2019 Cyber, Management and Professional Liability Conference
July 10-12, 2019
Boston, MA

Don't Let the Bytes Bite You: Avoiding Ethical Pitfalls in the Digital Age

Introduction

The interplay between technology and the law becomes more complex and intertwined each day. Lawyers and claims professionals must continually navigate treacherous waters in complying with an ever-increasing gauntlet of case law and legislation pertaining to technology. What is more, the legal industry is also increasingly becoming a prime target for cyber attacks. Law firms are particularly susceptible to such attacks simply by virtue of how they tend to operate – that is, with countless attorneys and other employees and vendors having unlimited access to the very same network of electronic data. Moreover, these law firms, along with insurance companies, maintain their clients and insureds' most sensitive information – privileged communications, trade secrets, personal health information/HIPAA material, sensitive financial data, bankruptcy files, and the list goes on and on. Insurance companies are likewise vulnerable to hackers for very similar reasons.

I. Ethical Minefields Involving Electronic Data

Attorneys and claims examiners face a host of potential issues pertaining to how electronic data is both obtained and maintained. Beginning with electronically recorded/stored conversations, myriad laws exist regulating this field at both state and local levels. By way of example, under California Penal Code Section 632, also known as the California Invasion of Privacy Act or the California Wiretapping Act, it is illegal to use an electronic device to monitor or record a "confidential communication" – whether the communication is in person, or by telephone, video camera, or another type of device. "Confidential communications" are defined as conversations in which one of the parties has an objectively reasonable expectation that no one is eavesdropping or overhearing the conversation. Unlike many other states, California is a "two-party" or "all-party" state, which means that recordings are not allowed unless all parties involved in the conversation consent to the recording. Violations of Section 632 can lead to criminal and civil liability, including fines and imprisonment, as well as actual damages (e.g. forensics costs) and penalties in the civil arena.

We have seen a remarkable number of recording incidents, including plaintiffs who foolishly seem to believe that these recordings will be of help to them in prosecuting their claims. In several recent cases, particularly in employment cases, we have filed cross-claims for violations

of this statute – or have used the threat of filing such claims – to strategically leverage the cases to our clients' favor.

A January 2, 2019 California Court of Appeal case, Zhang v. Jenevein, held that there is no Anti-SLAPP protection to secret/non-consensual recordings that were made in preparation for contractual arbitration (which is not a judicial or official proceeding and therefore not a protected activity – the Court held that neither recording the conversations, nor using them as evidence in the contractual arbitration was a protected activity, which could warrant constitutional protection). This case suggests that where the secret recordings are made in anticipation of litigation, i.e. a judicial proceeding (consistent with the Anti-SLAPP statute), California courts may be willing to grant Anti-SLAPP motions in response to Penal Code Section 632 claims where the "illegal" recordings were made in this particular context.

Next up in the arena of novel technology challenges involving electronically stored data is cyber attacks. Large law firms have been hit with ransomware attacks, impacting their computer network systems and causing extensive disruption to their operations. Several examples in recent years have served as a wake-up call to law firm management. For instance, in 2017, DLA Piper was affected by a ransomware worm called "Wanna Cry" that compromised 300,000 computer systems in 150 countries.

In January 2019, a hacking group that calls itself "The Dark Overlord" released confidential files that it stole from a law firm. These files pertain to litigation stemming from the 9/11 attacks and include for example, legal memos concerning details about post-9/11 insurance pay outs. In addition to publicizing the confidential material, the hackers offered to sell even more sensitive documents to the highest bidder. The targets of this extortion attempt include the insurance companies, as well as many other companies and government agencies involved in these 9/11 lawsuits, obviously along with the law firm from which the files were hacked.

What are an attorney's ethical obligations to protect e-files? When these files were in paper format, lawyers knew to keep them under lock and key. Nowadays, how many attorneys really know how to encrypt, scramble, mask, or otherwise technologically protect? Is hiring IT professionals enough? Is engaging a third party vendor the new standard of care, or is it a violation of the attorney-client privilege?

Law firms, insurance carriers, and similar organizations need to vigilantly review their cyber security policies and practices (taking into consideration tactics such as sophisticated security software, frequent password changes, multifactor authentication, etc.). These organizations need to require all of their attorneys, claims professionals, and employees, meaning anyone with access to their devices and network systems, to engage in up-to-date trainings on how to avoid and, when the unfortunate happens, effectively address and diffuse social engineering attacks. These proactive measures are tantamount to ensuring that your organization is not the next victim of The Dark Overlord or one of its catastrophic counterparts.

II. E-Discovery and Related Issues

Attorneys handling e-discovery have ethical duties to do so competently, and to protect their clients' confidentiality. Courts, as well as clients, are increasingly concerned about the manner in which attorneys conduct discovery, particularly e-discovery. Indeed, Judges seem to be more willing than ever to sanction parties and their attorneys for not fulfilling e-discovery obligations.

In 2012, the American Bar Association amended its Model Rules of Professional Conduct to enact an ethical requirement for attorneys to keep up with technological changes impacting their legal practice. Rule 1.1 of the Model Rules of Professional Conduct sets forth the general duty of competence. The 2012 amendments included the addition of the following language to Comment 8 of Rule 1.1: "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." [Emphasis added.]

Since then, the majority of states have adopted rules requiring that attorneys maintain knowledge and skill pertaining to relevant technological advances as part of their duty to provide competent representation to their clients. Nevertheless, courts frequently encounter attorneys who lack the ability to properly handle e-discovery.

In 2015, a landmark California ethics opinion expanded this requirement for lawyers to stay current relative to technology. Formal Opinion No. 2015-193 of the Standing Committee on Professional Responsibility and Conduct of the California State Bar opines that an attorney may violate ethical duties of competence by failing to understand and perform e-discovery skills. This Committee Opinion sets forth a list of nine specific e-discovery tasks that "attorneys handling e-discovery should be able to perform (either by themselves or in association with competent counsel or expert consultants)." Specifically, to be deemed competent attorneys, California attorneys are expected to know how to:

1. Initially assess e-discovery needs and issues, if any;
2. Implement/ cause to implement appropriate ESI preservation procedures;
3. Analyze and understand their clients' Electronically Stored Information or "ESI" systems and storage;
4. Identify custodians of relevant ESI;
5. Perform data searches;
6. Advise their clients on available options for collection and preservation of ESI;
7. Collect responsive ESI in a manner that preserves the integrity of the ESI;
8. Engage in competent and meaningful meet and confer with opposing counsel concerning an e-discovery plan; and
9. Produce responsive ESI in a recognized and appropriate manner.

Moreover, the California Standing Committee determined that a lawyer who lacks the requisite competence 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. [Emphasis added.]

Yet, how many attorneys have actually turned down business because they did not have the skill or resources to competently engage in e-discovery for a client? Also note, the 2019 California Rules of Court for conducting meet and confer efforts with opposing parties already encompass most of these e-discovery guidelines as requisite topics that must be addressed before the first case management conference in a lawsuit. According to Rule 3.724(8), "…no later than 30 calendar days before the date set for the initial case management conference, the parties must meet and confer, in person or by telephone,… to consider the following:…(8) Any issues relating to the discovery of electronically stored information…."

Federal courts are similarly concerned about ensuring that parties, through their counsel, engage in ongoing meet and confer discussions about e-discovery. For instance, the USDC, Northern District of California requires parties to comply with its ESI discovery guidelines, and has a Checklist for Rule 26(f) Meet and Confer Regarding Electronically Stored Information, as well as a model stipulated order. The primary objective of the Court is to exhort early communication amongst the parties about e-discovery issues.

As another example of how attorneys' ethical obligations are unfolding in the digital age, District of Columbia Ethics Opinion 256 pertains to the "Inadvertent Disclosure of Privileged Material to Opposing Counsel": Where a lawyer has inadvertently included documents containing client secrets or confidences in material delivered to an adversary lawyer, and the receiving lawyer in good faith reviews the documents before the inadvertence of the disclosure is brought to that lawyer's attention, the receiving lawyer engages in no ethical violation by retaining and using those documents. … Depending on the facts, the lawyer making the inadvertent disclosure may, by so doing, violate Rule 1.1, requiring a lawyer to use diligence and care in a representation.

In Mills Lane Management, LLC v. Wells Fargo Advisors, LLC, the attorney for the defendant bank used an outside e-discovery vendor to search for documents needed to respond to a subpoena served by the plaintiff. The defense attorney marked the emails that she determined to contain privileged or confidential information. Thereafter, she instructed the e-discovery service to produce to plaintiff all of the emails that she had not designated. The e-discovery vendor provided this production set of emails to the defense attorney on an encrypted CD, which she spot checked and then sent to the plaintiff.

The bank's attorney thought she had reviewed all of the vendor's search results, but it turns out that she had not. As a result, on her client's behalf, the attorney ended up producing billions of dollars' worth of confidential information regarding approximately 50,000 Wells Fargo clients. The plaintiff's attorney notified the bank's attorney about the disclosure, and the latter demanded the return of this confidential data. Nevertheless, the plaintiff leaked the information to the New York Times, which published an article about how because of this inadvertent disclosure, the Times had been shown extensive confidential material, including client names, along with their other identifying information and bank account details.

The Wells Fargo incident may be one of the most egregious cases of inadvertent disclosure thus far, but unfortunately, we anticipate more news of this magnitude in the future. Ever since the legal industry – and its clients -- started to use electronic communications, the extent of these

inadvertent disclosures has dramatically increased. Such disclosures are still extremely concerning but are no longer uncommon. In addition, the consequences are often more significant.

In California, frequent inadvertent disclosures of confidential data are not the only concern. Western Oilfields Supply Co. v. Superior Court (Martin) is a rather stunning California Court of Appeal decision (not published), which was recently remanded by the California Supreme Court. In the underlying case, defense counsel objected to voluminous document requests based on being burdensome and on other grounds, particularly given the extensive volume of ESI at issue. The trial court rejected the burdensome objection and also held that the (timely) attorney-client privilege objections were waived because counsel did not undertake the very burden of reviewing all of the documents at issue for specific claims of privilege.

Here are but a few of the best practices for competent e-discovery, e.g. in the context of preservation issues, storage/searching needs, having a thorough understanding of both the case and the ESI process, protective orders, and effective time management.

Preservation: Some states recognize spoliation of evidence as an independent tort (allowing for money damages); most states will allow awards of monetary or evidentiary sanctions, along with adverse jury instructions, against parties found to have destroyed evidence, regardless of whether this was done inadvertently. With the growing volume and variety of digital forums – countless types of electronic devices, applications, collaboration platforms, cloud storage, etc. – preservation of evidence has become quite challenging for litigation clients and their attorneys. ESI experts now recommend doing so much more when it comes to ensuring that a party's preservation obligations are met. This guidance could include interviewing custodians and using these interviews to carefully map out all potential sources of ESI. In other words, simply acquiring custodians' email accounts may be insufficient in this new age of technology.

Storage/Searching Data: Even the very largest law firms, with vast resources, are increasingly outsourcing their clients' ESI discovery needs to specialized vendors. In many cases, the volume and complexity of the ESI, along with the substantial cost of managing it, often make it very difficult for lawyers to administer the work on their own. We frequently rely on outside teams to partner with us and our clients in managing the storage of the data and the customized search processes necessitated by the litigation.

Key Knowledge: it is incumbent on the attorneys in a case, particularly a senior-level attorney, to have a meticulous understanding of both the case itself, as well as the ESI vendor's procedures for storage, as well as searching/ selection of ESI to be reviewed. Knowing what the case is about and understanding the mechanics of the e-discovery process will empower the attorneys to help avoid or minimize mistakes.

Protective Orders: While not a foolproof measure, filing a protective order with the court in advance of producing ESI certainly affords clients a means to safeguard their privileged and confidential information. It is imperative to negotiate comprehensive terms, including a claw-back provision that would allow the disclosing party the right to claw back any ESI that was accidentally produced and to ensure the opposing party is precluded from using or disclosing it.

Time Management: The e-discovery process typically takes much longer than anticipated. Attorneys can prevent problems by setting and managing the expectations of both their clients, as well as opposing counsel, very early on in the process. Indeed, judges expect parties and their counsel to take the meet and confer process very seriously and to avoid waiting until the last minute to engage in this process.

If an inadvertent disclosure occurs, and there is no protective order in place (or it is not effective) and the opposing party is not cooperating, injunctive relief should be sought right away. The disclosing party can ask the court to sequester the ESI until the court issues a permanent ruling as to whether the data should be returned.

III. Exposures posed by the internet of things

According to the Pew Research Center, close to 80% of Americans have smart phones. This means more than 250 million people nationwide are regularly using smart phones. Of further note, the use of wearable devices, such as Fitbits and Apple watches, has continued to rise (with at least one out of six Americans wearing them), and the Internet of Things ("IoT"), a remarkable variety of "smart" devices used throughout our homes, vehicles, and elsewhere, has become truly ubiquitous. Against this tech-heavy backdrop, litigants no longer rely solely on "old-school" sources of evidence to prosecute and defend claims. We now have opportunities – both lawful/ethical means and otherwise -- to acquire salient evidence concerning health/medical/biometric data, accident reconstruction metrics, employment information, and private financial/ proprietary details, by way of these electronic devices. In some cases, this evidence may be broader in scope than, or even contradictory to, the evidence obtained through customary means, e.g. police records; medical records from health care providers; employment records from employers.

An Arkansas criminal case involved a murder charge in which the accused's Amazon Echo device may have been prompted to record and save this recording to the cloud around the time of the alleged murder. The government served a subpoena for the recordings and transcript of these possible communications to and from the Amazon device. At the outset, Amazon vehemently challenged the subpoena, attempting to quash it based on the argument that requests for information through the product, as well as the service's responses, are protected speech under the First Amendment. However, Amazon ultimately relented and provided the data after the defendant informed the court that he did not object to the disclosure.

As discussed above, technological advances influence our clients and insureds' preservation obligations. ESI has a substantially broader meaning today; it is no longer sufficient to focus only on potentially relevant data in email accounts. For some time, courts have required chats and text messages to be preserved as well; yet, witnesses routinely delete old texts and discard old cell phones, which can be just as problematic as deleting emails. Simons v. Petrarch is a New York employment/harassment case in which the plaintiff replaced her phone twice and lost her original texts, but managed to save screenshots/ pictures of them. The court found this to be spoliation because the plaintiff did not save her old phones, which prevented the defendants from viewing the "complete and original text messages."]

Thoughtful consideration must be given to whether the obligation encompasses other forms of electronic data – in the cloud, on a FitBit, in an iTunes account, within a public or private Social Media account, and so forth. As we frequently read about in the news, this raises concerns about privacy rights, which continue to be developed in the courts.

On the civil side, lawsuits that often involve IoT devices and their data include personal injury cases, data breach cases, patent litigation, consumer fraud class action cases, defamation claims, and marital disputes. The Stored Communications Act ("SCA") generally prevents providers of electronic communications services from disclosing private communications. [See the decision, e.g. in Sines v. Kessler-- quashing the portion of a subpoena seeking communications from a private, invite-only social networking and instant messaging platform because disclosure from the provider would violate the SCA.] Courts may view certain data from IoT devices, such as recordings or transcripts of questions and answers exchanged with "Alexa" or "Siri," as protected communications under the SCA. However, the SCA does not preclude a court from compelling disclosure directly from a party (e.g. the social media account holder) who also has possession, custody or control of the communications. In sum, clients should be cautioned to carefully preserve ESI relative to all sources of IoT if and as soon as litigation is anticipated.

As for social media, across the board, courts have consistently held that social media that is potentially relevant to the claims or defenses at issue in the litigation is discoverable. Such discovery frequently comes up in connection with emotional distress, personal injury, employment, and other types of claims. Note that the discoverability of this evidence may hinge on whether the social media account is held with a "public" or "private" setting.

Attorneys regularly use social media searches to investigate other parties, attorneys and witnesses. However, in many states, it is an ethical violation for an attorney to utilize deception, or for an attorney to direct a third party to do so, in order to "friend" or connect with an adverse party or a witness for an adverse party. Moreover, at least some state bar associations have opined that even without using deceptive practices, attorneys may not access other parties' social media accounts if those parties are represented by counsel (unless specific disclosures are made).

Other ethical dilemmas to watch out for include the use of social media in hiring evaluations and background checks (including ethical and legal violations associated with these practices, e.g. FCRA and its state counterparts).

Conclusion

There will be no shortage of traps for the unwary and novel types of claims and liabilities arising from the exponential advances we will see as computers, artificial intelligence and big data interact ever more frequently with humanity. Inevitably it will fall to the legal system to sort out these issues and impose some semblance of order and predictability to the chaotic new frontier of technology; and of utmost importance in all of this will be maintaining an evolving and workable rule of law that will provide ethical consistency and certainty for society at large.