Affinity Programs

PROFESSIONAL COUNSEL℠

Advice and Insight into the Practice of Law®

For Your Eyes Only: Securing Lawyer-Client Communications

Introduction

It is axiomatic that clients do not wish to be ignored. This is as true today as it was fifty years ago. The difference, though, is how clients define being "ignored." While acceptable response times were once measured in days, modern communication channels have clients counting the hours or even minutes since they sent their email or text. File sharing also has accelerated, with clients able to review, revise and approve documents instantly and without touching a physical piece of paper.

This communication revolution has enhanced law firm efficiency and reduced startup and overhead costs. At the same time, however, lawyer-client communications have become vulnerable in entirely new ways. Bar associations have unanimously declared that attorneys have a duty to understand and respond to these new risks, and in 2017, the American Bar Association provided some useful recommendations in its Formal Opinion 477R: Securing Communication of Protected Client Information. Attorneys, however, may still be left wondering exactly how, when, and to what extent they need to protect client communications.

Top-of-the-line security is useless if the client gives the keys away.

Evaluating the Threat

Attorneys have a duty to protect all client communications, but not all communications require heightened security measures. Less secure methods of communication, specifically unencrypted emails or texts, are acceptable for routine client interactions. Such routine interactions include scheduling or administrative updates, as well as many communications involving legal analysis, case strategy, or other substantive discussions. Attorneys should still take reasonable security measures, including the use of a firewall and other basic network security systems involving password protection of devices and accounts. Routine client communications, however, do not require message encryption.

Sensitive client data, including social security numbers, driver's license numbers and financial account numbers, cannot be transmitted electronically without using encryption. Beyond these well-known targets, attorneys should avoid unencrypted communications containing or including medical records, financial records, trade secrets, industrial designs or other information related to a particularly sensitive industry or high-profile client. A client who is the subject of a government investigation, for example, may require additional security for communications typically considered routine based upon the heightened threat of interception or seizure by the National Security Agency or a foreign counterpart. For the vast majority of law firms, however, the primary consideration is whether or not the information is attractive to an unknown third party for financial gain.

Setting Expectations

The first step in securing lawyer-client communications, of any sensitivity, is conveying the importance of security to the client and getting the client to buy in at the outset of the representation. Top-of-the-line security is useless if the client gives the keys away. A client suing their employer, for example, should not use a work email account to communicate with their attorney or otherwise discuss their case. A client preparing for a divorce should change account passwords, avoid saving login information on shared devices, and preferably cease to share devices with their soon-to-be ex-spouse altogether. All clients should avoid posting about their case on social media.

With respect to highly sensitive communications, the client must understand the attorney's chosen methods to secure them. Based upon the nature of the representation, the attorney can anticipate the types of communications and documents that will justify those methods and prepare the client in advance.

With heightened security comes a diminished level of convenience. No secure solution is as easy as unencrypted email, so attorneys should educate clients on the importance of using secure methods of communication and doing so consistently. Although it is becoming rare, there may be clients who scoff at the inconvenience or lack the technical know-how to properly utilize the firm's security solutions. More commonly, the *client* may initiate the discussion on the firm's protections, especially if the representation involves an institutional client. The communication security will represent a value-added service instead of a burden on the lawyer-client relationship.

Regardless, despite the occasional grumbling client, attorneys should not revert to unencrypted email for sensitive communications or material for the sake of simplicity. The alternative, rather, is doing things the old-fashioned way: more phone calls, in-person meetings and transfers of physical documents. Once an attorney has recognized the need for secure communication, what should the attorney actually use?

More commonly, the *client* may initiate the discussion on the firm's protections, especially if the representation involves an institutional client.

Secure Communication Methods

Encrypted Email

Email is the lifeblood of a law firm. Clients expect their lawyers to communicate via email and lawyers are happy to oblige. Emails are fast, convenient, and create a reliable record of lawyer-client communications. As explained in ABA Opinion 477R, unencrypted email is acceptable for routine, low-sensitivity communications, at least in the current environment.

More sensitive messages, however, warrant greater security. Fortunately, email encryption has become more sophisticated and user-friendly in the last several years. The most popular email services for law firms, Google's G Suite and Microsoft's Office 365, offer Transport Layer Security (TLS) encryption by default. TLS encrypts an email in transit, meaning the message is encrypted as it moves within the public internet, between the sender's device and the servers of the email provider, and then from those servers to the recipient's inbox.

In order for TLS encryption to work, the recipient's email service must also support TLS. Most, but not all, email services are compatible with TLS. If the recipient's email service is not compatible with TLS, the sender is typically notified either that the message will be sent without encryption, or not sent at all, depending on the settings in place. Furthermore, while TLS is useful in preventing a third party from intercepting a sensitive email, it fails to prevent the email provider itself from decrypting and accessing the message upon reaching its servers. For example, a provider could, for instance, relay the email to a government agency or to a third party for marketing purposes.

In view of these TLS shortcomings, an attorney who is concerned with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the General Data Protection Regulations (GDPR) compliance, or whose matter involves highly sensitive information or an especially privacy-conscious client, should consider end-to-end encryption. This more thorough encryption method protects the content of a message across its entire lifecycle, permitting decryption only once the message reaches the intended recipient.

Secure email providers, such as ProtonMail, offer effective end-to-end encryption but exist as a standalone service. Therefore, users must migrate to and use an entirely separate email platform. Law firms may instead opt to use a third-party application that can fit onto their existing email infrastructure. Virtru, for example, has partnered with Google and Microsoft to create an end-to-end encryption plugin that integrates with Gmail and Outlook — even allowing recipients to use their existing Google or Microsoft login credentials to decrypt the email upon receipt. In the case of a sensitive email inadvertently sent to the wrong party, Virtru also enables the sender to see whether an email has been opened, disable forwarding, revoke access to an email or revoke access to an attachment even after it has been downloaded.

Regardless of the level of encryption, however, an email is only as secure as the account from which it originates. If a third party obtains access to an attorney's username and password, whether they were saved on a public device, entered on an untrustworthy network or offered up in a phishing scam, email encryption will not prevent that party from viewing emails in the attorney's inbox. Proper password hygiene, including frequently changed passwords and multi-factor authentication, remain critical.

Secure Client Portals

An alternative to end-to-end-encrypted email, secure portals offer client interaction in a fully encrypted environment. Secure portals are already commonplace in the financial services industry and healthcare, but have made substantial headway with law firms in recent years. Rather than accessing sensitive messages or documents within an email, clients receive an email notifying them of an item awaiting them in the portal. From there, the client clicks on a link, enters their login information, and accesses the content on the cloud-based platform.

While more bare-bones options designed strictly for file sharing and secure messaging exist, others are a component of more comprehensive law firm practice management software. Attorneys may prefer this all-inclusive experience, where messages, documents, calendar events, tasks and bills can be managed and shared with the client on a single platform. In effect, clients can access their complete file securely and remotely, without needing to comb through past emails or request additional copies from their attorney.

Secure portals likely represent a steeper learning curve for clients than encrypted email, at least initially. Clients cannot simply rely on their existing email accounts and must create and use unique login credentials to access the portal. In practice, however, clients may appreciate that case-related emails are segregated from personal emails, permitting them to remain organized and avoid accidental disclosure of sensitive messages on a shared device. By separating document sharing from email, secure portals may also reduce the risk that an attorney, client, or member of support staff forgets to encrypt a sensitive attachment before hitting the send button.

On the firm side, many portals offer integration with existing online accounts. Clio, one of the leaders in legal practice management software, integrates with G Suite and Office 365, allowing a firm to sync calendars, contacts, tasks, or even Google Drive documents. Whatever product attorneys select, they must be sure to apply updates as they are released by the developer, if this service is not provided automatically. The 2016 Mossack Fonseca data breach, which revealed the 11.5 million financial documents later known as the Panama Papers, was caused by a client portal the firm had neglected to update over a three-year period. Furthermore, just as with email, attorneys must properly secure their login credentials for the portal's encryption to be of any use.

Secure Instant Messaging

In a world of instant and constant communication, texting is king. Texting has become the preferred way to grab someone's attention or relay information quickly, so it comes as no surprise that more attorneys are incorporating text messages into their client-communication repertoire.

The content of these lawyer-client texts, however, is almost always mundane: "free for a quick chat in 15" or "meet you outside the courtroom at 9:45." Attorneys are not exchanging medical reports or patent application drafts via text message, and hesitation about client text messaging likely relates to concerns over their personal privacy, rather than the privacy of the information being exchanged. It is generally not recommended, or even particularly convenient, to engage in a lengthy discussion involving substantive legal guidance and sensitive client information over text message. For this reason, unencrypted text messages are acceptable for the types of texts a lawyer or client will typically send.

Perhaps, however, an attorney represents a government whistle-blower or a high-profile divorce client in which the very fact of seeking legal counsel may be harmful if disclosed. Or perhaps the client is privacy-conscious and insists on secure messaging. In these circumstances, the attorney should consider using an end-to-end-encrypted instant messaging application.

Signaling System No 7 (SS7), the set of protocols used by telecom companies to transmit standard text messages, remains vulnerable to third party or government interception. "Standard" text messages include SMS messages (shorter texts) and MMS messages (longer texts or those with multimedia content), both of which are unencrypted. SS7's vulnerabilities actually expose voice calls to interception as well, though the likelihood and accompanying risk is considerably lower compared with text messages.

Fortunately, several effective and reliable applications, including Silent Phone and Signal, offer end-to-end-encrypted instant messaging. These applications look and feel much the way traditional text messaging applications do, although both the sender and recipient must use the same application to exchange messages. For lawyers concerned about the security of client phone calls, both Silent Phone and Signal also support encrypted voice and video calling.

For Apple users, and solely for messaging, iMessage is built into iOS and encrypts text messages between Apple devices by default as long as both parties have access to cellular data. Although these tools are useful, from a practical perspective, best practice dictates that lawyers avoid substantive exchanges with their clients via text message.

Takeaways

- **Prioritize the danger.** All client communications are confidential, but evaluate where especially sensitive exchanges merit greater protection.
- **Get your client on board.** Ensure that your clients understand the importance of securing communications and their role in doing so.
- **Protect your passwords.** Encryption is only useful when paired with proper password hygiene, multi-factor authentication, and adequate network security.
- **Keep software updated.** Whatever security you implement, stay up-to-date with the most current version so security holes are patched.
- **Train your staff.** One weak link can break the chain, so train support staff to use appropriate safeguards consistently.

Modern communication security is constantly evolving, and it is far from what attorneys were trained to master. Enhanced security protocols really make a difference, however, and even small steps today can go a long way toward preventing a breach tomorrow.

For information on vendors that may be helpful in strengthening your firm's communication security, please consult CNA's Lawyer's Allied Vendor Program.

This article was authored for the benefit of CNA by:
Matthew Fitterer
Matthew Fitterer is a risk control specialist in the CNA Lawyers Professional Liability program. He provides risk control guidance to CNA insureds in the form of written publications, training seminars and direct consultations. Prior to joining CNA, Matt practiced law at a Chicago-area criminal appeals and civil rights firm, later transitioning to a firm specializing in commercial litigation. He received his bachelor's degree from the University of Illinois at Urbana-Champaign and his law degree from Chicago-Kent College of Law, and he is licensed to practice in Illinois. Matt has been designated as a Certified Information Privacy Professional (CIPP/US) by the International Association of Privacy Professionals and a Commercial Lines Coverage Specialist (CLCS) by the National Underwriter Company.

For more information, please call us at 866-262-0540 or email us at lawyersrisk@cna.com