Select Issues in "Techn-ethics"

One of my top professional objectives is to help other attorneys stay relevant. If I were to translate that into "ethics-ese" it would be helping attorneys "maintain competence." Regardless of how you state it, staying relevant and maintaining competence involves one key element-- staying up to date on cutting edge issues in the law. Believe it or not, the world of attorney ethics is a prime source of that information.

The questions we grapple with in the ethics world are usually raised because they represent new issues that aren't adequately addressed in the existing code. That, by definition, makes those matters the cutting edge issues of the day. For instance, the ABA has recently published papers on items like multi-jurisdictional practice and if you dig deep into issues like that you'd see that it's likely to change the face of the practice over the next few years. There should be no question, however, that chief among the issues are matters of technology and social media.

The explosion of social media in all areas of life has changed the way society functions. It has likewise had significant implications on the practice of law. But issues of technology stretch far beyond social media, thus prompting me to group these overall issues into the area of law that I call, "Technethics."

Technethics consists of the ethical implications of things like cloud computing, wikis, smartphones and flash drives. To some lawyers that sounds like a foreign language, but others know that it's actually a list of the hottest trends in technology. The use of these trends is expanding rapidly in the practice of law, but I'm not going to get into a description of those technologies in this paper because I cover that in the live portion of the seminar. The purpose

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

of these materials is to explain the threats associated with some of these platforms so that lawyers can use these technologies responsibly.

1. The Danger Zones

If you try to tackle the issues and read the myriad of articles swirling around legal circles it all seems pretty daunting. However, when you break it all down you realize that there are a few easy-to-understand concepts at issue– this is all about problematic situations that arise when we *move information*.

It's about using the potentially unsecured internet to move data and using potentially unsecured wireless routers and cellular networks to get the information onto the internet in the first place. It's also about the place you're moving that data to—whether you're moving it to a storage facility that's not on your computer or moving it into a program that utilizes that data and happens to be located "in the clouds." The primary ethical issues that are a concern are the potential release or disclosure of confidential information (Rule 1.6[1]) and the potential loss of client information/property (a failure to safeguard client property per Rule 1.15).

Let's expand upon that brief description of the issues. With email, texting and other communication we're talking about the transmission of data from one person to another. We are concerned about the channels upon which that data travels—the highways our information rides along to get from place to place. We take that information and put it on the

[1] One note about the Rules: As I'm sure you're aware, the overwhelming majority of states in our country have adopted the ABA Model Rules of Professional Responsibility, so I'd like to refer to those Rules throughout this paper. Copyright restriction, however, prohibit me from doing so. As a result, most references in this paper to the "Rules" are actually references to the Delaware Rules of Professional Conduct, which are virtually identical to the ABA Model Rules (at least the as far as the parts that I'm quoting are concerned), but are not subject to the same copyright restrictions. There may be some minor differences in the text, but any difference does not impact the concepts discussed herein.

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

internet to move it—we use the proverbial "information superhighway." One question we need to ask ourselves is whether that highway is secure. Can anyone jump onto it and intercept the data we're moving?

What about getting onto that highway to begin with? Just like a car uses an onramp to access a highway, you plug a cable into your computer and that carries your information onto the internet. We all know that you can access that information superhighway wirelessly these days, by using a wireless router to move the information from your computer to the internet. But if we use that type of a wireless "onramp," we have security issues. The data becomes vulnerable once we transmit it through the air. By connecting to a wireless router we essentially open up a door to our computer and invite other people to come in and see whatever we have loaded onto our computers. The whole question of wireless access is also raised when we talk about cell phones and tablets, like the iPad. Those devices access the internet and transmit information using unsecured networks as well.

How about once it's on the highway being carried from place to place. Those carriers—the people who drive the information on the highways – they are moving that information by using potentially unsecured channels.

Mobile storage devices also present an issue because we are moving our client's data to a portable device like a flash drive or cell phone. We're still dealing with moving information and the data could get inadvertently released or lost.

Not only do we have issues of moving data (transmission), but we also have issues about situations where you move information to another place and leave it there- to store it. Those storage companies, or "cloud storage companies" end up holding onto the data on their

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

own servers (in the "clouds"). Similarly, programs known as "Software as a Service" (SaaS) invoke all of the problems discussed because you are sending data to another company that is used in their programs, thus creating transmission issues, wireless problems and storage concerns.

2. The Ethical Issues In Play.

a. Confidentiality and Privilege

Anytime you talk about transmission and storage you have issues of confidentiality, which means that Rule 1,6 is implicated. These issues arise at every step of the technological journey detailed above, because in all instances we're talking about moving information--- situations where information leaves your possession. Those instances include transmitting it to other people for their viewing, giving it to other companies for them to store it, and putting it into SaaS programs based in the clouds.

The issue of confidentiality looks a bit different depending upon the circumstances. Sometimes it's an issue of "security"-- who can get at the information when it's transmitted and who can get at it (maybe improperly) once it's stored. Other times it's an issue of "access." Who are you giving the right to look at the data when you use their service to transmit it or use their servers to store it.

b. Safeguarding client property…loss, destruction

We all know that your client's file is the client's property and we also know that Rule 1.15 mandates that we take steps to safeguard that property. When you think about it,

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

however, the digital version of your client's file is also their property—you're simply holding it in computerized form. Thus, if we release that to another individual (like a cloud storage vendor) we need to make sure that we're taking steps to safeguard that client property appropriately. Here we're talking about the potential loss or destruction of client property. We're also concerned with whether we are entitled to release it to other vendors all together. Do we need proper permission to release the computerized version of a client's file to be stored on a vendor's server located in the clouds somewhere?

3. Standards that have emerged

a. E-mail and Cloud Computing

It has long been established that lawyers could send unencrypted email regarding client matters. The ABA issued a formal opinion in 1999 which stated that there is a reasonable expectation of privacy despite the risk of interception and disclosure (note that it was significant that legislation was enacted making the interception of email a crime). Specifically, the ABA Commission on Ethics and Professional Responsibility Formal Opinion 99-413 states:

> "The Committee believes that e-mail communications, including those sent unencrypted over the Internet, pose no greater risk of interception or disclosure than other modes of communication commonly relied upon as having a reasonable expectation of privacy. The level of legal protection accorded e-mail transmissions, like that accorded other modes of electronic communication, also supports the reasonableness of an expectation of privacy for unencrypted e-mail transmissions. The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of law.

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

> The Committee concludes, based upon current technology and law as we are informed of it, that a lawyer sending confidential client information by unencrypted e-mail does not violate Model Rule 1.6(a) in choosing that mode to communicate. This is principally because there is a reasonable expectation of privacy in its use."

Many states throughout the country have followed suit and issued opinions permitting the use of unencrypted email in the practice of law.

As time went by, jurisdictions were asked to opine on the ethical permissibility of new kinds of technology. In doing so they revisited the issue of confidentiality and the mandates of Rules 1.6, but also comments [16] and [17] of Rule 1.1 "Competence" which remind lawyers that we must, "act competently to safeguard information…against …unauthorized disclosure" and that when transmitting a communication we must, "take reasonable precautions to prevent the information from coming into the hands of unintended recipients." Over time, a "reasonable care" standard emerged regarding technology issues in the practice of law. See, New York State Bar Opinion 782 (2004).

As recently as April of 2010, for instance, North Carolina issued Proposed Formal Ethics Opinion 7 which addressed software-as-a-service programs (SaaS) and stated that, "a law firm may use SaaS if reasonable care is taken effectively to minimize the risks to the confidentiality and to the security of client information and client files."

Jurisdictions built upon that reasonable care standard with the advent of cloud storage. As different states reviewed that technology, an affirmative duty began to emerge. As early as 2004, Arizona stated that attorneys had the duty to, "take reasonable precautions to protect the security and confidentiality of client documents and information." Arizona also added that lawyers should, "be aware of their competence…and take appropriate actions to ensure that a

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

competent review of the proposed security measures [of the cloud storage company] is conducted." State Bar of Arizona Opinion 09-04.

Likewise, the New York State Bar Association's Committee on Professional Ethics declared in Opinion 842 (2010) that, a lawyer may use an online data storage system but in doing so that attorney must takes reasonable care to ensure that confidentiality is maintained. New York went a bit further, however, and also required that the lawyer, "stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and the lawyer should monitor the changing law of privilege to ensure that storing the information in the "cloud" will not waive or jeopardize any privilege protecting the information." Also See Alabama Ethics Opinion 2010-02.

The drafters are concerned because there are a host of open issues regarding the data turned over to cloud storage vendors and each involve potential disclosure or loss of client information. For instance, where are the vendor's servers located- is it a secure area? Who has access to those servers? What are the vendor's backup policies? What are the procedures for catastrophic failure of the servers (are there backups)? What type of data encryption is being used? A more detailed description of the issues can be found online in the ABA's Issues Paper Concerning Client Confidentiality and Lawyer's Use of Technology, dated September 20, 2010.

The Takeaway: These various opinions reveal that a lawyer's obligations regarding cloud computing systems is threefold: We must (1) understand, (2) anticipate, and (3) act. Our duties of competence, confidentiality and safeguarding client's property demand that we stay abreast of technology in general; we must remain aware of the pitfalls in the systems we

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

use; we must understand the underlying technology being used by our vendor; we must anticipate where we may risk disclosing and losing client information; we must be vigilant in monitoring the security technologies in use by our third party vendors, and; we must act, if necessary—speak to the vendor to ensure that they amend their systems to provide adequate protection to our clients, or maybe even move our client's information to a different vendor if our concerns are alleviated. We cannot simply chose a vendor and then forget about it. What is emerging is a proactive and continual obligation.

The duty to exercise reasonable care and take reasonable precautions to protect client information reveals itself every time we are faced with a new technology. We are starting to see it become an issue again these days in the matter of wireless communications. What's interesting in this case, however, is that the State Bar of California seems to have given a bit of teeth to the standard.

b. The Issues with Wireless Networks

Clearly, the use of wireless technology is on the rise. A laptop user who finds free Wi-Fi in a coffee shop is comparable to a deep sea diver who finds a tank of oxygen. The downside of many of those wireless networks, however, is that they are vulnerable to being compromised if they are unsecured. That poses a problem for attorneys because it means that if we use an unsecured wireless network to perform work on behalf of our clients, our confidential information may be exposed. The question then becomes, are lawyers permitted to use unsecured wireless networks to do client work.

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

The issue of course, is confidentiality because an unsecured wireless network is easily accessed by hackers. The concept of competence is also in question because comments [16] and [17] of Rule 1.1 ("Competence") remind lawyers that we must, "act competently to safeguard information…against …unauthorized disclosure" and that when transmitting a communication we must, "take reasonable precautions to prevent the information from coming into the hands of unintended recipients." California tackled the question directly in Formal Opinion No. 2010-179. The State Bar of California's Standing Committee on Professional Responsibility and Conduct stated that,

> "An attorney's duties of confidentiality and competence require the attorney to take appropriate steps to ensure that his or her use of technology in conjunction with a client's representation does not subject confidential client information to an undue risk of unauthorized disclosure." Formal Opinion 2010-179.

The Opinion went on to list 6 factors (with some sub-categories) that an attorney should consider when evaluating new technologies. The Committee further stated that it was their belief that lawyers should not use unsecured wireless connections when working on client matters. The opinion states,

> "With regard to the use of a public wireless connection, the Committee believes that, due to the lack of security features provided in most public wireless access locations, Attorney risks violating his duties of confidentiality and competence in using the wireless connection at the coffee shop to work on Client's matter unless he takes appropriate precautions, such as using a combination of file encryption, encryption of wireless transmissions and a personal firewall. [FN omitted] Depending on the sensitivity of the matter, Attorney may need to avoid using the public wireless connection entirely or notify Client of possible risks attendant to his use of the public wireless connection, including potential disclosure of confidential information and possible waiver of attorney-client privilege or work product protections, and seek her informed consent to do so. [FN omitted]
>
> Finally, if Attorney's personal wireless system has been configured with appropriate security features[FN omitted] the Committee does not believe that Attorney would

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

> violate his duties of confidentiality and competence by working on Client's matter at home. Otherwise, Attorney may need to notify Client of the risks and seek her informed consent, as with the public wireless connection."

The Takeaway: If your jurisdiction agrees with California, you might not be able to use wireless networks for client matters. The only way you will know for sure is when the Bar finally acts, either because they were asked to opine on the subject or they are disciplining someone. The question I ask myself is…do I want to be that person who "makes the law" by being the first person to be disciplined?

c. Implications for Smart phones, iPads and the Rest

Here's a scary extension of that wireless opinion. Let's say your jurisdiction agrees with the California rule and you are not permitted to connect your laptop to the internet through an unsecured wireless router and work on client matters. Then shouldn't you also be prohibited from connecting your iPad, Smartphone or other mobile device to an unsecured wireless router to work on client matters? It would seem that you are prohibited from connecting any mobile device in that manner. Take it one step further… while I'm not a tech-expert, I've been told by people who claim to be experts that wireless cellular service is just as vulnerable as a wireless router. Experts say that a cellular network is the functional equivalent (from a hacking/security perspective) as an unsecured wireless network.

The Takeaway: While there are no opinions on topic, logic seems to dictate that you are not permitted to utilize your device's cellular signal (i.e., 3G or 4G service) to access the internet and work on client matters. That means that you cannot use your iPad, Smartphone or other device to work on client matters unless it is using a secured internet connection.

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

d. Guidance for the Future

Earlier I mentioned that California Formal Opinion No. 2010-179 listed 6 factors (with some sub-categories) that an attorney should consider when evaluating new technologies. Those factors could be helpful for all attorneys when evaluating the permissibility of new systems in the future. Here is a list of the factors, but I encourage you to read the actual opinion because they explain the factors more fully and it makes more sense after you read the text. The factors include:

1- An attorney's ability to assess the level of security afforded by the technology, including (i) how the technology differs from other media use (ii) whether reasonable restrictions may be taken when using the technology to increase the level of security and (iii) Limitations on who is permitted to monitor the use of the technology to what extend and on what grounds.
2- Legal ramifications to third parties of intercepting the information
3- The degree of sensitivity of the information
4- the possible impact on the client of an inadvertent disclosure
5- The urgency of the situation
6- Client instructions and circumstances

The Takeaway: As time goes by, lawyers will find themselves asking new questions for technologies that are not yet even discovered and California's Formal Opinion 2010-179 is helpful to all lawyers. The opinion provides a list of (what I call) "technology permissibility factors" that a lawyer could use to evaluate the permissibility of those new technologies. California was essentially building upon the "reasonable are" or "reasonable precaution" standard-- it gave it teeth.

Granted, the California Opinion 2010-179 may not be binding in your jurisdiction, but it wouldn't be such a bad idea to consider these factors when you find yourself in a pickle in the

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

absence of a direct ruling from your home jurisdiction. Consider how a disciplinary board would react if you were faced with a new technology, but before using it you evaluated the California "technology permissibility factors" and wrote a memo to the file detailing your analysis. I would expect that a disciplinary board would look favorably upon you in a hearing situation.

e. The Communication Medium of the "Future." Text Messaging.

Issues of computer-based communication between lawyer and client have been debated since people were pecking out programs in "Basic" on their Commodore VIC-20s (yes, I'm dating myself). Text messaging is simply the latest extension of communication.

Text messaging may seem like the "future," but it's really part of the present—texting is quickly becoming the preferred method of communication among a significant part of society. Indeed, the college-level generation today communicates almost exclusively by text messaging. The students in m y law school classes confirmed that as well. I also conducted an informal survey of people in my community and I found that high school students are sending and receiving anywhere from 5,000 to 20,000 text messages per month! Many lawyers will attest that texting is quite common, even among members of the bar. The issue then becomes whether texting is a permitted method of communication between lawyer and client.

Before tackling whether texting should be permitted, I want to point out that it's questionable whether it should be "preferred." There are a host of practical reasons that a lawyer would want to avoid texting clients. For instance, because text messages are short,

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

they are unclear and it's easy to misinterpret what is being said. We also need to ask ourselves whether it's proper professional behavior to use text acronyms and abbreviations when speaking to clients. Is this the image of attorneys we want to present?

Issues that get a bit closer to ethical concerns include file retention issues (each of which could individually warrant a full blown law review article). Do we have an obligation to preserve the messages, like we preserve correspondence, or are they more like phone calls which don't necessarily all get logged and emails, which sometimes get deleted if they're not significant? If we are required to retain the texts, what happens if your client changes lawyers and they want you to send the file over, do you have to print out all of your text messages? Could you do so?

There aren't any actual ethics opinions on topic, so it's up to us to look at existing decisions/rules to figure this out. While texting may be the latest incarnation of communication, it doesn't appear to be much different from its major predecessor, email. A text message is a text-based communication that's sent directly to the account of a specific recipient.

One would therefore assume that since email is permitted, texting should be permitted as well. The major difference, however, is that emails are sent over the internet and text messages are transmitted over a wireless signal between mobile telephones.

Remember that problem we spoke about regarding wireless networks a few pages ago? Well, if we can't work on client matters when using an unsecured cellular network, are we prohibited from sending messages to our clients that contain confidential information through devices that use unsecured cellular networks?

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com

The Takeaway: Texting may not be permitted because it utilizes an unsecured cellular network. If that's the case, can we take it a step further—maybe we should not be permitted to email from our wireless devices either. Sure, opinions have held that unencrypted emails are permitted, but no Bar has opined on whether unencrypted emails that are send over an unsecure cellular network are permitted. If they adopt the California position, chances are that they won't find it acceptable.

Query- A Possible Solution? Maybe there's a solution: The California technology permissibility factors state that we should consider "client instructions and circumstances" in determining whether we could use certain technologies. Formal Opinion 2010-179. Footnote 18 of the opinion states, "In certain circumstances, it may be appropriate to obtain a client's informed consent to the use of a particular technology."

If that's the case, then couldn't we just include a clause in our standard retainer agreement stating that we use wireless technology or texting (or any other preferred technology) and that by signing the retainer the client is giving us permission to do so? If we explain the potential problem with the technology in the retainer and make a point of mentioning it to the client when the agreement is executed (so there's no argument that we buried the terms in the agreement) then aren't we obtaining informed consent to using the technology? I don't know if that, alone, will get you off the ethical hook, but it's something to think about-- maybe as one part of an overall responsible-use-of-technology-plan.

2 Winchester Dr., Suite 201, East Brunswick, NJ 08816
Tel: 732-986-7003 stuart@sit-law.com www.sit-law.com