Ethics in Technology and eDiscovery
Stuff You Know, But Aren't Thinking About

Kelly H Twigger, Esq.

Oil and Gas Symposium
Arkansas Law Review
October 16-17, 2014

Overview

In the last two decades, business and personal communications have become virtually entirely electronic. We use data to measure everything, and we keep it all. As the development, creation and maintenance of systems has become paramount, we've outsourced and moved data management to the cloud. All of these things have significant legal implications, and existing law is struggling mightily to keep up. Providing competent representation to our clients now means that lawyers not only have to understand the technology, they need to know how it works and what issues it creates for clients.

The rules that govern ethics for lawyers remain behind in what they require of lawyers, so the responsibility falls to the individual attorneys to understand what issues their clients are presented with and how to advise on them. State Bar opinions have started to arise that articulate in greater detail what attorneys need to be responsible for, or that hiring co-counsel with knowledge in the issues is necessary.

ABA Model Rules/Arkansas Rules of Professional Conduct

A. Amended Model Rule 1.1 and the Duty of Competence/Arkansas Rule 1.1

ABA Model Rule 1.1 and Arkansas Rule 1.1, which adopted the Model Rule, address the "client-lawyer" relationship and provide that a lawyer owes clients what is commonly referred to as a "duty of competence." Model Rule 1.1 explains that duty as follows:

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

Newly amended Comment 8 to Model Rule 1.1 provides additional guidance by explaining that:

> 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 amendment to Comment 8 illustrates the ABA's desire to nudge lawyers into the 21st century when it comes to technology, but it's a very gentle nudge:

> 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.

Effective June 26, 2014, Arkansas added comment 8 to Arkansas Rule 1.1, effectively adopting it. While the rule itself offers no substantive requirement for lawyer's to learn about technology for representation, evolving ethics opinions from state bar professionalism committees are taking it further and outlining specifically what competence means for lawyers in eDiscovery and information law.

B. State Bar Opinions on eDiscovery Competence and the Use of Technology

At least 15 state and local bar associations have issued individual ethics opinions relating to attorney competence in the areas of technology, cloud computing and security, and eDiscovery competence. Summaries of each of the ethics opinions as well as links to the opinions are available in the eDiscovery Assistant™ app for iPad. A discussion of some key opinions follows.

1. California

California has issued the most fact specific ethics opinion relating to eDiscovery competence. While advisory, the opinion answers the question: **What are an attorney's ethical duties in the handling of discovery of electronically stored information?**

By analyzing a hypothetical fact pattern, the opinion may provide all attorneys with valuable insight into the duties of counsel in electronic discovery. The opinion digest reads:

> An attorney's obligations under the ethical duty of competence evolve as new technologies develop and then become integrated with the practice of law. 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. An attorney lacking the required competence for the e-discovery issues in the case at issue has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation. Lack of competence in e-discovery issues 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.

AUTHORITIES
INTERPRETED: Rules 3-100, 3-110, 3-210, 5-200, and 5-220 of the Rules of Professional Conduct of the State Bar of California.
Business and Professions Code section 6068

Also notable in the interim opinion is the list of tasks that attorneys should be able to perform "either by themselves or in association with competent co-counsel or expert consultants":

Taken together generally, and under current technological standards, attorneys handling e-discovery should have the requisite level of familiarity and skill to, among other things, be able to perform (either by themselves or in association with competent co-counsel or expert consultants) the following:

- initially assess e-discovery needs and issues, if any;
- implement appropriate ESI preservation procedures, including the obligation to advise a client of the legal requirement to take actions to preserve evidence, like electronic information, potentially relevant to the issues raised in the litigation;
- analyze and understand a client's ESI systems and storage;
- identify custodians of relevant ESI;
- perform appropriate searches;
- collect responsive ESI in a manner that preserves the integrity of that ESI;
- advise the client as to available options for collection and preservation of ESI;
- engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan; and
- produce responsive ESI in a recognized and appropriate manner.

See, e.g., Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC (S.D.N.Y. 2010) 685 F.Supp.2d 456, 462-465.

2. Arizona

Arizona formal ethics opinion 09-04, issued in December 2009, addresses the storage of confidential client communications and was one of the first opinions on cloud computing. According to the opinion, confidential client information may ethically be stored using cloud computing or other online storage providing that reasonable precautions are taken to protect the security and confidentiality of client documents and information. The lawyer has a duty to act in a reasonable and competent manner to assure that confidential client information is kept confidential. In satisfying the duty to take reasonable security precautions, lawyers should consider firewalls, password protection schemes, encryption, anti-virus measures, etc. Lawyers should also be aware of limitations in their competence regarding online security measures and take appropriate actions to ensure that a competent review of the proposed security measures is conducted. As technology advances over time, a periodic review of the reasonability of security precautions may be necessary. A copy of the opinion is available at www.azbar.org.

3. Alabama

Alabama ethics opinion 2010-02 also addresses the use of third party vendors to store confidential client information in the cloud:

> A lawyer must ensure that electronic files are stored in a manner at least as secure as is required for traditional paper files. As such, the lawyer must have reasonable measures in place to protect the security and integrity of electronic files. Only authorized individuals may have access to the electronic files and reasonable steps must be taken to ensure that the files are secure from outside intrusion. Such steps may include the installation of firewalls and intrusion detection software. Although not required for traditional paper files, a lawyer must "back up" all electronically stored files onto another computer or media that can be accessed to restore data in case the lawyer's computer crashes, the file is corrupted, or his office is damaged or destroyed.
>
> A lawyer may also choose to store or backup client files via a third-party provider or internet-based server, such as a cloud-computing service, provided that the lawyer exercises reasonable care in doing so. A lawyer may use "cloud computing" or third‐party providers to store client data provided that the attorney exercises reasonable care in doing so. The duty of reasonable care requires the lawyer to become knowledgeable about how the provider will handle the storage and security of the data being stored and

to reasonably ensure that the provider will abide by a confidentiality agreement in handling the data. Additionally, because technology is constantly evolving, the lawyer will have a continuing duty to stay abreast of appropriate security safeguards that should be employed by the lawyer and the third - party provider. If there is a breach of confidentiality, the focus of any inquiry will be whether the lawyer acted reasonably in selecting the method of storage and/or the third party provider.

Specific Ethical Issues

A. Social Media

The stories of jurors using the internet to learn about the parties to a case, blogging and tweeting during trial and generally using social media to discuss cases are rampant. Judges have attempted to curtail this behavior with special jury instructions, etc. Part of the lawyer's job in a jury trial is to know the potential jury pool. Can you use social media to learn about them?

The ABA specifically addressed lawyers reviewing a juror's internet presence in Formal Opinion 466 and found that a lawyer can:

> [R]eview a juror's or potential juror's internet presence, which may include postings by the juror or potential juror in advance of or during a trial, but a lawyer may not communicate directly or through another with a juror or potential juror.

In short, you can't "friend" a potential juror on Facebook to see their account if it is otherwise protected, but if it's publicly available the information is fair game. The opinion applies to sites with user based account settings where the potential juror has limited the ability to view information.

Judicial use of social media has also been addressed by the ABA in Formal Opinion 62. In short, any use of social media must comply with the applicable provisions of the Code of Judicial Conduct and should avoid any conduct that "would undermine the judge's independence, integrity, or impartiality, or create an appearance of impropriety."

B. The Duty to Preserve

The common law and now rule based requirement to preserve evidence and now ESI requires a party to take steps to reasonably identify, locate, collect and keep information that is likely to be relevant in litigation. That litigation may be actual or reasonably anticipated. There are two ethical issues inherent in the duty to

preserve: the competence to do it properly, and delegating compliance with the hold.

Properly identifying what ESI may exist requires competency with technology. That notion is addressed only vaguely by Comment 8 to Rule 1.1 of the Model Rules and the Arkansas Rules of Professional Conduct, but is better done so by the California ethics opinion discussed above. In order to properly meet the ethical requirement of competence, lawyers putting legal holds in place in complicated systems should be able to:

- initially assess e-discovery needs and issues, if any;
- implement appropriate ESI preservation procedures, including the obligation to advise a client of the legal requirement to take actions to preserve evidence, like electronic information, potentially relevant to the issues raised in the litigation;
- analyze and understand a client's ESI systems and storage;
- identify custodians of relevant ESI;
- perform appropriate searches;
- collect responsive ESI in a manner that preserves the integrity of that ESI;
- advise the client as to available options for collection and preservation of ESI;
- engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan; and
- produce responsive ESI in a recognized and appropriate manner.

If an attorney does not have the expertise or background to do these tasks, Rule 1.1 should require that he engage someone with that level of expertise to assist.

The long gone days of paper also took with them the ability to allow your client to decide what information they have that might be relevant. Delegation to users to decide what they may have is no longer appropriate. *See, e.g., Nat'l Day Laborer Org. Network v. U.S. Immigration and Customs Enforcement Agency*, 877 F. Supp. 2d 87 (S.D.N.Y. 2012). Courts are holding in-house and outside counsel to much higher standards and outside counsel in meeting discovery obligations with ESI. *See, e.g., Zubulake v. UBS Warburg*, 2004 WL 1620866 (S.D.N.Y. 2004).

C. The Meet and Confer Process/Protecting Confidential Information

Following the 2006 amendments to the FRCP and many states that have followed, including Arkansas (see Arkansas Rule Civil Procedure 26.1) now require the parties to meet and confer regarding ESI at the outset of the litigation. Meaningful meet and confer sessions require preparation, candor and cooperation among the parties, and can often be seen as a conflict with the lawyer's obligation to be a diligent advocate for their clients. The same issues arise with the protection of

potentially privileged attorney client communications that may be implicated by discovery requests.

In short, attorneys are required to meet the duty of competence in being prepared and able to participate meaningfully in a meet and confer session, abide by their responsibilities under Model Rule 1.6 to keep client information confidential, act fairly towards opposing counsel (Model Rule 3.4) and not engage in conduct involving dishonesty, fraud, deceit or misrepresentation (Model Rule 8.4). The same rules apply to the protection of attorney-client information.

These ethical obligations go hand in hand in the eDiscovery process. A lawyer who takes the time to know and understand the technologies his clients use that are implicated in his representation (whether litigation, due diligence, etc.), and talks with his client about what needs to be preserved, provided and discussed with the other side will meet his ethical obligations. Those without the ability to do so should work with a professional who can make up for any shortfall to ensure compliance.