CLM Management & Professional Liability Conference
June 20-22, 2018
Boston, MA

Paradise Lost:
Challenges to Confidentiality and Privilege in the Use of Technology Post-Paradise Papers

I. Law Office Data Breach May Be Different Than Other Breaches

A. Common Law and Ethical Duties

Among the principles most valued in the attorney client relationship is that communications between a client and lawyer that occur during the course of the representation shall not be disclosed to the outside world. The sanctity of the attorney-client communication is a hallmark of legal representation. It affords the client with the reassurance that he can freely communicate with his counsel and vice versa, so that the attorney can provide fully informed legal advice to his client. Essentially, the concept allows the attorney to do his job to the fullest extent in order to best represent his client.

Although we often discuss a lawyer's duty in the context of attorney client privilege, a lawyer's duty of confidentiality is not limited to matters that are formally privileged from discovery. Rule 1.6 of the ABA's Model Rules of Professional Conduct ("Model Rules") provides that, a lawyer "shall not knowingly reveal confidential information."[1] According to Comment 2, it is a "fundamental principle" in the client-lawyer relationship that, in the absence of a recognized exception, "a lawyer must not knowingly reveal information gained during and related to the representation, whatever its source." Comment 18 to Rule 1.6, as recently amended, discusses the intersection of competency, confidentiality and inadvertent or unauthorized disclosure of confidentiality data and requires the attorney to take "reasonable steps" to protect client communication and data against cyber-intrusion.

[1] Many states have adopted the Model Rules in their entirety or in modified form or have used them as reference point for their state's standards. As such, the Model Rules are a good starting point for this multi-state analysis. A state-by-state comparison of the variance in rules can be found at https://www.americanbar.org/groups/professional_responsibility/policy/rule_charts.html and should be consulted before applying the Rules discussed herein.

The legal concept of attorney-client privilege generally protects certain communications from disclosure during legal proceedings. Under federal law, "the attorney-client privilege protects from disclosure communications between a client and his attorney that were undertaken to elicit or provide legal advice or other legal services, and that were made and retained in confidence." *Obeid v. La Mack*, 2015 WL 5581577, *2 (S.D.N.Y. Sept. 16, 2015). The privilege extends only to the communication, itself, and not to the underlying facts. *See e.g., Brigham & Women's Hosp., Inc. v. Teva Pharms*. USA, Inc., 2010 U.S. Dist. LEXIS 31573 *14, (D. Del. Mar. 31, 2010).

These long-standing principles pre-date both the pervasive reliance on technology in the practice of law, and the perception of law offices as high value targets for cyber-attacks. *See e.g. ABA Formal Opinion Formal Opinion 477* (May 4, 2017) ("Formal Opinion 477"). Such modern concerns caused the ABA to adopt the "technology amendments" to the Model Rules in 2012 in order to address the technological reality of law practice in the 21st Century and require lawyers to have technologic competence in order to identify and ameliorate the risks of cybersecurity. *Id. See also,* ABA Model Rule 1.1, Comment 8 thereto.

B. Ripped from the Headlines

In 2016, the Panamanian law firm, Mossack Fonseca was hacked. As a result, the International Consortium of Investigative Journalism ("ICIJ") released hundreds of thousands of documents, known as the "Panama Papers", containing confidential client data regarding hard-to-trace, off-shore dealings by hundreds of government officials and high net worth individuals. *See e.g. "Fallout from Panama Papers Echo Around the World",* https://www.npr.org/sections/thetwo-way/2016/04/05/473115334/fallout-from-panama-papers-echoes-around-the-world. The breach was accomplished by hackers' exploitation of a well-known bug in an outdated version of a plugin used to access the firm's servers. An update was available and publicized for at least a year prior to the hack that would have closed that vulnerability, but the firm continued to rely on the outdated version of the program.

In response, Mossack Fonseca criticized the hacker and subsequent disclosure by ICIJ as a criminal act. It denied it had committed any wrongdoing either in failing to safeguard its clients' confidential records from intrusion or in the legal services it provided to its clients regarding their off-shore dealings. https://www.theatlantic.com/business/archive/2016/04/panama-papers-crimes/477156/. Nevertheless, the disclosure of the firm's clients' private information was unflattering and unwelcome by their clients. In many cases, the disclosure led to actual harm, such as causing Iceland's prime minister to resign and suit by a hedge fund alleging that Mossack Fonseca was complicit in illegally hiding its clients' assets.

In November 2017, the ICIJ obtained documents via another law firm data breach, which resulted in the disclosure of 13.4 million documents held by the Bermudian law firm, Appelby. Known as the "Paradise Papers," this breach exposed the hidden financial dealings of many high-placed individuals and large corporations, such as U.S. Commerce Secretary Wilbur Ross, Queen Elizabeth II, Nike, and Apple. It also disclosed information connecting the Russian oligarchy to possible clandestine financial dealings with US and EU companies and individuals. Appelby, like

Mossack Fonseca, blamed the loss of the data on an outside "criminal attack" that happened a year earlier and denied any inside leak, although criminal interference may not excuse its failure to protect its clients' data from unauthorized access.

Legal news sources are replete with stories of law firms suffering cyber-attacks of all types. For example, in 2016, Russian hackers reportedly targeted 50 "Biglaw" firms, allegedly in search of confidential client information for purposes of insider trading. https://abovethelaw.com/2016/03/beware-of-big-hacking-in-biglaw/?rf=1. It has also been reported that Proskauer Rose was a victim of a "phishing scam" which resulted in the theft of Prokauer employees' personal information. https://abovethelaw.com/2016/04/biglaw - phishing-scam-results-in-identity-theft/?rf=1.

In June 2017, a ransomware attack on DLA Piper, resulted in the "shutdown" of the firm's Internet and phone service and paralyzed the firm's ability to service its clients. *See, It's a Nightmare – DLA Piper Ransomware attack sounds cybersecurity alarm for law firms,* LEGAL Week (Online), July 27, 2017.

Indeed in 2018, a UK security firm found that 1.16 million email addresses that had been held by London's 500 largest law firms were available on the "dark web" – often with their passwords. *Practical Law Firm Cybersecurity* at https://www.todaysgeneralcounsel.com/practical-law-firm-cybersecurity/ ?utm_source= cybersecurity.

Moreover, it would be an error to assume that only the big firms are targeted. A cyber study by Logicforce looked at 200 law firms ranging in size from 1 to more than 450 attorneys during 2016-2017. The firms practiced in a variety disciplines throughout the United States. The study found that whereas EVERY law firm in the study had been targeted, approximated 40% of them were not even aware the firm's resources had been breached. Logicforce also concluded that neither firm size nor revenue influenced the rate at which a law firm would be targeted. *See* https://www.logicforce.com/reports/detail/cyber-security-q1. Against this backdrop, ever greater vigilance may be required if lawyers are to meet their professional duty to protect their clients' confidences.

C. Challenges to the Practice of Law

The ABA's May 2017 Formal Opinion 477 addressed the impact that evolving technology has had on practice of law. It noted that in 1999, its Formal Opinion 99-413 addressed the relative recent growth of email in client communication and concluded that use of email, even unencrypted, was consistent with a lawyer's ethical duties to maintain client confidentiality pursuant to Rule 1.6. However, since 1999, when multiple means of communications were prevalent, lawyers presently primarily rely on electronic means to communicate and exchange documents with clients, other lawyers, vendors and the courts. *Id.* The Committee discussed the variety of devices now commonly used to create, transmit and store confidential communications, including desktop, laptop and notebook computers, tablets, smartphones, cloud resources and remote storage locations and noted that each presents opportunities for the

inadvertent or unauthorized disclosure of confidential information, thereby implicating a lawyer's ethical duties. *Id.* Accordingly, the Model Rules now require that, as part of the duty to safeguard a client's communications from "inadvertent or unauthorized" access, an attorney must undertake "reasonable" safeguards and keep current with the benefits and risks associated with relevant technology. *See Id.*

Attorneys in all areas of practice can easily identify ways in which technology has changed their practice and raised new challenges to the maintenance of confidentiality. For example, nearly ubiquitous e-filing requirements in state and federal court proceedings have given rise to redaction regulations regarding a party's personally identifiable, financial, and personal health information. E-filing also presents specific challenges to commercial or intellectual property disputes as critical proprietary or confidential terms may be central to the dispute and require court permission to be filed under seal. *See e.g., Verlese v. Liberty Mutual Fire Ins. Co.,* 2017 U.S.Dist. LEXIS 34520 (M.D.F, March 10, 2017)(Malware attack on firm which allegedly interfered with plaintiff's timely opposition to defendant's motion for summary judgement did not justify vacating default in light of availability of e-filed documents and court schedules.)

Corporate business plans, clients' intellectual property applications and communications between counsel and their clients concerning regulatory or legal advice are also frequently targeted for commercial espionage via hacking into legal counsel's computer systems. Clients in regulated industries, such as financial, medical, securities and insurance fields, have their own industry specific cyber requirements to meet, which may, by extension, apply to the confidential information held by their counsel. Nevertheless, law firms are often viewed as "softer" targets and more vulnerable to cyber-attacks then the regulated clients whose data the law firms hold.

Finally, attorneys are often consumers of technology services which also must secure the attorneys' confidential client data. Third party vendors may include cloud computing, back-up storage providers, software-as-a service (SaaS) programs, e-discovery vendors and outside information technology providers. To employ these services, lawyers must entrust their clients' and their own confidential data to the protection of others. However, lawyers may do so at their own peril as they could be found liable for the consequences if a cyber–breach is accomplished while the confidential data is in the vendor's possession.

Take, for example, the nearly ubiquitous use of cloud computing or SaaS. Lawyers are generally required to perform "reasonable" due diligence regarding the adequacy of security provided to protect client confidences when stored in the cloud. However, there is no universal mandate as to whether lawyers may ethically use cloud services as an adequate protection of confidential data. *See,* https://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/cloud-ethics-chart.html (U.S. map demonstrating a state by state analysis regarding requirements for the ethical use of cloud services).

II. Cyber Issues and Evolving Attorney Standards

A. Consequences of Attorney Data Breach Claims

In the post Panama and Paradise Papers era, it is reasonable to anticipate that a growing number of legal claims will be brought against lawyers by clients who suffer harm as a result of cyber-attacks on attorney held confidential data. An attorney's fiduciary responsibility to maintain the privacy of a client's confidences is well-established and pre-dates the proliferation of cyber-attacks. For example, in *Thiery v. Bye,* 228 Wis. 2d 231 (Wis. Ct. App. 1999), a firm inadvertently disclosed their prior client's name when using her medical records to teach a course after the case settled. The court found that a cognizable claim for legal malpractice and breach of fiduciary duty existed since the firm had an ongoing obligation to protect the confidentiality of those records by assuring that the prior client's name was completely redacted. The court reasoned that

> an attorney has a duty to maintain the confidentiality of documents in his possession as a result of legal services rendered to a client. This duty exists notwithstanding that litigation may or may not be pending or that services are completed. To contend otherwise is inconsistent with an agent's duty to protect a principal's confidential information and would limit an attorney's obligation to his client to only that conduct performed while litigation is being prosecuted. It would remove any obligation for the reasonable care and handling of confidential documents in counsel's possession as a result of his legal representation of a client. Accordingly, [the defendant's] duty to protect the confidentiality of [plaintiff's] records arose as a result of his representation of [the plaintiff] in her personal injury action, which had not yet been completed. However, even had that litigation terminated, [the defendant's] duty to protect the confidentiality of [the plaintiff's] records would have continued.

Thiery, 228 Wis. 2d at 243.

However, not every disclosure of private information has been treated as a basis for an attorney claim, particularly in the absence of an attorney client relationship. In *Good v. Khosworwhahi,* 296 Fed. Appx. 676 (10th Cir. N.M. 2008), the plaintiff brought claims for professional negligence, constitutional rights violations, violation of the court's privacy policy under Federal Rule of Civil Procedure 5.2, and the common law tort of invasion of privacy based on defendant's failure to redact the plaintiff's private information from a document filed on the electronic docket. The court dismissed the claims finding, among other things, that a private right of action for violation of Federal Rule of Civil Procedure 5.2 did not exist, and that New Mexico state law, which governed the dispute, precluded the professional liability claim in the absence of privity. *See also, Matthys v. Green Tree Serv., LLC (In re Matthys*), 2010 Bankr. Lexis 1765 (Bankr. S.D. Ind. May 26, 2010), (failure to redact personal identifying information as required by Bankruptcy Rule 9037 was sufficient to establish contempt under Bankruptcy Rule § 105(a), but no cognizable legal theory justified monetary recovery); *GUR. v. Intelligator,* 185 Cal. App. 4th

606 (Cal. Ct. App. 2010),)(plaintiff suit against ex-spouse's attorney for filing documents containing the plaintiff's social security number in violation of California statutes dismissed).

Recently, a class action complaint was filed against Chicago law firm, Johnson & Bell alleging that the firm failed to safeguard the security of its clients' sensitive and confidential data due to its continued reliance on an obsolete computer program, "JBoss Application" which plaintiffs' claimed was likely to render the firm's internet-accessible web services vulnerable to intrusion. *See Shore v. Johnson & Bell,* N.D. Ill. 16-cv-04363. 2016 U.S. Dist. Ct. Pleadings LEXIS 17. The complaint asserted counts for breach of contract (legal malpractice), negligence (legal malpractice), unjust enrichment, breach of fiduciary duty and sought class wide relief on behalf of the firm's present and prior clients whose confidential records were possessed by Johnson & Bell and at risk of unauthorized access. The complaint sought injunctive relief, declaring that the firm had failed to secure client data, directing it to notify its clients that their confidential data had been compromised as a result of the firm's substandard security measures and could be exploited in the future, compelling an independent security audit of the firm's systems to ensure the integrity of the clients' confidential data going forward, and disgorgement of all fees earned during the period that client data was exposed. The class action was dismissed when the Court enforced the retainer agreement's provision that required disputes to be submitted for individual arbitration. (*Shore v Johnson & Bell*, 2017 US Dist LEXIS 25612 [ND Ill Feb. 22, 2017, No. 16-cv-4363].) However, less favorable retainer terms or an action in a jurisdiction that does not enforce mandatory arbitration in attorney-client disputes could have led to a different result. Indeed, plaintiff's counsel, Edelson P.C. describes itself as a national class action firm, focusing on privacy, technology and class action litigation, which include targeting law firms for malpractice. *See e.g., https://juntoblog.net/law-firms-and-data-breaches-sensitive-data-and-dangerous-practices/*.

Even when tort liability may not exist, loss of confidential client information may have ethical consequences for a lawyer that does not take reasonable steps to safeguard client data from cyber-intrusion. ABA Formal Opinion 477 neither holds attorneys to be guarantors of the safety of electronic client data that they maintain nor mandates adoption of a one-size-fits all solution to data security. Instead, lawyers should consider various factors including the type of client data stored and its location, the cost and inconvenience of implementation of a security plan and the client's sophistication and particular needs. Another factor that may be germane to the analysis is whether the attorney's practice areas or clients are of particular interest to data thieves. For example, according to the Opinion, attorneys who represent clients in areas such as industrial design, mergers and acquisitions, or trade secrets, may be in possession of client information that is attractive to hackers. Likewise, attorneys who represent clients in regulated industries such as healthcare, banking, federal defense, insurance, or education, may have access to data that is governed by higher confidentiality standards in addition to those that arise in the context of the attorney-client relationship. Accordingly, "reasonable efforts" may require greater security efforts be considered based on the client's status and regulatory requirements. *See Formal Opinion 477.* Attorneys are not required to become security experts or information technologists but should have a general idea of their firm's electronic environment and consider implementing safeguards, such as use of robust passwords, encryption, firewalls, and designation of emails as "Attorney-Client Communication" as appropriate. *Id.*

An interesting confidentiality issue may arise in the context of a ransomware attack, which occurs when malware infiltrates the computer environment and encrypts data and programs to render them inaccessible and useless. The hackers offer a decryption key to release the data upon payment of a ransom, often in bitcoin. In responding to a ransomware attack, many chose to pay the ransom while others rely on robust encryption and back-up practices to avoid the need to pay. However, it is never certain that the decryption key will, in fact, be provided after payment or that hackers have not already accessed confidential data or will not access and perhaps disseminate it in the future.

One can readily see the problems faced by the legal practitioner who no longer has access to client and files essential to their practice. But an additional, and as yet, unresolved issue concerns whether ethical and legal duties of confidentiality are implicated in a ransomware attack. Does the hacker's exclusive control over client data violate confidentiality if there is no evidence that the client data itself was accessed after it was obtained? In analogous circumstances, the Health and Human Service's Office of Civil Rights has concluded that HIPPA-regulated entities may be required to report a ransom event as a breach, depending on the nature of the infiltration, whether the data was extracted, whether the data was encrypted by the regulated entity in storage and is unlikely to be read by the hackers, and the extent to which the data loss can be mitigated, such as through back-ups. State data breach laws vary, but often generally require notification of a ransomware incident, where the data has been extracted outside of its original environment, contain protected information, and were not encrypted when stolen.

It is reasonable to anticipate similar analyses in connection with a ransomware attack on confidential client data. Depending on state law, so long as the confidential data is never extracted and accessed by the hacker, there arguably should be no impact on confidentiality. However, there are states where access to confidential client data by individuals outside the attorney-client relationship destroys its confidential nature for all purposes, even if the access was unauthorized or inadvertent. Attorneys in states where such a bright line rule exists may risk inadvertent and unauthorized waiver of confidentiality as to their clients' data, which could result in ethical complaints and/or legal claims for damages.

Finally, cybersecurity is also an issue of law office management. Response to the ever-changing risk of cyber-attack is expensive and on-going. It requires "buy-in," not just from the information technology specialists, but also the highest echelon of the firm. It is also an issue of "client maintenance" as clients' are increasing requesting that their counsel establish robust cybersecurity practices and may seek other counsel in the event that a cyber event disrupts the clients' business or causes the client to sustain losses.

B. Cybersecurity as an Evolving Opportunity

Conversely, cybersecurity is also an evolving opportunity for lawyers.

For example, the ABA recently voted to accredit a privacy law specialty certification program to be administered by the International Association of Privacy Professionals. http://www.abajournal.com/news/article/privacy_law_specialization_program_narrowly_approved_after_spirited_debate.

In other news, the EU's General Data Protection Regulation, ("GDPR") has created the requirement that many organizations, including US businesses transferring EU data, be required to comply with a GDPR's requirement to appoint an in-house or outside Designated Privacy Officer ("DPO"). The DPO's qualifications are set forth in the GDPR, but in some circumstances, the role may be filled by a privacy savvy attorney.

Addressing cybersecurity requires that law firms take proactive steps to ameliorate the risk to the firm and their clients by 1) implementation of strong safeguards to prevent cyber intrusion and data breaches and 2) creation of a formal response plan to address a cyber event if and when it occurs. *See Prevention and Response a Two-Pronged Approach to Cyber Security and Incident Response Planning.* https://www.americanbar.org/groups/professional_responsibility/publications/professional_lawyer/2016/volume-24-number-3/preventiand-response-twopronged-approach-cyber-security-and-incident-response-planning.html. Many clients favor firms that have proactively taken steps to address the cyber risk and will include questions in requests for proposals as to the firm's cyber protections and available cyber insurance.

III. The Insurance Response

It is important to understand cyber insurance, including its benefits and limitation. Notably, despite its availability for some time, cyber insurance is still in its nascent stage. There is no standardization of cyber policy terms, so that each policy may define key aspects of coverage differently. For this reason, it is important that each policy be carefully read in comparison with other cyber insurance proposals and the firm's existing insurance program.

One critical, distinguishing aspect of cyber insurance is that it generally provides first party benefits, which are intended to compensate the insured for losses that the insured, itself, sustains as the result of a cyber breach. First party coverage addresses the insured's expenses in responding to an event such as forensic investigation into the cause of data breach the cost of amelioration, coordination with law enforcement, data breach notification, identification fraud monitoring, lost profits, etc. Policies may also provide for payment of ransom in the event of a ransomware attack and payment of certain regulatory fines that may be assessed as a result of a cyber-breach. In some cases, the insureds receive the services of the insurers' pre-selected preferred providers and in others the insured's expenses are reimbursed. Individual covered items may have their own sub limits, which vary from carrier to carrier, and may depend on the risk presented by the individual insured.

Third party coverage, on the other hand, provides coverage for claims by third parties that they were damaged by violation of their privacy due to unauthorized access to that party's confidential or private information while it was in the insured's control. As with other types of

liability coverage, third party coverage is designed to provide for defense and indemnity of a covered claim. However, how a "claim" is defined in a cyber policy may impact the availability of coverage. Availability of cyber coverage tend to focus on four factors: 1) whether the actor's access to the computer systems was authorized or in excess of the actor's authority; 2) whether the damages claimed were directly caused by a computer breach; 3) whether the breach is among the covered "acts" defined by the policy; and 4) whether the resultant injuries are the type that the policy covers. See Rutkin, *Cyber Health,* Best's Review, February 2018, http://www.rivkinradler.com/wp-content/uploads/2018/02/Cyber-Health-February-2018.pdf.

As discussed above, the loss of client data may also implicate a fundamental professional duty owed by the lawyer to safeguard the clients' confidential and private information. As such, a claim may be made, as it was in the *Shore v. Johnson & Bell* case, that an attorney's failure to diligently protect clients' records from cyber breach occurs in the course of providing legal service and is a departure from the standard of care. Put another way, a cybersecurity breach that results in the loss of clients' confidential data may arguably constitute malpractice, negligence or other professional claims that are typically covered by lawyers' professional liability policies. In anticipation of such claims, most lawyer professional liability policies now contain specific exclusions for claims that arise in the context of online or computer activity. Accordingly, lawyers must read the specific terms of their professional liability policies in the context of obtaining cyber insurance coverage.

Even so, some have posited that some types of cyber claims may fall between the gap between professional liability and cyber insurance. Consider, for example, the class claims asserted in *Shore v. Johnson & Bell* case where it was asserted that the firm's outdated technology put their clients' data at risk and primarily sought injunctive relief requiring the firm to update their computer resources, determine whether there had been a breach and notify clients of the risk. Because the claims asserted arguably arose in the context of office services and were not professional in nature, sought injunctive relief and disgorgement of fees, and did not identify an actual cybersecurity breach causing harm, but only the risk of harm, it is possible that neither the firm's cyber nor professional liability insurance would ultimately respond to cover the claim. *See Professional Service Firms Beware: Just Because You Haven't Suffered a Data Breach Doesn't Mean You Won't Be Sued – And the Worst Part, There May Not Be Covered.* http://www.mondaq.com/article.asp?articleid=575630&email_access=on&chk=2103150&q=1527520.

The takeaway – as with all aspects of cybersecurity – proactive understanding of the risks of loss of attorney-client data, prompt efforts to ameliorate the risk and an effective response plan for when a breach occurs are aspects of a lawyers "reasonable efforts" to protect the client confidential information with which the lawyer was entrusted.