UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

Managing Your Success: Practice

Management at the Next Level

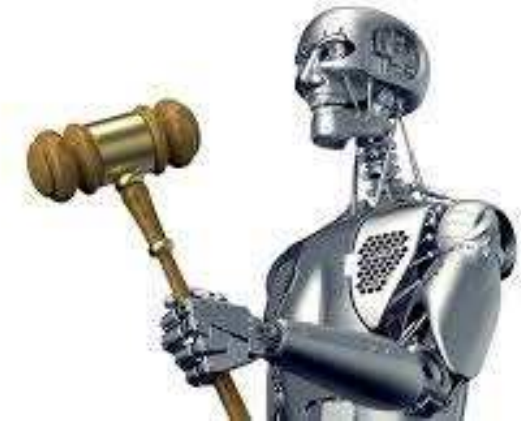
February 9, 2018

Dallas, TX

Cyber Ethics: Ensuring Compliance with Evolving Technology

Jim Calloway

Cyber Ethics: Ensuring Compliance with Evolving Technology



By Jim Calloway
Director, Oklahoma Bar Association Management Assistance Program
http://www.okbar.org/members/MAP.aspx
Blogger, Jim Calloway's Law Practice Tips
http://www.lawpracticetipsblog.com
Digital Edge: Lawyers and Technology podcast
http://legaltalknetwork.com/podcasts/digital-edge/
Twitter @JimCalloway https://twitter.com/jimcalloway

Your law firm is a technology business.

In 2015, *The Wall Street Journal* declared that "Every business is a technology business."[1] It renamed its popular Marketplace section's name to Business & Tech. This is now truer for law firms than many other businesses.

Attorneys handling litigation have to process huge amount of ediscovery information electronically. Few lawyers do legal research by relying on books. If your computer or network isn't working, essentially your law firm isn't working.

From social media evidence in divorce cases to understanding the issues when a client's child is accused of illegal music or movie downloads, even a lawyer in a small town general practice will be confronted with more and more legal questions that revolve around technology, such as "The school is trying to force my son to unlock his phone so they can examine it. Can they force him to do that?"

Your attention is directed to the September/October 2016 issue of *Law Practice Magazine* and the article "Every Law Firm Is a Technology Business."[2]. The concluding paragraph of my Practice Management Advice column is:

> A general counsel addressing a group of lawyers stated that she still saw a lot of Flintstones versus Jetsons when addressing technology in firms she has dealt with. Be a Jetson.

General counsel make the recommendations on which law firms to hire—and fire.

Ponder that a while.

A "Duty" of Technology Competence

Two provisions of the ABA Model Rules of Professional Conduct are those most cited as requiring lawyers to maintain an understanding of today's technology and to protect client's confidential information from being compromised via today's technology. But those requirements rationally spring from long-existing requirements of protecting client confidentiality and protecting clients' property held by the lawyer.

Model Rule 1.6 (c) states:

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.[3]

Model Rule 1.1 Rule 1.1 Competence 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.[4]

Comment 8 to Rule 1.1 provides:

[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.[5]

According to Robert Ambrogi, who tracks adoption of these rule change at his Lawsites blog, twenty-eight states have now adopted some version of comment 8 to their version of the Rules of Professional Conduct. [6]

These relatively recent rule changes would be considered a necessary and obvious to some, considering how critical technology is to the operation of all sorts of businesses today. But they also could be concerning for other members of the bar who are not confident with their understanding of technology advances.

Law practices have become, at least in significant part, technology businesses. This happened without lawyer's approval or consent. You may take some consolation from the fact that this is what has happened to most businesses. We all have to understand the risks and benefits of relevant technology and that was true even before it was officially enshrined into our Rules of Professional Conduct.

So what does this mean for you?

It means whether you are a lawyer in private practice or a lawyer working for an agency you have to be a competent technology user.

You have to protect confidential client information when you are entrusted with it.

You owe it to your clients, and your own enlightened self-interest, to protect your computer network from compromise and from destructive encryption malware and other dangers.

There are two broad categories of required cyber security:

1. **Security steps that have to be outsourced.** Your network setup and the security setup at each work station has been installed and configured by someone. Likewise, someone has vetted many of the software tools and cloud-based services you now use daily. Large law firms will have well-staffed IT departments or outsourced IT services. Medium-sized firms will have a relationship with a local provider who is likely a frequent visitor to the office. Lawyers in smaller firms rely on local service providers, including those that offer cloud-based practice management services with many features.
2. **Security steps that lawyers and law firm staff should understand to the law firm's cyber security and ensure it meets its ethical obligations.** Today training for all law firm staff and lawyers on client confidentiality, cyber security and digital ethical challenges is an important facet of running a law practice or legal department. This will be our subject matter for today.

In November 2014 hackers announced their successful intrusion into Sony Pictures and released personal information about its employees and their families, e-mails between employees, information about executive salaries at the company and copies of then-unreleased Sony films. Since the hackers demanded Sony pull release of its film *The Interview*, which was about North Korean leader Kim Jong-un, North Korea was blamed. Some Sony employees sued because their social security numbers and medical information were released. The Sony co-chairwoman stepped down.[7]

One 2015 leak from a Panamanian law firm was so massive and damaging, that it has its own name and Wikipedia entry: The Panama Papers.

In March 2016 it was revealed that nearly 50 large law firms, including some of the nation's most prestigious, were the targets of hackers[8], although there is some dispute about how successful the hackers were in obtaining client information.

Title search: Cyber Ethics: Ensuring Compliance with Evolving Technology

First appeared as part of the conference materials for the
2018 Managing Your Success: Practice Management at the Next Level session
"Cyber Ethics: Ensuring Compliance with Evolving Technology"