COMPUTATIONAL LAWYERING:
THE PRESENT AND FUTURE SHOCK
OF COMPUTING ON
LEGAL PRACTICE,
AND HOW IT WILL HELP YOU

CLE Credit: 1.0
Thursday, June 13, 2019
9:40 – 10:40 a.m.
Jones
Galt House Hotel
Louisville, Kentucky
A NOTE CONCERNING THE PROGRAM MATERIALS

The materials included in this Kentucky Bar Association Continuing Legal Education handbook are intended to provide current and accurate information about the subject matter covered. No representation or warranty is made concerning the application of the legal or other principles discussed by the instructors to any specific fact situation, nor is any prediction made concerning how any particular judge or jury will interpret or apply such principles. The proper interpretation or application of the principles discussed is a matter for the considered judgement of the individual legal practitioner. The faculty and staff of this Kentucky Bar Association CLE program disclaim liability therefore. Attorneys using these materials, or information otherwise conveyed during the program in dealing with a specific legal matter have a duty to research the original and current sources of authority.
TABLE OF CONTENTS

The Presenters........................................................................................................................................... i

Computational Lawyering: The Present and Future Shock
of Computing on Legal Practice, and How It Will Help You................................................................. 1
THE PRESENTERS

Amy D. Cubbage
Ackerson & Yann PLLC
734 West Main Street, Suite 200
Louisville, Kentucky 40202

AMY D. CUBBAGE is a member of Ackerson & Yann practicing litigation in the areas of complex business and commercial litigation, real estate litigation, construction litigation, employment law, and internet and technology issues, including internet defamation issues. She also counsels clients with respect to energy and environmental matters, including cases involving CERCLA, RCRA, OSHA, and related state regulatory programs. Ms. Cubbage also litigates and counsels clients in the area of general constitutional and governmental law, with an emphasis on First Amendment, campaign finance, elections, and other constitutional issues, including the commerce clause, public contracts, governmental ethics, and eminent domain. She serves on the Kentucky Bar Association's Board of Governors and is a member of the Committee on Diversity in the Profession and the Attorney Advertising Commission. Ms. Cubbage is also a member of the Louisville and American Bar Associations. She earned her B.A., summa cum laude, from Georgetown College and her J.D., cum laude, from the University of Kentucky College of Law. Ms. Cubbage is a frequent speaker on law and technology issues as well as attorney ethics issues.

Joseph Davis
Houchens Insurance Group
Bowling Green, Kentucky 42101

JOE DAVIS is a Large Account Producer for Houchens Insurance Group. His focus is the development and implementation of Risk Management Programs including Cyber Liability exposures. Mr. Davis frequently speaks on Cyber Liability topics and trends. He advises on best practices as well as reviews carrier forms to negotiate enhancements and endorsements. Joe works within various industries including, finance, retail, healthcare, education and manufacturing to identifying risk factors and assist loss control strategies. He earned his J.D. from Nashville School of Law. Mr. Davis is originally from Bowling Green KY and attended Bowling Green High School. His wife Caitlin Davis is also from Bowling Green KY and have twin boys, Lincoln and Walker that just turned four.
LAURIE DUDGEON has served as AOC director since 2009. She oversees the administrative arm of Kentucky's unified court system and supports 406 elected justices, judges and circuit court clerks. During her tenure, she has maintained a balanced Judicial Branch budget in spite of recurring state budget cuts; revised the AOC's organizational structure to meet the changing needs of the courts; and improved the personnel policies and salary structure. She has also led KY eCourts, a sweeping initiative to update Kentucky's court technology through statewide eFiling, an online case search program, and new trial and appellate court case management systems. She has worked closely with the legislature on policy initiatives, including felony expungement and penal code and juvenile justice reform. Ms. Dudgeon serves as president-elect for COSCA and is a member of COSCA’s Criminal Justice, Court Statistics, Education and Joint Technology committees. She is also on the board of the National Center for State Courts and is co-chair of the National Task Force on Fines, Fees and Bail Practices. She serves on the board of The Council of State Governments’ Justice Center. She previously practiced law and was executive director of the Kentucky Office of Drug Control Policy and a staff attorney in the Kentucky Justice & Public Safety Cabinet. Ms. Dudgeon received the 2018 Mary C. McQueen Award for Excellence and Leadership in Justice System Improvement and is an alumna of the Toll Fellowship Program. She has a bachelor's degree and juris doctor from the University of Kentucky.

STEPHEN EMBRY is a national litigator and advisor who is experienced in developing solutions to complex litigation and corporate problems. His mission is to find simple, successful and elegant solutions to civil litigation problems and dilemmas primarily in the mass tort, business and consumer class action, and privacy and data breach arenas. Mr. Embry is also a frequent speaker, blogger and writer. He is publisher of TechLaw Crossroads, a blog devoted to the examination of the tension between technology, the law and the practice of law. He is also co-author of a book entitled Mass Tort Claims Resolution Facilities and the 2017 and 2016 editions of the American Bar Association’s TechReports.
JEFF SALLEE is a member of Western & Southern’s Information Security Team, which he joined after retiring from Procter & Gamble. He is an alumnus of the Defense Language Institute, received three undergraduate degrees from Purdue University, obtained his J.D. from Chase College of Law, and is currently an adjunct professor at the University of the Cumberlands. His certifications include Certified Information Systems Security Professional (CISSP), Cloud Computing Security Professional (CCSP), and Certified Information Systems Auditor (CISA). Sallee is licensed to practice in Kentucky, Indiana, and before the Supreme Court of the U.S.
I. INTRODUCTION

We work with information and data. We find it, analyze it and argue it. Lawyering today weaves traditional methods with increasingly powerful support from computational information and communication technologies (ICT), which we may or may not fully comprehend.

We discuss these technologies – from Smart Forms to Google Scholar to Artificial Intelligence systems – and examine where they can help us serve our clients. And what dangers their use, misuse or non-use may present to the unwary, from malpractice to ethical complaints.

II. ETHICS QUESTIONS: COMPETENCE, CONFIDENTIALITY AND BEYOND...

A. Kentucky Rules of Professional Conduct

B. Attorney Concerns and Task Force on the Practice of Law Survey Results

III. KENTUCKY RULES OF PROFESSIONAL CONDUCT AT PLAY

A. Kentucky Rules of Professional Conduct

   SCR 3.130 Kentucky Rules of Professional Conduct

B. Maintaining the Integrity of the Profession

   SCR 3.130(8.2) Judicial and legal officials
   SCR 3.130(8.3) Reporting professional misconduct
   SCR 3.130(8.4) Misconduct
   SCR 3.130(1.0) Terminology
   SCR 3.130(1.1) Competence
   SCR 3.130(1.2) Scope of representation and allocation of authority between client and lawyer
   SCR 3.130(1.3) Diligence
   SCR 3.130(1.4) Communication
   SCR 3.130(1.6) Confidentiality of information
C. Advocate

SCR 3.130(3.1) Meritorious claims and contentions
SCR 3.130(3.2) Expediting litigation
SCR 3.130(3.6) Trial publicity

D. Transactions with Persons Other Than Clients

SCR 3.130(4.1) Truthfulness in statements to others
SCR 3.130(4.2) Communication with person represented by counsel
SCR 3.130(4.3) Dealing with unrepresented person
SCR 3.130(4.4) Respect for rights of third persons
SCR 3.130(4.5) Solicitation of clients
SCR 3.130(4.6) Waiver and forfeiture of fees for prohibited solicitation

E. Law Firms and Associations

SCR 3.130(5.1) Responsibilities of partners, managers and supervisory lawyers
SCR 3.130(5.2) Responsibilities of a subordinate lawyer
SCR 3.130(5.3) Responsibilities regarding nonlawyer assistants
SCR 3.130(5.4) Professional independence of a lawyer
SCR 3.130(5.5) Unauthorized practice of law; multijurisdictional practice of law

F. Information about Legal Services

SCR 3.130(7.01) Definitions
SCR 3.130(7.10) Communications concerning a lawyer's service
SCR 3.130(7.15) Advertising of fees
SCR 3.130(7.20) Advertising
SCR 3.130(7.40) Communication of fields of practice
SCR 3.130(7.50) Firm names and letterheads
iv. the techno-ethical-literature review


1. Because of the evolving security risks brought by the changes wrought by e-mail, the Internet, and cloud computing, lawyers must reassess their ethical duties of competence and confidentiality.

2. Although lawyers may have been comforted by ethical opinions finding the use of e-mail or cloud computing appropriate in the past, they can no longer rely on those opinions given dramatically altered security risks.

3. Lawyers must develop a greater awareness of the risks posed by the technology than they have had in the past because—like their clients—they are subject to rapidly escalating security threats.

4. Security is for all who deal with private, proprietary, and confidential data—including lawyers.

5. In its August 2014 cybersecurity resolution, the ABA found that “[t]he threat of cyber attacks against law firms is growing” and that “[l]awyers and law firms are facing unprecedented challenges from the widespread use of electronic records and mobile devices.”

6. Lawyers and law firms are targets because “[t]hey collect and store large amounts of critical, highly valuable corporate records, including intellectual property, strategic business data, and litigation-related theories and records collected through e-[D]iscovery.”

7. Legal Mandates

a. Section 5 of the FTC Act permits actions against enterprises that do not maintain “reasonable security for consumers’ sensitive personal information.”

b. HIPPA if a “business associate” of health care clients?

c. Kentucky Data Breach law.

8. Issue – Use of Public Wireless Connection

a. Obligation – ABA Model Rules, California Rules – A security program for a law firm should include:

   i. Governance standards;
ii. “development of security strategies, plans, policies and procedures;

iii. creation of inventories of digital assets;

iv. selection of security controls;

v. determination of technical configuration settings;

vi. performance of annual audits; and

vii. delivery of training.”


c. The Human Lawyer in the Age of Artificial Intelligence: Doomed for Extinction or in Need of a Survival Manual?


e. Institute for the future of law practice:
   

f. LopSider

Planning Your Next Legal IT Strategy Discussion (part III): Focus on Talent

B. Ethics Questions for Our Practice and Our Technology

1. Can we practice without technology?

2. Consider the KY Rules of Professional Conduct at play:

   a. **SCR 3.130 (1.1) Competence**

      ABA Model Rule 1.1 Competence: Since 2012, comment 8 to Rule 1.1 has provided that “[t]o 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…

   b. 1.3 Diligence

      A lawyer shall act with reasonable diligence and promptness in representing a client.
c. 1.4 Communication

(a) A lawyer shall:

(1) promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(e), is required by these Rules;

(2) reasonably consult with the client about the means by which the client's objectives are to be accomplished;

(3) keep the client reasonably informed about the status of the matter;

(4) promptly comply with reasonable requests for information;

d. 1.6 Confidentiality of Information

Acting Competently to Preserve Confidentiality

(14) A lawyer must act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3.

(15) When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

C. Email - ABA Formal Opinion 99-413 (adopted by Kentucky) that e-mail is OK is now obsolete and misguided. Formal Opinion 11-459 modified this:
[S]ending or receiving substantive communications with a client via e-mail or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access.

D. Webmail

1. Gmail – scanning.
2. Gmail – Terms of Service.
3. Gmail – expectation of privacy-but see United States v. Carpenter.

E. Cloud Services

1. Well, it’s outsourcing...
2. Per Toohey - So far ethics opinions say its OK: cloud computing ethical if lawyers “take reasonable steps to ensure that their law firm’s confidential data is protected from unauthorized third party access."
3. New York Bar Opinion 842 found that necessary “[r]easonable care . . . may include consideration” of four issues:

   (1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

   (2) Investigating the online data storage provider’s security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

   (3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

   (4) investigating the storage provider’s ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

   Opinion 842 cautioned that “[t]echnology and security of stored data are changing rapidly” and that “the lawyer should periodically reconfirm that the provider’s security measures remain effective in light of advances in technology.”

6
The lawyer also has the duty, if he or she learns that security measures are ineffective, to “investigate whether there has been any breach of his or her clients’ confidential information, notify any affected clients, and discontinue use of the service unless the lawyer receives assurances that any security issues have been sufficiently remediated.” Lawyers must also monitor the law relating to technology, which “is changing rapidly,” to see “when using technology may waive an otherwise applicable privilege.”

V. THE ELECTRONIC COURT

The Kentucky Court of Justice has made great efforts to embrace the Internet as a means of helping Kentucky attorneys:

A. KCOJ Forms via KYeCourts to attorneys with accounts – https://kcoj.kycourts.net/kyecourts/Forms/

B. KCOJ Forms via the KCOJ website – https://courts.ky.gov/resources/legalforms/Pages/legalformlibrary.aspx


D. Learn More about eFiling – https://courts.ky.gov/efiling/Pages/default.aspx


VI. COURT OF JUSTICE TECHNOLOGY EFFORTS

These are some additional technology-centric efforts from the KJOC to keep in mind:

A. Program Management Committee (PMC) – Governs and guides the eFiling/KYeCourts initiative; ultimate goal is the electronic record.


C. Court Efficiency Committee – Former Judge Doughlas George chairs.

D. Civil Case Cover Sheet – Both the commission and committee are working on this effort which aligns case types and categories for reporting and statistical purposes.

E. CourtNet – Online access to the case management system for attorneys and judicial partners.

F. eFiling – SRL and more.
G. Centralized Services – Service packages may be routed to the AOC for printing/mailing.

H. Forms Project – Reviewing, evaluating and categorizing forms in preparation for the eRecord.

VII. ETHICAL OBLIGATIONS

The codified obligations are easy to find and read. How should you think of these obligations in your daily work?

A. Your Clients

Do you understand technology enough to provide competent advice in matters relating to technology? Can you spot the issues relating to how your clients are using and protecting their IT?

Are you protecting your client’s confidences with how you are using your IT? Have you vetted your IT partners? Are you ensuring your old IT is disposed of properly?

B. Opposing Counsel

Do you know how to let opposing counsel know if you discover an accidental disclosure of client confidences? Do you know how to prevent accidental disclosures of your client data?

How realistic are your eDiscovery requests and the eDiscovery responses of opposing counsel? It is very easy to dump a huge haystack of data to make the other party spend their resources on finding the truly responsive data. Some judges are addressing this by assessing costs if the dumping appears intentional. Do you have partners who can use Technology Assisted Review (TAR) to expedite and prioritize document collection and analysis?

C. The Court

Although attorneys are required by Supreme Court rules to keep abreast of changes in technology, judges are not required, by rule, to do the same. Do you know how to use technology in court? Can you do the troubleshooting you need to do in case you have issues? Are you aware of the technology available in the court? Are you bringing the right cables and other hardware you need?

D. Your Colleagues

Technology use in the office can affect more than just yourself. Has everyone been trained on the proper use of IT? Have you included protections to prevent fraudulent transfers? Do you have procedures in place to remove access from people who leave your practice?
E. Yourself

Technology is one way for you to manage the complexity and chaos that can overwhelm your practice. You can automate tasks or create templates that can save you time and let you focus on the actual practice of law instead of repetitive business tasks.

You can take your work with you and do so securely. You can do some work while waiting for a child’s sporting event or to pick someone up from practice.

Technology can make you effective anywhere you happen to be but be sure to take time to disconnect and focus on your family and mental health as well.

VIII. INTERESTING DEVELOPMENTS IN TECHNOLOGY

A. Wire Transfers

According to the FBI’s 2018 Internet Crime Report, the FBI’s Internet Crime Complaint Center’s (IC3) Recovery Asset Team (RAT) was able to recover 75 percent of monies fraudulently wired in 2018. So, if you have a fraudulent wire situation, I would strongly suggest you contact the IC3 immediately to have them start the recovery process.

Trying to sue the bank for a fraudulent wire transfer may not work as well as you think. A real estate firm in Pennsylvania was a victim of a Business Email Compromise scam. The fraud was not discovered until after Bank of America had already wired $580k to China. BoA had already processed the wire and suggested contacting the receiving bank in Hong Kong. BoA’s Terms and conditions allow for a total refund, including fees, if requested within 30 minutes. You can still get a refund within three business days, as long as the funds have not been picked up or deposited into the recipient’s account. The firm lost in U.S. District court, where the court found that BoA did not breach any agreement with the firm, did not violate any federal banking regulations, and did not break the state commercial code.

The criminals gained access to the law firm’s email system, which let them search for a believable premise to have an employee start the wire transfer process. The email requesting the wire transfer had appeared to come from inside the company.

---


B. Rise of the Nation State as the Actor behind Data Breaches

Verizon publishes a Data Breach Investigations Report every year. In the 2019 report,\(^3\) they reported that nation states, and their proxies, were responsible for 23 percent of data breaches. Almost a quarter of all data breaches are now done on the behalf of foreign governments. The report explained how login credentials are sought, often on cloud-based email systems, and then used to access the company itself. Intellectual property and company secrets are the primary targets in these attacks.

C. Continued Use of Incredibly Ridiculous Passwords

First, you should use multi-factor authentication and not rely on just a password to authenticate your access to anything important to you. You should also avoid reusing passwords, both from a cyclical pattern perspective and from a cross platform perspective. There are several places on the Internet, such as [https://haveibeenpwned.com](https://haveibeenpwned.com), where you can find millions of breached credentials (IDs and passwords) now in the public domain. If you are still using passwords like 123456 or Spring2019, your accounts are vulnerable.

Naked Security, a blog by the European security company Sophos, reported in April 2019 that 123456 was once again the most popular password on the Internet.\(^4\) This report also included a gloomy statistic from a survey by the UK’s National Cyber Security Centre: 70 percent of the Brits surveyed expect to have their accounts breached in the next two years.

D. Most Companies have been Breached in the Past Year

Hiscox, a global insurer, reported in its The Cyber Readiness Report 2019,\(^5\) that 61 percent of firms have been breached in the past year. This is a 16 point jump from 2018. Although larger (>1,000 employees) and multinational companies are the primary targets, having more than a 70 percent risk of being breached, 47 percent of small firms, and 63 percent of mid-sized firms are at risk of being breached based on this report. Increasingly, your ability to protect yourself from a data breach is becoming a factor companies consider when deciding if they want to do business with you.

\(^3\) [https://enterprise.verizon.com/resources/reports/dbir/](https://enterprise.verizon.com/resources/reports/dbir/)


IX. ADDITIONAL MATERIAL


C. Dobrev, Dessislav, “The Human Lawyer in the Age of Artificial Intelligence: Doomed for Extinction or in Need of a Survival Manual,” 18 J. Int'l Bus and Law 1, Winter, 2018
