ATTORNEY-CLIENT PRIVILEGE IN THE DIGITAL AGE

WHY LAWYERS SHOULD BE USING END-TO-END ENCRYPTION TO PROTECT CLIENT COMMUNICATIONS

BY JENNIFER DETRANI, WICKR GENERAL COUNSEL

wickr

The relationship between an attorney and a client is unique — rooted in the premise that confidences and counsel passed between them is privileged, off-limits to anyone but client and counselor.

Today, privacy is difficult to achieve for individuals or businesses handling sensitive client information. With communications between practitioners of any industry being only as secure as the technological conduits used by the parties, the legal profession is no exception. Emails, text messages, phone conversations, teleconferences — attorneys encounter breaches of these confidential communications all too often. At least 80% of the 100 largest law firms have suffered some sort of data breach. Viruses, spyware, or malware infected nearly half of law firms' computer systems last year.

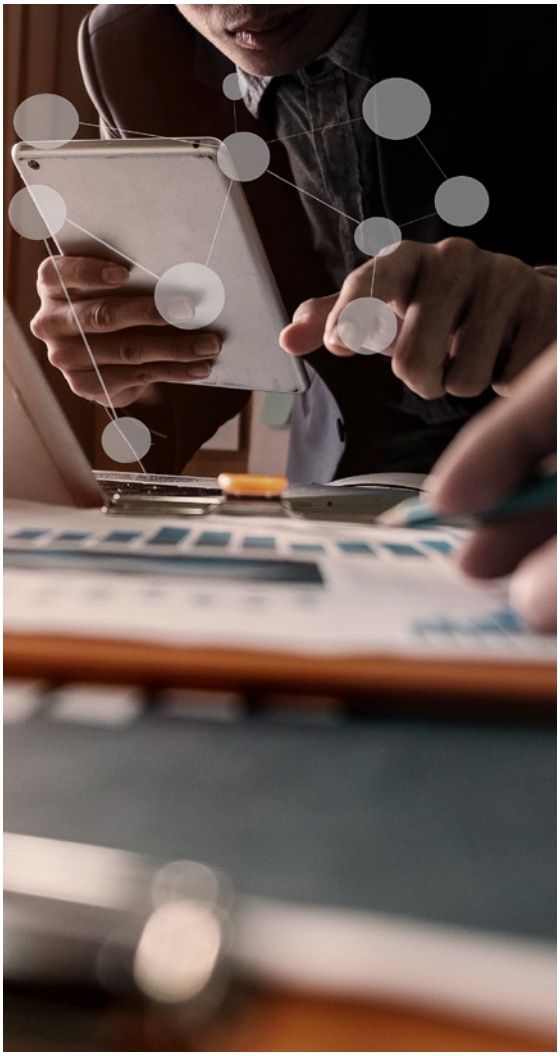
HOW DOES THE PROLIFERATION OF CYBER BREACHES AFFECT ATTORNEY-CLIENT PRIVILEGE?

The ABA Ethics 2000 Commission and the Ethics 20/20 Commission advised that attorneys should tread more carefully the more delicate their words with the client become. In other words, the more sensitive the information, the more seriously the lawyer should consider information security strategies when communicating with a client. This is particularly relevant as legal communications are increasingly transmitted via emails, which are more susceptible to breach than traditional use of phone and fax.

ENCRYPTING CLIENT RECORDS

Given the vulnerabilities of electronic communications transmitted by the legal profession, it is hardly surprising that their most recent Formal Opinion 477R on 'Securing Information of Protected Client Information' requiring that attorneys have a basic understanding of the communication technology they use as part of their essential duty of competence to their clients and that they make a case-by-case assessment of how best to secure communications with their clients. Lawyers need to be able to responsibly counsel their clients on the confidentiality risks versus the convenience benefits of various modes of electronic communication.

But the question remains: considering email's many vulnerabilities to breach—more obvious with every passing news cycle— does emailing a client confidential data violate the attorney's duty to protect client privilege?



The legal field is responding. While the Model Rules are not binding, their influence may be noted in a groundbreaking ethics opinion by the State Bar of Texas. In April 2015, the Texas State Bar determined that emailing unencrypted confidential client information may be unethical. Here are the identified situations in which email may be too insecure for confidential client communication—and therefore unethical for an attorney to use:

- Emailing to or from an account that is shared with others.
- Emailing an account that a third-party may access, especially when that third party is party to a dispute.
- Emailing to or from a public or borrowed computer, or one on an un-secure network.
- Emailing a device the attorney knows isn't password protected.
- Sending an email that the attorney suspects law enforcement will review, with or without a warrant.

The State Bar of Texas also noted additional risk management strategies to address the encryption-in-transit ethics dilemma:

- Speaking openly with clients about the dangers of unencrypted conversation.
- Obtaining informed consent from clients about maintaining unencrypted communications.
- Continuously re-evaluating and updating communication security practices.

Finally, the Texas State Bar noted that electronic mail may become obsolete in a breach-saturated era:

> "Changes in the risk of interception of email communication over time [may] indicate that certain or perhaps all communications should be sent by other means."

While this opinion is certainly weightiest in Texas, it echoes the growing awareness within the U.S. legal vertical of the short-comings of traditional modes of communication upon which lawyers have historically relied. And Texas is not the only state to formally identify the shortcomings of email.

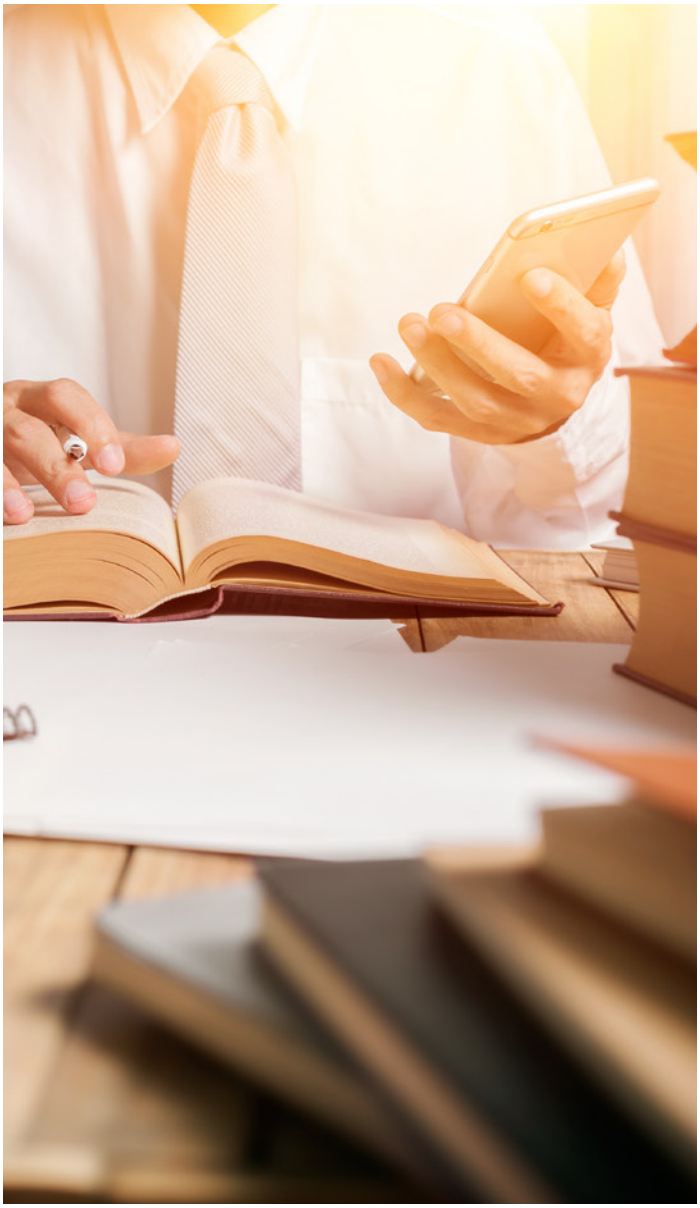
In 2010, the State Bar of California weighed in on the intersection of technology and privacy in its Opinion 2010-179. A digest of the opinion as it appears in the ABA/BNA Lawyers' Manual on Professional Conduct states as follows:

> Because the protection of confidentiality is an element of competent lawyering, a lawyer should not use any particular mode of technology to store or transmit confidential information before considering how secure it is and whether reasonable precautions such as firewalls, encryption or password-protection could make it more secure. The lawyer should also consider the sensitivity of the information, the urgency of the situation, the possible effect of an inadvertent disclosure or an unauthorized interception, and the client's instructions and circumstances, e.g., can others access the client's devices. A lawyer may use a laptop computer at home for client matters and email if the lawyer's personal wireless system has been configured with appropriate security features. However, if using a public wireless connection—for example in a coffee shop—the lawyer may need to add safeguards such as encryption and firewalls.

The Pennsylvania Bar Association followed suit in 2011 when its Committee on Legal Ethics and Professional Responsibility issued Formal Opinion 2011-200 to establish a threshold security level for its lawyers:

> …Compounding the general security concerns for email is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

As with most technical dilemmas, the answer to whether attorneys should protect information sent via email, messaging, or secure BYOD devices using end-to-end encryption is case-specific and complex but must take into account the ethical duties of the profession. Many variables—such as firm size and resources, financial capability, and sensitivity of data—are relevant when determining the communication tools appropriate for a discrete entity. But it is clear that momentum towards encryption is building not only among ethics authorities and commentaries, but amongst their clients who are proactively vetting law firms to assess their security prior to engagement. To maintain competitive advantage in the marketplace and ensure they meet their ethical obligations, attorneys would do well to keep the benefits of this fundamental security technology at the forefront of their minds, and seriously consider securing their client confidences via strong encryption.



Whatever measures are proactively taken by in-house or external legal teams, developing a clear and consistent information governance policy is a first step in ensuring that client information is predictably protected. Every party to privileged communications should be aware when it is appropriate to use which tools.

To enable attorney-client private communications, you may consider Wickr Pro as a means to enforce robust security and tighter digital hygiene. Wickr is a platform that enables end-to-end encrypted communications with clients and within legal teams internally on mobile or desktop. What's more, lawyers can enforce appropriate data retention policies for various types of content to ensure that information does not live beyond its useful life becoming a liability in case of a data breach.

Learn more about new strategies for protecting attorney-client communications here or start your free trial on Wickr Pro here.

TRY WICKR PRO FREE ►