that may increase a risk of accidents: (1) total miles driven; (2) hard braking; (3) fast acceleration and (4) driving between midnight and 5 a.m. when accidents are statistically more likely to occur. As advertised on the Company’s website:

³ <http://www.forbes.com/sites/bernardmarr/2015/12/16/how-big-data-is-changing-the-insurance-industry-forever/#73dd45cb435e>

⁴ <https://www.progressive.com/auto/snapshot/>

⁵ <https://www.nationwide.com/smartride.jsp>



1. Plug In and Drive

We'll send you a small device for your car within 10 days of signing up. Drive as you normally do.



2. Track Progress

Then go online to track your discount and get personalized feedback about your driving trends.



3. Lock In Your Discount

At the end of the program, simply send back your device and lock in your final discount. We'll apply the discount at your next policy renewal."

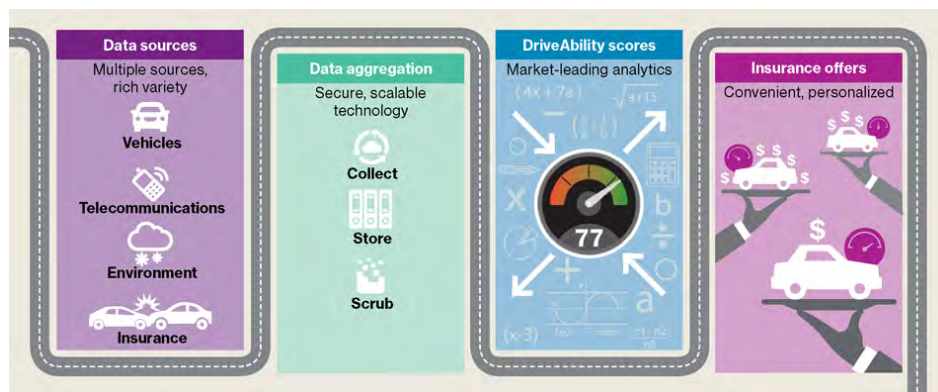
According to Progressive, its Snapshot program allows it to “**attract, identify and reward** good drivers while also retaining those customers longer.” Progressive reportedly now has more than 2 million Snapshot policies in force and has increased the number of Snapshot customers from a fifth of its total U.S. auto business two years ago to 35% today.

The efficacy of such programs obviously depends on the quality of data being obtained and the ability of insurers to properly understand and utilize the information received. In order to facilitate this progress, insurers are entering into strategic partnerships. For instance, Progressive is allowing users of GM's OnStar program to subscribe and obtain insurance discounts. According to a 2015 article in PropertyCasualty 360⁶

⁶ <http://www.propertycasualty360.com/2015/01/12/gms-onstar-partners-with-progressive-to-provide-us>

The new connected vehicle services will allow OnStar subscribers a chance to reenroll in a program that provides a detailed driving assessment spanning a 90-day evaluation period. The assessment, which will be provided only to OnStar subscribers, will detail their driving performance in important driving metrics, and will further indicate how they compare against an aggregate of anonymous subscribers also participating in the program. From there, OnStar will provide driving tips based on areas that have potential for improvement.

In early 2016, Liberty Mutual announced⁷ a joint venture with Subaru to allow drivers of new Subaru cars to obtain discounted insurance based on driving data submitted electronically through Subaru's "StarLink" cloud platform that "connects Subaru vehicles to a driver's smartphone to monitor driving habits, provide trip reports and offer tips to become a safer driver." Willis Towers Watson is also marketing its "Driveability" program to insurers as "the market's most predictive insurance telematics score"⁸ and cautions insurers about using the wrong telematic criteria for UBI. As outlined on its web site:



The use of tracking technology is not limited to liability insurance. In late 2015, the *Huffington Post* reported⁹ that Renaissance Dental had partnered with Beam Technologies to supply Bluetooth enabled electric toothbrushes to insureds that provide real time reporting to the insurer on whether teeth are getting brushed and for how long (it does not monitor flossing).

⁷<https://www.libertymutualgroup.com/about-lm/news/news-release-archive/articles/liberty-mutual-insurance-and-subaru-introduce-new-technology-to-promote-safe-driving-and-savings-on-auto-insurance>

⁸ <https://www.towerswatson.com/en/Services/Services/DriveAbility>

⁹ http://www.huffingtonpost.com/entry/smart-gadgets-insurance_us_55e5c6ffe4b0c818f6192558

Policyholders that brush regularly reportedly get free brush replacements and rebates on the cost of their insurance premiums.¹⁰

Nor is the applicability of inter-active technologies limited to auto insurance. Accenture's 2015 report explored the possibilities for expanding on devices like Nest to allow homeowner's insurers to evaluate risk, safeguard homes and expedite claim reporting.¹¹ Accenture claims to have developed an interconnected platform for Bluetooth-based devices like thermostats, motion sensors, burglar alarms, carbon monoxide detectors and home cameras that could be linked together to improve home safety and to provide data to insurers.

Indeed, a 2014 Deloitte report predicted that the "genie is out of the bottle":¹²

Before too long, the use of sensory technologies that permit behavioral underwriting by insurers is likely to be expanded beyond auto insurance into homeowners, life and health coverages, and perhaps even non-auto commercial lines as well, such as workers' compensation. Smart homes, biometric monitoring, wearable technologies, and the Internet of Things are all developing trends that could support and accelerate such initiatives.

IV. WILL CONSUMERS EMBRACE SUCH CHANGES?

Will insureds permit such intrusions into their personal privacy? Surprisingly (perhaps), the answer seems to be yes. A 2015 Accenture survey¹³ found that 78% of respondents would be willing to willing to share personal information in return for reduced premiums or expedited claims handling. Attitudes seem to be quite cost sensitive, however. A survey by LexisNexis found that ¹⁴50% of respondents said they would be likely to sign up in return for a 10% discount and 62% would for a 15% discount, only 23% would if the rebate was reduced to 5%.

There are also diverse attitudes to UBI within the consuming public. As Progressive Insurance CEO Glenn Renwick has recently commented: "You get about 30 percent of people

¹⁰ <http://www.insurancejournal.com/news/national/2017/01/19/438925.htm>

¹¹ <http://ins.accenture.com/rs/accenturefs/images/the-connected-home-new-opportunities-for-property-and-casualty-insurer-POV.pdf>

¹² <https://dupress.deloitte.com/dup-us-en/industry/insurance/telematics-in-auto-insurance.html>

¹³ <http://ins.accenture.com/rs/accenturefs/images/the-connected-home-new-opportunities-for-property-and-casualty-insurer-POV.pdf>

¹⁴ <http://www.insurancejournal.com/news/national/2013/10/29/309548.htm>

saying, 'Yeah, why not?'; you get another 30 percent of people saying, 'Maybe, I need to know more'; and you get about 40 percent of people saying, 'No way in hell.'

A Towers Watson survey has found that consumers do have concerns about privacy issues, including whether their data will be shared with others (41%), whether insurers will monitor and track driving destinations (42%) or use telematic data to deny claims (38%)

V. REGULATORY CONCERNS

The ability of insurers to evaluate risk on a more individualized and precise basis than may be true for pooled risk has given rise to concerns that some insureds may be prevented from getting insurance at all.

Michael Barry of the Insurance Information Institute disputes these fears, stating that "Insurance is such a heavily regulated industry that insurers must justify, in actuarial terms, the reason for any rate increase they're seeking in almost any line of business."

Insurers claim that telematics provides them with a means of encouraging policyholders to adapt safer behaviors. Indeed, there may be some support for this view. In a 2016 Towers Watson survey, sixty percent of the respondents said that UBI might help them to be better drivers by encouraging them not to speed (71%), avoiding tailgating (52%) and driving more considerately (49%).¹⁵

At the same time, some insurers seem more interested in using telematics as a tool to weed out poor risks. For instance, Ohio-based Root Insurance has recently begun using a smart phone that tracks driver behavior for two weeks before Root decides whether to accept a risk.¹⁶ According to company founder Alex Timm, telematics data gives Root a competitive advantage in making underwriting decisions as contrasted with traditional criteria:¹⁷

The majority of the market is still based on traditional underwriting variables—credit score, age, gender, year/make/model of vehicle, marital status. Some still have occupation, some ask your level of education They will use these reports and that information in order to try to predict whether you will get into an auto accident. It is not very granular."

¹⁵ <http://www.insurancejournal.com/news/national/2013/10/29/309548.htm>

¹⁶ <http://www.insurancejournal.com/news/national/2016/10/25/430423.htm>

¹⁷ <http://www.insurancejournal.com/news/national/2016/10/25/430423.htm>

How you drive—telematics data—can predict future accidents way more than any other individual element. That's why a telematics device has been such a huge focus of some carriers. What they haven't been able to do is align that with a really good consumer value proposition, again, still not giving good drivers the rate they deserve. We have taken away all of those barriers.

VI. CONCLUSION

The world of the Jetsons is no longer the stuff of TV fantasy and science fiction. As the Internet of Things transforms our personal lives, the opportunities for data collection that it presents will present enormous challenges and opportunities for insurers, regulators and consumers that can only now be imagined.

March
2017

The Legal & Insurance Implications of Drones in Canada

HEATHER A. SANDERSON

E hasanderson@sanderson-law.com
T 403-837-2508

SANDERSON LAW
Legal Counsel

Calgary | Alberta | Canada
www.sanderson-law.com



Heather A. Sanderson, the principal with Sanderson Law in Calgary, Alberta, Canada, is a nationally recognized author and insurance coverage counsel, who has provided expert evidence on CGL coverage issues to Canadian Courts and has appeared as counsel before a full panel of the Supreme Court of Canada.

Currently, Heather is a director of Canadian Defence Lawyers (CDL), Chair of CDL's Insurance Coverage & Practice Committee and Chair of the DRI's Insurance Law Sub-committee, Canadian Law and Cross-Border Issues and a member of the steering committee of DRI's Insurance Law Sub-Committee. She has both authored and co-authored the Canadian law chapter of The DRI Insurance Law Committee's Coverage B: Personal and Advertising Injury Compendium and a similar chapter in the soon-to-be-published Duty to Defend Compendium.

Copyright Notice: Heather A. Sanderson and FDCC hold the copyright for the original version of this paper according to the terms of an agreement that they have signed. © March, 2017.

Receipt or possession of this paper does not convey any right to reproduce its content.



Drones allow photography enthusiasts to create stunning aerial landscapes without renting a fixed wing plane and a pilot. The photo above was taken by a DJI Phantom 3 drone, pictured at right, which retails in Canada for about \$680.00. This is a typical quad-copter drone equipped with a 12 mega pixel camera that can capture still images and 4K video, all controlled by the operator on the ground. By connecting your smartphone to your handheld remote control unit, you can see on-screen exactly what the drone 'sees' through the camera lens. Source: Thomas, Andrew *How to Use Drones to do Stunning Aerial Photography*, <https://digital-photography-school.com/how-to-use-drones-to-do-stunning-aerial-photography/>



The Drone Emerges

We have entered the age of the drone.¹

The millions of dollars that military establishments devoted to the research and development of drones is being adapted to new, commercial uses that were not even imaged two years ago. At the same time, personal use of drones has skyrocketed.

Like all technology it is both useful and harmful. Although we cannot predict the uses to which drones will be put, we are in a position to regulate the use of drones to minimize the risk of harm and maximize the benefits that they will offer. The Canadian government and the insurance industry are working together to do just that. These efforts are timely for it is predicted that in a few years, drones will be as common as cars.

The Proliferation of Drones

Within the last five years, smartphone technology (the sensors, GPS and processors) was applied to the military drone model and the result is an autonomous flying robot that can be purchased for well under \$1,000 in most Canadian (and American) gadget stores and is usable 'right of the box'. Those with the ability and inclination can build their own drone for about \$300.00.

Drones can hover in midair, fly upside down and spin; they can maneuver smoothly and precisely through small spaces or in concert with other drones; and they can do all this while carrying things like a stabilized video camera and a multitude of other technologies on board. Drones come in all shapes and sizes. They can be as large as a fixed wing aircraft or fit in the palm of your hand.

¹ The writer is grateful for the research, facts and predictions regarding drones that is presented by the CBC, Doc Zone, "The Age of the Drone", originally aired September 17, 2016 at 2:00 p.m., www.cbc.ca/doczone/episodes, only viewable in Canada. Another invaluable source of information is The Future of Drones In America: Law Enforcement and Privacy Considerations, Hearing Before The Committee On The Judiciary United States Senate, March 20, 2013, <https://www.hsdl.org/?view&did=753761>



Figure 1 The Air Selfie –when you want an aerial selfie, you slip this out of your phone case, quickly assemble it and using a phone app, fly it over your group for an aerial selfie.

Manufacturers and promoters of drone technology are looking to make drones ‘the next big thing’. Some say we are ‘at the Kittyhawk stage’ of an amazing industry. Research groups studying the application of the technology have universally stated that in the next few years, drones will support a

multi-billion dollar industry²

Drones excel at doing what is dirty, or dangerous or dull.

In the oil and gas industry, drones can inspect the integrity of flare stacks without a shut down or using helicopters.³ Drones equipped with thermal imaging cameras can inspect thousands of kilometers of buried or above ground pipeline while the pipeline is in operation.⁴ Drones can efficiently inspect highway bridges and overpasses without endangering workers or shutting down the highway. They can drop medical supplies into hard to reach areas or areas cut off by a natural disaster. Drones can fly into swarms of mosquitos and identify those that carry disease. Drones can inspect jetliners for dents and scratches in about 10 to 15 minutes. It takes a person about two hours to do that. British researchers have fitted drones with a sensor that finds the abnormalities in plant life caused by the chemical that leaches from unexploded landmines; the drone flies over areas where landmines are suspected and finds the mines with risk of injury to humans.

Realtors use drones to produce fabulous video of properties they are selling. Wedding photographers are creatively using drones to video outdoor weddings.

There are at least 10 different manufacturers of drones equipped with ‘follow-me’ technology where the drone tracks the GPS signal of your smartphone or tablet and stays close to that signal. The drone will follow you and hover to capture video of you carving that perfect line through powder snow; your run down the skateboard park; your child’s first steps; the panoramic view of your hiking group at the top of a peak, or whether your

² This is the statement of Ian Glenn, CEO of ING Robotics Aviation, as quoted in Age of the Drones, *supra*, n.1.

³ In July, 2011 at a major oil refinery in Eastern Canada, a drone was successfully deployed by ING Engineering to complete a detailed aerial inspection of an active flare stack. The goal of the inspection was to obtain optical imagery of the flare stack head to allow refinery personnel to assess the images and determine damage to the piping, pilots lights and to look for other structural anomalies that may be detrimental to the operation of the flare stacks: <https://www.aeryon.com/casestudies/flare-inspection>

⁴ See www.barnardmicrosystems.com/UAV/pipeline_monitoring/pipeline_monitoring.html

rain gutters are plugged and are in need of a clean-out.⁵ Until now the only way the average person could see the world above eye level was through the window of a jet. The drone has changed that. The drone's eye view changes the way we view seminal events in our lives, sports and the news.

There are courses being offered in drone journalism. In June of 2013, video captured by a live streaming drone demonstrated police violently breaking up a demonstration in Istanbul's Taksim Square. The video went viral and publicised the situation even though police shot down the drone when they realized they were being filmed. Drones are tailor made to assess and report on damage caused by natural disasters.

A craft brewery in Minnesota filmed a hefty quadcopter delivering a 12-pack to ice fisherman on Lake Waconia in February of 2014. However, at that time the FAA prohibited drones being used for commercial purposes and shut down the enterprise. Amazon has seriously pursued the concept of delivering packages by drone but the regulatory framework prohibited research and development of the concept in the United States so Amazon set up a test facility in Coquitlum, British Columbia.

Through testing conducted in Queensland, Australia, Google's 'Project Wing' has developed a large and powerful drone that flies at the speed of a fixed wing plane but can hover like a helicopter. It will drop its payload carefully and gently through a tether, disengage the tether and head off for another delivery. The original goal was for Google to start delivering packages by 2017. Time will tell if that marker will be met. However, 7-Eleven, the world's largest chain of convenience stores has beaten Amazon and Google to be the first retailer with a drone delivery service, delivering 77 orders of sandwiches coffee and donuts to customers in Reno, Nevada in November, 2016.

ING Robotics Aviation, based in Ottawa, Ontario has been involved in drone technology from the beginning and spearheaded the Canadian military's use of drones during the Afghanistan war. Its CEO, Ian Glenn believes that drones are tailor-made for search and rescue operations. They can travel over rugged terrain; fly when it is too dangerous for manned aircraft to fly. Equipped with heat sensors and infrared cameras, they can find the lost and injured, as well as drop supplies to them with no danger to rescuers.

In May of 2013, using a drone manufactured by a Saskatoon company, Dragonfly Innovations, RCMP corporal Doug Green found a man who had rolled his car about 35 km from Saskatoon on a dark night, with high winds and dangerously low windchills. When a helicopter equipped with a night vision camera and ground crews could not find the man, a drone equipped with thermal imaging found his heat signature – curled up at the base of a tree, near a snowbank. In this fashion, ground crews rescued the 25-year-old man about an hour before he would have died due to hypothermia. In September of 2014,

⁵ See <http://www.top10drone.com/top-10-drones-follow-me-mode>. Unfortunately Airdroids, an earlier initiator of this technology began its life in 2014 but folded a year later, unable to make the leap from prototype to market.

another RCMP drone was used to find a missed Dartmouth family who had wandered off the designated trail while hiking.



Figure 2 Source: Kipper williams, The Institution of Engineering and Technology

In short, drones are proliferating in the commercial and recreational spheres. It has been estimated that by 2020 there will be about 20,000 drones operating in Canada and about 30,000 in the Continental USA. That's a lot of drones.

The Definition and Regulation of Drones in Canada

Drones are un-manned aerial robots that are controlled by an operator on the ground. They are defined in the *Canadian Aeronautical Regulations* (enacted under the Aeronautics Act) as:

unmanned air vehicle means a power-driven aircraft, other than a model aircraft, that is designed to fly without a human operator on board; (véhicule aérien non habité)

The Canadian *Aeronautics Act* defines “aircraft” as ...any machine capable of deriving support in the atmosphere from reactions of the air, and includes a rocket; (aéronef)

The same Aeronautical Regulations state:

602.41 No person shall operate an unmanned air vehicle in flight except in accordance with a special flight operations certificate or an air operator certificate.

The same regulations also regulate the use of model aircraft, kites and model rockets:

602.45 No person shall fly a model aircraft or a kite or launch a model rocket or a rocket of a type used in a fireworks display into cloud or in a manner that is or is likely to be hazardous to aviation safety.

model aircraft means an aircraft, the total weight of which does not exceed 35 kg (77.2 pounds), that is mechanically driven or launched into flight for recreational purposes and that is not designed to carry persons or other living creatures; (modèle réduit d'aéronef)

model rocket means a rocket that

- (a) is equipped with model rocket motors that will not generate a total impulse exceeding 160 N.s,

- (b) has a gross weight, including motors, not exceeding 1 500 g (3.3 pounds), and
- (c) is equipped with a parachute or other device capable of retarding its descent; (modèle réduit de fusée)

Currently in Canada, a drone is an “unmanned air vehicle” and they are deemed to be “an aircraft”. As drones are “aircraft”, the use and operation of drones is subject to the Canadian Aeronautical Act and its Regulations which is administered in Canada by the federal Canadian department known as Transport Canada.

Drones used for commercial purposes or for research purposes are subject to different rules than those used solely for recreational purposes.

i) The Regulation of Commercial Use Drones in Canada

Subject to two exceptions, drones used for commercial purposes, or for research purposes, must be operated under a special flight operation certificate (SFOC) or an air operator certificate. Transport Canada has advised that if the operator receives payment or other commercial benefit through the operation of the drone, then Transport Canada inspectors will deem the operation to be commercial.

Accordingly, if a person does not charge for the use of the drone but sells the photos or video taken by the drone, then the use is a commercial use and an SFOC is required. Further, if the drone is used solely on property owned by the operator for the benefit of the enterprise conducted on that property, then an SFOC is required as the use remains “commercial”.

Violations of a SFOC can result in a fine of \$3,000 for a person and \$15,000 for a corporation. Operating a drone without a SFOC when one is required results in a fine of \$5,000 for a person and \$25,000 for a corporation.

What are the requirements to obtain a SFOC to operate a drone? In addition to detailing the contemplated operation of the drone, the operator must be 18 years of age or older and convince Transport Canada that the operator can conduct their planned operation safely and in accordance with aviation regulations. In most cases there must be a person, other than the operator who works as a ‘spotter.’ Further, the applicant must adduce proof of public liability insurance with limits of at least \$100,000.⁶ Transport Canada Inspectors *are not required to obtain an actual copy of the applicant’s insurance policy. The applicant’s declaration of the fact that they have such insurance is sufficient*.⁷

Further, the application must detail, the who, what, where, when, and how of the planned use of the drone, including all the procedures for emergencies. The level of detail

⁶ Canadian Aviation Regulations, s. 606.2(8)

⁷ The words in italic are a direct quote from Transport Canada’s published guidelines for approval of SFOC applications: http://www.tc.gc.ca/eng/civilaviation/standards/general-recavi-uav-4161.html#toc12_4

required will depend upon the applicant's specific needs where the drone will be operated. The application is submitted to the applicable regional office of Transport Canada who will review it and then get back to the applicant with either the certificate applied for, or a rejection if the applicant does not cover all the necessary information. The process can take anywhere from two weeks to two months or longer, all dependent on how many other applications are in the backlog for your area.⁸ There is no application fee, no application form and no template for these applications. Applicants must create their applications from scratch. There are companies that will spearhead the application process for applicants. The usual fee is about \$1,300 for a 'basic' application.

An SFOC is required for each 'job'. If the applicant develops a track record of safe operation, then the applicant can apply for a blanket or standing SFOC that will be time limited. At the end of the time limit, the applicant can apply for another blanket SFOC.

Those using drones for commercial use do not require a SFOC if the drone is under 25 kg (55 lbs.) and it is not being operated within 9 km of an airport or a built-up area. "Built-up" area is not defined, but Transport Canada issued an Advisory Circular on December 22, 2016 that states that they are interpreting a built-up area as meaning anything more than one farm in the area of operation.⁹ But that is not all - the drone must be at least 100 feet away from any animal or person not involved in the operation.

This use requirement prevents the widespread commercial use of drones without a SFOC.

ii) The Regulation of Drones used for Recreational Use in Canada

If the drone is used solely for recreational purposes and is under 35 kg (77 lbs), then that drone is "a model aircraft", and a special flight operations certificate is not required.

The operation of that type of drone is subject to the Criminal Code and the provincial and territorial Trespass Acts unless and until the drone is flown into cloud or in a manner that is or is likely to be hazardous to aviation safety, or restricted areas designated in the Canadian Air Space Handbook (for example, Niagara Falls is a restricted airspace).

If a recreational drone is being operated in this fashion, then such use and operation is subject to investigation by Transport Canada. Transport Canada investigators can lay charges that carry the potential of fines up to a maximum of \$25,000 and the possibility of incarceration.

Although drones are "aircraft" and are subject to regulation under the Aeronautics Act, the current legislative framework was clearly not written with drones in mind. Further regulation is required.

⁸ See the website maintained by the Nova Scotia company, Flitelab.com which is involved in the design and construction of drones: <https://blog.flitelab.com/2015/01/17/canadian-commercial-drone-regulations-for-dummies/>

⁹ The circular is found at <http://www.tc.gc.ca/media/documents/ca-opssvs/AC-600-004.pdf>.

iii) New Canadian Regulations May be in Place by the Close of 2017

Since 2007, Transport Canada has had a working group studying the use, operation and regulation of drones due to the increased commercial and recreational use of drones. This group has created a set of proposed regulations which may be enacted sometime in 2017. These proposed regulations will be further amended in the event that the International Civil Aviation Authority enacts regulations on drones and upon study of the American regulation of drones.

The proposed regulations will be published in the Canada Gazette in the Spring of 2017 and slowly make their way through the legislative process. If enacted in their current form, they would require all drones, regardless of size, to be marked and registered with Transport Canada. Further, there would be age limits upon those who can operate a drone.

Unlike the current regulations, the proposed regulations do not distinguish between commercial and recreational use. Rather, the proposed regulations differentiate between complex operations (those that occur in urban or built-up areas) and limited operations (occur in remote areas).

It is anticipated that small UAV operators undertaking complex operations would need to hold a pilot permit issued by Transport Canada, while small UAV operators undertaking limited operations would not.

Transport Canada proposes that pilots applying for a permit complete a course in aviation, acquire practical training, and demonstrate competency in performing normal and emergency maneuvers with the small UAV.

Finally, manufacturers of small UAVs would also be required to meet a design standard, which would include requirements for flight performance, structure, systems and equipment, as well as launch and recovery systems.

The Definition and Regulation of Drones in the United States

The American federal government, through the Federal Aviation Administration (FAA) regulates American airspace. Individual states have no jurisdiction over the airspace.¹⁰

Since December of 2015, drones flown in American airspace must be registered with the FAA, unless they weigh less than .55 lbs.

Until August 31, 2016 commercial use of drones was severely restricted by cumbersome and expensive regulatory requirements. Firstly, operators required a manned aircraft pilot license, a visual observer and each flight had to be authorized by air traffic controllers.

¹⁰ This summary of the regulation of drones in the United States is premised upon a review of the FAA website as it stood in February of 2017.

On June 21, 2016, the FAA released new regulations for UAVs, which came into force at the end of August of 2016 that are applicable to routine commercial drones weighing less than 25 kilograms. These drones must be operated within visual line-of-sight (VLOS) and is subject to altitude limits (under 400 feet) and speed restrictions (a maximum groundspeed of 87 knots). Operators must be at least 16 years of age and hold a remote pilot airman certificate. To obtain a certificate, an operator must demonstrate aeronautical knowledge by passing an FAA- approved examination. The FAA regulations prohibit UAVs from being flown over any persons not directly participating in the operation, and prohibit flights at night. Additionally, the FAA regulations provide for a maximum groundspeed of 87 knots, and require that UAVs operate at an altitude not higher than 400 feet.

Drones operated solely for recreational purposes are not subject to these regulations. Rather, they are considered “model aircraft” and are to be flown subject to the voluntary rules of the Model Aircraft Association.

Drones and Privacy

Drones are a supremely capable surveillance tool. They can be equipped with technology that have the ability to capture data from great distances and through walls, through smoke, fog and debris and with a fine level of detail, for example the ability to capture the image of a person’s face from miles away.¹¹



Many fear that our ability to move unrecorded and undetected in public space may be at an end as drones can systematically and secretly record our movements for later use.

However, there is legislation to deal with that risk. Where drones are used for commercial purposes, the data they collect, be it video or still images, is protected by the

Personal Information Protection Electronic Documents Act (PIPEDA), and subject to the same requirements as with any other data collection practice. It is a common misconception that a company does not require permission to take an individual’s photograph in a public place. The privacy protections in PIPEDA are there to ensure that people know when their image is being captured for commercial reasons – whether by photograph or video - and what it will be used for. PIPEDA requires consent as a general rule, subject to only limited and specific exceptions.

¹¹ See the report of the Privacy Commissioner of Canada, *Drones in Canada*, March, 2013, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/drones_201303/

What is of concern is the incidental collection of information by a drone. The authorized use of a drone may incidentally collect information harmful to the interests of an individual. There is very little legal protection against that risk.

In addition to the privacy issue, there is the annoyance issue. Drones are intrusive and loud. Do the laws of trespass apply to the airspace above your property? That issue was playing out in a western Kentucky courtroom last fall. In July of last year, Hillview, Kentucky's William Merideth spotted a drone flying near his property and he blew it to smithereens with his shotgun. It turns out the drone belonged to Merideth's neighbour, David Boggs, a roofer. Boggs has filed a claim for damages against Merideth (who has since become known as the 'Drone Slayer') appeared in Federal court, claiming in part, that the drone was not trespassing. Merideth says it was hovering over his property, potentially filming his daughter. The case pits the right to occupy federal airspace over state rights to control property. To my knowledge, a decision in *Boggs v. Merideth*, has not been released.

The British Newspaper, the Telegraph reported in late 2016, that several drone trespass actions are before the English Courts.

Canadian courts in the years to come will grapple with issues such as, does the Criminal Code charge of voyeurism apply to drone intrusions? To what extent does the civil remedy of nuisance apply to prevent drones from disturbing the enjoyment of your property?

Drones & Property Damage

Crashes are common with inexperienced pilots of drones. Regardless of the experience level of the pilot, it is possible for a drone to lose a rotor and fly off course. Either way a crash and property damage is likely.

In late December of 2015, the CBC reported that a privately owned drone that had been flying east, crashed head-on into the grille of a westbound moving car on Old Madoc Road in Belleville, Ontario, causing \$1,000 in damage to the car. Transport Canada and local police investigated. Local police authorities reported to the media that they were at a loss as to what charges to lay, if any. They determined that the highway laws did not apply; the Criminal Code charges of vandalism and mischief did not apply. In the end, no charges were laid.¹²

On August 23, 2016, a recreational drone crashed into a brand new \$126,000 Mercedes as it was crossing the Sydney Harbour Bridge, in Sydney, Australia. At first, the terrified driver thought that a person had jumped from the superstructure of the bridge and hit her car but shortly realized that the car had been struck by a drone. The driver speculated as

¹² See *Transport Canada following up on drone vs. vehicle crash in Belleville, Ont.*, CBC News, posted January 4, 2016, <http://www.cbc.ca/news/canada/ottawa/drone-belleville-transport-canada-interview-1.3388189>

to what would have happened if the drone had entered their car through the open sun roof. The operator of the drone was located and fined by the Civil Aviation Safety Authority. The drone strike, was captured on CCTV footage and makes for interesting viewing.¹³

On November 14, 2016, a Porter Airlines Dash 8-400 turboprop was over Lake Ontario on its initial approach to Toronto's Billy Bishop Toronto City Airport from Ottawa, travelling at 450 km/hr at an altitude of 2,743m. (9,000 ft) when its pilots saw an object ahead that was about a metre wide. They put the plane in a sudden nose dive and successfully avoided it. The diving manoeuvre slightly injured two flight attendants who were on board. Investigators believe that the object the pilots saw was a drone.¹⁴

Aviation regulators are justifiably concerned about drones colliding with fixed wing and rotary aircraft. Similar to a bird strike, the drone can get sucked into jet engines, disabling them, causing a loss of propulsion and a crash. For that reason, drones are prohibited from being operated within 9 km of an airport or airfield. Despite that prohibition, a Calgary man was arrested when in January of 2016 he was found operating a privately owned drone under the flight path of an incoming jet at the Calgary International Airport.¹⁵ In September of 2016, he was convicted and fined \$500.00.

In June of 2016, a drone came within 60 metres of a landing Air Canada jet at the same airport. The operator of the drone was never found. Similar instances have been reported at the Vancouver International Airport in British Columbia.

In the first 24 weeks of 2016, Transport Canada reported that it was investigating 40 such incidents. It investigated a total of 43 in the whole of 2015.¹⁶

This is not just a Canadian problem. In July 2014, a drone narrowly missed colliding with an Airbus A320 as it was taking off from London's Heathrow airport. The plane was at about 700 feet when the incident occurred. The British Civil Aviation Authority (CAA) rated the incident as a "serious risk of collision," the top rating it can give.

Similar incidents have occurred in China, France and Poland.

¹³ Huffadine, Leith, *Shocking Moment a drone falls from the sky and smashes into a moving car on the Sydney Harbour Bridge*, Daily Mail, August 23, 2016, www.dailymail.co.uk/news/article-3754290/Drone-hits-moving-car-Sydney-Harbour-Bridge.html

¹⁴ Campion-Smith, Bruce *Porter Plane narrowly avoids collision with a mystery object*, Toronto Star, November 14, 2016 <https://www.thestar.com/news/canada/2016/11/14/porter-plane-in-near-miss-with-drone.html>

¹⁵ See CBC news, *Calgary man criminally charged for flying drone near airport*, January 21, 2016, <http://www.cbc.ca/news/canada/calgary/calgary-man-drone-airport-criminal-charge-1.3413818>

¹⁶ Calgary Herald, *Airliner Narrowly Missed Drone at Calgary airport*, June 20, 2016 <http://calgaryherald.com/news/local-news/airliner-narrowly-missed-drone-at-calgary-airport>

Drones & Bodily Injury

There is an immutable law applicable to drones: Gravity. Two kilos of drone falling from the sky can inflict significant injury or kill someone.

In December of 2015, Austrian skier, Marcel Hirscher was competing in a slalom race in Madonna di Campiglio, Italy, when a drone that was filming his race came crashing down two feet behind him as he raced the course. Serious injury or death was narrowly avoided.¹⁷

In December of 2014, a holiday promotion by TGI Fridays, a restaurant chain involved a drone in a promotional event. The drone was to deliver a sprig of mistletoe over diners' heads. The drone miscued, collided with a patron, clipping the tip of her nose and cut her chin.

Drones have crashed into crowds at sporting events.

In November of 2014, at the Geraldton Endure Batavia triathlon in Australia, a drone was being used to photograph competitors when it crashed into triathlete Raija Ogden, causing a minor head wound, which required stitches to close. The drone operator, photographer Warren Abrams, claims that the drone crashed after someone in the audience stole control of it from him. Nonetheless, the Australian Civil Aviation Safety Authority fined Abrams \$1,700 for operating the drone near a gathering of people, contrary to regulation. No criminal charges were laid as investigation proved that radio interference from the event's timing device caused Abrams to lose control of the drone.¹⁸

In the fall of 2013, a drone crashed into the stands of spectators gathered at Virginia Motorsports Park.

On February 20, 2017, three people were injured when a drone filming the annual Skijoring Race in Silverton, Colorado, which involves horses pulling skiers, flew too low, spooking the horse. The panicked horse charged the crowd, resulting in injuries.

Insurance Coverage for the Use and Operation of Drones

Several years ago, specialty insurers, AIG, Meadowbrook, XL Catlin, SwissRe, Global Aerospace Underwriting Managers Ltd., Lloyd's and Houston Casualty, reacted to the rise of the use of drones in the private sector by offering drone specific coverage in the United States, UK, Canada and Australia that is modeled on standard aviation policies. Appropriate licensing of operators and operating the drone in compliance with regulatory requirements are common conditions of coverage under these policies.

¹⁷ <http://www.telegraph.co.uk/technology/news/12065496/Skier-Marcel-Hirscher-nearly-killed-by-falling-camera-drone.html>

¹⁸ Tailler, Sarah, *Drone Operator Fined after UAV crashed into Geraldton Triathlete*, November 12, 2014, <http://www.abc.net.au/news/2014-11-13/drone-operator-at-geraldton-marathon-fined/5887196>

Pricing of this specialty coverage is high and it left out the small and medium sized business.

In response 2015, Zurich Canada began offering its own drone insurance package to the Canadian market which it developed in partnership with Global Aerospace. The coverage schedules all drones just as one would schedule aircraft in an aviation policy or in a fleet auto policy. On offer is first party property coverage for theft, or damage to the drone, any of its onboard equipment and any ground equipment used to operate the drone. Also offered is third-party property damage and bodily injury liability coverage for injury or damage caused by the use and operation of the drone as well as premises liability for locations used in connection with the use of the drone. There are additional, optional coverage extensions for malicious hacking and damage, as well as personal injury arising from the use and operation of the drone (i.e., violation of privacy rights, etc.).

In January of 2016, Intact Insurance Company announced that it is now offering coverage for small and medium-sized businesses who are using drones as part of their business plan. Intact offers a rider to the existing property coverage to extend property coverage for the drone and its equipment. Further, there is a rider available to the CGL to extend the third party liability coverage to instances of bodily injury and property damage caused by the use and operation of drones.

It is likely that other carriers will follow the lead of Zurich and Intact and enter the market. In the meantime, the lack of any reliable experience data means that rates for this coverage is high. Internet chat rooms provide anecdotal information that this coverage will run between \$600-\$1,000 a year for \$1 million CDN of per occurrence coverage, depending upon experience and the nature of the operations. This could cause many businesses to think twice before purchasing this coverage, meaning that the only coverage commercial drone operators may have is their CGL policy, which almost universally contain an exclusion for aviation risks.

What about the recreational user?

Homeowners' and renters' coverage contain personal liability riders that also contain exclusions for aviation risks. Despite this, the American National Association of Insurance Commissioners issued an un-dated 'Alert' in the fall of 2016 that states, "If your drone crashes into someone else's vehicle or a person, the accident is your responsibility. If you have a homeowners or renter's policy, generally the policy will cover liability for an accident caused by your drone. Check with your agent or insurer to verify your policy contains this important coverage."¹⁹

In contrast, in July of 2016, the San Francisco Chronicle ran a news story as to whether homeowners' insurance would cover damage to a drone and liability arising from the use and operation of the drone. The reporter interviewed four separate insurers and recorded their answers. As to property coverage, the insurers almost uniformly stated that their policies would cover the drone if it was lost or stolen. However, they would not replace a

¹⁹ http://www.naic.org/documents/consumer_alert_drone_insurance.htm

drone damaged because of a crash as drone crash is not a named peril. As to third party liability, there was some consistency in the answer: Coverage is unlikely. The insurers cited the aviation exclusion, the business pursuits exclusion and the intentional acts exclusion.²⁰

The British newspaper, 'The Telegraph' has reported that leading British homeowners' insurers are moving to specifically exclude the liability risks associated with the use and operation of drones (given that drones "are too easily operated by amateurs, fools and children") but may cover the risk of loss or damage to the drone itself as well as its equipment.²¹

Coverage Arguments under Unendorsed CGL and Homeowners' Policies

Despite the proliferation of drone specific coverage, it is highly likely that CGL insurers and homeowners' insurers will be forced to determine if these policies apply to bodily injury or property damage arising from the use and operation of a drone.

Both CGLs and homeowners' wording carry exclusions for the use and operation of boats (excepting boats under a certain size), airplanes and motor vehicles that are required to be insured under applicable auto policies. These exclusions were placed in these general liability policies to exclude these specialized risks, particularly as specialized coverage is available to cover them.

Regardless of the insuring intent behind the creation of the exclusions, the issue will be whether in any given policy, the aviation exclusion excludes third party injury or damage caused by the use and operation of a drone. (Ancillary issues will be whether the intentional acts exclusion applies; whether the conditions of the policy have been met and, under a homeowners' policy, whether the drone was being used for a commercial purpose at the time of the injury or damage so as to engage the business pursuits exclusion.)

In Canada, typical homeowners' wording excludes injury and damage arising from the use and operation of "aircraft, or premises, property or operations related to aircraft".

Typically, in Canada, a CGL carries the following exclusion:

²⁰ Pender, Kathleen *Does your homeowners/renters policy cover drones?*, San Francisco Chronicle, July 22, 2016, <http://www.sfchronicle.com/business/networth/article/Does-your-homeowners-renters-policy-cover-drones-8404104.php>

²¹ Turner, Camilla *Home Insurers rush to exclude drones as Christmas sees popularity soar*, The Telegraph, December 25, 2015, <http://www.telegraph.co.uk/news/shopping-and-consumer-news/12068861/Home-insurers-rush-to-exclude-drones-as-Christmas-sees-popularity-soar.html>

e. Aircraft or Watercraft

"Bodily injury" or "property damage" arising out of the ownership, maintenance, use or entrustment to others by or on behalf of any insured of:

- (1) Any aircraft, air cushion vehicle or watercraft that is owned, operated by, rented or loaned to any insured; or
- (2) Any premises for the purpose of an airport or aircraft landing area and all operations necessary or incidental thereto.

Use includes operation and "loading or unloading".

This exclusion applies even if the claims against any insured allege negligence or other wrongdoing in the supervision, hiring, employment, training or monitoring of others by that insured, if the "occurrence" which caused the "bodily injury" or "property damage" involved the ownership, maintenance, use or entrustment to others of any aircraft or watercraft that is owned, operated by, rented or loaned to any insured.

This exclusion does not apply to:

- (1) A watercraft while ashore on premises you own or rent;
- (2) A watercraft you do not own that is:
 - (a) Less than 8 metres long; and
 - (b) Not being used to carry persons or property for a charge;
- (3) "Bodily injury" to an "employee" of the insured on whose behalf contributions are made by or required to be made by the insured under the provisions of any Canadian provincial or territorial workers' compensation law, if the "bodily injury" results from an "occurrence" involving watercraft.

The term "aircraft" is not defined in either policy.

Insurers are likely to argue that drones are regulated in Canada and in the United States as "aircraft" as they meet the definition of "aircraft" under the legislation applicable to "aircraft"; drones operate in airspace which is highly regulated and therefore they are "aircraft". It does not matter that there a pilot's license is not required to operate them; that they can be operated by a child (would a Cessna cease being an aircraft if an 11 yearold was at the helm?). What matters is the nature of drones and where drones operate. There can be no reasonable expectation that drones are other than 'aircraft'.

Insureds are likely to argue that 'aircraft' is not defined and in the absence of a definition, the common, every-day definition of 'aircraft' applies. Drones do not look like 'aircraft' and are primarily (in the homeowners' sphere) used for amusement. They are a toy – not an aircraft. Just as a homeowners' policy insures the use and operation of a rubber dingy and does not declare that to be 'a boat', a drone ought not to fall into the meaning of aircraft in order to exclude its use and operation.

The debate will go on until the insurance industry moves to define "aircraft" in the general policies it issues and, by doing so, decides conclusively whether for the purposes of insurance coverage, drones are "aircraft".

Re-Shoring Manufacturing: The Legal & Insurance Implications of 3D Printing

By Heather A. Sanderson

SANDERSON LAW

Legal Counsel

Calgary | Alberta | Canada
www.sanderson-law.com

hasanderson@sanderson-law.com
T 403-837-2508

Heather A. Sanderson, the principal with Sanderson Law in Calgary, Alberta, Canada, is a nationally recognized author and insurance coverage counsel, who has provided expert evidence on CGL coverage issues to Canadian Courts and has appeared as counsel before a full panel of the Supreme Court of Canada.

Currently, Heather is a director of Canadian Defence Lawyers (CDL), Chair of CDL's Insurance Coverage & Practice Committee and Chair of the DRI's Insurance Law Subcommittee, Canadian Law and Cross-Border Issues and a member of the steering committee of DRI's Insurance Law Sub-Committee. She has both authored and co-authored the Canadian law chapter of The DRI Insurance Law Committee's Coverage B: Personal and Advertising Injury Compendium and a similar chapter in the soon-to-be-published Duty to Defend Compendium.

Copyright Notice: Heather A. Sanderson and DRI hold the copyright for the original version of this paper according to the terms of an agreement that they have signed. © December, 2015. Heather A. Sanderson and FDCC hold the copyright for this updated paper according to the terms of an agreement that they have signed © March, 2017

Receipt or possession of this paper does not convey any right to reproduce its contents.

Introduction

The American immigration system has a notoriously complex and slow process to obtain work visas that is impacting its ability to compete in the tech sector. If a significant percentage of a startup's work force requires visas, it is unlikely that there will be uniformity in the timing of the issuance of the visas. Unless the applicant for a visa has complete academic credentials in the area, it is unlikely that a visa will be granted. If and when a visa is granted, a worker's significant other will seldom qualify for legal work.

In contrast, Canada has instituted a start-up visa program, the first of its kind in the world. that targets immigrant entrepreneurs with the skills and potential to build innovative businesses in Canada that can create jobs for Canadians and compete on a global scale. Those who qualify earn immediate residency resulting in what the *New York Times* calls "an experiment in designer immigration." But Canada's visa program is working. Despite the lack of an entrepreneurial incubator program, such as 500 Startups in Mountain View, Ca., Canada, and, in particular, the lower mainland of British Columbia, is becoming Silicon Valley north. Jeremy Robbins, special counsel in the office of New York Mayor Michael Bloomberg, observed, "While we sit on our hands, our competitors around the globe are rolling out the red carpet to recruit the most talented individuals away from us."

In addition to an easier road to obtain work visas, in comparison to the United States, Canada offers better tax rates, research and development tax credits, a myriad of government funding programs aimed at tech entrepreneurs, lower cost of living and affordable talent. Additionally, a low Canadian dollar stretches any American seed money that a given company may have.

3D Printing is a technology that is emerging as a force in the tech sector. Canada's national newspaper, The Globe & Mail, reported in February 2015 that the technology is helping to sustain and create jobs as well as keep intellectual capital in Canada.

What is 3D Printing and How Does it Work?

3D Printing is a form of additive manufacturing, where a printer, that functions much like an ink-jet printer, creates a 3D object through a layer-by-layer deposition of material.

The first step is to create a design on computer-aided drafting software (CAD). This software models 3D objects for the printer and can even receive a virtual copy of an object from a 3D scanner. (A 3D scanner scans the dimensions of a real-life object.)

The CAD software then slices the virtual model into very thin cross-sections that are transmitted to the printer. The printer uses the dimensions of each of these tiny layers to build the 3D object through additive manufacturing. The objects created through this

process do not appear to be layered because each layer is so small; the average height of each of these layers is just 100 micrometers, about the diameter of a single human hair. Various forms of plastic are the most common mediums used by 3D printers to create these objects. Other mediums, called 'inks' are paper, powdered metals and even carbon fibre.



Figure 1 Capture from the Dremel website, demonstrating a laptop connected to a consumer grade 3D printer with the plastic filament 'ink' to the left of the 3D printer

What is 3D Printing used for? Just like a paper printer can print any kind of written word, a 3D printer can be used to print any object. The widespread use of 3D Printers is akin to the development of the printing press – it is revolutionary technology producing revenues for printers and inks that are growing exponentially.

Wholers Associates is an American consulting firm that has been covering the 3D printing industry since 1986, the year that the first American commercial 3D printing company opened its doors. In a 2015 report this firm states that the total global sales of 3D printers (both desktop and industrial printers) in 2014 was about \$1.1 billion USD. As for future growth, the same report predicts that total global sales in 2016 will increase to \$7.3B USD, while in 2018 it will be \$12.7B USD, and in 2020 the market is expected to reach \$21.2B USD. That growth is independent of the revenues generated by the imaginative and explosive applications of 3D printing that will have a significant impact on the worldwide economy in a myriad of ways.

Applications of 3D Print Technology

Canadian researchers join a long list of international researchers that are using the technology in ingenious ways that will impact longstanding practices in almost all industrial sectors.

3D printing applied in the health care sector is producing astonishing results.

Researchers at the University of Toronto and Toronto's Sunnybrook Health Sciences Centre, developed a printer that looks like a regular inkjet printer that uses the chemical building blocks of human skin in place of ink. In 45 minutes the printer produces one square meter of tissue closely resembling human skin that can be used to treat burn patients. Instead of painful skin grafting, printed skin will decrease pain, decrease the incidence of infection, speed healing and decrease time spent in hospital.

Other researchers at these institutions, with funding from the Canadian Institute of Health Research and the United States Army, are using a patient's own stem cells and a chemical phosphate compound to print artificial joints to be used in joint replacement surgery. Existing joint replacements that use metal or plastic parts, usually require cementing to bone, which can deteriorate or come loose over time, and usually require replacement after 10 to 20 years. A printed joint is preferable as it is a permanent solution. Natural bone regrows over the porous and biodegradable printed joint, which, in turn, dissolves over time as the patient's natural bone regrows. A news release on this research states "The bone attaches to the cartilage that was implanted, and you completely reconstruct a normal joint using the patient's own cells. So there are no metals or plastics, and no typical way of failure that's found in these prostheses."

Customized printed prosthetics are now available worldwide at greatly reduced costs reducing hospitalization costs and increasing quality of life.

Researchers worldwide are experimenting with printing organs such as kidneys, hearts and lungs for transplant. To date, printed shunts and blood vessels have been used with success.

The aviation, automotive and construction industries are other sectors that are witnessing significant impact from the technology. These sectors employ enormously expensive, industrial sized printers and inventive 'inks' to forever alter long-standing practices. When the technology is applied to this scale of operation it is sometimes called Big Area Additive Manufacturing (BAAM).

The aviation industry uses 3D printing technology because it has the capability of reducing aircraft weight. According to American Airlines, for every pound of weight removed from the aircraft, the company saves 11,000 gallons of fuel annually. The American Federal Aviation Authority already cleared GE Aviation's first 3D printed part to fly - following an investment of \$50 million GE Aviation is now producing 3D printed fuel nozzles for the next-generation LEAP jet engine. Boeing has delivered airplanes to customers that contain 3D printed parts upon which they have filed a series of patents. For example, the Boeing 787 Dreamliner apparently has 30 printed parts. Boeing is now experimenting to build an entire airplane wing using 3D print technology.

The aerospace industry is also using this technology. A specially adapted 3D printer is currently on the International Space Station to replace broken parts (perhaps eliminating the need for imaginative uses for duct tape and tube socks *à la* Apollo XIII).

The construction industry is experimenting with 3D printing. A Chinese company,

ZhuoDa Group has filed a series of patents for a two-storey modular home that is 'printed' in a factory and assembled on site using cranes in about three hours. The overall cost of the printed home is a fraction of what it would cost to build a comparable home at a building site. A Dutch company has filed similar patents.

For several years now the automotive industry has been using 3D print technology to rapidly create prototypes as they work through design changes. 3D printing is called the ideal tool to verify and visually communicate a design. Will we see a 3D printed car? American researchers assembled Urbee 2, a car that looks like a lozenge on wheels, from printed elements, which recently crossed the United States using ten gallons of fuel.

Having secured the prototyping niche in the automotive industry, automotive analysts, such as the consulting firm Carlisle & Company, predict that car dealerships may someday use their own 3D printers to make auto parts onsite. That raises a variety of issues. One of them: Who would need parts suppliers? (This is likely a futuristic prediction as traditional mold-injection line production can produce the volumes that the after market auto parts industry needs; 3D printing is not there yet.)

Using 3D print technology to manufacture replacement parts in obsolete equipment and appliances is an enormous growth area for 3D printing. The United States Navy and Maersk have combined to make 3D printers to allow a ship's crew to manufacture replacement parts for broken and obsolete ship parts while at sea.

The food industry is another growth area for the technology. Although we are far from experiencing in real life Star Trek's replicator which prepped, cooked and served food on command, by using edible inks (such as chocolate, dough, mashed potatoes and pureed food of any description), the technology can be used to create product differentiation and customization in the mass-produced food industry. It can also create unique food formulations for dietary needs; simplify distribution chains in remote locations, such as Canada's far north, where all food stuffs are twice the price of identical items available to the majority of the population that hugs the 49th parallel. Finally it can take unappetizing food sources that are plentiful and high in nutrients, such as protein rich insects, and transform them into visually appealing and tasty food.

A frightening application of the technology is the ability to print a plastic gun capable of firing live ammunition that can slip through metal detectors.

The Macro and Micro Benefits of 3D Printing

This ever so brief exploration of the applications of the technology has a theme – 3D print technology democratizes and localizes the manufacturing process.

It is well known that creating a prototype allows a design to be checked and tweaked. It is far easier to communicate the innovation when you can easily see it, feel it and use it. Further, a prototype permits easier communication with investors and creates a market for the product by allowing consumers at trade fairs to touch it and see its real-time use through demonstrations. The traditional prototype production costs of building molds for

the prototype, buying factory time for production and incurring the cost of freight are enormous and sometimes insurmountable barriers to innovation. The time delay allows others with easy access to production facilities to bring the innovation to market faster than a startup business.

3D print technology shrinks the cost of creating a prototype, as well as the sometimes equally important time-to-market factor. It allows almost anyone with the next new idea to rapidly create a prototype, sometimes on the same day as design completion, without the enormous cost of traditional methods of creating a prototype. The design can be tested and tweaked without the costs of re-jigging the prototype molds and repeating the traditional prototype production process.

There is a very real 'green' element to the technology. 3D print technology almost eliminates wastage of raw materials. Regular manufacturing involves machining of molded parts. This technology precisely creates objects layer by layer with no machining required. Further, obsolete parts can be replicated on a cost effective basis, breathing new life into aging appliances and machines.

Why would Toyota need to operate and staff a factory and a distribution chain to produce spare parts for my car when they could just sell me the design so that I can have it printed at Staples? This example illustrates that this technology allows for local production as consumers will buy a product's design (often over the internet) and 'print' the product locally, shortening or eliminating costly and environmentally unfriendly supply chains, thereby reducing our carbon footprint. But what happens to the factory workers, the truckers and the people who work in warehouses?

In 1907 a relative of mine left the farm in rural Quebec for Detroit, Michigan and soon obtained lucrative assembly-line work producing the Ford Model T at the newly opened Highland Park Ford Plant – which, when it opened, was the largest manufacturing plant in the world. This single plant used a massive economy of scale to render cars affordable and at the same time changed how everything – not just cars - were built. Two generations of his family have followed him, working in various manufacturing capacities at Ford.

Assembly line robots and 3D Printing will likely end this proud manufacturing tradition. Essentially unskilled manufacturing jobs will disappear in favour of highly skilled 'white' collar jobs as this technology reduces the labour intensive traditional manufacturing model but creates a need for designers and engineers.

How fast will we realize this change? The rate of change will be driven by price and quality.

Although I can drive to my local Walmart and buy a 3D printer to print and replace lost Lego blocks for the same price as a top-of-the-line laser printer, the industrial-sized 3D Printers (the ones that produce the market changing products) are hugely expensive; the 'inks' are equally expensive.

Currently there are difficulties in creating products that require multiple ‘inks’. Products that are made through the deposition of layers of ink sometimes lack critical vertical stability.

Current price and quality issues such as these render it difficult to envision that a locally produced item can effectively compete in all sectors with mass economies of scale, which created the factories and support industries of the industrialized world. However, we cannot fool ourselves into thinking that 3D printing is a fad that will fade - there is no doubt that like the printing press and Henry Ford’s assembly line, 3D Printing revolutionizes how things are made and will forever change the economics of the manufacturing sector by eliminating low skill jobs thereby altering the way of life for many North Americans.

Risks of 3-D Printing

There is a substantive quality issue associated with 3-D Printing. The additive layering process could result in hidden defects produced by lamination (weakness in material layers) or inclusions (foreign material between layers).¹ There is a risk of latent defects appearing in the years to come that does not exist with traditional manufacturing. Further there is a lack of standardization with respect to the “inks” or materials used to “print” the item. The process and climate within which the process is conducted could result in contamination. Those involved in the printing could be exposed to toxins.

Legal & Regulatory Issues Involving 3D Printing

Over the decades, traditional manufacturing developed a system of product standards that are well known and relied upon by consumers the world over. None of that is present with 3D Printing (which is really manufacturing as opposed to printing). As 3D Printing currently stands, there are significant legal issues stemming from the lack of regulation of the quality of the products produced through the process.

The traditional manufacturer, distributor and consumer divisions of liability will erode as the consumer begins to play a role in product design. Those who hold repositories for CAD files face issues of copyright, patent and trademark infringement. Online sources speak of the existence of demands that the sites who host these files take down certain CAD programmes. The risk of intellectual property infringement is passed down to those who acquire and then use the CAD files.

Enforcing traditional intellectual property rights on the design of a product will be difficult. How do you trace usage of the design? Identifying the infringer is difficult. Is the infringer the person who distributes the digital file without permission, the 3D printing shop or the end user, or all three? How do you identify them? Will print shops

¹ Tim Woods, AVP of Engineering/Risk Management for Aviva Canada, as quoted by Stelmach, Angela, *Possibilities of 3-D Printing*, Canadian Underwriter, published by Newcom Business Media Inc., Vol 83, Issue 2, February 1, 2016, at p. 30.

need a license from the intellectual property owner to print the object? How can print shops easily check whether a physical object, software or design has been patented or trademarked anywhere in the world?

This is an international issue as the use of CAD programmes transcend national boundaries and requires unified action on a global scale. Pending that development, those who host sites that offer CAD programmes and those who operate 3-D printers must take responsibility for this issue. Perhaps the printers themselves can be designed to block the printing of CAD files that have not been approved by management as being clear of intellectual property rights issues. However, regardless of what measures are put in place, pirated CAD programmes will remain in existence, just as pirated music is played the world over.

When there is a product failure resulting in bodily injury or property damage, arguments over contribution and apportionment of liability between designers of the CAD programme (should they be found), printing machine components, “ink” suppliers and end users will result in protracted litigation and enormous defence costs.

The end user who may have been the driving force behind the creation of the failed product will abound. Commercial applications of 3D printing will require stringent contracts with strict indemnity clauses to protect against the risk of this new wild west in manufacturing. Individuals involved in ‘man-cave’ manufacturing will have to utilize a significant degree of common sense and exercise great care over the use of their printed/manufactured items or risk the consequences.

In summary, 3D Printing will have the same impact on intellectual property rights over physical property that Napster had on the music industry. In addition, it will upend traditional product liability law and introduce untold liability on individuals who naively print and distribute items that they print from their consumer grade 3D printer. Perhaps the sense of complacency in the marketplace as to these risks arises as consumers equate 3D printers with photocopiers when in fact they have nothing to do with photocopiers. When individuals and organizations realize that they are operating a mini-manufacturing plant with the attendant risks and liabilities of a traditional manufacturer, then perhaps these liability issues will be addressed by government and trade organizations.

Insurance Coverage Implications of 3D Printing

General liability insurers will be hit with coverage challenges from the onslaught of intellectual property lawsuits and new challenges as to what is and what is not a professional service when it comes to the design of a product.

Cyber coverage challenges will emerge from the hacking of designs.

Homeowners’ insurers must look at their business pursuits exclusion through the lens of 3D Printing. Do existing exclusions cover the necessary angles? Where are the coverage challenges?

Professional liability insurers will face new, international liability risks as designs are sold and implemented outside of their intended market. The tweaking of existing exclusions to deal with that risk will create coverage challenges.

A benefit to the industry may be the reduction in the indemnity period for business interruption and machinery break down claims due to the ability to print a key replacement part or a whole machine. Will the failure to access this technology in an appropriate case create a new avenue to argue a failure to mitigate business interruption loss?

Product liability insurers have to act now to adjust risk and severity ratings to this shifting sea in manufacturing or face long-tail product liability exposures through flaws in the 3D printing process. New endorsements and exclusions will be issued in the years to come as underwriters attempt to rate the risk posed by this very new, very cool, yet very risky technology. Each new endorsement will introduce coverage challenges.

Closing Thoughts

3D print technology brings production back to first world countries - a process that industry watchers call 're-shoring'. However, this technology will only re-shore manufacturing to those countries and regions with the skill level to support it.

The need to foster and grow tech sector talent will promote significant and far-reaching socioeconomic change throughout the first world in the areas of education, wealth distribution and the use of human capital. Countries like Canada, whose national policies are geared to nurturing innovation, have a decided advantage with this emerging technology through its ability to actively recruit and employ the best and the brightest.

INSURANCE IN TIMES OF CLIMATE CHANGE

FDCC WINTER MEETING

MARCH 6-10 2017

CHARLESTON, SOUTH CAROLINA

BY

Richard K. Traub

Traub Lieberman Straus & Shrewsberry



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY LLP

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON OFFICE)

www.traublieberman.com

An aerial photograph showing a large, rectangular houseboat with a dark roof and white trim floating on a calm blue lake. The houseboat has a small dock attached to its right side. In the foreground, the rooftops and chimneys of several houses are visible, including one with a prominent red-tiled roof. To the left, a grassy shoreline with some trees meets the water. The text "This is not a house boat – Claimed wind damage" is overlaid in white on the lake.

This is not a house boat – Claimed wind damage

Does the Cause Matter?

The Denialists

- Global warming has little to do with global warming.
- H.L. Menchen – “The whole aim of practical politics is to keep the populace alarmed – and hence clamorous to be led to safety – by menacing it with an endless series of hobgoblins, all of them imaginary.”
- “The urge to save humanity is almost always only a false face for the urge to rule.”
- “It doesn’t matter what is true, it only matters what people believe is true.” Paul Watson, founder of Greenpeace.
- The threat to the world is not man-made global warming or climate change. It is, as is always the case, a current group of humans who want to impose their values and desires on others.
- “We routinely wrote scare stories...Our press reports were more or less true...We are out to whip the public into a frenzy about the environment.” Jim Sibbison, former public relations official for the EPA.



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY LLP

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON OFFICE)

www.traublieberman.com

The Oceans will Give us the Answer – Humankind or Random Events?

- Warming of late 70's correlates almost 1:1 with Pacific warming.
- Cycle flipped in 1978. 30 year stretch now over and starting to cool.
- Atlantic still in its warm cycle but will soon turn cold.
- If the naturalists are right, the temperatures will cool. If they do not, those that say it is CO2 will be proven right.
- Oceans of the planet have 1,000 times the heat capacity of the atmosphere. Thus if you warm the ocean, you warm the air.



The Human Cause



- Some have argued that there has been a pause in global warming.
- NOAA – never stalled, just masked by incomplete data.
- Temperature rate of increase during the last half of the 20th century virtually identical to that of the 21st century.
- Warming from 1998-2012 was more than double the previous estimates.
- Humanity is the cause of earth getting hotter primarily by burning fossil fuels and deforestation.



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com



What Climate Change? Superstorm Sandy

What Should be Done? 10 Suggestions

- Limit power plant production.
- Prioritize China's pollution problem.
- Expand carbon markets around the world.
- Unleash clean energy in the US.
- End fossil fuel subsidies.
- Slow deforestation.
- Stop methane leaks.
- Cut deadly soot.
- Phase out super polluting hydrofluorocarbons (HFCs).
- Reduce fertilizer production.



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com

What The Question/Answer?

- Not who is right or wrong!
- Should we be spending time and treasure on something that will be proven by objective testing over the next few years?



Why Not Let the Forecast Happen?

- Will need the Apollo program to find another place to live.



- Can't we still improve air quality regardless?
- What should the industry be doing and what is the liability for harms resulting from climate change?



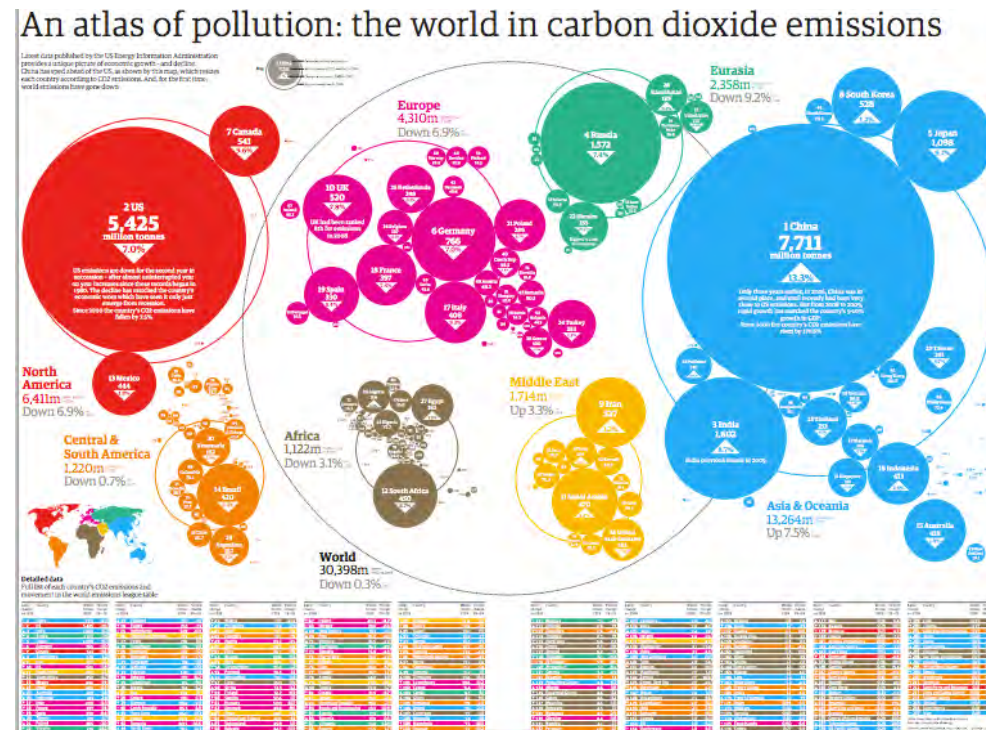
TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com

Liability for Climate Change

- Standing and Political Question.
- Judges barred from imposing their own limits on GHG emissions.
- Clean Air Act supersedes and federal common law.
- No common law claim of nuisance.



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com

Insurance Coverage for Injury or Liability Associated with Climate Change

- “Associated” not “Arising From.”
- Severe or Extreme Weather Events.
- Its Real and Will Lead to Increased \$ for Covered Events.
- No coverage for “resulting from” but there is for “associated” with climate change.
 - Wind, flood, freezing, heat, earth movement, collapse.



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com

The Industry

- Insurance industry is uniquely qualified to understand climate change and broaden society's awareness of it and provide solutions.
- Losses from extreme events to increase by as much as 40% by end of decade.
- Bad year could exceed \$1 Trillion.
- Duty to society and to shareholders to minimize exposure.
- Historically taken the lead in minimizing risk:
 - Building codes for fire and earthquakes.



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com

Loss Prevention Solutions

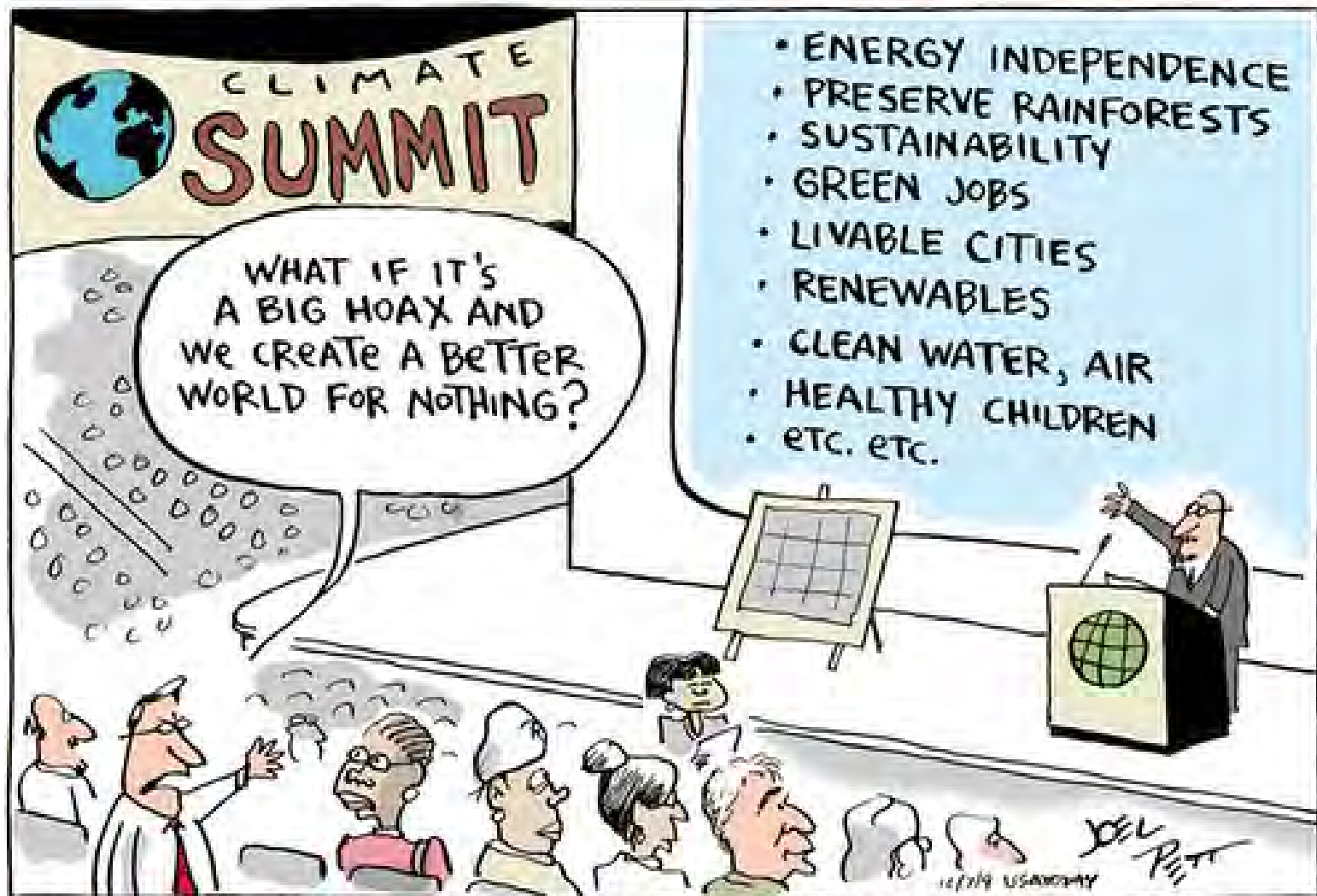
- Energy Efficient Programs.
- Green building designs.
- Sustainable driving practices.
- Carbon emission trading.
- Financing mortgages for those with efficient homes or home upgrades.
- Reduce their own GHG's.



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com

- Industry is responding:
 - Wind farms and other alternative fuels.
 - Emerging financial risks from carbon trading.
 - Protect those that invest in clean technology projects against failure to deliver agreed emission rates.
 - Carbon risk management consulting services.
 - Discounts on auto insurance for driving fewer miles.
 - Discounts for green building construction.
 - Coverage for loss of income for those that sell excess energy created from private sources.
 - Innovative insurance products that can become profit centers.



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com

Last Thoughts



- 2016 probably the hottest ever on record.
- More heatwaves, extreme rainfall, higher impact of tropical cyclones/hurricanes.
- Arctic sea melted early and fast.
- CO2 levels reached new highs.
- June was 14th consecutive month of record heat for land and oceans.
- 378th consecutive month above 20th century average.
- El Nino event of 2015 was one of the most powerful on record.
- Temps in Coral Sea and Great Barrier Reef highest on record resulting in bleaching of the reef. Impacts lifetime of reefs.
- Depending on where you are, you are either too wet or too dry.
- Enough said.



TRAUB LIEBERMAN
STRAUS & SHREWSBERRY

NEW YORK - NEW JERSEY - CHICAGO - CALIFORNIA - FLORIDA - LONDON (LIAISON)

www.traublieberman.com

Insurance in Times of Climate Change – Does the Cause Matter?

By Richard K. Traub

Traub Lieberman Straus &
Shrewsberry LLP

322 Highway 35, Red Bank,
New Jersey, 07701

+1 (732) 985-1000

+1 (732) 985-2000

www.traublieberman.com

INSURANCE IN TIMES OF CLIMATE CHANGE

Does the Cause Matter?

The Denialists¹

There are many scientists that truly believe that climate change is not under control of humankind, i.e. that CO₂ is not the controlling factor, rather, it is nature that controls by way of sun, oceans, and random events. What these naturalists point to is what they consider to be objective science-based evidence developed from satellite imagery that began measuring events in 1978, after the Pacific Ocean had been in its “cold cycle” for some 30 years. That cycle is now in its second half. They argue that the last 15 years have not shown any increase in temperature.

The warming that occurred from the late 1970's to the mid '90s correlates almost 1 to 1 with the Pacific warming. This massive body of water with vast stores of energy warmed the air until the global atmosphere adapted and the temperature rise leveled off. The Pacific flipped to its warm cycle in 1978, that 30 year stretch is now over, and it is beginning its cold cycle. The Atlantic is still in its warm cycle but also will soon turn cold. At that time, we will see – or so say these naturalists - that global temperatures will undoubtedly come down. If they do not, then those that say it is CO₂ will be proven right and the naturalists, wrong.

Consider, however, that the oceans of the planet have about 1,000 times the heat capacity of the atmosphere. Naturally, therefore, if you warm the ocean, you warm the air. If they cool as predicted – back to where they were in the mid to late 1970's - then the global temperatures will come down.

Those that deny human involvement in climate change believe that it is power and money that lead the argument. They point to a quote by H.L. Mencken, the famous columnist: "The whole aim of practical politics is to keep the populace alarmed — and hence clamorous to be led to safety — by menacing it with an endless series of hobgoblins, all of them imaginary." And, "[t]he urge to save humanity is almost always only a false face for the urge to rule it"². They believe that his insights to those whose lives are addicted to the seeking of power, or control or fame or money are still as valid today, as they were 70 years ago. I have attached as an exhibit, quotes from some other powerful; rich; religious; studious; famous; and fanatics all sharing a

¹ Global Warming Has Little to Do with Global Warming, Joe Bastardi, The Patriot Post, July 26, 2014; and private conversations with Mr. Bastardi.

² Global Warming Quotes & Climate Change Quotes: Human-Caused Global Warming Advocates/Supporters; Copyright 2009-2014 C3 Headlines, Climate Change Conservative.

common theme of keeping "the populace alarmed" to further their own personal, sometimes selfish, goals.³

Finally, they argue that the threat to the world is not man-made global warming or climate change. The threat to the world, as is always the case, is a current group(s) of humans who want to impose their values and desires on others.

The Human Cause

There has been a long debate over what some say has been a pause in global warming. However, it now appears that this so-called pause never happened at all. A new study by NOAA (National Oceanic and Atmospheric Administration) found that the warming never stalled at all during the last 15 years; it was just masked by incomplete data that have been improved and expanded in recent years. In fact, it now appears that the rate of temperature increase during the last half of the 20th Century was virtually identical to that of the 21st Century. Not good.

Global temperature trends were missing measurements from key locations such as Asia, South American and Africa, where measurements were scarce. Within the last 10 years, thousands of new weather stations have been built in those under-reported areas on land and a huge network of buoys have been deployed in the oceans and seas to measure sea surface temperatures. The conclusion – warming from 1998-2012 was more the double the previous estimates. What is more concerning is that these measurement do not factor in what has happened in the Arctic, where temperatures have increased rapidly in recent decades but where there are, again, a limited number of weather recording stations.

Some scientists say the case is closed-humanity is causing the earth to get hotter primarily by burning fossil fuels and with smaller contributions from deforestation. Natural amounts of CO₂ in the air vary from 180 to 300 parts per million. Today's levels are around 400 parts per million; that is 40% higher than the highest natural levels over the past 800,000 years. Scientists also can tell that most of the CO₂ comes from burning coal and oil because the chemical composition has a unique fingerprint. Deforestation contributes, as we do not have as many trees to absorb the extra CO₂⁴.

So what do we do about it? The scientists that argue humanity as a cause have 10 suggestions⁵:

1. Limit power plant production – they are the largest source of CO₂.

³ Supra.

⁴ How are Humans Responsible for Global Warming? Environmental Defense Fund; undated.

⁵ 10 Climate Solutions That Will Help Turn the Corner, Environmental Defense Fund; undated.

2. Prioritize China's pollution problem – no climate plan can succeed without this. China burns half of the world's coal, but is also the largest producer of clean energy. They have 45% of the world's new wind energy production.
3. Expand carbon markets around the world. These create economic incentives for reducing greenhouse gas pollution and reward innovators who develop clean energy.
4. Unleash clean energy in the US – there are older, obsolete laws that govern electric companies that block the way to clean energy. There is a neighborhood in Austin, TX called Pecan Street, Inc. where residents live with almost totally clean energy.
5. End fossil fuel subsidies. We are spending six times as much on subsidies as we are on renewable energy.
6. Slow deforestation, which accounts for 15% of global greenhouse gas emissions. Give credits in a carbon market for keeping forests standing.
7. Stop methane leaks. About 1/3 of global warming comes from methane and similar pollutants. Colorado was the first state to adopt regulations for methane pollution.
8. Cut deadly soot. In developed nations, black carbon is on the decline due to better controls on burning diesel fuel. Not so in developing nations.
9. Phase out super polluting hydrofluorocarbons (HFCs). These are man-made chemicals used for industrial processes such as in air conditioning and refrigeration. Years ago, it was determined that HFCs do not harm the ozone layer, so production went rampant. But we now know that they are 1000 times more potent than CO₂ in trapping heat.
10. Reduce fertilizer production – if not applied carefully when used in agriculture, the excess converts to nitrous oxide, a greenhouse gas 300 times more potent than CO₂. Advances in science have allowed for more precise levels of fertilizer. There also are fertilizer efficient grains that can be used in farming.

What Should the Question and Answer Be?

The answer depends, of course on the question, and the question today is not who is right and who is wrong, it is, should we be spending time and treasure on something that will be proven by objective testing over the next few years? Vast resources have been poured into climate change issues by the United States and others, while other nations, with far greater CO₂ contamination, ignore the issue. Between 1993-2014, the U.S. spent \$165 Billion on climate change, \$35 Billion of it on climate science. The entire Apollo project, whereby we put a man on the moon, cost less. Why not let the forecast, which is already underway and simple enough to score, happen? Why? Because if we do not do something, we will need the Apollo program to find another place to live after we destroy this beautiful planet. Secondly, who cares? What if the denialists are correct? Can't we still improve our air quality by reducing the use of fossil fuels? Lastly, from an insurance perspective, what should the industry be doing and what is the liability for harms resulting from climate change?

What is the Liability for Harms Resulting from Climate Change?

In the United States, there are two primary threshold barriers to litigation over climate change. The first is “standing” and the second “political question”. “Standing” limits jurisdiction in the Federal Courts to cases or controversies. That, in turn, means that a person who sues must show an “injury in fact”; causation; and redressability – that is, the relief sought would remedy the injury. Claimants complaining of injury from climate change may have their claims defeated on any one of these issues. For example, how can one argue that his or her crops were destroyed by climate change and/or that the defendant’s specific green house gases (GHG) contributed to same? There have been decisions giving states more latitude to meet standing, but not individuals. The “political question” doctrine asks whether there is a justiciable claim – that is, the courts will not interfere with the business of other branches of government. The courts have found very few situations and issues that present political questions that it will hear.⁶

If these hurdles are jumped, there are additional issues that claimants face in the context of climate change. First the U.S. Supreme Court has read the Federal Clean Air Act⁷ to bar federal judges from imposing their own limits on GHG emissions from fossil fuel fired power plants – separate from those imposed by the EPA under the Act. Thus, the courts have held that the CAA supersedes any federal common law of nuisance that might otherwise give grounds for relief.⁸

Further, in 2013, the Federal Court for the Southern District of Mississippi held in *Comer v. Murphy Oil Co.*⁹ that those suffering from climate change impact could not assert either claims based on federal common law of nuisance seeking monetary damages (as opposed to injunctive relief) or state law claims, either common law or statutory. In that case, landowners sued Murphy Oil arguing in tort (nuisance, trespass and negligence) that it and other chemical, oil and coal companies emitted GHG’s in such amounts that it caused warmer ocean temperatures, which causes Katrina to intensify, causing rising sea levels that aggravated the hurricane’s impacts. The court found that it could not control the level of emissions – that this was left to the CAA. In the end, the U.S. Supreme Court, having now refused to hear further argument on those cases; leaves little room for any significant common law response to GHG emissions.¹⁰

⁶ Climate Change and Existing Law: A Survey of Legal Issues Past, Present, and Future, Robert Meltz, Legislative Attorney, Congressional Research Service, August 20, 2014.

⁷ 42 U.S.C. §7401 et seq. (1970).

⁸ Supra.

⁹ *Comer v. Murphy Oil USA, Inc.* (5th Cir. May 28, 2010).

¹⁰ *Comer v. Murphy Oil USA, Inc.* (U.S. Sup. Ct. Jan 10, 2011).

In another seminal decision is *Kivalina v. ExxonMobil Corporation, et al.*¹¹ This lawsuit was filed on February 26, 2008 and was based on the common law theory of nuisance. It claimed monetary damages from the energy industry for the destruction of Kivalina, Alaska by flooding caused by climate change. The damage estimates made by the U.S. Army Corps of Engineers and the Government Accountability Office were placed between \$95 million and \$400 million.

The suit was dismissed by the United States district court on September 30, 2009, on the grounds that regulating greenhouse emissions was a political rather than a legal issue and one that needed to be resolved by Congress and the Administration rather than by courts. An appeal was filed with the Ninth Circuit Court of Appeals in November 2009. In September 2012, the panel of appeals judges decided not to reinstate the case. The city appealed the court of appeals decision to the U.S. Supreme Court and on May 20, 2013 the Supreme Court justices decided not hear the case, effectively ending the city's legal claim.

Insurance Coverage for Injury or Liability Associated with Climate Change

The first order of business is to note that we use the word “Associated” here and not “arising from”. Thus, we are referring to events that result from severe or extreme weather events. Insurers are well aware that whether or not scientific consensus is correct – climate change is indeed an issue and that it will almost certainly, in time, bring on more frequent extreme weather events, which, in turn, will lead to substantially increased payments for covered events. I am not aware of any policies that provide coverage for injuries “resulting from climate change” but there are many policies that cover many of the injuries “associated” with climate change, such as flood, wind, freezing, heat, earth movement, and collapse.

Some of these issues are more relevant to climate change than others. Obviously, the impact of coastal hurricanes can be magnified by rising sea level; coverage is impacted by whether a given item of damage is caused by wind or flood and whether the flood exclusion covers man-made causes such as the alleged failure to maintain levees, as was alleged in Katrina-related litigation. Another issue of coverage is – can coverage be defeated if a given event was contributed to by the insured’s own GHG emissions? There is at least one Virginia case¹² which held that a carrier was not obligated to defend an insured under a GL policy in such an instance.

Another insurance dilemma is whether GHG emissions constitute a pollutant. The Massachusetts courts have held that indeed GHG emissions are pollutants under the CAA, raising the question of whether coverage would be expanded to bring in damage traceable to GHG emissions or whether coverage would be precluded by a pollution exclusion.

¹¹ 663 F. Supp. 2d 863 - Dist. Court, ND California, 2009.

¹² AES Corp. v. Steadfast Ins. Co., 725 S.E. 2d 532 (Va. 2012).

How Should the Insurance Industry Respond to Climate Change?

With its resources financially, in risk management and in scientific knowledge, the insurance industry is uniquely qualified to understand climate change, broaden society's awareness of climate change, and provide solutions to minimize the impact of climate change. Predictions are that losses from extreme events will increase by as much as 40% by the end of the decade; and losses in a bad year could exceed \$1 Trillion.¹³ Query whether there is a duty to society, and, indeed, to shareholders, to take action to minimize this exposure. Some carriers responded by refusing to renew policies in Gulf States or in Wild Fire States.

What is more difficult to track, beyond refusing to renew or increasing premium, is the reduction in coverages; that is, increased deductibles, reduced limits and sub-limits, and new exclusions. This is financial risk management. But what about a proactive or holistic approach to risk management? That is, spending dollars on clean energy technologies which represent, in, turn a large new capital base with associated business operations, all requiring insurance of its own.

By way of example, the insurance industry has historically taken a leadership role in minimizing risks – starting with building fires and earthquakes. The industry today has an opportunity to develop creative loss prevention solutions and products that might reduce climate change related losses for consumers, government and insurers. The industry can partake in a wide range of activities that help improve extreme event resistance and adaptation. These include energy efficient programs, green building designs, sustainable driving practices and carbon emission trading, and even financing mortgages for those with efficient homes or home upgrades. They must also lead by example by reducing their own GHG's. All insurers have to contribute to the understanding of climate change.

Opportunities exist on many other fronts. Just as the industry adapted from insuring horse drawn carriages to automobiles, they are responding to climate change initiatives today. There are wind farms and other alternative fuel facilities and emerging financial risks from carbon trading. Those policies protect those that invest in clean technology projects against failure of the project to deliver the agreed-upon emission levels¹⁴. Some are offering carbon risk management consulting services. Others offer incentives to policy-holders who contribute to the effort to curb global warming. These include discounts on auto insurance for driving fewer miles and policies for green building construction. There is even coverage for loss of income for

¹³ Responding to Climate Change – The Insurance Industry Perspective, Dr. Evan Mills, www.climatereactionprogramme.org.

¹⁴ Carbon trading is the process of buying and selling permits and credits to emit carbon dioxide. It has been a central pillar of the EU's efforts to slow climate change. The world's biggest carbon trading system is the European Union Emissions Trading System (EU ETS).

those that sell excess energy created from private sources such as solar power and wind back to the grid when systems fail. These are all innovative insurance products that can become profit centers for insurers as well as helping them become good world citizens.

Last Thought¹⁵

According to the United Nations, 2016 will be recorded as the hottest year ever on record. This means more heatwaves, more extreme rainfall, and potential for higher impact tropical cyclones/hurricanes. Arctic sea ice melted early and fast, another indicator of climate change. CO₂ levels have reached new highs. June of 2016 was the 14th consecutive month of record heat for land and oceans. It also marked the 378th consecutive month with temperatures above the 20th century average. The last month with temperatures below the 20th century average was December of 1984 – almost 32 years ago. Another month, another record.

The average temperature for the first half of 2016 was 1.3° C (2.4° F) warmer than the pre-industrial era of the late 19th century. The global land and ocean average temperature was 1.05° C (1.89° F) above the 20th century average beating the previous record set in 2015 by .20° C (.36° F). The El Nino event of 2015 was one of the most powerful on record and that indeed contributed to the record temperatures; but that dissipated in May and one must ask, which came first? The extent of Arctic sea ice at the peak of the summer melt season now leaves 40% less area than it did in the last '70s and early '80s.

Temperatures in the Coral Sea, including the Great Barrier Reef, were the highest on record for extended periods of time since last summer. This has caused bleaching of the Great Barrier Reef as well as others reefs in other parts of the world. This, in turn, leads to changes in the coral community and negatively impacts the lifetime of the reef.

Depending on where you are, you are either too wet or too dry. Enough said.

¹⁵ 2016, on pace to be hottest year ever as climate change trends reach “new climax” –UN; UN News Centre, July 21, 2016.