The Twenty-First Century Lawyer's Evolving Ethical Duty of Competence

By Andrew Perlman

Andrew Perlman is a professor at Suffolk University Law School, where he is the Director of the Institute on Law Practice Technology and Innovation. He was the Chief Reporter of the ABA Commission on Ethics 20/20 and is the Vice Chair of the newly created ABA Commission on the Future of Legal Services. This article contains the author's own opinions and does not reflect the views of any ABA entity or any other organization with which he is or has been affiliated.

Just twenty years ago, lawyers were not expected to know how to protect confidential information from cybersecurity threats, use the Internet for marketing and investigations, employ cloud-based services to manage a practice and interact with clients, implement automated document assembly and expert systems to reduce costs, or engage in electronic discovery. Today, these skills are increasingly essential, and many lawyers want to know whether they are adapting quickly enough to satisfy their ethical duty of competence. This short article describes several relevant recent changes to the Model Rules of Professional Conduct and identifies new skills and knowledge that lawyers should have or develop.

The Duty of Competence in a Digital Age

The ABA Commission on Ethics 20/20 was created in 2009 to study how the Model Rules of Professional Conduct should be updated in light of globalization and changes in technology. The resulting amendments addressed (among other subjects) a lawyer's duty of confidentiality in a digital age, numerous issues related to the use of Internet-based client development tools, the ethics of outsourcing, the facilitation of jurisdictional mobility for both US and foreign lawyers, and the scope of the duty of confidentiality when changing firms.

One overarching theme of the Commission's work was that twenty-first century lawyers have a heightened duty to keep up with technology. An amendment to Model Rule 1.1 (Duty of Competence), Comment [8] captured the new reality (italicized language is new):

> 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.

The Model Rules had not previously mentioned technology, and the Commission concluded that the Rules should reflect technology's growing importance to the delivery of legal and law-related services.

New Competencies for the Twenty-First Century Lawyer

The advice to keep abreast of relevant technology is vague, and the Commission intended for it to be so. The Commission understood that a competent lawyer's skillset needs to evolve along with technology itself. After all, given the pace of change in the last twenty years, the specific skills lawyers will need in the decades ahead are difficult to imagine.[1] In the meantime, a few new competencies appear to be critical.

Cybersecurity

Long gone are the days when lawyers could satisfy their duty of confidentiality by placing client documents in a locked file cabinet behind a locked office door. Lawyers now store a range of information in the "cloud" (both private and public) as well as on the "ground," using smartphones, laptops, tablets, and flash drives. This information is easily lost or stolen; it can be accessed without authority (e.g., through hacking); it can be inadvertently sent; it can be intercepted while in transit; and it can even be accessed without permission by foreign governments or the National Security Agency.[2]

In light of these dangers, lawyers need to understand how to competently safeguard confidential information. Newly adopted Model Rule 1.6(c) requires lawyers to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." New comments advise lawyers to examine a number of factors when determining whether their efforts are "reasonable," including (but 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)."

The particular safeguards lawyers need to use will necessarily change with time. For now, and at a minimum, competent lawyers need to understand the importance of strong passwords (lengthy passwords that contain a mix of letters, numbers, and special characters; the word "password," for example, is a lousy password), encryption (both for information stored in the "cloud" and on the "ground," such as on flash drives and laptops), and multifactor authentication (ensuring that data can be accessed only if the lawyer has the correct password as well as another form of identification, such as a code sent by text message to the lawyer's mobile phone). Lawyers also need to understand what metadata is and how to get rid of it, how to avoid phishing scams, the dangers of using public computers and Wi-Fi connections (including cloning and twinning of public Wi-Fi networks), the risks of using file sharing sites, and how to protect devices against malware.

Law firms with internal networks (also sometimes referred to as private clouds) should consult with competent data security experts to safeguard the information, and law firms that outsource these services (i.e., use a public cloud to store client data) need to ensure they select a service that uses appropriate security protocols. Recent changes to Rule 5.3, Comment [3] offer additional guidance on these issues, as do numerous ethics opinions related to cloud computing.[3] A growing body of federal and state law also governs the area.

In sum, basic knowledge of cybersecurity has become an essential lawyer competency. Although lawyers cannot guard against every conceivable cybersecurity threat, they must take reasonable precautions. Failing to do so threatens the confidentiality of clients' information and puts lawyers at a heightened risk of discipline or malpractice claims.

Electronic Discovery

A sound grasp of e-discovery has become a necessity, especially for litigators, and lawyers face discipline and sanctions if they do not understand the basics of electronically stored information (ESI) or fail to collaborate with those who do. For example, a Massachusetts lawyer was recently disciplined for failing to take appropriate steps to prevent a client's spoliation of ESI.[4] In addition to violating Rule 1.4 (for failing to communicate to his client the nature of the discovery obligations) and Rule 3.4 (for unlawfully obstructing access to evidence), the lawyer was found to have violated Rule 1.1 because he represented a client on "a matter that he was not competent to handle without adequate research or associating with or conferring with experienced counsel, and without any attempt to confirm the nature and content of the proposed deletions [of electronically stored information by the client]."[5]

In New York, e-discovery competence is now mandated in section 202.12(b) of the Uniform Rules for the Supreme and County Courts:

> Where a case is reasonably likely to include electronic discovery, counsel shall, prior to the preliminary conference, confer with regard to any anticipated electronic discovery issues. Further, counsel for all parties who appear at the preliminary conference must be sufficiently versed in matters relating to their clients' technological systems to discuss competently all issues relating to electronic discovery: counsel may bring a client representative or outside expert to assist in such e-discovery discussions.[6]

In California, a recently released draft of an ethics opinion covers similar ground and once again emphasizes the importance of e-discovery competence:

> Attorney competence related to litigation generally requires, at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, i.e., the discovery of electronically stored information ("ESI"). On a case-by-case basis, the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a given matter and the nature of the ESI involved. Such competency requirements may render an otherwise highly experienced attorney not competent to handle certain litigation matters involving ESI.[7]

Competence is not the only ethical duty at stake. The California draft opinion (like the Massachusetts disciplinary case) observes that the improper handling of e-discovery "can also result, in certain circumstances, in ethical violations of an attorney's duty of confidentiality, the duty of candor, and/or the ethical duty not to suppress evidence."[8] The opinion concludes that, if lawyers want to handle matters involving e-discovery and do not have the requisite competence to do so, they can either "(1) acquire sufficient learning and skill before performance is required; [or] (2) associate with or consult technical consultants or competent counsel. . . ." [9]

Related issues arise when lawyers advise their clients about social media content that might be discoverable. Recent opinions suggest that lawyers must competently advise clients about this content, such as whether they can change their privacy settings or remove posts, while avoiding any advice that might result in the spoliation of evidence.[10] The bottom line is that e-discovery is a new and increasingly essential competency, and unless litigators understand it or associate with those who do, they risk court sanctions and discipline.

Internet-Based Investigations

Lawyers no longer need to rely exclusively on private investigators to uncover a wealth of factual information about a legal matter. Lawyers can learn a great deal from simple Internet searches.

Lawyers ignore this competency at their peril. Consider an Iowa lawyer whose client received an email from Nigeria, informing him that he stood to inherit nearly $19 million from a distant Nigerian relative by paying $177,660 in taxes owed to the Nigerian government. The client's gullible lawyer raised the "tax" money from other clients in exchange for a promise to give them a cut of the inheritance. Unsurprisingly, the "inheritance" was a well-known scam, and the lawyer's clients lost their money. The lawyer was disciplined for subjecting his clients to the fraud and was expressly criticized for failing to conduct a "cursory internet search" that would have uncovered the truth.[11]

Internet research is also essential in more routine settings. For example, the Missouri Supreme Court recently held that lawyers should use "reasonable efforts," including Internet-based tools, to uncover the litigation history of jurors prior to trial in order to preserve possible objections to the empanelment of those jurors.[12] In Maryland, a court favorably cited a passage from a law review article that asserted that "[i]t should now be a matter of professional competence for attorneys to take the time to investigate social networking sites."[13] Other cases have emphasized the importance of using simple Internet searches to find missing witnesses and parties. Simply put, lawyers cannot just stick their heads in the sand when it comes to Internet investigations.

At the same time, lawyers need to be aware of the ethics issues involved with these kinds of investigations, especially when researching opposing parties, witnesses, and jurors. If the information is publicly available, these investigations raise few concerns. But when lawyers want to view information that requires a request for access, such as by "friending" the target of the investigation, a number of potential ethics issues arise under Model Rules 4.1, 4.2, and 4.3. A rapidly growing body of ethics opinions addresses these issues, including a recent ABA Formal Opinion.[14]

Internet-Based Marketing

A growing number of lawyers use Internet-based marketing, such as social media (e.g., blogs, Facebook, Twitter, and LinkedIn), pay-per-lead services (paying a third party for each new client lead generated), and pay-per-click tools (e.g., paying Google for clicks taking Internet users to the law firm's website). Given the increasing prevalence of these tools, lawyers need to understand how to use them properly.

A recent Indiana disciplinary matter illustrates one potential risk. A lawyer with over 40 years of experience and no disciplinary record received a private reprimand for using a pay-per-lead service whose advertisements failed to comply with the Indiana Rules of Professional Conduct. The Indiana Supreme Court concluded that the lawyer should have known about the improper marketing methods and stopped using the company's services.[15] The takeaway message is that lawyers need to understand how these new marketing arrangements operate and cannot ignore how client leads are generated on their behalf.

Even when lawyers take control of their own online marketing, they need to tread carefully. Potential issues include the inadvertent creation of an attorney-client relationship under Rule 1.18, the unauthorized practice of law under Rule 5.5 (when the marketing attracts clients in states where the lawyer is not licensed), and allegations of improper solicitation under Rule 7.3. (Newly adopted comments in Rules 1.18 and 7.3 can help lawyers navigate some of these issues.)

Leveraging New and Established Legal Technology/Innovation

Technological competence is not just a disciplinary or malpractice concern. It is becoming essential in a marketplace where clients handle more of their own legal work and use non-traditional legal service providers (i.e., providers other than law firms). To compete, lawyers need to learn how to leverage "New Law" – technology and other innovations that facilitate the delivery of legal services in entirely new ways. Lawyers are also being pressed to make better use of well-established technologies, such as word processing.

Examples of "New Law" include automated document assembly, expert systems (e.g., automated processes that generate legal conclusions after users answer a series of branching questions), knowledge management (e.g., tools that enable lawyers to find information efficiently within a lawyer's own firm, such as by locating a pre-existing document addressing a legal issue or identifying a lawyer who is already expert in the subject), legal analytics (e.g., using "big data" to help forecast the outcome of cases and determine their settlement value), virtual legal services, and cloud-based law practice management. These kinds of tools can be identified and implemented effectively through the sound application of legal project management and process improvement techniques (which reflect another set of important new competencies). Lawyers are not ethically required to use these tools and skills, at least not yet. But if lawyers want to remain competitive in a rapidly changing marketplace, these competencies are quickly becoming essential.

Clients also have less patience with lawyers who fail to use well-established legal technology appropriately.[16] For instance, a corporate counsel at Kia Motors America (Casey Flaherty) has conducted "technology audits" of outside law firms to ensure they make efficient and effective use of available tools, such as word processing and spreadsheets. He has found they do not. On average, tasks that lawyers should have been able to perform in an hour took them five. (Casey Flaherty has partnered with my law school to automate the audit so that it can be used widely throughout the legal industry. I am working closely with Casey on the project.) Lawyers who fail to develop (or maintain) competence when using these established technologies risk alienating both existing and potential clients.

Conclusion

The seemingly minor change to a Comment to Rule 1.1 captures an important shift in thinking about competent twenty-first century lawyering. Technology is playing an ever more important role, and lawyers who fail to keep abreast of new developments face a heightened risk of discipline or malpractice as well as formidable new challenges in an increasingly crowded and competitive legal marketplace.

Endnotes

1. *See generally*RICHARD SUSSKIND, TOMORROW'S LAWYERS: AN INTRODUCTION TO YOUR FUTURE (2013).
2. 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.
3. *See, e.g.*, *Cloud Ethics Opinions Around the U.S.*, A.B.A., http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (last visited Oct. 6, 2014).
4. Kenneth Paul Reisman, Public Reprimand, No. 2013-21, 2013 WL 5967131 (Mass. B. Disp. Bd. Oct. 9, 2013).
5. *Id*. at *2.
6. N.Y. UNIF. R. TRIAL CT. §202.12(b), *available at*http://www.nycourts.gov/rules/trialcourts/202.shtml#12 (last visited Oct. 7, 2014).
7. State Bar of Cal. Standing Comm. on Prof'l Responsibility & Conduct, Formal Op. 11-0004 (2014).
8. *Id.*
9. *Id.*
10. NYCLA Comm. on Prof'l Ethics, Formal Op. 745 (2013); Phila. Bar Ass'n Prof'l Guidance Comm., Formal Op. 2014-5 (2014).
11. Iowa Supreme Court Att'y Disciplinary Bd. v. Wright, 840 N.W.2d 295, 301-04 (Iowa 2013).
12. Johnson v. McCullough, 306 S.W.3d 551, 558-59 (Mo. 2010).
13. Griffin v. Maryland, 995 A.2d 791, 801 (Md. Ct. Spec. App. 2010) (quoting Sharon Nelson et al., *The Legal Implications of Social Networking*, 22 REGENT U. L. REV. 1, 13 (2009-2010)), *rev'd on other grounds*, Griffin v. State, 419 Md. 343 (Md. 2011).
14. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 466 (2014).
15. *In re* Anonymous, 6 N.E.3d 903, 907 (Ind. 2014).
16. Casey Flaherty, *Could You Pass This In-House Counsel's Tech Test? If the Answer Is No, You May Be Losing Business*, A.B.A. J. (Jun. 17, 2013, 1:30 PM), http://www.abajournal.com/legalrebels/article/could_you_pass_this_in-house_counsels_tech_test.