ARTICLE: LITIGATION, TECHNOLOGY & ETHICS: TEACHING OLD DOGS NEW TRICKS OR LEGAL LUDDITES ARE NO LONGER WELCOME IN UTAH

May/June, 2015

Reporter
28 Utah Bar J. 12 *

Length: 5860 words

Author: by Randy L. Dryer

RANDY DRYER is a Professor of Law (Lecturer) at the S.J. Quinney College of Law and is Of Counsel to the Salt Lake City based law firm of Parsons Behle & Latimer.

Text

[*12] Technology is growing on an exponential curve and is touching every aspect of our lives. Changes that once took decades or centuries now take years. Even our judicial system, a system based on centuries-old jurisprudence and historically resistant to rapid change, is being impacted. The legal profession, viewed by some as a notoriously technophobic profession, is undergoing significant technological disruption. The litigation process, in particular, has been affected by technological advancement in ways unimaginable ten, or even five, years ago. We now do much of our Rule 11 pre-suit investigation through online search. Personal service of process through social networks is now acceptable in certain circumstances; complaints, exhibits, and other court filings are made electronically; the collection and production of discoverable evidence is aided by computer-assisted review and predictive coding; case-management software is commonplace as disputes involve vast amounts of digital information stored not only on servers, but on mobile devices and remotely in the cloud; case outcome and damage assessments are done by computers using complicated algorithms; jury selection is assisted by real-time social media research and software; and trials feature sophisticated presentation technologies, such as 3D modeling, animation, digital exhibits, and computer-generated simulations and re-creations.

All of these technological advances, of course, have potential ethical implications for the way we lawyers conduct ourselves. In August 2012, the American Bar Association recognized the impact of technology on the practice of law by amending the Model Rules of Professional Conduct after a three-year study by the Commission on ***Ethics*** 20/20. Although only a handful of states have incorporated the changes into their rules, most states are actively studying the Model Rule revisions. For a state-by-state recap of the status of the consideration of the revised Rules, see the link provided in the ABA ***Ethics*** Tip (May 2014), *available at* http://www.americanbar.org/groups/professional_responsibility/services/ethicsearch/ethicstipofthemonthmay2014.html. Numerous commentators have observed how the Model Rule changes, when adopted, will affect lawyers in every area of practice.*See* Daniel J. Siegel, *Lawyers Can No Longer Stick Their Heads in the Sand*, LITIG., Vol. 41, No. 2 (Winter 2015), *available at* http://www.americanbar.org/publications/litigation_journal/2014-15/winter/lawyers_can_no_longer_stick_their_heads_the_sand.html. Most importantly for Utah lawyers is the fact that on March 4, 2015, the Utah Supreme Court adopted all the ABA changes to Rule 1.1 on Competence and Rule 1.6 on Confidentiality of Information. Despite the significance of these changes, there was not a single comment

filed by any Utah lawyer when the proposed rules were posted for comment in October 2014. The changes became effective May 1, 2015, and have far-reaching implications for practitioners.

The bottom line is that being a legal Luddite [1] is no longer acceptable in Utah. The revisions to these two rules make it abundantly clear that ethical practice now requires technological competence. *See* Megan Zavieh, *Luddite Lawyers Are Ethical Violations Waiting to Happen*, LAWYERIST (December 2, 2013) *available at* https://lawyerist.com/71071/luddite-lawyers-ethical-violations-waiting-happen/.

This article reviews the revisions to Rules 1.1 and 1.6 and sounds the warning on the potential ethical issues created by technological advances in four areas -- communicating with clients, electronically **[*13]** stored information, social media, and data management.

RULE OF PROFESSIONAL CONDUCT 1.1

Utah Rule 1.1 is now identical to the ABA Model Rule and addresses the duty of competence that every lawyer owes to a client. That duty of competence now extends to having a working understanding of technology. Rule 1.1 provides: "A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonable necessary for the representation."

Comment 8 to Utah R. Prof'l Conduct 1.1 was amended to make clear that an understanding of technology is an expected duty of every lawyer. Comment 8 provides,

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology*, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. [2]

Model R. Prof'l Conduct 1.1, cmt. 8 (emphasis added). Of course, understanding the risks and benefits of relevant technology necessarily implies that lawyers will keep abreast of new technologies and will understand how they work. Our clients are increasingly technologically competent, and the newly adopted comment requires us to be likewise. As explained in greater detail below, these seemingly simple nine new words have significantly expanded the practical scope of what today's ethical lawyer must understand and confront. *See* Carolyn Fairless, ***Ethics**: Attorney's Duty of Competence with Technology, available at* www.trial.com/cle/materials/2013/fairless.pdf.

RULE OF PROFESSIONAL CONDUCT 1.6

---

[1] The Luddites were 19th Century English artisan workers who protested against the use of machinery in the industrial revolution because technology threatened their jobs. They organized themselves into groups and went on rampages in factories physically destroying machines. They were led by a John Ludd and referred to as "Luddites." *See* http://en.wikipedia.org/wiki/Luddite. The term has since been used to describe people who are incompetent when using new technology.

[2] Although the drafters of the revised Comment 8 noted that the revised comment "does not impose any new obligation on lawyers," they nonetheless believed it important to make explicit that the duty of competence includes the duty to understand technology.

> Lawyers must understand technology in order to provide clients with the competent and cost-effective services that they expect and deserve… Because of the sometimes bewildering pace of technological change, the Commission believes that it is important to make explicit that a lawyer's duty of competence, which requires the lawyer to stay abreast of changes in the law and its practice, includes understanding relevant technology's benefits and risks. Comment [6] of Model Rule 1.1 (Competence) implicitly encompasses that obligation, but *it is important to make this duty explicit because technology is such an integral -- and yet at times invisible -- aspect of contemporary law practice*. The phrase "including the benefits and risks associated with relevant technology" would offer greater clarity regarding this duty and emphasize the growing importance of technology to modern law practice.
>
> ABA Commission on ***Ethics*** 20/20 Report, at 8 (2012) (emphasis added).

Utah Rule 1.6 is also now identical to the ABA Model Rule. It addresses the duty to preserve client information and requires a lawyer to act competently to safeguard against unauthorized access to information and prevent inadvertent disclosure. The rule requires a lawyer to take "reasonable efforts" to prevent unauthorized access to or disclosure of client information. New Comment 18 to the rule was written with technology in mind **[*14]** and gives guidance as to what may constitute reasonable efforts:

> Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

Model R. Prof'l Conduct 1.6, cmt. 18. As discussed in greater detail below, technology has dramatically impacted the practice of law, and we are just beginning to see the interplay between technology and the revised Rules of Professional Conduct.

No Utah ***ethics*** advisory opinions address the ethical issues arising from recent technological advances. [3] As a consequence, Utah lawyers must look to other jurisdictions, which are just beginning to interpret and apply the revised ABA Model Rules or otherwise address the ethical implications of technological change.

Communicating with Clients (New Channels and New Ethical Challenges)

The ways lawyers and clients communicate with one another have changed dramatically since the advent of the Internet. Email remains the predominant communication channel for businesses and lawyer--client communications, although new communication platforms offering text messaging, direct messaging through social networks, VOIP, and video-conferencing are growing in popularity.

The ABA has opined in Formal Opinion 99-413 that encryption is not required when communicating with clients via email, but that opinion was issued in 1999 and is based on an anlysis of obsolete technology. *See* ABA Formal Opinion No. 99-413 (March 10, 1999), *available at* http://cryptome.org/jya/fo99-413.htm. Moreover, 1999 was eons ago as far as technology is concerned. As encryption becomes more and more available in user-friendly formats, the continued reliance on Opinion 99-413 may be misplaced and risky. Model Rule 1.6 imposes a duty upon a lawyer to protect the confidentiality of client information, including communications, and Comment 19 specifically requires a lawyer to take "reasonable precautions to prevent protected communications from coming into the hands of unintended recipients." Model R. Prof'l Conduct 1.6, cmt. 19. Depending on the nature and sensitivity of the information being communicated, encryption may be appropriate and considered reasonable. In 2011, the ABA issued Formal Opinion 11-459 which imposes an ethical duty to warn clients of the privacy and confidentiality risks of communicating through email.*See* ABA Formal Opinion 11-459 (August 4, 2011), *available at* www.americanbar.org/content/dam/aba/administrative/professional_responsibility//11_459_nm_formal_opinion. Although this opinion was in the context of warning employees that employers may lawfully be entitled to access an employee's email sent from a work computer, the underlying rationale extends to non-employer--employee settings. Today, more and more law firms are adopting encryption software for their email communications, and some argue it will soon become a best practice.*See* Albert Barsocchini, *It's Time to Secure Privileged Communications*, **[*15]** LAW TECHNOLOGY NEWS (August 5, 2014), *available at* http://www.legaltechnews.com/home/id=1202665752496?slreturn=20150214182249. The ABA Legal Technology

---

[3] According to the listing of ***ethics*** advisory opinions maintained on the state bar's web site, the last advisory opinion to address Utah's Rule 1.1 was in January of 2008 and dealt with whether an attorney may provide legal assistance to a pro se litigant (Opinion No. 08-01) *available at* http://www.utahbar.org/category/***ethics***-advisory-opinions/1-1-competence/.

Research Center noted, after Model Rules 1.1 and 1.6 were revised, that email encryption clearly reduces the risk of a breach of the duty to preserve the confidentiality of attorney--client communications.

We are also witnessing the emergence of a fledgling industry that offers ephemeral messaging platforms to professionals such as lawyers and accountants. Relatively new services such as Privatext, Confide, Wickr, and TigerText offer varying degrees of encryption, self-deleting functions, and privacy protections. At a minimum, counsel should be aware of these platforms so they may intelligently inquire of a client or prospective client if he or she is using such platforms. Moreover, if a client wishes to communicate with counsel using a more private or secure way than traditional email, the revised rules require a lawyer to do so. It is incumbent on the lawyer to understand how such services work, what protections they actually provide, and what their limitations may be. For example, some encryption services, while protecting the contents of an email, nonetheless leave a trail of metadata as it is routed through a third-party server. Avoiding a metadata trail may or may not be important to a client, but the issue should likely be discussed. Pleading ignorance about the technology is ethically no longer a satisfactory excuse. Although beyond the scope of this article, there is a looming question about whether a lawyer may ethically advise a client to use ephemeral messaging as a way to reduce the amount of discoverable evidence and thus mitigate the high costs of e-discovery.

Encryption is not the only security issue with email. The "reply all" and "blind copy" features of email are potential ways to unintentionally send privileged communications to improper persons. The "autofill" function of most email platforms is also a potentially troublesome feature as a non-attentive lawyer may unintentionally send an email to someone other than the client. The New York Legal ***Ethics*** Reporter in March of this year identified several recommended "best practices" to mitigate the ethical risks of using email. *See* Robert Barrer, *Ethical Implications & Best Practices for Use of Email*, NEW YORK LEGAL ***ETHICS*** REPORTER (March 1, 2015), *available at* http://www.newyorklegalethics.com/ethical-implications-best-practices-for-use-of-email/.

Electronically Stored Information("Where Angels Fear to Tread")

Countless new information systems, social media platforms, and mobile devices are generating electronic data at staggering rates. It is estimated that businesses with 1,000 or more employees produce on average a petabyte of data, or 1.04 million gigabytes, every year. This tsunami of electronic information will only grow larger as the internet of things becomes a reality and billions of internet-connected devices continuously gather information about us and our environment. This deluge of data has changed the very nature of discovery. Not only has it expanded the universe of potential evidence, it also has fundamentally altered the way evidence is collected, reviewed, and produced. Technology assisted review (TAR) of electronically stored information (ESI) is now a practical necessity in many cases due to the large volume of potentially discoverable ESI and the huge cost of manually reviewing the data. Discovery is no longer measured in the number of documents, but in the number of bytes. One particular form of TAR is predictive coding, which is the use of computer algorithms and machine learning to conduct the review of ESI. Predictive coding was initially met with skepticism by lawyers and judges alike, and it was not until 2012 that the first court approved its use. *See* *DaSilva Moore v. Publicis Groupe, 287 F.R.D. 102 (S.D.N.Y. 2012).* Today, it is receiving growing judicial acceptance. See *Rio Tinto, PLC v. Vale S.A., 2015 WL 872294* (S.D.N.Y. March 2, 2015), and cases cited therein. Some have forecast that TAR will become an ethical obligation. Others have warned about the "ethical and malpractice horrors" for any lawyer who outsources his or her duties to **[*16]** machines or non-lawyers. Regardless of one's view about TAR, it cannot rationally be denied that today's discovery landscape has been dramatically altered due to ESI, and technology is playing a role in that new landscape.

The legal and ethical risks associated with the improper preservation, assessment, and production of electronically stored information have never been greater. Today's lawyers must become conversant with a new lexicon -- filtering, deduplication, machine learning, predictive coding, metadata, and seed sets -- and adept at utilizing the related technologies or associating with someone who does. The California State Bar has issued an ***ethics*** opinion that says an attorney lacking the required competence for e-discovery issues in a case must either acquire the necessary expertise, associate with or consult with others who do, or decline the representation. *See* Standing Committee on Professional Responsibility and Conduct Formal Opinion No. 11-0004, *available at* www.calbar.ca.gov/Portals/0ldocuments/publiccomment//2014_11-0004ESI03-21-14.pdf.

Social Media (A Communications Revolution and an Ethical Quagmire)

Every litigator knows how social media has become a goldmine of discovery for impeachment, admissions, and inconsistent statements. During my thirty years as a civil litigator, I increasingly observed the "smoking gun" document being replaced by the smoking gun Facebook post, tweet, or Instagram photo. Ten years ago, the word Facebook or Twitter would never have appeared in a court opinion. Today, there are literally thousands of published opinions where social media is referenced. There are 1.4 billion Facebook accounts in the world and hundreds of other social networks. Enterprise social media platforms (internal Facebook-like platforms used by companies to facilitate communication between employees) are growing in popularity and exponentially expand the volume of discoverable information. Sometimes, even lawyers cannot resist the allure of social media in representing their client and make ill-advised use of social media platforms in advancing their litigation. A Louisiana lawyer was recently recommended for suspension for being complicit with her client in a "social media blitz" aimed at influencing two judges in a child custody case. *See* Debra Cassens Weiss, *Social Media Blitz in Custody Case Yields Possible Suspension for Louisiana Lawyer*, ABA JOURNAL(Feb. 17, 2015), *available at* http://www.abajournal.com/news/article/social_media_blitz_in_custody_case_brings_possible_suspension_for_louisiana.

Lawyers are adopting social media for marketing and other purposes but are just now beginning to think through the potential ethical issues. Much has already been written on the ethical pitfalls when lawyers use social media for professional purposes, and this article does not address this issue. However, lawyers must address numerous ethical issues when clients or opposing parties use social media during litigation. The New Hampshire Bar Association in Opinion 2012-13/05 has noted that lawyers "have a general duty to be aware of social media as a source of potentially useful information in litigation, to be competent to obtain that information directly or through an agent, and to know how to make effective use of that information in litigation." Some state bars are also imposing an ethical duty to advise a client about the potential impact of social media posts on their lawsuit. Another potential issue is whether a lawyer has an ethical duty to investigate a juror's response on *voir dire* or to monitor the public posts of jurors during trial to *see* if jurors are following the court's admonition to not discuss the case until they retire to deliberate. For a listing (as of December 1, 2014) of links to state bar opinions addressing social media ethical concerns, see the Library Guide prepared by the University of Georgia Law School Library, *available at* http://libguides.law.uga.edu/content.php?pid=551040&sid=4540186. Technology in general, and social media in particular, has become such an integral part of our lives that the day is not far off where the failure to "Google" the opposing party or key witness prior to their deposition or the failure to review a client's social media posts and advise them what they may or may not delete, will fall below the standard of care expected of a prudent lawyer and thus constitute legal malpractice.

One of the first things a technologically competent lawyer should do in an initial client interview is dispel several online "myths" that many clients believe.

The first is the great "delete" myth. "Don't worry," says your client, "I deleted that incriminating email, that social media rant, that intimate photo." In cyberspace, there is no such thing as deletion in an absolute sense. A post, even if removed from the site on which it was originally posted, will be cached somewhere, or it will appear on the "Wayback Machine" website. [4] It may still be on the original website's server, or it was automatically uploaded to a cloud account or was downloaded by a third party. A good forensic expert can almost always retrieve or find a deleted piece of online content. Snapchat, the popular app that many teens use for sexting, was recently fined several hundred thousands of dollars by the Federal Trade Commission for false advertising and deceptive business practices for falsely stating that "snaps" disappear and are deleted. Snaps may not be deleted from Snapchat servers, and a recipient may take a screenshot of the photo or message before it is erased from the

---

[4] The Wayback Machine is a digital archive of the World Wide Web and other information on the internet created by the Internet Archive, a non-profit organization based in San Francisco, California. Established in 1996, the non-profit archives cached pages of web pages. The name Wayback Machine is drawn from the animated cartoon series, The Rocky & Bullwinkle Show, where the two main characters, Mr. Peabody and Sherman, used a time machine to witness and participate in famous events in history. *See* Wikipedia, Wayback Machine, *available at* http://en.wikipedia.org/wiki/Wayback_Machine.

recipient's phone. Moreover, there are third-party apps that make it possible to save Snapchat **[*17]** images without the sender knowing and before they disappear. Lawyers need to inform clients that all their social media posts, even those they think have been deleted, are likely discoverable and that you, as a lawyer, have an ethical duty to preserve any evidence that potentially may be relevant to the litigation.

With respect to the ethical discovery and management of information on social networks, there is little guidance in Utah, but the consensus in other states is that a lawyer *can* (a) review any public social network of a witness or party, (b) conduct a Google search of a party, and (c) engage in formal discovery to gain access to private social network accounts and to discover any past social media posts or surreptitious surveillance activities. Most courts will allow access to social media posts by an adverse party upon a showing of potential relevance to the proceeding and that counsel is not simply engaging in a fishing expedition. This is a very low threshold, as virtually everything may have impeachment value. Note, however, that in all jurisdictions that have addressed the issue, an attorney cannot ethically "friend" a witness or opposing party to gain access to non-public account information. For a compilation of materials relating to the ethical issues for lawyers and social media, see Susan Carle, *Materials for Legal* ***Ethics*** *in the Age of Social Media*, American University Washington College of Law, *available at* https://ecf.vid.uscourts.gov/.../Materials_for_Legal_**Ethics**_in_the_Age_.

Every litigator knows he or she has both a legal and an ethical obligation to preserve relevant evidence when litigation is filed or reasonably anticipated. This duty, however, is particularly challenging when it comes to social media because it is often so easily detected. We are seeing more and more cases where sanctions are being imposed on clients and counsel for not taking steps to prevent spoliation of social media posts. The most infamous case involved a wrongful death claim in Virginia where an experienced personal injury lawyer told his client to "clean up" his Facebook page before filing of the complaint. As a result, the client deleted sixteen photographs from his account, including a photo of him shortly after his wife's death while at a party wearing an "I love hot moms" T-shirt with a drink in his hand. The court considered the deletions to constitute spoliation and fined the lawyer $ 542,000 dollars and the client $ 180,000. The lawyer ended up agreeing to a five-year suspension from the practice of law. *See* Patzakis and Murphy, *Facebook spoliation Costs Lawyer $ 522,000; Ends His Legal Career*, eDiscovery blog, (Nov. 11, 2011), *available at* http://blog.x1discovery.com/2011/11/15/facebook-spoliation-costs-lawyer-522000-ends-his-legal-career/.

[*18] Two related questions may arise for the lawyer who is confronted with troublesome social media posted by their client. First, may a lawyer ethically advise a client to change the privacy settings to a more restricted setting so as to remove the social media posts from public view? Second, may a lawyer ethically advise a client to remove certain posts if doing so does not constitute spoliation under the governing substantive law? These are unanswered questions in Utah, but the most recent ***ethics*** opinions elsewhere to address these questions answer both questions in the affirmative with one important caveat, i.e., the lawyer must make an appropriate record of the social media information that is removed. *See, e.g.*, New York County Lawyers Association ***Ethics*** Opinions 745 (2013); North Carolina Formal ***Ethics*** Opinion 5; Florida ***Ethics*** Advisory Opinion 14-1 (Jan. 23, 2015); Pennsylvania Bar Association Opinion 2014-300.

The second online myth is "My privacy settings are limited to my 'friends,' so the opposing party cannot access what I post." Nothing on the internet is truly private regardless of one's privacy settings. Social media may be found on computers, mobile devices, networks, and in the cloud. For example, depending on one's settings, photos taken on your mobile phone may automatically be synched to a cloud account and may remain there even if deleted from the device. Some celebrities recently found out how secure the cloud is when their explicit photos were hacked and posted on the internet.

The third online myth has to do with anonymity and ephemeral messaging. Interest in ephemeral messaging apps and services has grown in light of the revelations that the NSA has been monitoring the electronic communications of tens of millions of Americans without their knowledge. Despite their promises of deletion and anonymity, there are too many ways that ephemeral messaging may be retrieved or reconstructed. Moreover, if your client sends an ephemeral message to someone, the contents of the information is still discoverable the old fashioned way by questioning the sender and the recipient in a deposition.

Data Management(A New Frontier Fraught with Ethical Risk)

The year 2014 has been called the "Year of the Data Breach," and data security has been deemed one of the major risks for law firms. *See generally* ABA Cybersecurity Legal Task Force Report, *available at* http://mntech.typepad.com/msba/2013/10/aba-cybersecurity-legal-task-force-issues-report-and-resolution-118.html. Indeed, many large corporations are insisting that their outside law firms implement specific safeguards to protect data. Some financial institutions are requiring outside counsel to answer lengthy questionnaires about their firm's cybersecurity measures, while others are doing on-site inspections. The professional liability insurance industry now offers cyberinsurance to protect against data breaches, and law firms would be well advised to consider adding it to their standard malpractice coverages. The potential legal liability and reputational damage when a law firm mishandles client information is obvious and often catastrophic. In light of the revisions to Model Rules 1.1 and 1.6, lawyers should now add potential ethical discipline to the list of risks flowing from a data breach.

The ethical issues (and potential legal liability) surrounding data management may arise in countless ways but usually occur in one of the following four situations: (1) information stored in the cloud; (2) the disclosure or receipt of metadata; (3) the negligent or unintentional release of client information; or (4) a data breach by outside parties.

Cloud storage: Storage of files in remote online servers is becoming increasingly common in the business world due to its low cost, ease of use, and flexibility. Lawyers, however, have been hesitant to embrace cloud storage due to concerns about its acceptability under applicable ***ethics*** rules. A 2014 ABA survey showed that only 30% of lawyers responding reported they used cloud-based services in their practice with one-fourth **[*19]** noting a lack of ethical guidance as a reason. Fewer than half of the state bars have issued ***ethics*** opinions addressing cloud services (Utah is not one of them), but all have held that they are ethically permissible if the lawyer/vendor takes reasonable precautions to ensure that client data is protected. Importantly, many opinions impose a duty on the lawyer to exercise due diligence in selecting a cloud service provider. Each state reflects slightly different views on what constitutes reasonable precautions. Some states impose a generally worded duty to ensure client data is secure and accessible (*e.g.*, Vermont), while others list specific safeguards that should be considered (*e.g.*, Pennsylvania, which identifies fifteen possible safeguards). For a listing and a link to each state's opinions, see the chart and accompanying analysis prepared and posted by the ABA Legal Technology Resource Center, *available at* http://www.lawtechnologytoday. org/2014/05/cloud-***ethics***-opinion-chart-updated/. Given the dramatic rise in the number of data breaches involving the cloud over the past few years, a prudent practitioner would be wise to monitor this area closely and obtain consent from a client or at least give notice of the use of cloud services in a retainer agreement, particularly if the client is sensitive.

Because of the growing number of cloud providers, industry trade groups have developed prescriptive guidelines and best practices on how to prevent and remediate the risk and impact of data breaches. In February 2015, the Online Trust Alliance issued a "Data Protection and Breach Readiness Guide," which, among other things, identifies twelve questions to ask a cloud service provider before entrusting your data to them. The guide is available at https://otalliance.org.

Given the new obligations imposed by Rules 1.1 and 1.6, it would be ethically risky for lawyers to not conduct reasonable due diligence before engaging a cloud service provider.

Disclosure or receipt of metadata. The ethical dangers in this area are numerous, and what ethical duties exist depend on the jurisdiction. The ABA has not issued any ethical opinion imposing a duty on lawyers to strip documents of metadata, but several states require reasonable care to be taken to avoid transmitting metadata. As one commentator recently noted, "metadata is the smoking gun in court, and e-discovery is the ballistics test that uncovers it." Shelley Powers, *Don't Mess with One of the E-Discovery Triumvirate* (Feb. 11, 2014), *available at* http://burningbird.net/dont-mess-one-e-discovery-triumvirate. Widely available software can scrub metadata, and every lawyer should consider utilizing this software to avoid potential ethical problems. The ABA has issued an opinion regarding lawyer receipt of metadata. Formal Opinion 06-442 holds that there is no ethical prohibition against lawyers mining the metadata of documents they receive, even from opposing counsel.*See* ABA Formal Opinion 06-442, Aug. 5, 2006, *available at* www.americanbar.org/.../aba/.../YourABA/06_442.authcheckdam.pdf.

This position has been criticized, however, and a majority of state bars have taken the contrary position that metadata is confidential information and cannot be mined. For a listing of states that have addressed the ethical issues of metadata, see the chart and accompanying opinion links prepared by the ABA Legal Technology Resource Center,*available at* http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html. Utah has issued no ethnical opinions in this area.

Unintentional release of data. One of the greatest risks of data breaches comes not from malicious outside hackers, but from the inadvertent disclosure or loss due to internal lax controls. The increased prevalence of lawyers and other staff using personal devices to practice law and the widespread use of flash drives and other portable storage devices dramatically raises the likelihood of an unintentional breach. There are numerous examples of lawyers losing laptops or flash drives containing client information. Everyone knows you need to take care to delete information from old computers and tablets, but **[*20]** many copy machines and printers have hard drives that capture the data copied. Proper disposal of any device that stores data is essential to protecting client and other confidential information. Regular employee training on the importance of data protection is essential, and many clients are requiring their lawyers to have acceptable data protection safeguards in place. Where lawyers use personal devices in their practice, having a BYOD (Bring Your Own Device) policy with appropriate data protection provisions is of vital importance.

Data breach by outside parties. Law firms reportedly have become ripe targets for hackers and thieves since many firms handle sensitive client information but do not employ the same level of cyber security their clients do. *See* Andrew Conte, *Unprepared Law Firms Vulnerable to Hackers*, TribLive News (Sept. 13, 2014), *available at* http://triblive.com/news/allegheny/6721544-74/law-firms-information#axzz3T5U5g3W4. In 2012, Bloomberg News reported that Chinese-based hackers deliberately targeted specific Canadian firms in Toronto to seek confidential business information. In 2014, federal prosecutors charged Chinese military hackers with stealing attorney-client communications from SolarWorld, an Oregon-based solar panel manufacturer. In January of this year, a California-based personal injury firm reported the theft of a laptop computer with personal identifying client information. Security experts report there is a lively trade in stolen legal data, and 14% of lawyers responding to a recent ABA survey experienced a data theft or breach in 2014.

In sum, sound data management is arguably an ethical obligation in light of the revisions to Rules 1.1 and 1.6. These revisions dictate that lawyers (a) make appropriate disclosures to their clients about their use of technology; (b) obtain consent to use that technology; (c) make sure vendor and expert contracts include provisions for security and confidentiality; (d) exercise due diligence in selecting any vendor of cloud services; (e) implement appropriate employee training on security to guard against unintentional data loss; and (f) develop a comprehensive security and data breach plan. The online Trust Alliance recently completed a review of more than 1,000 data breaches from 2014 and concluded that more than 90% of them could have been avoided. *See 2015 Data Protection & Breach Readiness Guide*, Online Trust Alliance (Feb. 13, 2015), *available at* https://otalliance.org/news-events/press-releases/online-trust-alliance-releases-2015-data-protection-breach-readiness.

CONCLUSION

Substantive law often lags behind technology and the updating of legal ethical standards is no different. However, on May 1, 2015, the gap between technology and ***ethics*** in Utah was dramatically reduced. Utah lawyers must now accept the new digital reality in which they practice and, if not welcome technology with open arms, at least understand how technology has irretrievably impacted the practice of law. Legal Luddites are soon to become a dying breed.

End of Document