Technology and Ethics

Lee Marlow, Esq.

This article will discuss the most prevalent ethical concerns for lawyers practicing in the digital age. The first rule of ethics is that a lawyer must represent his or her client competently. Accordingly, we will concentrate on the duties and obligations that are required under the rules of professional conduct, as well as the sanctions one may be exposed to if that lawyer is practicing below the standard of care. We will also address other ethical concerns for lawyers practicing in a technology-driven world, specifically, client confidentiality and conflicts of interests.

In 2009, ABA President Carolyn Lamm created the Commission on Ethics 20/20 which undertook a three year study in order to conduct a thorough review of the Model Rules of Professional Conduct and lawyer regulation in light of the advances in technology as they relate to the practice of law.

The rule and comment changes to the Model Rules of Professional Conduct focus on the digital practice of law. The practice of law has undergone a digital transition. Technology has an effect on attorneys and their clients everyday. It would be unusual for a person not to be utilizing at least one of the following technological tools on a daily basis:

- Email
- Web browsing
- On-line banking
- Texting
- Social media
    - Facebook
    - LinkedIn
    - Twitter
    - Instagram

Because of the nature of these tools and the fact that they are being used so frequently, the result is that the user's statements, comments, thoughts, reflections, observations,

actions and transactions are digitally memorialized. Accordingly, with the proper marshaling and authentication, they become sources of invaluable admissible evidence in court. Such evidence may be particularly useful in presenting divorce-related issues including:

Drug and alcohol abuse
Gambling addictions
Extramarital relationships
Involvement (or lack of) with children
Pre-filing manipulation of assets and finances
Hiding or dissipation of marital assets, and
Surveillance of spouse's activity

The ABA Model Rules of Professional Conduct (MRPC) have been adopted in each of the fifty states, as well as the District of Columbia and the U.S. Virgin Islands. The Connecticut Rules of Professional Conduct adopt the MRPC with some minor language changes and have been effective since January 1, 2007.

As a result of technology transforming the practice of law and the belief that the regulation of lawyers should be updated in light of these developments, the Commission submitted various resolutions to the ABA House of Delegates. The new comments to the Model Rules are more revealing than the amendments to the rules. The changes demand lawyers to consider and use technology. The Commission's main concern is COMPETANCE. The Commission also intends the amendments to the Model Rules "to provide guidance regarding lawyers' use of technology and confidentiality". It submitted resolutions on Technology and Confidentiality; Model Rule 1.6 (Confidentiality of information), as well as on Technology and Client Development.

The Commission proposed the revision to the comment to Model Rule 1.1. Specifically, Comment 8 related to maintaining competence. The rule states that "[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 to Rule 1.1, previously stated "[t]o maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

The Commission's resolution has resulted in Comment 8 being revised as follows: "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." (new language italicized for emphasis)

Although the italicized language is new, the Commission goes on to let us know that the obligation is not a new one but instead a reminder that lawyers should remain aware of technology including the benefits and risks associated with it as part of our general duty to remain competent in a digital world. Effective January 1, 2014, the comment to Rule 1.1 of the Connecticut Rules of Professional Conduct has now also been revised to include the language requiring lawyers to consider "the benefits and risks associated with relevant technology". However, it is clear that the obligation to consider those benefits and risks already existed. (See Connecticut Rules of Professional Conduct, Rule 1.1, Appendix, page 1)

Lawyers must keep pace with technology and assess the benefits and risks associated with each new relevant development or they risk practicing below the standard of care. This is a difficult task as it requires keeping one's focus on a moving target as advances in technology are occurring constantly. The benefits and risks associated with relevant technology relate to how lawyers communicate with and advise their clients,

conduct investigations, engage in legal research, conduct discovery and present trials. Consider how the following relate to these benefits and risks:

- Law practice tools
  - Practice management software;
  - Digital dictation software;
- Legal and factual research tools
  - Westlaw
  - Lexis
  - Google
- Communication
  - Means of communication
  - Its security
- Discovery
  - Access to electronically stored information (ESI)
  - Preservation of digital evidence
- Video technology
  - Depositions
  - Conferences
  - Investigations
- Court room technology
  - Trial presentation software
  - Evidence display technology

Although the benefits of relevant technology are apparent, the associated risks are concerning. They relate to security, privacy, confidentiality and exposure to conflicts of interest.

Let's consider a few examples of the ethical risks associated with technological advances:

Email

Communicating with your clients through email is convenient, but is it secure? Not only is it good practice to get your client's express consent to communicate through

email, its required. Also, although having a secure communication link with your client by having all out-going and in-coming emails encrypted is recommended, it is not required pursuant to the Connecticut Rules of Professional Conduct. The CBA's Committee on Professional Ethics set forth in Informal Opinion 99-52 that a lawyer's use of unencrypted email to communicate with clients does not violate Rule 1.6 (a) in ordinary circumstances. (See, Appendix, page 3). However, the committee went on to opine that where the lawyer is on notice of a heightened risk of interception or the information to be transmitted is extraordinarily sensitive, a level of security proportional to the heightened risk should be utilized.

When in doubt, do too much not too little. Have a notice in your signed retainer letter or provide your clients with separate authorizations to execute regarding communicating through email. Also, use an encryptor for an additional level of security for all attorney-client communications through the internet.

You also need an ESI management plan for your office. Do you know where your data is stored? Do you know how long it is accessible? You have a responsibility to protect and preserve your clients' information. Implicit in that obligation is that you have the ability to retrieve the preserved information.

Text Messaging

As stated above, you have a duty to preserve your own ESI. This becomes particularly problematic if you communicate by texting with your client. Most cell phone services only retain approximately 200 texts. After that the text messages start getting erased to compensate for limited storage space. Unless you are prepared to take a screen shot or screen capture of every communication sent back and forth between you and the client, it is a much safer practice to refuse to communicate through texting even if your client is willing to give you consent. If you are going to text with clients, get their signed acknowledgements regarding the potential inability to secure and preserve the communication.

Social Media

Although Social Media pages and firm websites are becoming commonplace and a productive and inexpensive way to provide information to clients and prospective clients, as well as promote your firm, the ethical lawyer must be aware of the possible pitfalls that exist. Be certain that only accurate information about your firm is presented and that there are no misrepresentations. For example, the profile screen on LinkedIn allows you to list "skills and expertise". By indicating that you do divorce and custody cases or perhaps, family and matrimonial cases are you holding yourself out as an expert or specialist without the appropriate certification? To do so without actually being certified by the appropriate board approved by the Rules Committee violates Rule 7.4A, Certification as a Specialist. (See Appendix, page 7)

Similar misrepresentations, whether intentional or inadvertent may also be contained in your firm's Facebook page or website. Take the time to review the content of your website. Also, make sure that if the website encourages viewers to contact the firm, that there is an appropriate notice intended to prevent the receipt of confidential information, the review of which may present a conflict of interest in the event you represent the sender's spouse or that spouse desires your future representation. (See suggested website email contact notice, Appendix, page 9)

Cloud Computing

Although storing data in "the Cloud" sounds mystical, the Cloud is merely a group of servers at some off-site location. That location may be around the corner from your office, in another state or even in another country. The benefits of using the Cloud are apparent and include reducing a law firm's expenses related to the ownership of equipment, including networks and servers, for processing, transmitting and most importantly, storing data. However, our ethical obligations also require us to consider the associated risks.

In simple terms, a lawyer can not insure the confidentiality of a client's information as required by Connecticut Rules of Professional Conduct, Rule 1.6 or appropriately preserve and safeguard a client's property as required by Connecticut Rules of Professional Conduct, Rule 1.15, if that material, including ESI is not maintained by

the lawyer, but is instead within the possession and control of another. (See, Appendix, page 10). Nevertheless, Cloud computing is permitted under the Connecticut Rules of Professional Conduct provided that the lawyer engages in due diligence.

According to Rule 1.6(e), a lawyer must not hold or transmit data by a method that presents an unreasonable risk of unintended disclosure and access by unauthorized third parties. A lawyer's obligation under the rule is clear but what may or may not be considered unreasonable is subject to debate.

There are various factors to be considered when determining whether a lawyer has made a reasonable effort to prevent access or disclosure of a client's information. They include:

> The sensitivity of the information;
>
> The likelihood of disclosure without additional safeguards;
>
> The cost of those additional safeguards;
>
> The difficulty of implementing the safeguards; and
>
> The extent to which the safeguards have an adverse affect on the lawyer's ability to represent clients.

Accordingly, in Connecticut, as well as many other states, the use of the Cloud is ethical and permitted if the lawyer has made appropriate efforts to determine that the reasonably reliable cloud service provider's possession and control of the data does not have a detrimental affect on the lawyer's ownership and free access to the client's data and that the cloud service provider also has appropriate security policies and methods in which to segregate the lawyer's data and prevent access by all others, including the service provider, itself.

Additionally, in order to determine whether the cloud service provider is reasonably reliable, a lawyer must also be cognizant of his ethical obligations pursuant to Rule 5.3 governing the supervision of those hired by or associated with the lawyer. Therefore, one must use appropriate efforts to choose a cloud service provider whose conduct is compatible with the lawyer's professional obligations, has the ability to preserve data and limit its unauthorized access while continuing to make it reasonably available to the lawyer. (See CBA Committee on Professional Ethics Informal Opinion

2013-07, Appendix, page 17, Connecticut Rules of Professional Conduct, Rule 5.3, Appendix, page 20).

It would be a mistake to determine that mere familiarity with the referenced ethical rules and opinion coupled with an understanding of the considerations set forth above, authorize you to start using the Cloud. Instead, you must actually discharge your ethical obligations. Knowing what has to be done and not doing it can lead to ethical violations and malpractice claims as easily as never knowing what to do in the first place.

Trial Presentation

As previously indicated, due to the prevalent use of email, texting, web browsing and social media, invaluable admissible evidence may be more easily available than it would have been twenty years ago. However, the availability of the discovered ESI may be of little value if the lawyer lacks the necessary competence to have the materials properly admitted into evidence at trial. Although presenting how to do so is beyond the scope of this article, generally, a lawyer attempting to have ESI admitted must overcome those hurdles traditionally encountered during the admission of more traditional evidence.

In order for ESI to be admissible, it must be

(1) relevant,

(2) authentic,

(3) not hearsay or admissible under an exception to rule barring hearsay evidence,

(4) original or duplicate, or admissible as secondary evidence to prove its contents, and

(5) probative value must out-weigh its prejudicial effect.

Counsel must have a step by step plan for admission and be prepared to anticipate and appropriately respond to possible objections to crucial evidence. It is recommended that particular attention be given to the authentication process. (See Lorraine v. Markel, Appendix, page 35)

E-Discovery

Lawyers have various duties to their clients related to the discovery process. It is well recognized that there is a common law duty to preserve evidence. Zubalake v. UBS

Warburg, LLC 229 FRD 435 (SDNY 2004). This duty, of course, applies to all information and documentation regardless of whether it is stored electronically. However, the proliferation of ESI, presents unprecedented ethical duties for lawyers participating in the E-discovery process. Some of these duties that lawyers must be aware of include the following:

- The duty to preserve ESI runs first to counsel! (See sample hold letters to client, adversary and third party, Appendix, pages 22, 24 and 28)

- The affirmative duty to explain discovery obligations to his client Metropolitan Opera v. Local 100 Union 212 FRD 178, 222 (SDNY 2003)

- The duty to be actively involved in or monitor E-discovery collection and to assist and monitor litigation holds. Negligence or lack of basic knowledge regarding E-discovery requirements constitutes incompetence. Zubalake

- Attorney bears responsibility for client misconduct known or assisted by counsel. Qualcomm v. Broadcom 548 F3rd 1004 (2008)

- The duty to advise client of the type of information potentially relevant to the case and advise regarding the necessity of preventing its destruction Green v. McClendon 262 FRD 284 (SDNY 2009)

- The duty to conduct reasonable investigation of foundation for E-discovery responses and representations 1100 West, LLC v. Red Spot Paint 2009 US Dist. Lexis 47439 (SDInd 2009)

The lawyer also has the duty to inform herself about the evidence in client's possession and to adequately counsel the client regarding the kinds of records that are responsive. Accordingly, she must have a reasonable understanding of client's ESI and computer systems. Tarlton v. Cumberland County Corr. Fac. 192 FRD 165, 170 (DNJ

2000). Furthermore, a lawyer must not only know how to prepare appropriate E-discovery requests, but also how to arrange so that her clients respond adequately. In order to do so the lawyer needs to be familiar with computer-assisted review, how it works, how systems are trained to respond, including Boolean searches and predictive coding, as well as whether a hands-on review of the data produced by the computer must be conducted in order to protect privileged ESI. If the lawyer isn't able to become competent, she must associate herself with the appropriate venders, experts or other lawyers.

Lawyers should be aware and concerned that the Courts have issued significant financial sanctions against lawyers and in some cases referral to the Bar for ethical violations such as:

- Failing to notify opposing counsel and Court that responsive ESI was discovered after production of the responses

- Telling Court ESI doesn't exist when you don't know one way or the other (relying on your client)

- Assisting the client with discovery misconduct (selecting only certain demands for response)

- Participating with client in the destruction of evidence (spoliation)
  In Lester v. Allied Concrete 285 Va. 295, 736 S.E.2d 699 (2013) plaintiff's counsel was sanctioned $542,000.00!)

- Signing a false affidavit of compliance with an E-discovery demand
  Failing to supervise client's preservation (spoliation) (See Connecticut Rules of Court 13-14, Appendix, page 32)

As stated above, Attorneys should be aware that the Commission noted that these technology obligations are not new and that the amended comment to Rule 1.1 is intended to serve as a reminder that YOU MUST BE TECHNOLOGICALLY COMPETENT! This requires that lawyers have a firm grasp on how electronic information is created, stored and retrieved! This means that a competent lawyer must understand the following as they are all relevant to litigation competence:

Metadata
Directories
Active files
Encryption
Document retention policies
Deleted information
Unallocated space
Fragmentation, and
Inaccessible storage media

Although not every cases will require an understanding of all these technological terms, those cases where there are several business ownership interests, or where there is likely to be an abundance of important electronically stored information, will certainly require a lawyer participating in the E-discovery process, to have a thorough understanding of how ESI is created, stored and retrieved or work with other capable professionals, whether they be partners, associates, co-counsel or experts in order to achieve a thorough understanding.

Now more than ever is the time for lawyers to commit to understanding digital change and insure that they can competently handle their clients' needs.