From Technophobe to Technolawyer: A Lawyer's Duties Related to Technology Competence and Prevention of Inadvertent Disclosure

By Heather L. LaVigne
Assistant Bar Counsel
March 2018

Introduction

While many lawyers' chosen profession was born of an aptitude for law over science, there is no hiding from technology in a society that is becoming increasingly paperless. Many lawyers have adopted new technologies to save time, money, and headaches. Other lawyers endeavor to stay relevant as the new millennium ushers in a workforce of increasingly tech-savvy individuals who demand tech-savvy legal representation.

Many courts and administrative agencies use electronic filing and communication methods, requiring lawyers to have some facility with technology. For litigators, gone are the days when discovery consisted primarily of collecting boxes full of dusty pages that a lawyer could see, touch, and even smell. In addition to houses and jewelry, estate lawyers must now contend with their client's digital assets which may be stored on physical devices or the internet.

For all lawyers, the documents and information necessary to carry out one's legal work exist in an intangible, digital space that cannot be navigated or even found without an understanding of modern technology. The ubiquity of technology in all aspects of modern society, therefore, gives rise to an expectation that all lawyers, in all practice areas, will encounter the mysteries of the internet, metadata, and the emergence of what has been fittingly named "the cloud," because it is over most of our heads. Regardless of whether one welcomes these changes, lawyers have an ethical duty to keep up.

Effective July 1, 2015, the Supreme Judicial Court amended the Massachusetts Rules of Professional Conduct by adding a new Comment 8 to Mass R. Prof C. 1.1. This comment states,

> 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, and engage in continuing study and education.

This addition brought Rule 1.1 current, in relevant part, with the ABA Model Rules of Professional Conduct as amended in 2012. While Comment 8 emphasizes the increasing role of technology in the practice of law, Rule 1.1.'s broad mandate that lawyers provide competent representation to their clients always included technology competence. Indeed, prior to the adoption of Comment 8, the Board of Bar Overseers issued a public reprimand, in part because the lawyer handled an electronic discovery matter he was not competent to handle without appropriate research or consultation with experienced counsel. *In Re Reisman*, 29 Mass. Att'y Disc. R. 556 (2013). Prior to that, the Board issued a public reprimand, in part because the lawyer lacked diligence in preserving a client file on his laptop and lost all the data. *In Re Doyle*, 26 Mass. Att'y Disc. R. 143 (2010).

Competence

So, what does a lawyer have to do to be considered competent in technology? As with many legal questions, the answer is: it depends. Rule 1.1 defines competent representation to include the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

At a minimum, lawyers should take care to learn and understand the technology they use, such as computers, mobile devices, operating systems, and software applications. Lawyers must ensure that their use of such technology is compatible with their professional obligations including maintaining confidentiality pursuant to Rule 1.6, safekeeping of trust property pursuant

to Rule 1.15, and supervising lawyer and non-lawyer assistants pursuant to Rules 5.1 and 5.3. Lawyers must also be aware of and in compliance with data privacy and other relevant laws. For example, lawyers who are owners of personal information as defined by the Massachusetts Data Privacy Act must have a comprehensive written information security program or ("WISP"). See G.L. c. 93H; 201 C.M.R. 17 *et seq*.

With respect to electronic discovery, it is likely that all litigators will encounter some electronically stored information, or "ESI," in their practice. As noted in Comment 2 to Rule 1.1, "Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve." Accordingly, litigators must have the ability to assess the potential electronic discovery needs of their cases and evaluate their own competence to handle those issues.

Further, all litigators should understand the electronic discovery rules in relevant jurisdictions. The United States Supreme Court first introduced comprehensive procedural rules relating to electronic discovery in 2006. The SJC did so in 2014. As time progresses, technology, the rules, and case law develop and change. Comment 8 recognizes the evolving nature of both technology itself and the law related to technology. A lawyer's duty of competence includes keeping up with changes in both areas.

Electronic discovery procedural rules can provide litigators with more specific guidance on the scope of competence required. For example, litigators in Massachusetts should be competent to participate in an ESI conference. Pursuant to Mass. R. Civ. P. Rule 26, an ESI conference must include discussing preservation of discoverable evidence; time frames for production, format of production, costs of production; metadata production; and issues relating to privileged, confidential, and proprietary information. Even non-litigators must have familiarity with electronic discovery as in-house counsel are often tasked with advising their clients on

document retention policies, issuing litigation holds, monitoring and enforcing the hold, and assisting outside counsel with the collection of ESI for review and production.

All lawyers should also consider whether competent and diligent representation imposes additional duties upon them to use technology. For example, many courts have found fault with lawyers who failed to perform internet searches, giving rise to the phrase "duty to Google." Missouri requires that attorneys search potential jurors' litigation history prior to empanelment. Mo. Sup. Ct. R. 69.025. In other instances, courts have found fault with attorneys who failed to use the internet to locate people to effect service. See e.g., *DuBois v. Butler*, 901 So.2d 1029 (Fla. Dist. Ct. App. 2005); *Munster v. Groce*, 829 N.E.2d 52 (Ind. Ct. App. 2005). Diligent representation might require attorneys to consider whether evidence exists on a client's Facebook page or on the Facebook page of an opposing party or a witness, to the extent that those pages are public. A lawyer may identify new witnesses by following up on social media posts relating to the underlying matter. Lawyers should therefore consider using social media and internet search engines to gather public information in order to zealously represent their clients.[1]

The requirement of technology competence also intersects with a lawyer's duty to safeguard money held in trust pursuant to Mass. R. Prof. C. 1.15. Lawyers should therefore be aware of common email and wire fraud scams that can result in a lawyer releasing client money to the wrong recipients. Lawyers must take precautions to ensure that wired or electronically transferred funds are only provided to the intended recipient.[2] Some states have issued formal opinions and even disciplined lawyers who fell victim to these scams. See, e.g., *Iowa Attorney*

[1] For a comprehensive discussion on the use of social media and the "duty to Google," see John G. Browning, *Keep Your "Friends" Close and Your Enemies Closer: Walking the Ethical Tightrope in the Use of Social Media*, available at http://www.stmaryslawjournal.org/pdfs/Browning_final.pdf and ABA Formal Opinion 466, *Lawyer Reviewing Jurors' Internet Presence* (April 24, 2014).

[2] For more information, see, for example, a discussion of scams targeting real estate lawyers involving compromised wire instructions. *Real Estate Bar Association Blog* available at http://rebama.blogspot.com/2016/09/alarming-scams-targeting-real-estate.html.

Disciplinary Bd. v. Wright, 840 N.W.2d (295 (2013) (one-year suspension in part because the lawyer failed to verify the identities of people requesting disbursement of funds); NYC Bar Formal Opinion 2015-3 (describing the duties of a lawyer who suspects he or she is the target of a scam).

As with competence in other areas, lawyers may develop competence in technology through necessary study or association with a lawyer who has established competence. Many lawyers and law firms also choose to hire or contract with non-lawyer technology and electronic discovery specialists. As noted above, lawyers who do so must keep in mind their obligations under Rules 1.6, 5.1, and 5.3 to ensure that internal and external non-lawyer assistants carry out their duties in a manner that is compatible with the lawyer's professional obligations. While lawyers can and should align themselves with experts, Rule 1.1 makes clear that lawyers cannot simply delegate or outsource technology competence.

Confidentiality

Just as lawyers must take precautions to protect confidential information in tangible paper documents, lawyers must protect the intangible, electronically stored information in their possession. Effective July 1, 2015, the SJC added a new subsection (c) to Mass. R. Prof. C. 1.6 to address this issue. Rule 1.6(c) states,

> A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, confidential information relating to the representation of a client.

This addition brought Rule 1.6(c) current, in relevant part, with the ABA Model Rule 1.6(c), amended in 2012.

As noted in Comment 18, Rule 1.6(c) not only requires lawyers to act competently to safeguard confidential information against their own inadvertent disclosures and those of others

participating in the representation, it also requires lawyers to act competently to safeguard confidential information against unauthorized access by third parties. Lawyers who make reasonable efforts to prevent the access or disclosure, however, will not be found in violation of Rule 1.6(c).[3] 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.

Comment 19 to Rule 1.6 requires a lawyer to take reasonable precautions to prevent confidential information from coming into the hands of unintended recipients when transmitting a communication that includes confidential information relating to the representation of a client. Lawyers using a method of communication that affords a reasonable expectation of privacy are not required to take special security measures. Comment 19 makes clear, however, that lawyers must assess whether circumstances warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement.

While using the internet to transmit and store ESI is not incompatible with Rule 1.6, lawyers must understand the risks of doing so and implement appropriate security measures. See also ABA Formal Opinion 477, *Securing Communication of Protected Client Information* (May 11, 2017); Massachusetts Bar Association Ethics Opinion Nos. 00-1 and 12-03. As noted in

[3] For discussion of what to do if you are on the receiving end of an inadvertent disclosure, see *Inadvertent Disclosure: When Your Opponent Has Let the Cat Out off the Bag,* by Assistant Bar Counsel Richard C. Abati, April 2016.

ABA Formal Opinion 477, the reasonableness of a lawyer's efforts to protect electronically stored or transmitted confidential information is a fact-specific inquiry. Lawyers must therefore consider whether special precautions, such as encryption or other available precautions, are required when transmitting highly sensitive information (e.g. financial and medical records) and information protected by privacy laws. Further, lawyers should abide by a client's instruction to not use internet-based storage and communication methods or inform the client that complying with such an instruction is not possible.

In addition to the comments to Rule 1.6(c), lawyers may look to relevant data privacy laws for guidance on protecting the security and confidentiality of electronic information. For example, 201 C.M.R. 17.03 outlines the elements of a WISP. It delineates important measures for limiting security risks to personal information including ongoing employee training, employee compliance with policies and procedures, and maintaining a means for detecting and preventing security system failures. Additionally, 201 C.M.R. 17.04 outlines several elements necessary for an effective computer security system such as secure user authentication protocols, secure user access control measures, encryption and firewall protection in certain circumstances, up-to-date security software, system monitoring, and employee training.

In addition to email and cloud storage, lawyers are increasingly using a variety of technologies in their practice. While it is beyond the scope of this article to address each type of technology a lawyer might use, lawyers must understand the risks and make decisions about whether their use of these tools is compatible with their professional obligations.[4] For example, lawyers should not simply download a messaging app to connect with clients without first

[4] Stay tuned for future articles about technology including common pitfalls relating to the use of email, social media, and scams.

vetting the program and determining whether it is appropriate. Similarly, while it is nice to work on your cases while sipping a latte in your favorite coffee shop, lawyers should understand the risk of interception when using unsecured public wi-fi. Similarly, lawyers should take care to ensure that if they provide wi-fi to their guests, they do so separately from the network they use for their case work.

Conclusion

The amendments to Mass. R. Prof. C. 1.1 and 1.6(c) make clear that lawyers have a duty to be competent in technology and ensure the security of electronically stored information. At a minimum, these obligations include: assessing the need for electronic discovery and technologies like social media in handling one's cases, supervising lawyer and non-lawyer assistants including providing education and training, understanding the risks of the technology in use, implementing reasonable security measures, taking reasonable efforts to prevent inadvertent disclosures of confidential information, and safeguarding money held in trust. Lawyers cannot claim ignorance of complex technology and must endeavor to keep up.

The Massachusetts Law Office Management Assistance Program (LOMAP), a program of Lawyers Concerned for Lawyers, is an excellent place to start.[5] LOMAP can help provide the operational and educational support you may need to bring your practice into the new millennium and meet your ethical obligations while doing so. Publications and legal education opportunities are also available through Massachusetts legal education organizations and bar associations. If you have not made the transition from technophobe to technolawyer, now is the time!

[5] www.masslomap.org; http://www.lclma.org