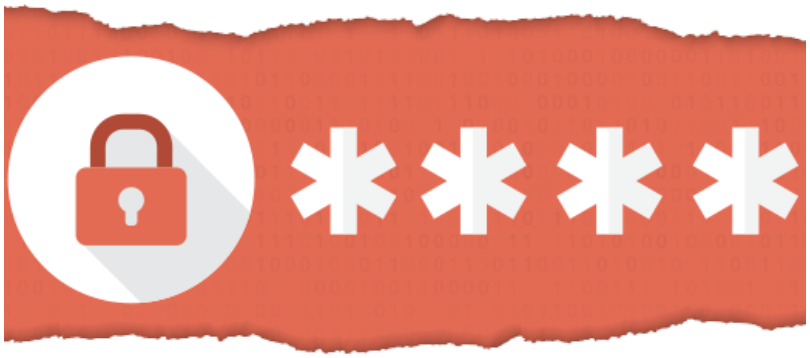
LEGAL MANAGEMENT
THE MAGAZINE OF THE ASSOCIATION OF LEGAL ADMINISTRATORS

Protecting Confidential Client Information in the Digital Age

By Christopher R. Blazejewski



Gone are the days when lawyers could simply practice law without understanding how client information is created, shared and stored. With evolving communication and data storage technology, clients create, share and store sensitive information — from trade secrets and intellectual property to business strategies and legal analyses — in many formats and in many places. Attorneys who are provided such sensitive client information must take certain steps to help ensure that it is kept confidential.

Securing client data and information is critical to protecting the attorney-client privilege and providing ethical legal representation to clients. Attorneys are generally governed by rules of professional conduct that prohibit them from revealing confidential client information without consent. The attorney-client privilege protects confidential communications between an attorney and client from disclosure.

This privilege, however, can be waived when there is no reasonable expectation that the communication will remain confidential. A waiver of privilege grants litigation opponents access to information they otherwise would not be entitled to during the course of discovery.

Furthermore, the legal landscape also continues to change. For example, in 2014's unanimous decision *Riley v. California*, the United States Supreme Court recognized the increased expectations of privacy and confidentiality for communications and information stored and transmitted on cellphones.

Securing client data and information is critical to protecting the attorney-client privilege and providing ethical legal representation to clients.

As the court specifically recognized, "One of the most notable distinguishing features of modern cellphones is their immense storage capacity. Before cellphones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read — nor would they have any reason to attempt to do so."

With cellphones, however, "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet."

In light of the fact that cellphones today broadcast with encrypted digital signals, a court would likely rule that an attorney has a reasonable expectation of privacy in discussions over a digital cellphone.

Today's fast-changing technology increases the risk of potential waiver. Fortunately, the Electronic Communications Privacy Act of 1986 ("ECPA") criminalized the interception of email transmissions and provides that interception does not result in the loss of the attorney-client privilege. Some states, including New York and California, have statutes expressly providing that the interception of email does not vitiate privilege. Cases from federal and state courts around the country throughout the last decade reinforce the protection of privacy and privilege for email communication.

Rulings in these cases have held that electronic communications between counsel and client remain privileged.

KEEPING INFORMATION PRIVATE

With the changing landscapes of law and technology, what can law practices do to protect confidential client information? Firms and practices should create and implement the following policies:

1. An information security policy that covers all information systems, including email, voicemail, text messages, the Internet, computers, work stations, laptops, cellphones, software, passwords, remote access and cloud computing.
2. A social networking policy that covers firm hardware, software and Internet sites, including Facebook, Twitter, LinkedIn, Google+ and other social networking sites. The policy should prohibit transmitting unauthorized information relating to clients or the firm.
3. Document management policies that cover the collection, transmission, maintenance and storage of client information. This should include documents stored in hard copy, electronically or remotely, or covered by a confidentiality agreement or court order, and the policies should be based on the needs of each client.

These policies, if properly implemented and followed, will help law firms protect client information in the digital age.

ABOUT THE AUTHOR

Christopher R. Blazejewski is a Partner at Sherin and Lodgen LLP, with offices in Boston and Providence, concentrating on commercial litigation, professional ethics and business law.

Email
617-646-2023

CHRISTOPHER R. BLAZEJEWSKI
Partner
Sherin and Lodgen LLP