"To Infinity and Beyond: the New, the Hot, and the Stuff We Don't Understand Yet"

Time was in the FDCC that "AI" pretty much meant "Auto Insurance." Now, it's Artificial Intelligence. Or Age of Information. How will this and other things drive what will be hot in the law's future? Every day it seems there are new legal issues popping up as our judicial system tries to keep track with technology, innovation and disruption. This tension should bode well for litigators since unsettled law usually means more work.

So what will be the new hot areas in near (or not so near) future and how can we position ourselves to take advantage of the issues? Here's the list of some of the new areas:

E-Cigarette Litigation

Anyone who has walked through a college campus recently has seen groups of people standing under clouds of what looks like smoke… but isn't. It's people "vaping," using e-cigarettes. And while traditional cigarettes were commonly used for well over half a century before the advent of serious liability litigation, the plaintiffs' bar has been much quicker this time around. E-cigarettes have only been on the market for about a decade, but cases blaming them for various sort of harms now exist in state and federal courts across the country, and the wave has not even begun to crest.

The first e-cigarette cases looked very different from traditional tobacco litigation. They did not allege that e-cigarettes caused chronic diseases, such as cancer or heart disease, but rather, in the manner of standard product defect cases, alleged that something had gone wrong in the use of the product, such as it catching fire or exploding. Numerous e-cigarette cases were brought for injuries such as burns and lost teeth, and one federal case in California case even alleged that such an explosion resulted in death, though the case was dismissed in March 2018 (with leave to refile in state court) on grounds of lack of diversity jurisdiction. See Order on Motion to Dismiss/Lack of Jurisdiction, Gangi v. Flawless Vape Wholesale & Distribution Inc., et al., No. SACV 17-02016 (C.D. Cal., March 8, 2018). Other cases have resulted in spinoff insurance coverage litigation. For example, in Rubertt v. Lilac City Vapor, LLC, No. 16023995-7 (Wash. Super. Ct., Spokane Cty.), filed in 2016 in state court in Spokane, Washington, the plaintiff claimed she was using an e-cigarette in her home when the device exploded, causing burns to her mouth, face, and neck. The defendant's insurer, Atlantic Casualty Insurance Company, successfully denied coverage under the "products completed operations hazard" exception to the policy, on the grounds that the injuries occurred away from the defendant's premises. See Order Granting Plaintiff's Motion for Summary Judgment, Atlantic Casualty Insurance Co. v. Bellinger et al., 2:16-cv-0422-SAB (E.D. Wash., September 8, 2017).

While these defect cases regarding burning or exploding devices cases continue to be brought, a new wave of e-cigarette litigation seems to be upon us. These cases involve claims regarding elements alleged to be intrinsic to the use of e-cigarettes themselves -- that they are addictive, or that they cause disease in users -- even when the products "work" as intended. Seven such cases have been brought against the largest seller of "vape" products in the United States, JUUL

Labs. Most of these cases have been brought in federal or state court in California, though cases have also been filed in Florida, Pennsylvania, and New York. The lead case is Colgate et al. v. JUUL Labs, filed earlier this year and currently pending in the federal court in San Francisco (3:16-cv-2499, N. D. Cal.). The cases alleges that that JUUL Labs falsely and deceptively advertised and unlawfully marketed JUUL e-cigarettes to minors and non-smokers as safe, "candy like," products when, in fact, they were highly addictive and posed a number of undisclosed health risks. The plaintiffs allege that JUUL used social media to market their products to youth, and that JUUL's products did not contain a warning regarding the addictiveness of nicotine. To date, the court has granted JUUL Labs' motion to dismiss (i) the false advertising and fraud claims as not being plead with the required particularity; (ii) claims based on state consumer protection laws, finding that plaintiffs had not identified the laws relied on sufficiently. (plaintiffs have been given leave to replead both of these claims); and (iii) certain aspects of the plaintiffs' allegations regarding the addictiveness of nicotine "[t]o the extent that plaintiffs' claims are based on the product label failing to disclose the greater potency and addictiveness of JUUL's benzoic acid and nicotine salt formulation…" on the grounds that such claims are preempted by the federal Tobacco Control Act. However, the court permitted (as not preempted by the TCA) claims based the allegation that JUUL Labs had mislabeled the dose of nicotine in its products. The case filed in Pennsylvania, and one of the cases filed in Florida, have since been consolidated in with the Colgate case in the Northern District of California, and a similar motion is before the Southern District of New York in the case filed there.

California is also home to a case alleging that the use of e-cigarettes caused illness. In Petrucci et al. v. 7-Eleven Distribution Co. et al., filed in February 2018 in California Superior Court in Los Angeles (No. BC695450, Super. Ct., Los Angeles Cty.), the plaintiff claims that her use of e-cigarettes caused her to develop a rare lung condition, bronchiolitis obliterans organizing pneumonia, or "BOOP" (sometimes referred to as "cryptogenic organizing pneumonia," or "COP"). The complaint alleges that:

The chemical products which Plaintiff was exposed to contained significant concentrations of diacetyl, vegetable glycerin, propylene glycol, nicotine, acetyl propionyl, acetoin, artificial flavors, volatile organic compounds, and other toxic chemicals. As a direct and proximate result of Plaintiff's exposure to said toxic chemical constituents of Defendants' products and emitted from Defendants' delivery devices, Plaintiff… sustained serious injuries to her internal organs, including Bronchiolitis Obliterans Organizing Pneumonia.

The complaint further alleges that the defendants fraudulently concealed the "toxic hazards of the chemical products from Plaintiffs," and in addition contains allegations of negligence and strict liability. The complaint further asserts that the defendants intentionally misrepresented that e-cigarettes could be used to assist an individual in quitting smoking cigarettes. The defendants have filed motions seeking dismissal of several counts in the complaint.

It is likely that the most significant future litigation regarding e-cigarettes will be of the type seen in the Colgate and Petrucci cases: claims alleging damages resulting from the purported

addictiveness or disease-causing nature of the product, as well as claims related to the marketing of the products, particularly allegations that the products were marketed to youth. In this way, they will look very much like the allegations previously brought in cases involving the smoking of traditional cigarettes. It remains to be seen how this type of litigation will fare in the courts.

CBD

Few topics have been in the news over the past few years to a greater degree than the "legalization" of marijuana and other cannabis-related products. Much consumer interest has focused on cannabidiol ("CBD"), a non-psychoactive chemical typically derived from the cannabis plan, and currently marketed in various supplements as a treatment for conditions as disparate as anxiety, diabetes, epilepsy, and even cancer. CBD has been described as "the new 'it' drug" by the Washington Post (Lavyana Ramanathan, CBD Is Cannabis that Won't Get You High. So Why Are So Many People Using It? March 29, 2018. https://www.washingtonpost.com/lifestyle/style/cbd-is-cannabis-that-wont-get-you-high-so-why-are-so-many-people-using-it/2018/03/29/3836922a-2d2c-11e8-8ad6-fbc50284fce8_story.html?noredirect=on&utm_term=.27dbfaf22889). CBD is big business: sales in the U.S. grew to $820 million in 2017, with projections that it will reach nearly $2 billion in the next four years. Hemp Business Journal (https://www.hempbizjournal.com/size-of-us-hemp-industry-2017/, accessed December 14, 2018).

The difficulty is that the legal status of CBD has been the subject of a fair bit of uncertainty. While, as of this writing, ten states plus the District of Columbia permit the sale of cannabis for recreational use, and 33 additional states permit the sale of marijuana for medical purposes (with several jurisdictions having voted to "legalize" marijuana in the most recent election), marijuana and its derivatives remain illegal under federal law. Under the Controlled Substances Act, marijuana is a still a "controlled substance," and its manufacture, possession, and distribution are prohibited. 21 U.S.C. §§ 841(a) and 844. As noted above, CBD is not psychoactive, and is at best a distant cousin chemically to tetrahydrocannabinol, or "THC," the compound in marijuana that gets you high. CBD is typically derived from the hemp plant, essentially cannabis sativa, the same plant as marijuana, except bred to contain less than 0.3% THC. However, federal law has historically addressed compounds derived from the cannabis plant based not on THC levels but rather on the part of the plant from which the compound was derived. To this end, in March 2017, the DEA issued a "clarification" of its definition of marijuana, stating:

…cannabinoids, such as tetrahydrocannabinols (THC), cannabinols (CBN) and cannabidiols (CBD), are found in the parts of the cannabis plant that fall within the CSA definition of marijuana, such as the flowering tops, resin, and leaves. According to the scientific literature, cannabinoids are not found in the parts of the cannabis plant that are excluded from the CSA definition of marijuana, except for trace amounts…

The federal Farm Bill of 2014 allowed hemp cultivation -- and hence production of CBD derived from these plants -- but only under a very narrow set of circumstances. It allowed production of hemp under state "pilot programs," or for academic research," but did not allow such cultivation generally. However, the most recent Farm Bill, the 2018 version, which has been passed by Congress, though not as of this writing signed into law by President Trump (his signing the bill is likely to have occurred by the time you read this) permits hemp cultivation more generally, and permits the transport of hemp and hemp-derived products across state lines. It provides for a system of joint regulation of hemp-related products, such as CBD, including an as-yet-to-be-developed licensing system. See John Hudak, The Farm Bill, Hemp Legalization, and the Status of CBD: An Explainer, Brookings, December 14, 2018 (https://www.brookings.edu/blog/fixgov/2018/12/14/the-farm-bill-hemp-and-cbd-explainer/).

So it looks like CBD will soon be legal for sale. But what then? The FDA has already begun to examine claims regarding CBD's health benefits, and high-quality scientific analyses of the effects of the compound are few and far between. There is little in the way of effective control of the potency of the supplements sold in stores across the country. Further, the THC level in many CBD products varies greatly, even within a given product. If the THC level exceeds 0.3%, the product is no longer "hemp," it is "marijuana." How will this play out on the regulatory front? How long before the first CBD-related liability cases hit the courts? Perhaps we'll have answers by the time of the next FDCC meeting…

Privacy

Privacy related issues may become a hotbed of litigation in coming years. Why?

First, the proliferation of apps and Internet of Things (IoT) devices mean more things that can collect more and more data. Issues will abound with respect to who owns that data, what can be done with it, and what does informed consent mean in the context of these devices and apps. Can we sell the data we own? What is its value?

A couple of recent cases demonstrate some of these issues.

For example, in a recent decision by Judge Freeman in Svenson v. Google Inc. 2015 WL 1503429, a plaintiff paid for a Goggle app believing that Google's privacy policies would be followed. She claimed she was injured in some undefined amount when they weren't. Her argument was that Google breached its contract with respect to her data-a contract that was set out so she claimed in Goggle's privacy policies. Svenson also advanced –and the Court accepted—the theory that she was to have received from Google a service that was to have kept certain personal and valuable information private. Because Google did not keep this information private under its policies, Svenson claimed her information was no longer worth what it once was if sold on the open market. Not surprisingly, Svenson claimed she would not have used Google wallet and made the $1.77 purchase had she known his information would

not be safeguarded from revelation. Her theory was similar to the claim accepted in the Target breach consumer class action case in federal court in Minnesota. There Judge Magnusson accepted the theory that a claim that class members would not have shopped at Target had they known sooner of the breach supplied requisite standing.

And as a recent 6th Circuit Court of Appeals decisions suggests, if we expect our information to be private, we better act like it: we need to be prepared to exhibit and demonstrate our "expectation of privacy" with respect to information we want to protect and that expectation must be reasonable. See *Bertha and James Huff v. Carol Spaw*, (http://www.ca6.uscourts.gov/opinions.pdf/15a0157p-06.pdf),

So, where common security measures aren't used, establishing that expectation may prove daunting. Huff involved the disclosure of information through an inadvertent pocket dial. Because the plaintiff had involuntarily pocket dialed before, and because he failed to use well known measures to prevent his phone from making such calls (for example locking the phone), he had no expectation of privacy. The Court likened the plaintiff to a homeowner who fails to close his drapes and then claims he expects what he does in his home to be private.

> "…a person who knowingly operates a devise that is capable of inadvertently exposing his conversation to third party listeners and fails to take simple precaution to prevent such exposure does not have reasonable expectation of privacy with respect to statements that are exposed to an outsider…"

Under the Court's reasoning, it's not hard to envision that the failure to use and employ passwords would evidence a lack of an expectation of privacy. The use of cell phones in public where expected private conversations can be overheard may also demonstrate a lack of a privacy expectation.

As more security measures become used and well known, the zone of privacy expectations may continue to shrink. For example, would Two-Factor Authentication (2FA) fall within the "simple and well-known" privacy protection category contemplated by the Court at some point? Would the failure to use unique passwords? How about the failure to promptly download software or app updates? And what happens when the Internet of Things creates a world where every device with an off-on switch is connected to the web?

"What's scary is that we've gotten to a point where many of the things we do and the tools we use are such a big part of our lives that we HAVE to use them today. Are you really going to delete your Facebook account, stop using Google, no longer buy products online, or ditch your iPhone? No, you're not because everyone else that you know on this planet is using those same things as well." Jacob Morgan, Forbes, 8/19/2014: http://www.forbes.com/sites/jacobmorgan/2014/08/19/privacy-is-completely-and-utterly-dead-and-we-killed-it/

And states are getting in on the action as well. Illinois, for example, passed the Biometric Information Privacy Act (BIPA), designed to protect employees and consumers against perceived abuses associated with the collection of bio metric data by businesses and providing a statutory cause of action for its violation. This in turn has already led to significant litigation. California recently enacted tough new privacy legislation also allowing private causes of action for certain violations.

These issues and more will create a whole new specialty in the future around privacy and privacy rights.

Artificial Intelligence

There has been a lot of publicity, angst and hype about the brave new world of artificial intelligence (AI) and how it may be affecting businesses, and for that matter, all of us. Every day we hear more and more about AI and what it can do, and the danger and benefits it portends. When we talk about AI, what we are technically talking about are machine learning algorithms that can assist, and sometimes even replace, human decision-making in everything from medical diagnoses to investment strategy, to building design. The uses are growing every day. (One of the more creative recent uses is a new chatbot called "Do Not Pay," which uses automated questions and then takes the human responses that enable you to contest parking tickets.)

AI advancements are now happening faster and are considerably more impactful. Why? Under Moore's law, the computational and microchip powers continue to roughly double every year. We also have more and more data to use to assist in the machine learning of computers. At the same time, it's important to keep in mind the limitations of AI: it requires lots of (quality) data and learning. A common problem arises when the data set is not sufficiently robust and AI creates a model that agrees with the data, but has no predictive value. For example, although AI may determine there are more orange cars involved in accidents than cars of any other color, that does not mean orange cars *cause* accidents. Such a false deduction is called "overfitting," and points to one weakness with artificial intelligence.

As AI gains more control over more common objects and services, but also becomes more sophisticated and potentially unpredictable, it is inevitable that AI will cause harm and determining what legally happens when that occurs will inevitably produce litigation in the future

Today, we have a legal framework that deals with simple machines that make no decisions. If a factory robot injures a worker, for example, we don't blame the robot; the employee's injuries

are typically covered by workers' compensation. We look at such things as whether the employer had sufficient safety protocols in place.

In the non-employment situation, we look to such things as products liability principles and consider whether there is a manufacturing or design defect with the robot, or whether the manufacturer failed to provide adequate safety warnings.

And for simple AI decision makers existing legal concepts may still suffice. If an AI is programmed to make narrow autonomous decisions along specific lines and injures someone then we could look to the AI's creators and to negligence principles. Was the injury reasonably foreseeable? Was the victim also negligent in some way? If the AI's creators reasonably should have anticipated this harm, then they could be responsible. (Certainly, problems still arise: What if the AI's creators are no longer in business? Do we also look to the owner of the AI to bear some responsibility?)

But these problems become magnified as the AI gets more complex or starts behaving in unpredictable ways. What if AI makes complex decisions and take actions completely unforeseen by their creators? Where do we look to apportion blame? After all, you can't sue a robot. (And more importantly, even if you could, it doesn't have any assets.) There is no perfect analogy under the law to deal with a fully autonomous and somewhat unpredictable AI, but we can still look to existing legal frameworks for ideas.

One form of AI use, that in autonomous driving cars is progressing rapidly and may help define the legal framework governing AI sooner than later. Self-driving cars, with AI systems, will present all sorts of liability issues particularly at the interface with human drivers. And the decisions and judgments the AI system makes in the car could be subject of litigation as well as we grapple with fault and responsibility. The number and types of questions in this context boggle the mind.

Health Care

It has been estimated that in 2017 approximately 75% of organizations experienced some type of phishing attack. Healthcare has risks associated with the cybersecurity industry that most other businesses do not. Hospitals and physician practices collect payment and patient information that require significant security, as well as the Health Insurance Portability and Accountability Act (HIPAA) and PCI regulatory requirements. Healthcare lawyers who may be experiencing a decline in business due to tort reform or consolidation in the market should consider developing a regulatory line of business to address the new threat of privacy breaches. Before a breach even occurs, each provider should have in place a security plan and policy. The same policy should not be used for each client and should be individually tailored. Unfortunately, clients are often under the erroneous impression that it is sufficient to download or purchase a generic agreement. Lawyers can draft these agreements and

specifically design a plan that actually meets the requirements of the organization and the regulations.

When a breach is detected, immediate steps must be taken to protect the healthcare provider. Even after the scope of the breach is detected and the threat eliminated by I.T. professionals, there are legal issues remaining. HIPAA governs the response. Patients must be informed of the breach. The Department of Health and Human Services must be notified. If the breach affects more than 500 individuals, the provider must provide notice to the media. Litigation may result.

On an ongoing basis, healthcare professionals should engage counsel to provide annual reviews of their security policy, hold training for their employees and update business associate agreements. The insurance business is now writing policies that cover breaches. Lawyer can assess the policies and help healthcare professionals make informed decisions.

The healthcare industry is changing more rapidly than the regulations can keep up. When HIPAA was drafted the government didn't envision doctors using text messages to communicate with patients and other healthcare providers. The battleground between the convenience of communication and protection of patient privacy is coming to a head. In the future, lawyers who master the privacy regulations will have no shortage of work. This doesn't even take into consideration the impact of labor and employment access to healthcare records will have. For example, if an employer requires an employee to participate in a wellness program and share protected healthcare information, legal implications may arise. Lawyers who master the health care labor law interface will not lack for work.