TECHNOLOGY FOR LAWYERS: WHAT'S NEW? WHAT'S HOT? WHAT IS MY ETHICAL DUTY AND WHAT DO I NEED TO KNOW?

Sponsor: Young Lawyers Division
CLE Credit: 1.0 ethics
Thursday, June 22, 2017
12:00 noon - 1:00 p.m.
West Ballroom C-D
Owensboro Convention Center
Owensboro, Kentucky
A NOTE CONCERNING THE PROGRAM MATERIALS

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

The Presenter ................................................................................................................................. i


Ethics Opinion KBA E-437: Use of Cloud Computing ............................................................ 15
STEPHEN E. EMBRY is a member of Frost Brown Todd, LLC and is a member of the firm’s Class Action, Privacy and Mass Tort groups. He is also a member of fbtTECH, the firm’s technology industry group that focuses on the future and anticipating the ways in which technology will impact the legal system and the issues facing clients. Mr. Embry is a member of the American Bar Association’s Law Practice Division, Vice Chair of the ABA Law Technology Resource Center, member of the Editorial Board of the Law Practice Division’s Law Practice Today publication and member of the Kentucky Bar Association Law Practice Task Force. He is also Chair of the Data Breach, Privacy and Cyber Insurance Section of the Federation of Defense and Corporate Counsel (FDCC) and a member of the ABA Science and Technology Committee, sub committees: Internet of Things, Discovery and Digital Evidence and E-Privacy Law. Mr. Embry writes frequently on issues of technology and its impact on the practice of law and was recently a co-author of the ABA TechReport 2016. He received both his B.A. and J.D. from the University of Kentucky and is a member of the Louisville, Kentucky, West Virginia, and American Bar Associations.
I. INTRODUCTION

Much has been written about the need for lawyers to have at least core competency in technology. While many lawyers prefer to adopt the ostrich approach and stick their heads in the proverbial sand ("I have people that know about that. I don't need to know anything."), such an approach is likely to lead to trouble and may not satisfy ethical obligations.

Like it or not, technology is a part of our everyday practice. Email. E-discovery. The cloud. Practice management. Social media and discovery, and its use and impact on such things as jury selection. The dangers that some forms of technologies and their use pose for our duty to maintain confidences. The list goes on and on.

Technology plays an ever-expanding role in our daily life and practice, and we have to be able to at least spot issues. One must only consider the recent hack\(^1\) at a Panamanian law firm to see there are significant threats to clients' privacy and confidences on an ongoing basis.

And like it or not, our clients and the public more and more expect and demand some knowledge of technology risks and benefits from their lawyers. Failure to be knowledgeable enough to at least see issues and pitfalls and adequately supervise projects and cases where technology is being used or is an issue could lead to some unwelcome results and frustrations.

And finally, perhaps to state the obvious given the above, fundamental technological proficiency is something you likely owe your client generally, morally and ethically. Technology issues are so ingrained in everything we all do that in most matters they just can’t be completely delegated to others. It’s a matter of competence, protecting your client and living up to expectations. While you may not have to be a tech geek, lawyers need some working knowledge of technology to ask the right questions and spot issues. And this duty is more and more being recognized by State Bar Associations.

II. COMMENT 8 TO MODEL RULE 1.1

In 2009, the American Bar Association created the Ethics 20/20 Commission\(^2\) to examine in depth how changes in technology might affect the ABA Model Rules of Professional Conduct. The Commission made many recommendations; most

---


\(^2\) ABA Commission on Ethics 20/20 (http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20.html).
notably, it provided additional comments to Rule 1.1 regarding lawyer competence.

In August 2012, the ABA House of Delegates passed several amendments to the Model Rules of Professional Conduct recommended by the Commission including Comment 8 to Rule 1.1.\(^3\)

Rule 1.1 provides:

**Client-Lawyer Relationship**

**Rule 1.1 Competence**

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

Comment 8 provides:

**Maintaining Competence**

[8] 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.

*Id.* Emphasis added.

Certainly, the Model Rules are just that – a model. By design, they guide states in formulating their own rules of professional conduct: each state may adopt, reject, ignore or modify the Model Rules. **Almost all states**\(^4\) have adopted the Model Rule 1.1, however.

To date, some twenty-six states have also adopted Comment 8. They are:

- Arizona, effective Jan. 1, 2015.\(^5\)
- Arkansas, approved June 26, 2014,\(^6\) effective immediately.

---

3. ABA Comment on Rule 1.1 ([http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html](http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_1_competence/comment_on_rule_1_1.html)).


• Colorado, approved April 6, 2016.\(^7\)
• Connecticut, approved June 14, 2013, effective Jan 2014.\(^8\)
• Delaware, approved Jan. 15, 2013,\(^9\) effective March 1, 2013.
• Idaho, approved March 17, 2014,\(^11\) effective July 1, 2014.
• Kansas, approved Jan. 29, 2014,\(^14\) effective March 1, 2014.
• Massachusetts, approved March 27, 2015,\(^15\) effective July 1, 2015.
• Minnesota, approved Feb. 24, 2015.\(^16\)
• New Hampshire, approved Nov. 10, 2015,\(^17\) effective Jan. 1, 2016.
• New Mexico, approved Nov. 1, 2013 (text of approved rules), effective Dec. 31, 2013.\(^18\)

---

\(^7\) Colorado Bar Association: Rules for Professional Conduct (http://www.cobar.org/RulesofProfessionalConduct).
\(^13\) ABA: Comparison of Newly Adopted Iowa Rules of Professional Conduct with ABA Model Rules. (http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/mrpc_iowa.authcheckdam.pdf).
\(^16\) State of Minnesota Supreme Court: Amended Order Regarding Proposed Amendments to the Minnesota Rules of Professional Conduct (http://lprb.mncourts.gov/Pages/Amendment%20to%20MRPC%202015.pdf).
• New York, adopted on March 28, 2015, by the New York State Bar Association.
• North Carolina, approved July 25, 2014. Note that the phrase adopted by N.C. varies slightly from the Model Rule: "... including the benefits and risks associated with the technology relevant to the lawyer’s practice."
• North Dakota, approved Dec. 9, 2015, effective March 1, 2016.
• Ohio, approved Feb. 14, 2015, effective April 1, 2015.
• Oklahoma, approved Sept. 19, 2016, effective immediately.
• Pennsylvania, approved Oct. 22, 2013 (text of approved rules), effective thirty days later.
• Utah, adopted March 3, 2015, effective May 1, 2015.
• Virginia, approved Dec. 17, 2015, effective March 1, 2016.

18 Supreme Court of New Mexico (http://www.nmcompcomm.us/nmrules/NMRules/13-8300-038.pdf).
Florida has not only adopted the Comment but now requires attorneys to participate in at least three hours of CLE devoted to technology competence and issues annually. According to the Florida Supreme Court, members of the Florida bar are now required to take three CLE credit hours per year on technology-related topics. Significantly, some ethical commentators believe the requirement appears to put attorneys on notice they risk malpractice if they fail to competently navigate technology-related issues, such as properly safeguarding confidential electronic communications or not engaging technical advisers when necessary. (Indeed the well-known tech and class action plaintiffs firm Edelson PC, filed a class action in federal Court against a large Chicago law firm alleging that the firm was negligent and engaged in malpractice by allowing security vulnerabilities to develop that posed security risks to clients even though no breach of security had yet occurred. According to the Complaint, the firm had implicitly and explicitly represented to its clients that its cyber security was appropriate when in fact it was not, lowering the value of the representation provided).

Other states, while not having formally adopted the change to their rules of professional conduct, have nonetheless acknowledged a duty of lawyers to be competent in technology. For example, the New Hampshire Bar Association, in Advisory Opinion #2012-13/4 concerning cloud computing, said in language similar to Comment 8:

Competent lawyers must have a basic understanding of the technologies they use. Furthermore, as technology, the regulatory framework, and privacy laws keep changing, lawyers should keep abreast of these changes."


31 Supreme Court of Florida; In Re: Amendments to Rules Regulating the Florida Bar 4-1.1 and 6-10.3. (http://www.floridasupremecourt.org/decisions/2016/sc16-574.pdf).


In Delaware, the Supreme Court set up its own Commission on Law & Technology\(^\text{35}\) in 2013 to issue guidance on the use of technology in the practice of law. The guidance issued so far includes Leading Practice papers on multiple computing subjects, including "Basic Skills." The Commission makes the rather obvious and yet extremely important comment in the Basic Skills paper that "it is impossible to practice law in Delaware today, or even to become a lawyer, without a basic understanding of how to use technology."

That is exactly the point. A lawyer must have basic skills on technology to get by.

Other states have also codified rules regarding protecting client data and electronic communications stored on law firm servers. Connecticut, for example, considers several factors in determining whether a lawyer has reasonably tried to prevent unauthorized access to client documents and communications, such as the nature, complexity and cost of various technical safeguards the attorney and his or her firm used. This requirement, at the very least, demands that attorneys know the kinds of software appropriate for encrypting and protecting client data, and be able to either implement this software or find an expert who can.

Even jurisdictions that have not adopted technical competency requirements have also cautioned attorneys to focus on E-discovery and client data protection best practices. While the District of Columbia’s Bar Association,\(^\text{36}\) for example, has only addressed technological competency issues involving metadata, it has also stated that attorneys should be able to sufficiently understand whatever software their firms use to properly protect client data.

III. THE CALIFORNIA OPINION

Perhaps one of the best and thorough opinions concerning the need for lawyers to have baseline technology competency came recently from the California Bar Association. Although California has not adopted Comment 8 and the Opinion did not directly focus on the Comment, the Opinion articulates that technological competence is an expectation and what the parameters of that expectation are. See Formal Opinion No. 2015-193.\(^\text{37}\)

_Citing_ Comment 8, the California Bar Association stated:

> Legal rules and procedures, when placed alongside ever-changing technology, produce professional challenges that attorneys must meet to remain competent. Maintaining learning and skill consistent with an attorney’s duty of competence includes keeping "abreast of changes in the law and its practice, including

\(^{35}\) Delaware Courts: Commission on Law and Technology (http://courts.delaware.gov/declt/).


the benefits and risks associated with relevant technology, . . ."
ABA Model Rule 1.1, Comment [8]...

Attorney competence related to litigation generally requires, among other things, and at a minimum, a basic understanding of, and facility with, issues relating to e-discovery, including the discovery of electronically stored information ("ESI")...

Not every litigated case involves e-discovery. Yet, in today’s technological world, almost every litigation matter potentially does.

And:

Depending on the factual circumstances, a lack of technological knowledge in handling e-discovery may render an attorney ethically incompetent to handle certain litigation matters involving e-discovery, absent curative assistance under rule 3-110(C), even where the attorney may otherwise be highly experienced. It also may result in violations of the duty of confidentiality, notwithstanding a lack of bad faith conduct.

The Opinion recognizes that where an attorney lacks sufficient capability, they can effectively "contract out" the necessary competence to someone else. That someone else could be another attorney in a firm, an outside attorney, a vendor or even your client, the opinion says, provided the person has the necessary expertise. Not surprisingly, according to the Opinion, the lawyer cannot, however, contract out the duty to supervise the case and protect client confidentiality. The lead lawyer remains the captain of the ship.

According to the California Association, the specific tasks that attorneys must either possess an understanding of, or retain an experienced lawyer or non-lawyer technology expert who does, include:

- Initially assessing E-discovery needs and issues;
- Implementing or causing to implement appropriate ESI preservation procedures;
- Analyzing and understanding a client’s ESI systems and storage;
- Advising the client on available options for the collection and preservation of ESI, and identifying custodians of potentially relevant ESI;
- Adequately conferring with opposing counsel on managing E-discovery plans;
- Performing data searches; and
- Collecting responsive ESI in a manner that preserves the integrity of that ESI, and producing non-privileged ESI in a recognized and appropriate manner.

The Opinion also recognizes "Lack of competence in e-discovery issues also may lead to an ethical violation of an attorney’s duty of confidentiality."
So perhaps the biggest take away from this Opinion may be that even in a state that has not formally adopted Comment 8, there is ethical support for requiring some technological competence by lawyers.

For a good analysis of the Opinion see a recent analysis by Redgrave law firm.  

IV. WHAT DOES THE COMMENT REALLY DO?

Comment 8 certainly reflects the ABA’s view and desire to give lawyers a subtle push when it comes to technology; according to the report accompanying the proposal:

The proposed amendment, which appears in a Comment, does not impose any new obligations on lawyers. Rather, the amendment is intended to serve as a reminder to lawyers that they should remain aware of technology, including the benefits and risks associated with it, as part of a lawyer's general ethical duty to remain competent.

In other words, the ABA's position seems to be that Rule 1.1 does not actually impose any new obligations on lawyers but simply reiterates the obvious: for lawyers to adequately practice and be competent under the Rules in today’s world, they need to understand the technological tools by which they can zealously advocate for and protect their clients. Id.

The ABA also used the word "should" in its revised language, rather than the words "shall" or "will," which are normally used to express a duty. The rule does not outline what technology skills a lawyer should actually know to provide competent representation.

Finally, the Comment requires nothing in specific and is directed toward technology that is "relevant." If you don't have a practice that touches Twitter, for example, the Comment does not necessarily require you to know much about it. But where technology touches an attorney’s practice, that attorney must have some level of competence.

Putting all this together, it seems clear that the Model Comment does not appear to contemplate attorneys getting the technical proficiency of a software engineer or any place close. Instead, somewhat like the California Bar Association concluded, it seems to contemplate that lawyers should at least be able to spot potential issues — the benefits and risks — of the technology that impacts


40 American Bar Association Resolution 105A; May 2012 (http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a Filed_may_2012.authcheckdam.pdf).
attorneys every day. The ABA wants basic understanding: we need not know everything. We need to know some things.

So, on the one hand, it's easy to conclude that nothing has changed and the Comment adds little duties that already exist. On the other hand, some commentators have concluded that by merely having the recommendations / duty in writing a sea change has occurred. Either way, I don't think lawyers can safely ignore technology and be ignorant.

V. WHAT ABOUT KENTUCKY?

Kentucky has not adopted Comment 8 – at least not yet. But this does not mean that Kentucky lawyers are free from technological responsibilities. The Kentucky Bar Association (KBA) addressed a lawyer's duty regarding technology in a formal opinion in 2014.

In Ethics Opinion E-437, entitled "Use of Cloud Opinion," the Association was primarily concerned with whether lawyers could ethically use cloud storage services for materials containing client confidences. In affirmatively answering this question, the Association also commented on technology: "Technology provides an ever-changing environment in which to apply The Rules of Professional Conduct."

While the Association declined to mandate specific practices regarding technology given its evolving nature, it did specifically reference these duties, at least with respect to the use of cloud storage:

- Abiding by the Ethical Rules in connection with the safeguarding of client confidences;
- Acting competently with respect to the use of cloud technology;
- Properly supervising the provider;
- Communicating with the client with respect to the services.

The Association specifically cited the Kentucky version of Comment 8 which does not reference technology per se but recognizes the duty of Kentucky lawyers to keep abreast of changes in law and practice. The Association then specifically referenced the ABA version: "While the ABA version is not controlling, it is helpful." (Emphasis added).

The Association then expanded on the duties set out above, clearly expressing the duty "to act consistent with his or her duty of competence in selecting and monitoring the providers of cloud based services." So, for example, the Association noted that, "When a lawyer selects a provider of any support service,

---

41 Legal Talk Network: "The Lawyer’s Duty of Technology Competence" (http://legaltalknetwork.com/podcasts/digital-edge/2016/03/lawyers-duty-technology-competence/).
the duty to protect a client’s property, and the duty of confidentiality require the lawyer to investigate the qualifications, competence and diligence of the provider." According to the KBA, a lawyer must investigate such things as the provider’s reputation and longevity. A lawyer must do a reasonable investigation of the provider and its security.

In addition, like the California Bar Association, Kentucky recognizes the supervision responsibilities. Calling this responsibility ongoing, the KBA noted that the duty is "extremely important" at the time of selection. And, more generally, the KBA stated that the ethical rules "require supervision of a provider of online storage just as they require the supervision of an offsite provider of services such as a storage warehouse operator and just as they require supervision of a paralegal…"

Finally, the KBA also offered a series of questions that a lawyer should consider to ensure that the provider is competent. These issues include:

- The protections offered by the provider to prevent disclosure of client information;
- The provider’s contractual commitment to protect the security of the information;
- Properly addressing the ownership of the data in the agreement;
- The procedures the provider commits to use when responding to judicial and/or government attempts to obtain the information;
- The return of the information at the conclusion of the relationship;
- The emergency procedures the provider has in place; and
- Where the server used by the provider is located geographically.

So, while Kentucky has not formally adopted Comment 8, it’s hard to see how a Kentucky lawyer could comply with Ethics Opinion E-437 and consider the KBA enumerated issues without keeping abreast of technological developments and "the benefits and risks associated with relevant technology" such as that offered by cloud storage providers. And while the KBA was specifically addressing the use of cloud storage providers in E-437, the duties recognized by the KBA in E-437 and their breadth could be similarly applied to any technology related issue.

VI. WHAT CAN I DO?

Exactly what technology do lawyers need to understand? If a lawyer lacks a solid grounding in technology to begin with, how can he or she be expected to know which topics are important? How do lawyers interested in learning more about technology filter out the geek hype, vendor sales pitches and general misinformation to get to the real information they need?
Courteous of Josh Poje of the American Bar Association’s Law Practice Division, below are five simple strategies to help lawyers develop and maintain the expected and minimum understanding of relevant technology.

First, it’s easy to get overwhelmed by the technology and technology information that’s out there. The constant development of new technology happens at a dizzying pace and can quickly cause lawyers to turn away under the theory they can never master the issues so why try? Instead, Josh believes lawyers should ask some fundamental questions about any technology they encounter:

When scanning through the latest technology news, always ask yourself: *Is this relevant to my practice?* Or perhaps more directly: *Can this technology help me be a better lawyer?* In the end, your objective is to provide exceptional representation to your clients or employer, and the technology you’ll want to explore and understand is the technology that will help you achieve that goal. *Id.*

Second, make it a point to pick out a good technology blog or another source of information and scan at least the headlines. This will at least keep you conversant with major trends and issues. Some good sources are Bob Ambrogi’s Law Sites blog, the Kennedy-Mighell podcast, Ars Technica, ZDNet, The Verge, and Wired.

Third, we all know lawyers or other legal professionals that are tech geeks. Talk to them. You can learn a lot just by chatting with those who have an interest in the subject and are keeping relatively up-to-date. Don’t be afraid to ask the stupid question – it’s probably not as stupid as you think. (And unless you are truly a geek yourself, the geeks will probably think whatever question you ask is stupid, anyway). Use more formal means to engage your peers in sharing knowledge about software, hardware and other technology tools. Get involved in email

---


44 Law Sites by Robert Ambrogi (http://www.lawsitesblog.com/).


46 Ars Technica (https://arstechnica.com/).

47 ZDNet (http://www.zdnet.com/).

48 The Verge (http://www.theverge.com/).


50 Wired (https://www.wired.com/).
discussion lists, bar networking events, alumni meetings, and even simple conversations in the hallways outside the courtroom.

Fourth, discuss issues with experts. Most consultants are all too happy to share their thoughts, opinions and predictions. Often, if you or your firm has an expert it uses for technology related issues, they will talk to you for free. If not, buying an hour or two of their time to talk about the trends, risks and opportunities he or she sees in the tech world is a good investment. These kinds of discussions may not make you a tech expert, but it will help you understand the landscape.

Fifth, contact your state Bar Association and the ABA. Many state Bars offer guidance on practice management issues, including the use of technology. This guidance is often easy to obtain and tends to be free. It also is more neutral and free of the vendor bias. It’s often written specifically for lawyers, often by lawyers. And some state bars have practice management advisers available to answer technology questions. The ABA also has excellent guides and helpful information. See the ABA Legal Technology Resource Center, the Law Technology Today blog, the ABA Law Practice Management Section, and ABA TECHSHOW.

Obviously, trying to keep up with the constantly changing world of legal tech products and services can be daunting. But the ABA sponsors a website called ABA Blueprint that references and provides information about various products and services. The Lawyerist also recently began providing a similar service.

VII. CONCLUSION: WHAT'S THE SO WHAT?

So, you may ask, what does all this mean to me? As my friend and one of the most astute observers of the legal landscape, Bob Ambrogi, so well put it:

What does all this mean to you? It is simple. You cannot assess the benefits and risks associated with various kinds of technology if you know nothing about the technology. Even if your state has yet to adopt this change, it is only a matter of time before it does. Don’t be a Luddite who fears or resists technology. Neither do you have to become a geek. Make an effort to understand the basics of the technology you use. Get on social media, if you’re not...

51 Law Technology Today Blog (http://www.lawtechnologytoday.org/).

52 American Bar Association (http://www.americanbar.org/groups/law_practice.html).

53 ABA TECHSHOW (http://www.techshow.com/).

54 ABA Blueprint (http://www.abablueprint.com/).

55 Lawyerist (https://lawyerist.com/).

56 Law Sites by Robert Ambrogi: "26 States Have Adopted Ethical Duty of Technology Competence" (http://www.lawsitesblog.com/2015/03/11-states-have-adopted-ethical-duty-of-technology-competence.html).
already. Ask questions. Learn. When it comes to technology, there is no more burying your head in the sand.

*Special thanks to Susanne Quigley, legal professional at Frost Brown Todd for her help with this article.*
Formal Ethics Opinion
KENTUCKY BAR ASSOCIATION
Ethics Opinion KBA E-437
Issued: March 21, 2014

Use of Cloud Computing

Question:
May lawyers use cloud computing with clients' confidential information?

Answer:
Yes. Lawyers may use cloud computing with clients' confidential information. In so doing, lawyers must follow the Rules of Professional Conduct with regard to

- safeguarding client confidential information,
- acting competently in using cloud computing,
- properly supervising the provider of the cloud service, and
- communicating with the client about cloud computing when such communication is necessary due to the nature of the representation.

References


Discussion

Technology provides an ever-changing environment in which to apply the Rules of Professional Conduct. Cloud computing is technology that allows a lawyer to store and access software or data though the software or data is stored and/or operated in the cloud – that is, a remote location that is not under the control of the lawyer but is controlled by a third party who provides the storage or other service. The service may be long-term storage of confidential client information or may be shorter-term storage or services to enable data processing or web-based email.²

Lawyers long have had "a duty to make reasonable judgments when protecting client property and information." Pa. Eth. Op. 2011-200 (2011). This duty is the same whether the lawyer is selecting a security system to protect a brick-and-mortar law office, selecting an offsite warehouse for the storing of client files, or selecting a provider of a service such as online storage for confidential client information.

Because technology evolves every day, we decline to mandate in this opinion specific practices regarding the protection of confidential client information in the world of the cloud. The reality is that such practices soon would be obsolete – and our opinion would be obsolete as well. Rather, we choose to guide lawyers in the exercise of reasonable judgment regarding the use of cloud technology. See Vt. Eth. Op. 2010-6 (2010) (constantly changing nature of cloud technology makes establishing "specific conditions precedent" to use not appropriate); Ohio Informal Adv. Op. 2013-03 (2013) ("applying existing principles to new technological advances while refraining from mandating specific practices – is a practical one").

Use of this technology by a lawyer is ethically proper if the lawyer abides by the Rules of Professional Conduct by safeguarding client confidential information, by acting competently in using cloud computing services, by properly supervising the provider of the cloud service, and by communicating with the client about use of cloud services when such communication is necessary given the nature of the representation.³


**Confidential Information and Competence**

Lawyers have a duty to protect confidential client information. SCR 3.130 (1.6(a)) states the basic rule that "[a] lawyer shall not reveal information relating to the representation of the client unless the client gives informed consent, the disclosure is impliedly authorized or the disclosure is permitted by paragraph (b)." The permitted disclosures of paragraph (b) are not relevant here. SCR 3.130 (1.9(c)) and SCR 3.130 (1.18)(b)) make clear that the duty not to reveal information relating to the representation continues to apply when the client becomes a former client and applies to prospective clients as well, even after the prospective client has moved on. See also SCR 3.130 (1.6 cmt. 16) ("The duty of confidentiality continues after the client-lawyer relationship has terminated.").

Lawyers also have a duty to act with competence. SCR 3.130 (1.1) states:

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

Comment six to SCR 3.130 (1.1) states in part that "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice." While Kentucky's competence rule, SCR 3.130(1.1) has not been modified since 2009, the ABA, in August of 2012, amended its version of this comment to state specifically that the duty of competence includes the duty to "keep abreast" of technology. While the ABA comment is not controlling, it is helpful.

Comment fourteen to SCR 3.130 (1.6) clarifies that a part of the lawyer's duty of competence is 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." As with storage of files in a brick-and-mortar law office or in an off-site warehouse, client information stored in the cloud cannot be protected absolutely. Burglars can break into law offices and warehouses despite the utmost care to protect against such happenings. Likewise, sophisticated hackers can access online information despite the utmost care to protect confidential client information.

Comment fifteen to SCR 3.130 (1.6) provides:

When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of

---

4 The comment to ABA Model Rule of Professional Conduct Rule 1.1 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, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject." ABA Model Rules of Professional Conduct Rule 1.1 cmt. 8.
confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.5

From these statements it is clear that a lawyer has a duty to take reasonable measures to protect confidential client information in any setting: brick-and-mortar law office, offsite warehouse, or online storage or service site in the cloud.

Taking such reasonable measures is also consistent with the duty, as stated in SCR 3.130 (1.15(a)), to "appropriately safeguard[]" the client's property.

When a lawyer selects a provider of any support service, the duty of competence, the duty to protect a client's property, and the duty of confidentiality require the lawyer to investigate the qualifications, competence, and diligence of the provider. A lawyer who does not investigate whether a warehouse he or she is considering for the storage of files has adequate security to safeguard client files fails in his or her confidentiality and competence obligations to the client. Likewise, an attorney selecting an online provider of storage or other service must investigate the provider to be sure that client information is reasonably sure to remain confidential and secure.

5 The ABA amended its version of Rule 1.6 to state that a lawyer "shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client." See ABA Model Rules of Professional Conduct Rule 1.6(c). The supporting comment language added by the ABA in August of 2012 states, in part:

Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. The unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. 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. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].
Supervision

A lawyer has a duty to supervise nonlawyers engaged by the lawyer to assist the lawyer in practicing law. SCR 3.130 (5.3(a)) states that with regard to a nonlawyer assistant, "[a] partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer." SCR 3.130 (5.3(b)) states that a lawyer with "direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer."

These rules require supervision of a provider of online storage just as they require supervision of an offsite provider of services such as a storage warehouse operator and just as they require supervision of a paralegal working within a brick-and-mortar law firm. A lawyer must make "reasonable efforts" to ensure that the online storage provider's conduct "is compatible with the professional obligations of the lawyer." SCR 3.130 (5.3(a)). This duty, though ongoing, is extremely important at the point that the lawyer selects the provider because it is at that point the lawyer must determine whether the provider is capable of conduct compatible with the lawyer's ethical responsibilities.6

Communication

SCR 3.130 (1.4(a)) states that a lawyer must "reasonably consult with the client about the means by which the client's objectives are to be accomplished." While cloud computing does not always require client consultation, there may be situations in which consulting with the client may be proper. A lawyer must exercise judgment to determine if a particular client matter involves highly sensitive information such that the lawyer should consult with the client about the use of the cloud. See also Mass. Eth. Op. 12-03 (2012) (lawyer "should refrain from storing or transmitting particularly sensitive client information by means of the Internet without first seeking and obtaining the client's express consent to do so"); N.H. Eth. Op. 2012-13/4 (2012) (informing the client "may become necessary" if particularly sensitive data is at issue); Pa. Eth. Op. 2011-200 (2011) (communication with client may be necessary depending on the sensitivity of the information involved and the scope of the representation).

Issues to Consider in Light of the Lawyers Responsibilities

In order to abide by these duties a lawyer owes a client, a lawyer should investigate the provider's qualifications, the provider's reputation, and the provider's longevity as well as understand the nature of the service provided. Just as a lawyer should review the terms of storage for a warehouse for storage of client files, so too should a lawyer review the terms of the arrangement7 regarding online storage or treatment of confidential client

---

6 Comment three to ABA Model Rules of Professional Conduct Rule 5.3, added in August 2012, specifically notes use of "an Internet-based service to store client information" as the kind of assistance a lawyer may have.

7 The terms often are found in the "Service Level Agreement." See Sharon D. Nelson & John W. Simek, "Have Attorneys Read the iCloud Terms and Conditions?" Slaw (Jan. 30, 2012), available at http://www.slaw.ca/2012/01/30/have-attorneys-read-the-icloud-terms-and-conditions/.
information or other cloud-based service. Some questions that a lawyer should consider in this regard include the following:

What protections does the provider have to prevent disclosure of confidential client information?

Is the provider contractually obligated to protect the security and confidentiality of information stored with it?

Does the service agreement state that the provider "owns" the data stored by the provider?  

What procedures, including notice procedures to the lawyer, does the provider use when responding to governmental or judicial attempts to obtain confidential client information?

At the conclusion of the relationship between the lawyer or law firm and the provider, will the provider return all information to the lawyer or law firm?

Does the provider keep copies of the confidential client information after the relationship is concluded or the lawyer or law firm has removed particular client information from the provider?

---

8 This list is based on a list provided by the Ohio State Bar Association. See Ohio Informal Adv. Op. 2013- 03 (2013). Florida Ethics Opinion 12-3 (2013) sets forth other issues to consider:

As suggested by the Iowa opinion, lawyers must be able to access the lawyer's own information without limit, others should not be able to access the information, but lawyers must be able to provide limited access to third parties to specific information, yet must be able to restrict their access to only that information. Iowa Ethics Opinion 11-01 also recommends considering the reputation of the service provider to be used, its location, its user agreement and whether it chooses the law or forum in which any dispute will be decided, whether it limits the service provider's liability, whether the service provider retains the information in the event the lawyer terminates the relationship with the service provider, what access the lawyer has to the data on termination of the relationship with the service provider, and whether the agreement creates "any proprietary or user rights" over the data the lawyer stores with the service provider. It also suggests that the lawyer determine whether the information is password protected, whether the information is encrypted, and whether the lawyer will have the ability to further encrypt the information if additional security measures are required because of the special nature of a particular matter or piece of information. It further suggests that the lawyer consider whether the information stored via cloud computing is also stored elsewhere by the lawyer in the event the lawyer cannot access the information via "the cloud."


9 SCR 3.130 (1.15(a)) provides that client property must be "identified as such and appropriately safeguarded." Any statement that the service provider owns the information is inconsistent with the demands of this rule.
What are the provider's policies and procedures regarding emergency situations such as natural disasters and power interruption?

Where, geographically, is the server used by the provider for long-term or short-term storage or other service located? \(^{10}\)

**Conclusion**

A lawyer may use cloud-based services with regard to confidential client information. In using cloud-based services, a lawyer must use reasonable care to assure that client confidentiality is protected and client property is safeguarded. See SCR 3.130 (1.6(a)) & (1.15(a)). A lawyer must act consistent with his or her duty of competence in selecting and monitoring the providers of cloud-based services. See SCR 3.130 (1.1). A lawyer must use "reasonable efforts" to ensure that the conduct of providers of cloud-based services assisting him or her is compatible with ethical obligations of the lawyer, and, if the lawyer is a partner or otherwise has managerial authority in a law firm, the lawyer must use "reasonable efforts" to make sure that the firm has measures in place to assure that providers of cloud-based services engage in conduct compatible with ethical obligations of the lawyer. See 3.130 (5.3(a) & (b)). Finally, a lawyer must consult with the client about the use of the cloud if the matter is sufficiently sensitive such that the duty to "reasonably consult with the client about the means by which the client's objectives are to be accomplished" is implicated. See SCR 3.130 (1.4(b)). \(^{11}\)

---

\(^{10}\) Lawyers should be aware that search and seizure law as well as the law relating to ownership of information stored electronically on a server may vary greatly by country.
