THE ILLINOIS ASSOCIATION OF DEFENSE TRIAL COUNSEL
IDC QUARTERLY

Technology Law

Patrick W. Stufflebeam
HeplerBroom LLC, Edwardsville

Encryption Edition: Be Sure To Drink Your Ovaltine

Technology has come a long way from poor Ralphie's decoder ring in *A Christmas Story*, and as lawyers, we are faced with our ethical duty to safeguard electronic client data, not a "crummy commercial." At its root, however, Ralphie's Little Orphan Annie decoder ring is a perfect example of how encryption works. Today's encryption, however, is light years ahead and should be utilized by all lawyers.

Lawyers know that we have a duty to safeguard client information, including electronic client information. Technology evolves quickly, however, and I think a lawyer's duty to understand the risks and benefits of utilizing technology in your practice, as prescribed in Rule of Professional Conduct 1.1, Comment 8, requires continuous scrutiny.

With the near universal use of email and the growing use of electronic files, lawyers need to be even more mindful of how that information is being protected while being stored and transmitted. Consider the postcard example. How many lawyers would send a postcard to a client with attorney-client information detailing case strategy? How many lawyers would send an email to that client with the same information? Unencrypted emails containing the same information may be the equivalent of sending a postcard.

"A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Ill. R. P. C. 1.6(e). Comment 18 to Rule 1.6 states, "[t]he unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (e) if the lawyer has made reasonable efforts to prevent the access or disclosure."

The Comment continues, "[f]actors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, by making a device or important piece of software excessively difficult to use)." *Id*. Further, a client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule.

"When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy." Ill. R. P. C. 1.6, Comment 19. Lawyers need to understand that not all email is created equal and depending on how the email is sent, it may not afford a reasonable expectation of privacy. A good rule of thumb is to consider everything sent over the internet to be written on a postcard unless you take the necessary to precautions to protect it.

Email is not the only consideration. Consider for a moment where you store client data. On an average day, I work with client data on my desktop, laptop, smartphone, tablet, and possibly a flash drive or external hard drive. Every time I use client data on a device, I ask myself how I am physically safeguarding my client data.

One of the best ways to safeguard data on your devices is by encrypting the devices themselves. Unlike decoder rings, there are many programs that use algorithms that will encrypt devices, *i.e.*, converting any data on the device to ciphertext, making it unintelligible to someone who opens it without having the code to decrypt the data. Such programs are important, especially as some devices are extremely portable and can be lost or stolen. Encryption software is often included with flash drives or external hard drives. Although client data within your office environment may have multiple layers of security to safeguard the data, such security does not always automatically extend to the data once transferred to a portable device.

An everyday example of using portable devices includes copying client documents to a flash drive to be reviewed for privilege before produced and the device encrypted with a password. Even though the portable device is encrypted, the encryption is only as good as the password. Therefore, passwords must also be strong. And, passwords must be remembered. You can write the password down, but you should use a zero-knowledge password manager, *i.e.*, a program (also protected with a password or biometrics) that does not store your master password. Therefore, if the master password is forgotten, all data is unrecoverable. Remember to never keep the password to the encrypted external device with the external device.

Some encryption software also allows for the device to be automatically wiped with all data erased after a certain number of failed login attempts. Such safeguards are also available for most smartphones. As a best practice, all lawyers should consider enabling remote wiping on any phone or external device when the option exists when client data is stored on that device. Smartphones that store client data should also be encrypted. Most smartphones are automatically encrypted if a passcode is used, but with the various hardware and operating systems, you should verify.

Attachments to emails are another consideration. Not only do attachments to emails need to be safeguarded if they contain client data, but also in the event other methods are not available or are cost-prohibitive, you may consider encrypted attachments as a method to communicate with your client, opposing counsel, or the court. Many applications, such as word processors or PDF suites allow you to encrypt that document before transmitting in an email. Again, such a method often utilizes a password, so the same password considerations exist. The other person will also have to know the password in order to access the encrypted document. Do not send the password in the same email as the encrypted attachment protected by that password.

Text messaging with clients is becoming more common. If communicating about sensitive information, a lawyer needs to consider the security of that text. Are you are using the same platform? For example, if both you and your client have iPhones and text through iMessage, those texts are encrypted. If your client, however, uses an Android-based device and you send him or her a message—the blue bubble to green bubble situation— those messages are not encrypted. As security is becoming more important, we have seen the rise of end-to-end encryption messaging apps. Not only are the messages encrypted while in transit, but the messages cannot be decoded by anyone other than the recipient. There are a number of popular messaging apps, but lawyers should investigate whether the chosen app offers end-to-end encryption and whether or not certain metadata is retained by the app developer if that is a concern between you and your client.

I think it is also important to address cloud storage. There are many providers, and some platforms make it extremely easy to store and share information. I have a different inquiry regarding documents uploaded to a cloud service. I may not care if my Bob Marley *Exodus* album is encrypted; I cannot say the same about my client's confidential data. Before

uploading client data, you should consider whether the data is encrypted before uploading and while in transit to the cloud. Note that once client data is placed in the cloud, it is outside the control of your firm where a number of security layers may be in place. Who has access to the cloud service account? Can the IT department access the account? Such a consideration may be important in the event of a terminated employee. Always ask yourself, what client information would be disclosed if the cloud service itself was hacked?

Be aware of your client data at rest. Data at rest is not encrypted. For example, when you have your laptop open and you can read the email you are typing to the client, it is not encrypted. That is a no-brainer. One of the biggest security concerns about safeguarding client data may not come from a flash drive, a weak password, or a hacked cloud service. It could come from the person next to you at the airport lounge or the person, who was unfortunate enough to obtain the C35 Southwest Airlines boarding pass and squeezed into the middle seat next to you.

You should consider how you are actually sending the email once you send it. Although the technical discussion of how emails are actually authenticated and encrypted is beyond the scope of this article, everyone should be cognizant of the risks associated with connecting to and communicating through the internet over an open WiFi connection. If such a connection is all that is available, you should ensure you use software that will automatically encrypt the email before and while in transit to the recipient or make use of a VPN.

Being able to safeguard electronic data is not going away. This issue is a big concern to our clients, and as lawyers, we need to embrace and utilize available technology. Failure to do so and the loss of client data would be just like shooting your eye out.

About the Author

Patrick W. Stufflebeam is a partner of *HeplerBroom's* Litigation and Cybersecurity practice groups. He concentrates his practice primarily on the defense of civil litigation including toxic tort (asbestos, benzene, and mixed toxin), premises liability, product liability, and commercial litigation. Mr. Stufflebeam counsels clients and attorneys regarding cybersecurity and the use of technology in the law. He lives and offices in office in Edwardsville, Illinois (Madison County). He is admitted to practice in Illinois, Missouri, and the Southern District of Illinois. He received his J.D. from Saint Louis University School of Law and his B.A. from Western Illinois University. Mr. Stufflebeam is a frequent lecturer on many topics, most recently on the issues of legal technology and ethics. He is listed as AV Preeminent/Peer Reviewed by Martindale-Hubbel and a 2018 Leading Lawyer in the areas of Product Liability and Toxic Tort. He served as an elected Director of IDC from 2011-2017 and is also a memer of the Madison County Bar Association.

About the IDC

The Illinois Association Defense Trial Counsel (IDC) is the premier association of attorneys in Illinois who devote a substantial portion their practice to the representation of business, corporate, insurance, professional and other individual defendants in civil litigation. For more information on the IDC, visit us on the web at www.iadtc.org or contact us at PO Box 588, Rochester, IL 62563-0588, 217-498-2649, 800-232-0169, idc@iadtc.org.