Richmond Journal of Law & Technology

Volume 22 | Issue 4 Article 1

2016

Digital Direction for the Analog Attorney-Date Protection, E-Discovery, and the Ethics of Technological Competence In Today's World of Tomorrow

Stacey Blaustein

Melinda L. McLellan

James A. Sherer

DIGITAL DIRECTION FOR THE ANALOG ATTORNEY—DATA PROTECTION, E-DISCOVERY, AND THE ETHICS OF TECHNOLOGICAL COMPETENCE IN TODAY'S WORLD OF TOMORROW

Stacey Blaustein,[*] Melinda L. McLellan,[**] and James A. Sherer[***]

Cite as: Stacey Blaustein et al., *Digital Direction for the Analog Attorney—Data Protection, E-Discovery, and the Ethics of Technological Competence in Today's World of Tomorrow*, 22 RICH. J.L. & TECH. 10 (2016), http://jolt.richmond.edu/v22i4/article10.pdf.

I. INTRODUCTION

[1] Over the past twenty years, the near-constant use of sophisticated technological tools has become an essential and indispensable aspect of the practice of law. The time and cost efficiencies generated by these resources are obvious, and have been for years.[1] And because clients expect their counsel to take full advantage,[2] savvy attorneys understand that they must keep up with ever-evolving legal technologies to stay

[*] Stacey Blaustein is a Senior Attorney - Corporate Litigation with the IBM Corporation.
[**] Melinda L. McLellan is Counsel in the New York office of Baker & Hostetler LLP.
[***] James Sherer is Counsel in the New York office of Baker & Hostetler LLP.

[1] *See* Roger V. Skalbeck, *Computing Efficiencies, Computing Proficiencies and Advanced Legal Technologies*, VIRGINIA STATE BAR – RESEARCH RECOURSES (Oct. 2001), http://www.vsb.org/docs/valawyermagazine/oct01skalbeck.pdf, *archived at* https://perma.cc/8YWX-YAHF.

[2] *See* Ed Finkel, *Technology No Longer a 'Nice to Learn' for Attorneys*, LEGAL MANAGEMENT, ASSOCIATION OF LEGAL ADMINISTRATORS (Oct. 2014), http://encoretech.com/wp-content/uploads/2014/10/Technology-No-Longer-a-Nice-to-Learn-for-Attorneys_ALA-Legal-Management_Oct2014.pdf, *archived at* https://perma.cc/HUT3-672F.

competitive in a crowded marketplace.[3]

[2] With increased globalization and exponential growth in the creation, collection, use, and retention of electronic data, the challenges to all lawyers—especially those who may not have tech backgrounds or a natural aptitude for the mechanics of these innovations—are multiplying with breathtaking speed.[4] Nevertheless, many attorneys are either blissfully unaware of the power and potential danger associated with the tools they now find themselves using on a daily basis, or they are willfully avoiding a confrontation with reality. For lawyers, technological know-how is no longer a "nice to have" bonus; it now poses an ethical obligation. Where competent client representation demands a minimum level of tech proficiency, however, many lawyers come up short with respect to this fundamental component of their professional responsibilities.[5]

[3] What types of privacy and data security threats do various technologies pose to attorneys, their firms, their clients, and the legal

[3] *See, e.g.*, Evan Weinberger, *Fintech Boom Prompts Lawyers to Add Tech Know-How*, LAW360 (Sep. 4, 2015, 6:05 PM), http://www.law360.com/articles/692081/fintech-boom-prompts-lawyers-to-add-tech-know-how, *archived at* https://perma.cc/WVE8-UPGP; *see also* Allison O. Van Laningham, *Navigating in the Brave New World of E-Discovery: Ethics, Sanctions and Spoliation*, FDCC Q. 327(Summer 2007), http://www.thefederation.org/documents/V57N4-VanLaningham.pdf, *archived at* https://perma.cc/9L48-MPLU.

[4] *See* Frank Strong, *Beautiful Minds: 41 Legal Industry Predictions for 2016*, LEXISNEXIS LAWBLOG (Dec. 17, 2015), http://businessoflawblog.com/2015/12/legal-industry-predictions-2016/, *archived at* http://perma.cc/BG5W-R4DB.

[5] To further complicate matters, for attorneys and law firms practicing in the financial technology area such as payment, online lending, bitcoin and other virtual currencies, these lawyers need to be competent in "fintech", financial technology, another outgrowth of the expertise in technology requirement. *See* Evan Weinberger, *Fintech Boom Prompts Lawyers to Add Tech Know-How*, LAW360 (Sep. 4, 2015, 6:05 PM), http://www.law360.com/articles/692081/fintech-boom-prompts-lawyers-to-add-tech-know-how, *archived at* https://perma.cc/L76C-FZRL.

profession in general? What rules and regulations govern how attorneys may make use of technology in their practice, and how might clients seek to impose restrictions around such use when it comes to their corporate data? Must attorneys gain mastery over the intricate mechanics of the technological resources they employ, or is basic knowledge sufficient? How can we weigh the potential risks and rewards of cutting-edge, emerging digital products and electronic resources about which clients—and indeed, even the lawyers themselves—may understand very little? These are just a few of the questions that arise when we consider the issue of technological competence in the legal profession and corresponding ethical requirements.

[4] To begin to answer these questions, we look to the applicable Model Rules issued by the American Bar Association ("ABA"), various state-level professional ethics rules that incorporate the Model Rules, associated ethics opinions and guidance issued by the states, state and federal court decisions, and guidelines issued by sector-specific agencies and organizations.[6] Our focus in this investigation concerning lawyerly "technological competence" will be on privacy and data security risks and safeguards, e-Discovery-related challenges, and the potential perils of various uses of social media in the legal sphere.

II. THE THREAT LANDSCAPE: LAW FIRMS AS PRIME TARGETS

[5] In recent years, the volume and severity of attacks on electronically-stored data, and the information systems and networks that house that data, have increased exponentially. The modern-day "threat environment" is "highly sophisticated," and "massive data breaches are occurring with alarming frequency."[7] For attorneys, such perils implicate

[6] *See infra* Part III (explaining that agencies such as the FDA have issued guidance in their arena- Postmarket Management of Cybersecurity in Medical Devices).

[7] Report to the House of Delegates, ABA Cybersecurity Legal Task Force Section of Sci. & Tech. Law 1, http://www.americanbar.org/content/dam/aba/administrative/house_of_delegates/resoluti

multiple ethical and professional responsibilities with respect to how they handle data, including the duty to protect the confidentiality of client information and the obligation to provide "competent" representation.

[6] Unfortunately, law firms can provide a proverbial back door for hackers seeking access to a company's data, as attorneys often are custodians of a veritable "treasure trove" of valuable client information "that is extremely attractive to criminals, foreign governments, adversaries and intelligence entities."[8] Some hackers even focus their efforts primarily on law firms, especially those firms collecting vast amounts of data from corporate clients in the course of E-Discovery or corporate due diligence.[9] Corporate secrets, business strategies, and intellectual property all may be found in a law firm's collection of its clients' data.[10] In some cases, the interceptors may be looking for competitive information relevant to merger negotiations, or trying to suss out evidence of as-yet unannounced deals for insider trading purposes.[11]

[7] A 2015 report estimated that 80% of the biggest 100 law firms

---

ons/2014_hod_annual_meeting_109.authcheckdam.pdf, *archived at* https://perma.cc/KQT3-AFAJ.

[8] Ellen Rosen, *Most Big Firms Have Had Some Hacking: Business of Law*, BLOOMBERG (Mar. 11, 2015, 12:01 AM), http://www.bloomberg.com/news/articles/2015-03-11/most-big-firms-have-had-some-form-of-hacking-business-of-law, *archived at* https://perma.cc/YDR6-ZUV8.

[9] *See* Melissa Maleske, *A Soft Target for Hacks, Law Firms Must Step Up Data Security*, LAW360 (Sep. 23, 2015, 10:09 PM), http://www.law360.com/articles/706312/a-soft-target-for-hacks-law-firms-must-step-up-data-security, *archived at* https://perma.cc/6V7K-2WB4.

[10] *See id.*

[11] *See* Susan Hansen, *Cyber Attacks Upend Attorney-Client Privilege*, BLOOMBERG BUSINESSWEEK (Mar. 19, 2015, 2:56 PM), http://www.bloomberg.com/news/articles/2015-03-19/cyber-attacks-force-law-firms-to-improve-data-security, *archived at* https://perma.cc/29A5-MUNG.

have experienced some sort of data security incident.[12] And as is the case with so many companies that suffer a breach, law firms that *have* been hacked may not know about it for a considerable period of time. Moreover, unlike other industry sectors subject to various reporting requirements, law firms generally do not have a statutory obligation to publicly report cybercrimes that do not involve personally identifiable information.[13] Lack of obligations notwithstanding, a recent report indicated that "[t]he legal industry reported more "cyber threats" threats in January [2016] than nearly any other sector," topped only by the retail industry and financial services.[14]

[8] Although these reported "threats" might not necessarily result in data compromises, the fact that the legal industry frequently is among the most targeted for data theft should concern attorneys.[15] Anecdotal evidence of actual and attempted interference with law firms' data security systems abounds as well. In 2014, a report indicated that communications between lawyers from the law firm of Mayer Brown and officials with the Indonesian government were intercepted by an Australian intelligence agency that had ties with the U.S. National Security Agency ("NSA").[16] And the managing partner of the Washington-area offices of Hogan Lovells LLP recently noted that her firm "constantly intercept[s]

[12] *See* Rosen, *supra* note 8.

[13] *Id.*

[14] Mark Wolski, *Report: Legal Industry Was Heavily Targeted with Cyber Threats in January*, BLOOMBERG BNA (Mar. 9, 2016), https://bol.bna.com/report-legal-industry-was-heavily-targeted-with-cyber-threats-in-january, *archived at* https://perma.cc/ZCR9-2WRX.

[15] *See id.*

[16] James Risen & Laura Poitras, *Spying by N.S.A. Ally Entangled U.S. Law Firm*, N.Y. TIMES, Feb. 15, 2014, http://www.nytimes.com/2014/02/16/us/eavesdropping-ensnared-american-law-firm.html, *archived at* https://perma.cc/F8M4-TEQ7.

attacks."[17]

[9] The message to law firms seems clear: first, if "you're a major law firm, it's safe to say that you've either already been a victim, currently are a victim, or will be a victim."[18] Second, "[f]irms have to make sure they are not a weak link…which at its most basic level means their standards for protecting data need to be at least equivalent to those of the companies they represent."[19]

[10] It seems inevitable that client expectations and demands with regard to their legal service providers' security will continue to evolve and expand. One commentator recently predicted that in the future "clients across the board will demand firms demonstrate they're prepared for all shapes and sizes of cybersecurity breaches,"[20] while another prophesized that "in the name of risk management and data leakage prevention, a large financial industry corporation will challenge their outside counsel's [Bring Your Own Device] program."[21] Indeed, according to a 2014 report in the New York Times:

> Banks are pressing outside law firms to demonstrate that their computer systems are employing top-tier technologies to detect and deter attacks from hackers bent on getting their hands on corporate secrets for their own use of sale to others….Some financial institutions are asking law firms to fill out lengthy 60 page questionnaires detailing the [law

[17] *See* Rosen, *supra* note 8.

[18] *See* Hansen, *supra* note 11.

[19] Blake Edwards, *Verizon GC: Law Firms Prime Targets for Hackers*, BLOOMBERG BNA (Feb. 4, 2016), https://bol.bna.com/verizon-gc-law-firms-are-prime-targets-for-hackers/, *archived at* https://perma.cc/F6WU-N6FW.

[20] Strong, *supra* note 4.

[21] *Id.*

> firm's] cybersecurity measures, while others are demanding on-site inspections....Other companies are asking law firms to stop putting files on portable thumb drives, to stop emailing non-secure iPad or working on computers linked to a share network in countries like China and Russia.[22]

[11] In short, lawyers, law firms, and other legal services providers cannot afford to be complacent when it comes to cybersecurity.

A. Lawyering in the Cloud

[12] Firm adoption of cloud services is on the rise, especially among boutiques and solo practitioners that previously lacked the resources to compete effectively with larger law firms when it came to technology and data storage.[23] At first, the added value of cloud services created a perception that "nirvana had arrived" in terms of leveling the playing field for smaller firms.[24] Notwithstanding the apparent advantages of the cloud, attorneys were quick to identify concerns associated with the technology and its supporting practices, including "increased sensitivity to cyber-threats and data security."[25] Some commentators opted for a cautious and conservative approach, noting that the "legal profession has developed many safeguards to protect client confidences," and that the use of cloud hosting, among other practices, fell on a continuum where, as "an individual attorney gives up direct control of his or her client's

---

[22] Matthew Goldstein, *Law Firms Are Pressed on Security for Data*, N.Y. TIMES (Mar. 26, 2014), http://dealbook.nytimes.com/2014/03/26/law-firms-scrutinized-as-hacking-increases/, *archived at* https://perma.cc/Q77A-8BN3.

[23] *See* N.Y. CITY BAR COMM. ON SMALL LAW FIRMS, THE CLOUD AND THE SMALL LAW FIRM: BUSINESS, ETHICS AND PRIVILEGE CONSIDERATIONS 2 (Nov. 2013), http://www2.nycbar.org/pdf/report/uploads/20072378-TheCloudandtheSmallLawFirm.pdf, *archived at* https://perma.cc/A8EG-AH7E.

[24] *Id.*

[25] Strong, *supra* note 4.

information, he or she takes calculated risks with the security of that information."[26]

[13] There is hope for attorneys drawn to the advantages of cloud services, but vigilance and diligence is required. As noted in tech law guidance from March 2014, "[u]sing the cloud to hold data is fine, so long as you understand the security precautions."[27] Security concerns have put a damper on adoption rates and the development of attorney-specific cloud services lags behind other industries. This reluctance is unsurprising given the slow rate of technological advancements within the profession generally,[28] and a deserved reputation that the tendency of firms is "to be technology followers, not leaders."[29] That said, lawyers do seem to be embracing the cloud to some extent,[30] with the majority utilizing cloud

[26] Patrick Mohan & Steve Krause, *Up in the Cloud: Ethical Issues that Arise in the Age of Cloud Computing*, 8 ABI ETHICS COMM. NEWS L. 1 (Feb. 2011), http://www.davispolk.com/sites/default/files/files/Publication/a2e048ea-3b12-45fe-a639-9fc2881a4db8/Preview/PublicationAttachment/0f8af440-1db0-4936-8d0d-a1937a0e6c8f/skrause.ethics.clouds.feb11.pdf, *archived at* https://perma.cc/SW3C-FYT5.

[27] Sharon D. Nelson & John W. Simek, *Why Do Lawyers Resist Ethical Rules Requiring Competence with Technology?*, SLAW (Mar. 27, 2015), http://www.slaw.ca/2015/03/27/why-do-lawyers-resist-ethical-rules-requiring-competence-with-technology/, *archived at* https://perma.cc/6HNN-UCDZ.

[28] Ed Finkel, *Technology No Longer a 'Nice to Learn' for Attorneys*, Legal Management, Association of Legal Administrators (Oct. 2014) http://encoretech.com/wp-content/uploads/2014/10/Technology-No-Longer-a-Nice-to-Learn-for-Attorneys_ALA-Legal-Management_Oct2014.pdf, *archived at* https://perma.cc/TW7N-4WP5.

[29] Leslie Pappas, *The Security Concerns Holding Up One Firm's Cloud Usage*, BLOOMBERG BNA (Jan. 22, 2016), https://bol.bna.com/the-security-concerns-holding-up-one-firms-cloud-usage/, *archived at* https://perma.cc/Z4LJ-H83Q.

[30] *See* Casey C. Sullivan, *Is It Time for a Law Firm Cloud Computing Security Standard?*, FINDLAW (Feb. 18, 2016), http://blogs.findlaw.com/technologist/2016/02/is-it-time-for-a-law-firm-cloud-computing-security-standard.html, *archived at* https://perma.cc/78HF-KKX4.

solutions in some capacity,[31] even if implementation is mostly through "sporadic action and adoption among firms and law departments."[32]

[14] With respect to professional obligations, this type of implementation may not require specific technological expertise on the part of the attorneys. New York State Bar Association Opinion 1020, which addressed ethical implications of the "use of cloud storage for purposes of a transaction," determined that compliant usage "depends on whether the particular technology employed provides reasonable protection to confidential client information and, if not, whether the lawyer obtains informed consent from the client after advising the client of the relevant risks."[33]

[15] Further, New Jersey Opinion 701 addresses the reality that it is

> [N]ot necessarily the case that safeguards against unauthorized disclosure are inherently stronger when a law firm uses its own staff to maintain a server. Providing security on the Internet against hacking and other forms of unauthorized use has become a specialized and complex facet of the industry, and it is certainly possible that an independent [Internet Service Provider] may more efficiently and effectively implement such security precautions.[34]

---

[31] *See* Jonathan R. Tung, *Survey: Law Departments Are Warming Up to the Cloud*, FINDLAW (Feb. 18, 2016), http://blogs.findlaw.com/in_house/2016/02/survey-law-depts-are-warming-up-to-the-cloud.html, *available at* https://perma.cc/M89M-LC3M.

[32] Strong, *supra* note 4.

[33] N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Op. 1020 (Sept. 12, 2014), http://www.nysba.org/CustomTemplates/Content.aspx?id=52001, *archived at* https://perma.cc/8MPU-62BR.

[34] N.J. Advisory Comm. on Prof'l Ethics, Op. 701 (2006), https://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf, *archived at* https://perma.cc/2H5Y-UYWX.

[16] Opinion 701 does include an additional caveat, that

> [W]hen client confidential information is entrusted in unprotected form, even temporarily, to someone outside the firm, it must be under a circumstance in which the outside party is aware of the lawyer's obligation of confidentiality, and is itself obligated, whether by contract, professional standards, or otherwise, to assist in preserving it.[35]

B. E-Discovery Tools

[17] To begin with, federal judges are unconvinced that many of the attorneys appearing before them understand how to make proper use of the technologies and related strategies associated with E-Discovery. A recent report, "Federal Judges Survey on E-Discovery Best Practices & Trends,"[36] compiled some of the judges' concerns, noting first "the typical attorney…does not have the legal and technical expertise to offer effective advice to clients on e-discovery."[37] Some of the judges' comments were quite blunt, with one noting that "[s]ome attorneys are highly competent; but most appear to have significant gaps in their understanding of e-discovery principles."[38]

[18] Legal ethical rules and related opinions and scholarship provide guidance for what attorney E-Discovery competence should look like. At least one author has made the connection between professional responsibility and technological savoir-faire, noting that:

---

[35] *Id.*

[37] Aebra Coe, *Judges Lack Faith in Attys' E-Discovery Skills, Survey Says*, LAW360 (Jan. 28, 2016), http://www.law360.com/articles/751961/judges-lack-faith-in-attys-e-discovery-skills-survey-says, *archived at* https://perma.cc/5UJB-D2YX.

[38] *Id.*

> There is growing recognition across the country that the practice of law requires some degree of competence in technology. In the forum of litigation, competence in technology necessarily equates with competence in e-discovery. It is only a matter of time before ethics bodies across the nation call for competence in e-discovery.[39]

[19] The opinions of courts and bar associations may carry the most weight, but a number of influential professional and industry groups also have offered useful commentary on technological competence. For example, competence is

> …highlighted in the very first rule of legal ethics, according to the American Bar Association['s] Rule 1.1 of the ABA Model Rules of Professional Conduct," which "specifically recognized the need for technological competence through a significant change in August 2012 that formally notified all lawyers (and specifically those in jurisdictions following the Model Rules) that competency includes current knowledge of the impact of e-Discovery and technology on litigation.[40]

[20] This guidance predated and perhaps presaged a number of state and federal reactions to technology and the impact of these developments on the practice of law, especially within the realm of E-Discovery. Delaware amended its Lawyers' Rules of Professional Conduct as they

---

[39] Bob Ambrogi, *California Considers Ethical Duty to Be Competent in E-Discovery*, CATALYST BLOG (Feb. 27, 2015), http://www.catalystsecure.com/blog/2015/02/california-considers-ethical-duty-to-be-competent-in-e-discovery/, *archived at* https://perma.cc/2FXD-8KM4.

[40] Karin S. Jenson, Coleman W. Watson & James A. Sherer, *Ethics, Technology, and Attorney Competence*, THE ADVANCED EDISCOVERY INST. (Nov. 2014), http://www.law.georgetown.edu/cle/materials/eDiscovery/2014/frimorndocs/EthicsIneDiscoveryBakerHostetler.pdf, *archived at* https://perma.cc/TFR6-VZNG.

related to technology in 2013;[41] North Carolina[42] and Pennsylvania[43] did the same shortly thereafter.

[21] California's relatively recent Formal Opinion No. 2015-193 (the "California Opinion") addresses a number of issues associated with attorney ethical duties vis-à-vis E-Discovery. Although advisory in nature, the California Opinion states "attorneys have a duty to maintain the skills necessary to integrate legal rules and procedures with 'ever-changing technology.'"[44] That reads broadly, but the California Opinion has been interpreted to indicate that, because E-Discovery arises "in almost every litigation matter, attorneys should have at least a baseline understanding of it."[45] Specifically, the California Opinion begins with the premise that E-Discovery requires an initial assessment of its inclusion at the beginning of a matter.[46] If E-Discovery will be a component of a matter,

> [T]he duty of competence requires an attorney to assess his or her own e-discovery skills and resources as part of the attorney's duty to provide the client with competent

[41] *See* Order Amending Rules 1.0, 1.1, 1.4, 1.6, 1.17, 1.18, 4.4, 5.3, 5.5, 7.1, 7.2, and 7.3 of the Delaware Lawyers' Rules of Professional Conduct, DEL. R. PROF'L CONDUCT (2013), http://courts.delaware.gov/rules/pdf/dlrpc2013rulechange.pdf.

[42] *See* N.C. STATE. BAR RULES OF PROF'L RESPONSIBILITY & CONDUCT R. 1.1 (2014), http://www.ncbar.com/rules/rules.asp?page=4, *archived at* https://perma.cc/7R44-4JAG.

[43] *See* Notice of Proposed Rulemaking, 43 Pa. Bull. 1997 (Apr. 13, 2013), http://www.pabulletin.com/secure/data/vol43/43-15/652.html, *archived at* https://perma.cc/WS5G-MHKQ.

[44] Bob Ambrogi, *California Finalizes Ethics Opinion Requiring Competence in E-Discovery*, CATALYST BLOG (Aug. 6, 2015), https://www.catalystsecure.com/blog/2015/08/california-finalizes-ethics-opinion-requiring-competence-in-e-discovery/, *archived at* https://perma.cc/V7NV-QCWW.

[45] *Id.*

[46] *See id.*

> representation. If an attorney lacks such skills and/or resources, the attorney must try to acquire sufficient learning and skill, or associate or consult with someone with expertise to assist.[47]

[22] Other commentators have noted that the California Opinion focuses on "nine (9) core competency issues" which would offer "solid guidelines for attorneys…to maintain competency and protect client confidentiality in the era of eDiscovery."[48] One author notes that one of these core competency issues and its related directive, that of performing data searches, stretches across the entirety of the E-Discovery process "occurring at each of these steps, from preservation and collection to review and redaction."[49]

[23] Soon after the California Opinion was decided, Magistrate Judge Mitchell Dembin issued a Southern District of California decision that addressed "counsels' ethical obligations and expected competency" in *HM Electronics, Inc. v. R.F. Technologies, Inc.*[50] The *HM Electronics* case focused both on specific steps the attorneys *should have taken* (such as

---

[47] State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 2015-193 (2015), https://ethics.calbar.ca.gov/Portals/9/documents/Opinions/CAL%202015-193%20%5B11-0004%5D%20(06-30-15)%20-%20FINAL.pdf, *archived at* https://perma.cc/8GWJ-BVJ2.

[48] Adam Kuhn, *The California eDiscovery Ethics Opinion: 9 Steps to Competency*, RECOMMIND BLOG (Aug. 11, 2015), http://www.recommind.com/blog/california-ediscovery-ethics-opinion-9-steps-to-competency, *archived at* https://perma.cc/2X2K-FCRQ.

[49] *Id.*

[50] H. Christopher Boehning & Daniel J. Toal, *E-Discovery Competence of Counsel Criticized in Sanctions Decision*, NEW YORK LAW JOURNAL (Oct. 6, 2015), http://www.newyorklawjournal.com/id=1202738840840/EDiscovery-Competence-of-Counsel-Criticized-in-Sanctions-Decision#ixzz42wNK34Ms, *archived at* https://perma.cc/4BMP-T76U.

implementing a legal hold and doing the legwork necessary to certify discovery responses as true) as well as behavior actively detrimental to the case (instructing client personnel to destroy relevant documents).[51] Of note in Judge Dembin's excoriation of the misbehaving attorneys is his statement that "a judge must impose sanctions for a violation of the Rule that was without substantial justification."[52] One article suggests that part of the problem may be simply that "counsel and clients alike…fail to take seriously judges' expectations for how they conduct themselves throughout the discovery process."[53]

[24] New York attorneys followed the California Opinion with interest, first noting that it merely presented "the standard tasks one should engage in and competently execute to properly collect and produce responsive ESI [Electronically Stored Information] to the opposing party."[54] A 2009 S.D.N.Y. opinion had chastised attorneys who would otherwise disclaim experience, warning that it was "time that the Bar—even those lawyers who did not come of age in the computer era" understood E-Discovery technologies and their application.[55] A recent article indicated that there is "an ample basis to discern a framework for ethical obligations, derived from ethics rules, court rules, and sanctions decisions in the e-discovery

[51] *See generally* HM Elecs., Inc. v. R.F. Techs., Inc., 2015 U.S. Dist. LEXIS 104100 (S.D. Cal. Aug. 7, 2015) (arguing the invalidity of the steps that the defendants took in order to certify discovery as true).

[52] Boehning & Toal, *supra* n. 50.

[53] *Id.*

[54] Samantha V. Ettari & Noah Hertz-Bunzl, *Ethical E-Discovery: Core Competencies for New York Lawyers*, NEW YORK LAW JOURNAL (Nov. 2, 2015), http://www.kramerlevin.com/files/Publication/60607051-f018-43b7-8a3c-7d43b4ff6e50/Presentation/PublicationAttachment/1e570a52-e27d-425f-a75b-9e25811df796/NYLJ%20Article-EDiscovery%2011.2.15.pdf, *archived at* https://perma.cc/F3R8-UWM6.

[55] William A. Gross Constr. Assocs., Inc. v. Am. Mfrs. Mut. Ins. Co., 256 F.R.D. 134, 136 (S.D.N.Y. 2009).

context" based in part on the history of New York courts as "leaders in the advancement of e-discovery law."[56]

[25] But such a "framework for ethical obligations" might not even be necessary where competence is the ethical rule at issue. Competence "requires that lawyers have the legal knowledge, skill, thoroughness, and preparation to conduct the representation, or associate with a lawyer who has such skills"[57] and that supervision is appropriate to ensure that the work of others "is completed in a competent manner."[58] The issue of supervision came up in another advisory opinion, Ethics Opinion 362 of the District of Columbia Bar, which indicated that retaining an e-Discovery vendor that provided all of the E-Discovery services was both impermissible (as the unauthorized practice of law on the part of the vendor) as well as a circumstance where the attorney engaging such a vendor was not absolved from understanding and supervising the work performed, no matter how technical.[59]

1. Metadata in Electronic Files

[26] A very basic threat to client confidentiality (as well as the secrecy of counsel's strategy) is the existence of metadata embedded in electronic files exchanged between the parties or produced as evidence. Most frequently this threat exists in the form of automatically created information about a file, including changes made to the file, that can be recovered and viewed by a third party if not removed (or "scrubbed") prior

[56] *See* Ettari & Hertz-Bunzl, *supra* n. 54.

[57] *See* Ettari & Hertz-Bunzl, *supra* n. 54 (citing New York Rules of Professional Conduct (N.Y. Rule) 1.1.5).

[58] *See* Ettari & Hertz-Bunzl, *supra* n. 54 (citing N.Y. Rule 5.1(c)).

[59] *See generally* D.C. Comm. on Legal Ethics, Formal Op. 362 (2012), https://www.dcbar.org/bar-resources/legal-ethics/opinions/opinion362.cfm, *archived at* https://perma.cc/TXA5-26ZG (discussing the permissibility of non-lawyer ownership of discovery service vendors).

to disclosing the file. This "application metadata" can include information about the document itself, the author, comments and prior edits, and may also detail when the document was created, viewed, modified, saved or printed.[60] In addition to the fact that access to metadata can provide opposing parties with everything from revealing insights to damning evidence, there's also a "real danger" that "application metadata may be inaccurate."[61]

[27] Further, disputes related to metadata regularly arise in the E-Discovery context. Indeed, one of the "biggest challenges in electronic discovery" concerns "[u]nderstanding when metadata is relevant and needs to be preserved and produced."[62] To cite just one example, the concurring opinion in *State v. Ratcliff* noted that judges must determine whether submitted evidence contained more than the information visible on the face of the document, or whether metadata was included as well, where the distinction "is critical, both on an ethical and adjudicative basis."[63]

[28] Accordingly, understanding and managing metadata has become a baseline requirement for technological competence when dealing with client data and attorney work product. Numerous products exist to help save lawyers from themselves when it comes to accidental disclosure of metadata, including software applications that may be integrated into email programs to prevent documents from being sent outside the network

---

[60] *See generally* The Sedona Conference Working Group, *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, THE SEDONA PRINCIPLES: SECOND EDITION, June 2007, at 60, 61 https://thesedonaconference.org/publication/The%20Sedona%20Principles, *archived at* https://perma.cc/UU5K-V8KQ (explaining the composition and functionality of metadata).

[61] *Id.* at 4.

[62] *Id.*

[63] State v. Ratcliff, 849 N.W.2d 183, 196 (N.D. 2014).

without first passing through a scrubbing filter. And the e-filing portal in many jurisdictions "contains a warning reminder that it is the responsibility of the e-filer to strip metadata from the electronic file before submitting it through the portal."[64] Reliance on these tools, however, may not suffice for long as the sophistication and complexity of issues related to the creation and manipulation of metadata continue to evolve.

III. OVERVIEW OF U.S. DATA PRIVACY AND INFORMATION SECURITY LAW

[29] The sectoral approach to privacy and data security law in the United States often is described as "a patchwork quilt" comprised of numerous state and federal laws and regulations that apply variously to certain types of data, certain industries, the application of particular technologies, or some combination of those elements. These laws may be enforced by a variety of regulators, with state Attorneys General and the Federal Trade Commission often leading the way.[65] Plaintiffs' lawyers also are prominent actors in this space, bringing an ever-increasing number of class action and other civil suits alleging violations of privacy rights, data protection laws, and information security standards.

[30] Although there are no federal or state privacy statutes specifically applicable solely to lawyers, numerous data protection laws and regulations may apply to attorneys in their role as service provider to their clients or in other contexts. The obligations associated with these laws often implicitly or explicitly demand that lawyers handling client data (1) have a thorough understanding of the potential privacy and security

[64] *See* Christian Dodd, *Metadata 101 for Lawyers: A 2-Minute Primer*, LAW360 (Oct. 15, 2015, 4:30 PM), http://www.law360.com/articles/712714/metadata-101-for-lawyers-a-2-minute-primer, *archived at* https://perma.cc/3VCT-TJRB.

[65] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 587 (2014).

risks to that data; (2) assess and determine how best to secure the data and prevent unauthorized access to the data; and (3) supervise anyone acting on their behalf with respect to the data to ensure the data is appropriately protected at all times.

[31] Below we describe a few of the privacy and data security laws that tend to come up frequently for lawyers and impose requirements on their handling of client data that may involve technological competence. This discussion is by no means exhaustive, as technology touches upon virtually every aspect of data protection regulation and information security counseling by attorneys in the field. To provide just a few examples, advising companies on restrictions applicable to cross-border data transfers, data localization requirements, cybersecurity standards and information sharing obligations, and regulatory action around the use of biometrics and geolocation technologies are just a few examples of areas where a lawyer must have an understanding of the underlying technology to effectively assist clients.

A. HIPAA – Business Associate Agreements

[32] The Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), is the most significant health privacy law in the United States, imposing numerous obligations on "covered entities" and "business associates" of those "covered entities" to protect the privacy and security of "protected health information" ("PHI").[66] As required by HIPAA, the Department of Health and Human Services ("HHS") issued two key sets of regulations to implement the statute: the Privacy Rule[67] and the Security Rule.[68]

---

[66] *See* Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. §§1320d to 1320d-8 (2007) [hereinafter HIPAA].

[67] *See* Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462 (Dec. 28, 2000) (codified at 45 C.F.R. pts. 160, 164).

[68] *See* Security Standards, 68 Fed. Reg. 8333, 8334 (Feb. 20, 2003) (codified at 45 C.F.R. pts. 160, 162, 164).

[33] Although attorneys and law firms are not themselves considered covered entities directly subject to HIPAA's requirements,[69] when attorneys obtain PHI from covered entity clients in the course of a representation, the law firm may be subject to certain HIPAA Privacy Rule requirements[70] in its role as a business associate.[71] The Privacy Rule and the Security Rule apply to a covered entity's interactions with third parties (e.g., service providers) that handle PHI on the covered entity's behalf.[72] The covered entity's relationships with these "business associates" are governed by obligatory contracts known as business associate agreements ("BAAs") that must contain specific terms.[73] With respect to technological competence specifically, for example, the BAA requires the business associate to implement appropriate safeguards to prevent use or disclosure of PHI other than as provided for by the BAA, and states that the business associate must ensure that any agents/subcontractors that receive PHI from the business associate also protect the PHI in the same manner. And attorneys who "hold HIPAA data or [other PII] may be governed by state or federal law beyond the scope of the proposed rules, which is noted in the new comments"[74] to ABA Rule

[69] The health plan within an organization, such as a law firm's employee health plan, may itself be a "covered entity" for HIPAA compliance purposes, but a firm generally is not, itself, a covered entity. *See, e.g.*, HIPAA, *supra* note 66.

[70] *See* John V. Arnold, *PRIVACY: What Lawyers Must Do to Comply with HIPAA*, 50 TENN. B.J. 16, 17 (Mar. 2014).

[71] *See* Lisa J. Acevedo et. al., *New HIPAA Liability for Lawyers*, 30 GPSOLO, no. 4, 2013, http://www.americanbar.org/publications/gp_solo/2013/july_august/new_hipaa_liability_lawyers.html, *archived at* https://perma.cc/F88Y-U928.

[72] *See* Standards for Privacy of Individually Identifiable Health Information, *supra* note 67; *see* Security Standards, *supra* note 68.

[73] Both the Privacy Rule and the Security Rule dictate certain terms that must be included in a BAA.

[74] *See* Nelson & Simek, *supra* note 27.

1.6, discussed further below.

B. GLBA Safeguards Rule Requirements

[34] Pursuant to the Gramm-Leach-Bliley Act ("GLBA"), the primary federal financial privacy law in the United States, various federal agencies promulgated rules and regulations addressing privacy and data security issues.[75] For example, the Safeguards Rule requires financial institutions to protect security of personally identifiable financial information by maintaining reasonable administrative, technical, and physical safeguards for customer information.[76] To comply with the Safeguards Rule, a financial institution must develop, implement, and maintain a comprehensive information security program, and that program must address the financial institution's oversight of service providers that have access to customers' nonpublic personal information ("NPI").[77]

[35] Again, although a law firm is not a financial institution directly subject to the GLBA, when it acts as counsel to a financial institution, GLBA requirements may apply to its handling of NPI received from that client. To the extent a financial institution's law firm will have access to such NPI in the course of the representation, the financial institution-client must take reasonable steps to ensure the law firm has the ability to safeguard such data prior to disclosing it to the firm, and require the firm to contractually agree (in writing) to safeguard the NPI. Assuming such data will be stored electronically (a safe assumption in virtually all cases), it is incumbent on the law firm to understand the potential data security risks and how to prevent unauthorized access, use, transfer, or other processing of their clients' NPI.

---

[75] *See* 15 U.S.C. §§ 6801–6809 (2012).

[76] *See* 16 C.F.R. §§ 314.2, 314.3(b).

[77] *See* 16 C.F.R. § 314.4(a-c).

C. State Data Security Laws

[36] At the state level, there are numerous laws and regulations regarding the protection of personal information (and other types of data) that apply to all entities that maintain such data, including lawyers, law firms, and other legal service providers.

[37] A number of states, such as California, Connecticut, Maryland, Nevada, Oregon, and Texas, have enacted laws that require companies to implement information security measures to protect personal information of residents of the state that the business collects and maintains.[78] These laws of general application are relevant to attorneys and law firms with respect to the personal information they maintain—both client data and data relating to their employees. Typically, these laws are not overly prescriptive and include obligations to implement and maintain reasonable security policies and procedures to safeguard personal information from unauthorized access, use, modification, disclosure, or destruction (though most do not offer a definition or description of what is meant by "reasonable" security). Some laws, such as California's, impose a requirement to contractually obligate non-affiliated third parties that receive personal information from the business to maintain reasonable security procedures with respect to that data.[79]

[38] Massachusetts was the first state to enact regulations that directed businesses to develop and implement comprehensive, written information security programs ("WISPs") to protect the personal information of Massachusetts residents.[80] These regulations apply to all private entities

[78] *See, e.g.*, CAL. CIV. CODE § 1798.81.5 (Deering 2009); CONN. GEN. STAT. § 42-471 (2010); MD. CODE ANN., COM. LAW §§ 14-3501 to 14-3503 (LexisNexis 2009); NEV. REV. STAT. § 603A.210 (2009); OR. REV. STAT. § 646A.622 (2009); TEX. BUS. & COM. CODE ANN. §§ 72.001–72.051 (West 2009).

[79] *See* CAL. CIV. CODE § 1798.81.5 (Deering 2009).

[80] *See* 201 MASS. CODE REGS. 17.01–17.05 (2008).

(including law firms) that maintain personal information of Massachusetts residents, including those that do not operate in Massachusetts; they also list a number of minimum standards for the information security program.[81] The Massachusetts regulations are relatively prescriptive as compared to other similar state laws of this nature, and they include numerous specific technical requirements.

[39] These requirements apply to law firms directly, but they also apply to law firms as service providers to businesses that maintain personal information of Massachusetts residents. A compliant WISP must address the vetting of service providers, and the contract must include provisions obligating the service provider to protect the data.[82]

IV. APPLICABLE ETHICAL RULES AND GUIDANCE

[40] The myth of the Luddite[83] or caveman[84] lawyer persists, even if this type of anachronism is, in fact, an ethical violation waiting to happen.[85] But even attorneys who "only touch a computer under duress,

[81] *See id.*

[82] *See id.*

[83] *See* Debra Cassens Weiss, *Lawyers Have Duty to Stay Current on Technology's Risks and Benefits, New Model Ethics Comment Says*, ABA Journal Law News (Aug. 6, 2012, 7:46 PM) http://www.abajournal.com/news/article/lawyers_have_duty_to_stay_current_on_technologys_risks_and_benefits/, *archived at* https://perma.cc/WPZ4-2DYH.

[84] *See Unfrozen Caveman Lawyer*, SATURDAY NIGHT LIVE TRANSCRIPTS, http://snltranscripts.jt.org/91/91gcaveman.phtml, *archived at* https://perma.cc/M7GB-DGJZ ("Sometimes when I get a message on my fax machine, I wonder: 'Did little demons get inside and type it?' I don't know! My primitive mind can't grasp these concepts.") (last visited Apr. 5, 2016).

[85] *See* Megan Zavieh, *Luddite Lawyers Are Ethical Violations Waiting to Happen*, LAWYERIST.COM (last updated July 10, 2015), https://lawyerist.com/71071/luddite-lawyers-ethical-violations-waiting-happen/, *archived at* https://perma.cc/6V4W-94J7.

and take comfort in paper files and legal research from actual books"[86] must deal with technology.[87] The adequate practice—or perhaps simply "the practice" of law does not exist without technology, and there is no longer a place for lawyers who simply "hope to get to retirement before they need to fully incorporate technology into their lives."[88]

[41] "Really?" goes the refrain. "Why can't I just practice the way I always have, without [insert mangled, vaguely-recognizable technology portmanteau] getting in the way?"

[42] Well, for one thing, to the extent attorneys rely on the protections of privilege to serve their clients, said attorneys must understand how the confidentiality of their communications and work product may be compromised by the technology they use. Technologies introduce complexity that, in turn, may affect privilege—especially when "many lawyers don't understand electronic information or have failed to take necessary precautions to protect it."[89] But how much understanding,

[86] Lois D. Mermelstein, *Ethics Update: Lawyers Must Keep Up with Technology Too, American Bar Association – Business Law Today*, BUSINESS LAW TODAY (Mar. 2013), http://www.americanbar.org/publications/blt/2013/03/keeping_current.html, *archived at* https://perma.cc/T8CF-ZWND.

[87] *See* Blair Janis, *How Technology Is Changing the Practice Of Law*, GP SOLO, http://www.americanbar.org/publications/gp_solo/2014/may_june/how_technology_changing_practice_law.html, *archived at* https://perma.cc/23P5-PGM7 (last visited Apr. 5, 2016).

[88] Kevin O'Keefe, *We Need Laws Requiring Lawyers to Stay Abreast of Technology?* LEXBLOG: ETHICS & BLOGGING LAW (Mar. 28, 2015), http://kevin.lexblog.com/2015/03/28/we-need-laws-requiring-lawyers-to-stay-abreast-of-technology/, *archived at* https://perma.cc/8DR5-XK43.

[89] *Attorney-client Privilege: Technological Changes Bring Changing Responsibilities for Attorneys and Legal Departments,* CORPORATE LAW ADVISORY, http://www.lexisnexis.com/communities/corporatecounselnewsletter/b/newsletter/archive/2014/01/06/attorney-client-privilege-technological-changes-bring-changing-responsibilities-for-attorneys-and-legal-departments.aspx, *archived at* https://perma.cc/XQ53-P3MF (last visited Apr. 5, 2016).

exactly, may be required to competently represent clients in matters concerning E-Discovery, or data security, or even privacy? At many organizations, "[p]rivacy issues get handled by anyone who wants to do them" because the subject matter area is understaffed or ignored.[90] The key technological issues relevant to E-Discovery versus data privacy may be somewhat different, but the "solutions" companies find are eerily similar: the practitioners that are actually doing the work are often those who have been delegated the work, whose "expertise" is somewhat home-grown and may, in fact, not really represent true technological competence at all.[91]

[43] What, then, are the requirements for expertise? Perhaps a pragmatic approach is best. Certainly, practitioners who use technology—again, likely all of them—must take some well-defined, initial steps toward acquiring the appropriate skill set. This might be as straightforward as the lawyer familiarizing herself with the relevant technologies at issue. Although it may sound a bit *too* easy, "just being well-versed enough to understand the issues is a big plus."[92] That being said, "those considering a career in cybersecurity or privacy will need to spend time developing some level of technical expertise."[93] In short, the answer is "it depends"

---

[90] Daniel Solove, *Starting a Privacy Law Career*, LINKEDIN PULSE (Aug. 27, 2013), https://www.linkedin.com/pulse/20130827061558-2259773-starting-a-privacy-law-career?forceNoSplash=true, *archived at* https://perma.cc/G78L-DM2X.

[91] *See* Peter Geraghty & Sue Michmerhuizen, *Think Twice Before You Call Yourself an Expert*, YOUR ABA (Mar. 2013), http://www.americanbar.org/newsletter/publications/youraba/201303article11.html, *archived at* https://perma.cc/HJK7-RSLG .

[92] Solove, *supra* note 90.

[93] Alysa Pfeiffer-Austin, *Four Practical Tips to Succeed in the Cybersecurity and Privacy Law Market*, ABA Security Law (Dec. 9, 2015), http://abaforlawstudents.com/2015/12/09/four-practical-tips-to-succeed-in-the-cybersecurity-and-privacy-law-market/, *archived at* https://perma.cc/AH9A-JCTU.

and "no one really knows – yet." In this relatively new space, actual decisions and definitive standards for "technological competence" are thin on the ground. Below we will examine some of the relevant rules and guidelines to consider.

A. Recent Guidelines in the Ethics Rules

[44] Most attorneys do not have specialized training focused on a particular technological field. Certainly the vast majority do not hold themselves out as experts in cybersecurity, cloud-based storage, social media, biometrics, or any of a variety of related disciplines. However, even in the absence of expertise, there are some basic ethical rules that provide a framework for determining a practitioner's professional duties and obligations with regard to technology—specifically, rules pertaining to competent client representation, adequate supervision, confidentiality, and communications.[94]

1. Competent Client Representation (Model Rule 1.1)

[45] As discussed briefly above, almost four years ago, the America Bar Association formally approved a change to the Model Rules of Professional Conduct to establish a clear understanding that lawyers have a duty to be competent not only in the law and its practice, but also with respect to technology. Detailed below, the passage of this rule contemplated changes in technology and eschewed specifics. Rather than a paint-by-numbers approach, ABA Model Rule 1.1 puts the responsibility on attorneys to understand their own—and their clients'—needs, and how new technologies impact their particular practice.

[46] ABA Model Rule 1.1 states that:

---

[94] *See* David G. Ries, *Cybersecurity for Attorneys: Understanding the Ethical Obligations*, LAW PRACTICE TODAY (Mar. 2012), http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/cyber-security-for-attorneys-understanding-the-ethical-obligations.html, *archived at* https://perma.cc/N4VM-N4NG.

> A lawyer shall provide competent representation to a client. Competent representation requires legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.[95]

[47] ABA Model Rule 1.1 was amended in 2012 by Codified Comment 8 as follows:

> To maintain the requisite knowledge and skills, 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.[96]

[48] Some note that Rule 1.1 "does not actually impose any new obligations on lawyers;"[97] neither does it require perfection.[98] Instead it "simply reiterates the obvious, particularly for seasoned eDiscovery lawyers, that in order for lawyers to adequately practice, they need to understand the means by which they zealously advocate for their clients."[99] One article noted, in fact, that Comment 8 was evidence of "the ABA's desire to nudge lawyers into the 21st century when it comes to

[95] MODEL RULES OF PROF'L CONDUCT R. 1.1 (2014).

[96] MODEL RULES OF PROF'L CONDUCT R. 1.1 cmt. 8 (2014) (emphasis added).

[97] Jenson, Watson & Sherer, *supra* note 40, at 2.

[98] *See* James Podgers, *You Don't Need Perfect Tech Knowhow for Ethics' Sake—But a Reasonable Grasp Is Essential*, ABA JOURNAL (Aug. 9, 2014), http://www.abajournal.com/news/article/you_dont_need_perfect_tech_knowhow_for_ethics_sake--but_a_reasonable_grasp, *archived at* https://perma.cc/CB3P-R7YL.

[99] Jenson, Watson & Sherer, *supra* note 40, at 2.

technology."[100] It did, however, caution that it was "a very gentle nudge."[101]

[49] Nudge or not, that message has resonated across the United States. In the four years since that amendment was approved and adopted by the ABA, twenty-one states since have adopted the ethical duty of technological competence for lawyers.[102] As for many of the states that have not formally adopted the change to their Model Rules of Professional Conduct, those may still explicitly or implicitly acknowledge this emerging duty to be competent in technology, having a basic understanding of technologies their clients use, and a duty to keep abreast of such changes including a required awareness of regulatory requirements and privacy laws.[103]

---

[100] Kelly H. Twigger, Symposium, *Ethics in Technology and eDiscovery – Stuff You Know, but Aren't Thinking About*, ARK. L. REV. (Oct. 16, 2014), http://law.uark.edu/documents/2014/10/TWIGGER-Ethics-in-Technology-and-eDiscovery.pdf, *archived at* https://perma.cc/LTG8-7AYU.

[101] *Id.*

[102] These states are: Arizona, Arkansas, Connecticut, Delaware, Idaho, Illinois, Iowa, Kansas, Massachusetts, Minnesota, Nebraska, New Hampshire, New Mexico, New York, North Carolina, Ohio, Pennsylvania, Utah, Virginia, West Virginia, and Wyoming. *See* Robert Ambrogi, *20 States Have Adopted Ethical Duty of Technological Competence*, LAW SITES (Mar. 16, 2015), http://www.lawsitesblog.com/2015/03/11-states-have-adopted-ethical-duty-of-technology-competence.html, *archived at* https://perma.cc/B5TF-D6NJ (last updated Dec. 23, 2015) (listing 20 states not including Nebraska); *see also Basic Technology Competence for Lawyers*, Event Details, NEBRASKA BAR ASSOC. (Apr. 6, 2016), https://nebar.site-ym.com/events/EventDetails.aspx?id=788239&group=, *archived at* https://perma.cc/SMU6-58TU ("[T]he need to be aware of and have a working knowledge of technology…is ethically required of all lawyers.").

[103] Ann M. Murphy, *Is It Safe? The Need for State Ethical Rules to Keep Pace with Technological Advances*, 81 FORDHAM L. REV. 1651, 1659, 1665–66 (2013), http://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4876&context=flr, *archived at* https://perma.cc/V69A-EETR.

2. Supervision (Model Rules 5.1 and 5.3)

[50] ABA Model Rule 5.1 also bears on a lawyer's duties regarding technology insofar as duties aided or supported by technology are performed by someone other than the attorney. This responsibility extends to immediate as well as remote support staff, with ABA Model Rule 5.1 requiring that "[l]awyers must also supervise the work of others to ensure it is completed in a competent manner."[104] This attempt at establishing "the principle of supervisory responsibility without introducing a vicarious liability concept"[105] has led to considerations regarding inexperience generally,[106] but the implications for technological applications should be clear—an associate or other paralegal professional is much more likely to use technology to support legal work[107] than she is to make a representation before a court or like body.

[51] ABA Model Rule 5.3 also sets forth responsibilities of partners and supervising attorneys to non-lawyer assistants. This set of ethical considerations further reinforces the responsibilities attorneys have to apply sufficient care in their practice when outsourcing supporting legal

---

[104] Samantha V. Ettari & Noah Hertz-Bunzl, *Ethical E-Discovery: What Every Lawyer Needs to Know*, LEGALTECHNEWS (Nov. 10, 2015), http://www.kramerlevin.com/files/Publication/d7dec721-693a-4810-a4b9-32dfe9c1864b/Presentation/PublicationAttachment/018a444a-d7de-46b2-bc16-506cff88d346/EDiscovery-Legaltech%20News11.10.15..pdf, *archived at* https://perma.cc/4YMR-XL9U (referring to MODEL RULE OF PROF'L CONDUCT 5.1).

[105] AMERICAN BAR ASSOCIATION, A LEGISLATIVE HISTORY: THE DEVELOPMENT OF THE ABA MODEL RULES OF PROFESSIONAL CONDUCT, 1982-2005 560 (2006).

[106] Jeffrey P. Reilly, *Rule 5.1 of the Rules of Professional Conduct: What Must Corporate General Counsel Do?* ASSOCIATION OF CORPORATE COUNSEL, BALTIMORE CHAPTER FOCUS 2Q12 5–6 (2012), http://www.milesstockbridge.com/pdf/publications/ReillyACCArticle.pdf, *archived at* https://perma.cc/G26J-NTJE.

[107] *See* Jennifer Ellis, *What Technology Does a Modern US Lawyer Generally Use in Practice?*, QUORA (Mar. 22, 2014), https://www.quora.com/What-technology-does-a-modern-US-lawyer-generally-use-in-practice, *archived at* https://perma.cc/4FX4-2UV7.

work to inexperienced non-professionals, and to ensure that confidentiality is maintained with outsourcing staff.[108] This is not just a matter of supervising specific tasks. It also contemplates knowing which tasks are appropriate for delegation, both within the firm and to third-party vendors. For example, if a delegate of the attorney uses technology to begin an engagement, it's possible that such an arrangement could be viewed as "establish[ing] the attorney-client relationship," which may be prohibited under ABA Model Rule 5.5.[109]

3. Duty of Confidentiality (Model Rule 1.6)

[52] ABA Model Rule 1.6 states that it is critical that lawyers do not reveal confidential or privileged client information.[110] When information was kept in an attorney's head, or perhaps committed to a sheet of paper, historical precedent on how to comply with this duty may have been helpful. In the "world of tomorrow,"[111] looking to the past for answers makes little sense, especially in those instances where the attorney is unclear as to how information is stored, accessed, maintained, or utilized.

[53] Model Rule 1.6 also considers a duty of confidentiality that resides at the core of every attorney's role and serves as one of the attorney's most important ethical responsibilities. Model Rule 1.6 generally defines the duty of confidentiality as follows: "A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the

[108] *See* MODEL RULES OF PROF'L CONDUCT R. 5.3.

[109] Frances P. Kao, *No, a Paralegal Is Not a Lawyer*, ABA BUS. LAW TODAY, (Jan./Feb. 2007), https://apps.americanbar.org/buslaw/blt/2007-01-02/kao.shtml, *archived at* https://perma.cc/3J2N-ELPA.

[110] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6.

[111] *See* Jon Snyder, *1939's 'World of Tomorrow' Shaped Our Today*, WIRED (Apr. 29, 2010, 8:00 PM), http://www.wired.com/2010/04/gallery-1939-worlds-fair/, *archived at* https://perma.cc/D5V4-36R5.

representation or the disclosure is permitted [elsewhere]."[112]

[54] This rule is broad. It encompasses any client information, confidential or privileged, shared or accessible to the attorney and is not limited to just confidential communications. Further, it may only be relinquished under the most onerous of circumstances.[113] A lawyer shall not, therefore, reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation, or the disclosure is permitted elsewhere in the rules.

[55] In 2000, the Advisory Committee looked into its crystal ball and considered ESI on various platforms, in different repositories, in various forms. It then added Comment 18 to Rule 1.6, requiring reasonable precautions to safeguard and preserve confidential information. Comment 18 states that, "[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."[114] Indeed, "[p]artners and supervising attorneys are required to take reasonable actions to ensure that those under their supervision comply with these requirements."[115]

---

[112] MODEL RULES OF PROF'L CONDUCT R. 1.6.

[113] *See* Saul Jay Singer, *Speaking of Ethics: When Tarasoff Meets Rule 1.6*, WASHINGTON LAWYER (May 2011), https://www.dcbar.org/bar-resources/publications/washington-lawyer/articles/may-2011-speaking-of-ethics.cfm, *archived at* https://perma.cc/A7E4-DSH6.

[114] MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 18.

[115] David G. Ries, *Cybersecurity for Attorneys: Understanding the Ethical Obligations*, LAW PRACTICE TODAY (Mar. 2012), http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/cyber-security-for-attorneys-understanding-the-ethical-obligations.html, *archived at* https://perma.cc/59Q2-55Q4.

[56] In addition to the ABA's commentary, state and local professional organizations have issued guidance as well. In establishing a specific roadmap for lawyers to attain the skills necessary to meet their ethical obligations with respect to relevant technology in the practice of law, and returning to the California Bar's Formal Opinion 2015-193, there is a sort of checklist that may assist lawyers in meeting their ethical obligations to develop and maintain core E-Discovery competence in the following areas:[116]

- Initially assessing E-Discovery needs and issues, if any;
- Implementing or causing (the client) to implement appropriate ESI preservation procedures, ("such as circulating litigation holds or suspending auto-delete programs");[117]
- Analyzing and understanding the client's ESI systems and storage;
- Advising the client on available options for collection and preservation of ESI;
- Identifying custodians of potentially relevant ESI;
- Engaging in competent and meaningful meet and confers with opposing counsel concerning an E-Discovery plan;
- Performing data searches;
- Collecting responsive ESI in a manner that preserves the integrity of the ESI; and
- Producing responsive, non-privileged ESI in a recognized and appropriate manner.

[57] But this technological competence inherent in the Duty of Competence represents only one third of the ethical duties that govern an

---

[116] *See* State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2015-193, 3–4 (2015) [hereinafter Cal. Ethics Op. 2015-193] (discussing what an attorney's ethical duties are in the handling of discovery of electronically stored information).

[117] Ettari & Hertz-Bunzl, *supra* note 104.

attorney's interaction with technology. This ESI and litigation skills checklist does *not* address "the scope of an attorney's duty of competence relating to obtaining an opposing party's ESI;"[118] nor does it consider the skills required of non-litigation attorneys, which must be inferred from the rule.

[58] In addition, the State Bar of California's Standing Committee on Professional Responsibility and Conduct, Formal Opinion 2010-179 states that "[a]n attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representations does not subject confidential client information to an undue risk of unauthorized disclosure."[119]

[59] In reference to the duty of confidentiality, the New York County Lawyer's Association's Committee on Professional Ethics examined shared computer services amongst practitioners in Opinion 733, noting that an "attorney must diligently preserve the client's confidences, whether reduced to digital format, paper, or otherwise. The same considerations would also apply to electronic mail and websites to the extent they would be used as vehicles for communications with the attorney's clients."[120] The New York State Bar's Committee on Professional Ethics Opinion 842 further stated that, when "a lawyer is on notice that the [client's] information…is of 'an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the

[118] Cal. Ethics Op. 2015-193, *supra* note 116, at fn. 7.

[119] State Bar of Cal. Standing Comm. on Prof'l Responsibility and Conduct, Formal Op. 2010-179, 7 (2010) (discussing whether an attorney violates the duties of confidentiality and competence she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties).

[120] N.Y. Cnty. Lawyers' Ass'n Comm. on Prof'l Ethics, Formal Op. 733, 7 (2004) (discussing non-exclusive referrals and sharing of office space, computers, telephone lines, office expenses, and advertising with non-legal professionals).

lawyer's control,…the lawyer must select a more secure means of communication than unencrypted Internet e-mail.'"[121]

4. Communications (Model Rule 1.4)

[60] ABA Model Rule 1.4 on Communications also applies to the attorney's use of technology and requires appropriate communications with clients "about the means by which the client's objectives are to be accomplished," including the use of technology.[122]

[61] In construing all of these Model Rules and comments, it is clear that attorneys who are not tech-must (1) understand their limitations; (2) obtain appropriate assistance; (3) be aware of the areas in which technology knowledge is essential; and (4) evolve to competently handle those challenges; or (5) retain the requisite expert assistance. This list applies equally to data security issues, such as being aware of the risks associated with cloud storage, cybersecurity threats, and other sources of potential harm to client data, and can easily be extended to include awareness and understanding with respect to domestic and foreign data privacy issues.

[62] The ethical obligations to safeguard information require reasonable security, not absolute security. Accordingly, under such rules and related guidance from the Proposal from the ABA Commission on Ethics 20/20,[123] the factors to be considered in determining the reasonableness of

---

[121] N.Y. State Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 842 (2010) (discussing using an outside online storage provider to store client's confidential information).

[122] MODEL RULES OF PROF'L CONDUCT R. 1.4 (1983); *see also* 204 PA. CODE § 81.4 (1988), http://www.pacode.com/secure/data/204/chapter81/chap81toc.html, *archived at* https://perma.cc/6FG5-9VP3 (incorporating ABA Model Rule 1.4 into Pennsylvania's Model Rule 1.4).

[123] *See* ABA Comm. on Ethics 20/20, *Introduction and Overview* (Feb. 2013), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20121112_ethics_20_20_overarching_report_final_with_disclaimer.authcheckdam.pdf, *archived at* https://perma.cc/D2ZY-NYEU.

the lawyers' efforts with respect to security include:

> (1) The sensitivity of the information;
> (2) The likelihood of disclosure if additional safeguards are not employed;
> (3) The cost of employing additional safeguards;
> (4) The difficulty of implementing the safeguards; and
> (5) The extent to which the safeguards adversely affect the lawyer's ability to represent the client.[124]

As New Jersey Ethics Opinion 701 states, "[r]easonable care however does not mean that the lawyer absolutely and strictly guarantees that the information will be utterly invulnerable against all unauthorized access. Such a guarantee is impossible."[125]

B. Ethics and Social Media

[63] When considering their ethical duties with respect to technology, lawyers today must confront a host of challenges that would have been almost unimaginable even ten years ago. The rise and proliferation of social media as a daily part of most people's personal and professional lives has created one such challenge.[126] Numerous courts have

---

[124] MODEL RULES OF PROF'L CONDUCT R. 1.6(c) cmt. 18 (1983).

[125] Opinion 701 also highlights, if inadvertently, the challenges attorneys face when trying to modify existing practices to fit new technologies. As part of the inquiry underpinning Opinion 701's guidance, the opinion notes that "nothing in the RPCs prevents a lawyer from archiving a client's file through use of an electronic medium such as PDF files or similar formats." This note is nearly laughable when read in the context of current practice, as it suggests that attorneys were (or are?) concerned about whether PDF files are appropriate for retaining paper documents. N.J. Advisory Comm. on Prof'l Ethics, Formal Op. 701 (2006), https://www.judiciary.state.nj.us/notices/ethics/ACPE_Opinion701_ElectronicStorage_12022005.pdf, *archived at* https://perma.cc/EV9H-BN3T.

[126] *See* Brian M. Karpf, *Florida's Take on Telling Clients to Scrub Social Media Pages*, LAW 360 (Sept. 15, 2015, 4:33 PM), http://www.law360.com/articles/702288/florida-s-

addressed—and continue to address—attorney duties with respect to social media in the context of spoliation motions when social media evidence has been lost, destroyed, or obfuscated due to negligence, or in accordance with attorney advice.[127] In addition, given the novelty and complexity of the issues, and in the interest of consistency, state bar associations have begun to address issues associated with attorney use of, counseling on, and preservation of social media.

[64] The Association of the Bar of the City of New York's Committee on Professional and Judicial Ethics, in Formal Opinion 2010-2, provided some helpful guidelines on attorney access to social media, stating that "[a] lawyer may not use deception to access information from a social networking webpage," either directly or through an agent.[128] While focused on behaviors that attorneys and their agents should not undertake when developing a case, the opinion does note that the "potential availability of helpful evidence on these internet-based sources makes them an attractive new weapon in a lawyer's arsenal of formal and informal discovery devices," and also offers up "the Court of Appeals' oft-cited policy in favor of informal discovery."[129] Simply put, the duty is twofold: an attorney must both be aware of social media and know how to use social media to provide effective representation.

2. State Bar Association Guidance

[65] State bar associations are becoming increasingly involved in

take-on-telling-clients-to-scrub-social-media-pages, *archived at* https://perma.cc/NZ3W-FHPS.

[127] *See id.*

[128] N.Y.C. Bar Ass'n Comm. on Prof'l. Ethics, Formal Op. 2010-2 (2010), http://www.nycbar.org/ethics/ethics-opinions-local/2010-opinions/786-obtaining-evidence-from-social-networking-websites, *archived at* https://perma.cc/JT9K-2EGV (discussing lawyers' obtainment of information from social networking websites).

[129] *Id.*

providing guidance on social media and its implications for the practice of law. For example, in 2014, the New York and Pennsylvania State Bar Associations and the Florida Professional Ethics Committee issued guidance on social media usage by attorneys and addressed the obligations of attorneys to understand how various platforms work, what information will be available to whom, the ethical implications of advising clients to alter or change social media accounts, and the value of ensuring adequate preservation of social media evidence.

i. New York

[66] The Social Media Ethics Guidelines of the Commercial and Federal Litigation Section of the New York State Bar Association provide specific guidance for the use of social media by attorneys.[130] Guideline 4, relating to the review and use of evidence from social media, is divided into four subparts, all of which provide specific and pertinent guidance to attorneys:

- Guideline No. 4.A: Viewing a Public Portion of a Social Media Website, provides that "[a] lawyer may view the public portion of a person's social media profile or public posts even if such person is represented by another lawyer. However, the lawyer must be aware that certain social media networks may send an automatic message to the person whose account is being viewed which identifies the person viewing the account as well as other information about such person."[131]

- Guideline No. 4.B: Contacting an Unrepresented Party to View a Restricted Portion of a Social Media

[130] Mark A. Berman, Ignatius A. Grande & James M. Wicks, *Social Media Ethics Guidelines of the Commercial and Federal Litigation Section of the New York State Bar Association*, THE NEW YORK STATE BAR ASSOCIATION (June 9, 2015), http://www.nysba.org/socialmediaguidelines/, *archived at* https://perma.cc/4ZSN-BXT4.

[131] *Id.*

> Website, provides that "[a] lawyer may request permission to view the restricted portion of an unrepresented person's social media website or profile. However, the lawyer must use her full name and an accurate profile, and she may not create a different or false profile to mask her identity. If the person asks for additional information from the lawyer in response to the request that seeks permission to view her social media profile, the lawyer must accurately provide the information requested by the person or withdraw her request."[132]

- Guideline No. 4.C: Viewing A Represented Party's Restricted Social Media Website, provides that "[a] lawyer shall not contact a represented person to seek to review the restricted portion of the person's social media profile unless an express authorization has been furnished by such person."[133]

- Guideline No. 4.D: Lawyer's Use of Agents to Contact a Represented Party, "as it relates to viewing a person's social media account," provides that "[a] lawyer shall not order or direct an agent to engage in specific conduct, or with knowledge of the specific conduct by such person, ratify it, where such conduct if engaged in by the lawyer would violate any ethics rules."[134]

ii. Florida

---

[132] *Id.*

[133] *Id.*

[134] *Id.*

[67] In Advisory Opinion 14-1, the Florida Bar Association's Professional Ethics Committee confirmed that an attorney could advise a client to increase privacy settings (as so to conceal from public eye) and remove information relevant to the foreseeable proceedings from social media as long as an appropriate record was maintained—the data preserved—and no rules or substantive laws regarding preservation and/or spoliation of evidence were broken.[135]

iii. Pennsylvania

[68] In 2014, the Pennsylvania Bar Association issued a Formal Opinion that included detailed guidance regarding an attorney's ethical obligations with respect to the use of social media. Among other guidelines, the Opinion specifically stated that:

- Attorneys may advise clients about the content of their Social networking websites, including the removal or addition of information;
- Attorneys may connect with clients and former clients;
- Attorneys may not contact a represented person through social networking websites;
- Although attorneys may contact an unrepresented person through social networking websites, they may not use a pretextual basis for viewing otherwise private information on social networking websites; and
- Attorneys may use information on social networking websites in a dispute.[136]

[135] *See* Fla. State Bar Comm. on Prof'l Ethics, Proposed Op. 14-1 (2015), http://www.floridabar.org/TFB/TFBResources.nsf/Attachments/B806500C941083C785257E730071222B/$FILE/14-01%20PAO.pdf?OpenElement, *archived at* https://perma.cc/DK9W-A44Z.

[136] Pa. Bar Ass'n. Comm. on Ethics, Formal Op. 2014-300, 2 (2014), http://www.americanbar.org/content/dam/aba/events/professional_responsibility/2015/M

3. ABA Model Rule 3.4

[69] Finally, although ABA Model Rule 3.4 on Fairness to Opposing Party and Counsel does not directly address social media, the principles behind the rule apply in the social media context. The Rule provides that an attorney shall not "unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value" nor shall the attorney "counsel or assist another person" to undertake such actions.[137]

C. Guidance on Duties Related to Cybersecurity

[70] As we discussed above in Section II, attorneys face a complex threat landscape when it comes to security concerns related to the protection of their clients' data.[138] Although the scope of an attorney's ethical obligations in this regard remains somewhat unclear, there are several sources of guidance relevant to how lawyers are expected to manage cybersecurity risks.

[71] One such source that squarely addresses the issue is the Resolution issued by the ABA's Cybersecurity Legal Task Force. The Resolution contains a detailed Report explaining the ABA's position regarding the growing problem of intrusions into computer networks utilized by lawyers and law firms, and urges lawyers and law firms to review and comply with the provisions relating to the safeguarding of confidential client information.[139] As the ABA noted in its Report, defending the

ay/Conference/Materials/pa_formal_op_2014_300.authcheckdam.pdf, *archived at* https://perma.cc/G6EY-PBFF.

[137] MODEL RULES OF PROF'L CONDUCT R. 3.4 (1983).

[138] *See supra* Part II.

[139] *See* ABA Cybersecurity Legal Task Force, Resolution 118, 2 (August 2013), http://www.americanbar.org/content/dam/aba/administrative/law_national_security/resolution_118.authcheckdam.pdf, *archived at* https://perma.cc/UQ44-3Q2C.

confidentiality of the lawyer-client relationship and preservation of privilege in communications and attorney work product are fundamental to public confidence in the legal system.[140] Attorneys are directed to (1) keep clients reasonably informed as set forth in the Model Rules of Professional Conduct, as amended in August 2012 and adopted in the jurisdictions applicable to their practice; and (2) comply with other applicable state, federal, and court rules pertaining to data privacy and cybersecurity.[141] The ABA further urges the respect and preservation of the attorney client relationship during the pendency of any actions in which a government entity aims to deter, prevent, or punish unauthorized, illegal intrusions into computer systems and networks used by lawyers and law firms.

[72] The comment to ABA Model Rule 5.7 states, perhaps somewhat axiomatically, that when "[a] lawyer performs law-related services or controls an organization that does so, there exists the potential for ethical problems."[142] This, combined with Model Rule 1.6's requirement for attorneys to safeguard and protect client information, suggests further potential duties associated with cybersecurity.[143] As one author notes

> Fulfillment of a law firm's duty to maintain client confidences in today's world of cyberattacks requires much more than legal knowledge and legal skills. It requires sophisticated computer knowledge and skills far beyond legal practice. That is why cybersecurity experts should be used to assist in any law firm's client's data protection

---

[140] *See id.* at 4.

[141] *See id.* at 16.

[142] MODEL RULES OF PROF'L CONDUCT R. 5.7, cmt. 1 (1983).

[143] *See* MODEL RULES OF PROF'L CONDUCT R. 1.6.

> efforts.[144]

Indeed, "[t]raining in security, including cybersecurity should be a part of every lawyer's education. It is especially important for lawyers who do electronic discovery".[145]

[73] On a related subject, in Formal Opinion 2015-3, the New York City Bar Association issued guidance indicating that lawyers do *not* violate their ethical duties by reporting suspected cybercrime to law enforcement.[146] If an attorney has performed "reasonable diligence" to determine whether a prospective client is actually attempting fraud, the opinion says, then the attorney is free to report.[147] The Opinion continued, highlighting the lack of duty associated with individuals who are not actually clients, stating that an

> attorney who discovers that is he the target of an Internet-based trust account scam does *not* have a duty of confidentiality to the individual attempting to defraud him, and is free to report the individual to law enforcement authorities, because that person does not qualify as a prospective or actual client of the attorney.[148]

---

[144] Ralph C. Losey, *The Importance of Cybersecurity in eDiscovery*, E-DISCOVERY LAW TODAY (May 9, 2014) http://www.ediscoverylawtoday.com/2014/05/the-importance-of-data-security-in-ediscovery/, *archived at* https://perma.cc/P64J-NYQ7.

[145] Ralph C. Losey, *The Importance of Cybersecurity to the Legal Profession and Outsourcing as a Best Practice – Part Two*, E-DISCOVERY TEAM (May 18, 2014), http://e-discoveryteam.com/2014/05/18/the-importance-of-cybersecurity-to-the-legal-profession-and-outsourcing-as-a-best-practice-part-two/, *archived at* https://perma.cc/W3HW-AHCC.

[146] N.Y.C. Bar Ass'n Comm. on Prof'l Ethics, Formal Op. 2015-3, 4–5 (2015), http://www2.nycbar.org/pdf/report/uploads/20072898-FormalOpinion2015-3-LAWYERSWHOFALLVICTIMTOINTERNETSCAMS.pdf, *archived at* https://perma.cc/6BHV-V2YC.

[147] *Id.* at 1.

[148] *Id.* at 6 (emphasis added).

V. CONCLUSION

[74] It goes without saying that we live (and work) in interesting times. Cloud technology offers convenience, flexibility, cost savings—and a host of potential security issues that existing "hard-copy world" rules aren't fit to address. The details of top-secret corporate transactions are now hashed out on collaborative virtual platforms that may be vulnerable to damage, destruction, or unauthorized access. And the increasing ubiquity of social media makes it ever more likely that lawyers and clients alike may post information without appreciating the potential legal ramifications. New technologies have the capacity to enrich our personal lives and enhance our professional lives, but they also create complex and novel challenges for lawyers already subject to a web of ethical duties concerning competence and confidentiality.

[75] Given the speed with which this dynamic area is changing, the issues raised in this piece may well feel dated within months of publication as the next new product or service revolutionizes another fundamental aspect of human interaction and connectivity. Nevertheless, in this article we have outlined some of the many challenges facing attorneys operating in a threat-laden high-tech landscape, taken a look at the ways in which existing and emerging ethical rules and guidelines may apply to the practice of law in the digital age, and opened a door to further conversation about all of these issues as they continue to evolve.