Alan Romero
ROMERO LAW, APC

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
March 2021

L'eggo my e-mail

THE ETHICS OF RUNNING A SECURE VIRTUAL LAW OFFICE AND TIPS ON HOW TO SECURE YOUR EMAIL COMMUNICATIONS

"Sorry, my email got hacked." How many times have you seen those words from a colleague in your inbox? What some lawyers may not be aware of is that in 2020, the State Bar of California issued Formal Opinion No. 2020-203, which effectively set forth a series of affirmative obligations incumbent upon an attorney who has become aware of an unauthorized disclosure of their electronically stored confidential client information ("CCI"), which consists of all attorney-client privileged communications as well as information protected from disclosure under Business & Professions Code section 6068, subdivision (e)(1) and State Bar Rule 1.6.

While the State Bar makes it clear that lawyers must "take reasonable steps to secure their electronic systems to minimize the risk of unauthorized access," State Bar Formal Opinion No. 2020-203 elucidates what tangible steps the attorney must take in anticipation of, and in the wake of a suspected breach.

The lawyer's duties of competence and confidentiality

The primary ethical duties arising out of the running of a virtual law office are those of competence and confidentiality, as they relate to taking "reasonable steps to secure … electronic systems to minimize the risk of unauthorized access. These affirmative duties become even more acute in the event of a breach, where the lawyer must "conduct a reasonable inquiry to determine the extent and consequences of the breach and to notify any client whose interests have a reasonable possibility of being negatively impacted by the breach."

Reasonable efforts expected to be exerted by the lawyer in protecting CCI invoke the duty of competence (State Bar Rule 1.1), the duty to safeguard client's confidences and secrets (State Bar Rule 1.6), and the duty codified by Business & Professions Code section 6068, subdivision (e)(1), "[t]o maintain inviolate the confidence, and at every peril to himself or herself to preserve the secrets, of his or her client."

The 2017 ABA Cybersecurity Handbook proposes a legal standard for "reasonable efforts" engaged in to protect CCI that adopts "a fact-specific approach to business security that requires a 'process' to assess risks, identify and implement appropriate security measures responsive to those risks, verify that the measures are effectively implemented, and ensure that they are continually updated in response to new developments. (*Id.* at 73.)

What both the State Bar and ABA standards have in common is they require that the lawyer educate themselves of the risks of, and vulnerabilities to, potential CCI disclosure with respect to the unique software and hardware ecosystems used in the lawyer's practice. As each piece of technology in a lawyer's practice holds specific benefits and risks associated with its deployment, it is incumbent upon the attorney to be able to appreciate and properly conceptualize the potential risk for unauthorized disclosure of CCI related to each specific method by which it is stored or transmitted on a device or stored remotely in the cloud.

As a result, every prospective use of CCI should be subject to a pre-deployment risk-benefit analysis in order to maintain best practices relating to data security. If the lawyer is incapable of adequately evaluating the risk posed by a particular use of CCI, both prudence and the State Bar dictate that competent data security experts be employed to evaluate the risks of unauthorized data extrusion and configure systems and devices with security policies that have the best opportunity to avoid disastrous breaches of CCI data. This obligation that lawyers be possessed of a basic understanding of technological risks is the foundation of this area of ethics, as lawyers cannot satisfy their obligation to intelligently evaluate risks, if they do not understand the full scope of these risks.

State Bar Formal Opinion No. 2020-203 sets forth the proposition that "[s]ome security precautions are so readily available and user-friendly… that failure to implement them could be deemed unreasonable." Some of these tools such as remote device management (the ability to track/erase a laptop or phone remotely), encryption, virtual private networks (VPNs), biometrics, or Two-Factor Authentication, require little technological expertise and yet have the potential of increasing data security exponentially. The use of stronger, randomized passwords via password management utilities is another option that significantly increases CCI data security, even more so when combined with some of the other tools referenced above.

Further, lawyers in management roles have the obligation to implement adequate data security protocols within their legal organization "to protect confidential client information from the risk of inadvertent disclosure and data breaches as a result of technology use, which includes monitoring the use of technology and office resources connected to the internet and external data sources." (ABA Formal Opinion No. 18-483.)

ABA Formal Opinion No. 18-483 further describes three basic categories of "reasonable efforts" that lawyers must undertake in terms of ensuring best practices with sensitive CCI data. First, there is a duty to have monitoring tools in place to determine when and if a CCI breach has occurred. Secondly, when a breach is reasonably believed to have occurred, lawyers must take prompt and reasonable steps to prevent or mitigate the damage caused by the breach. Finally, lawyers must have the means available to assess the nature and scope of the breach.

The lawyer's duty of disclosure

"Sorry, my email got hacked," triggers a number of affirmative obligations upon the lawyer, most importantly the obligation to keep any potentially affected client "reasonably informed of significant

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
March 2021

developments" arising out of the representation, as contemplated and set forth by State Bar Rule 1.4(a)(3) and Business and Professions Code section 6068, subdivision (m). Then, as the State Bar ominously advises: Consider notifying your insurance carrier about a potential claim arising out of the data breach.

A "data breach" is defined by the ABA as a "data event where material client confidential information is misappropriated, destroyed, or otherwise compromised, or where a lawyer's ability to perform the legal services for which the lawyer is hired is significantly impaired by the episode." (ABA Formal Opinion No. 18-484 at 4.)

Part of the "reasonable efforts" taken by the lawyer to minimize the risk of unauthorized access to CCI data is the ability to utilize software utilities to identify abnormal network traffic or unusual read/write activity with respect to protected CCI computer files. Upon ascertaining that a break has, or potentially has, occurred, the lawyer must undertake efforts, or have a qualified expert undertake such efforts, to "ascertain, among other things, the identity of the clients affected, the amount and sensitivity of the client information involved, and the likelihood that the information has been or will be misused to the client's disadvantage." (State Bar Formal Opinion No. 2020-203 at 7.)

In the event of a suspected data breach, the breadth and scope of the breach must be accurately ascertained. Any clients likely to have had their CCI exposed by the data breach must be promptly notified of the nature of the data breach, and the extent to which their CCI has been exposed, damaged, or otherwise tampered with. "When in doubt, lawyers should assume that their clients would want to know and should err on the side of disclosure." (*Ibid.*) Additionally, an affected lawyer may have additional statutory obligations mandating disclosure of a data breach pursuant to Civil Code section 1798.82, HIPAA, or other applicable laws in jurisdictions where the firm operates or collects data from.

In the event of a data breach, the lawyer, after taking immediate corrective action to block the intrusion pathway, should promptly notify affected stakeholders in order to allow them to take steps to mitigate the potential harm of the data breach. Stakeholders such as clients have the most to lose and should be notified first. However, communications between your office, co-counsel, or other interested parties may now be in the hands of hostile actors, so plan for the best, but prepare for the worst. Some professional liability policies (e.g., Lawyers' Mutual) contain included "cyber insurance" endorsements, and there is no better time than the present to check whether your policy includes such coverage.

Two-Factor Authentication

Breaching email security is surprisingly easy. In fact, there are likely a great number of U.S. attorneys who are presently having their email traffic monitored by malicious actors without their knowledge. Fortunately, a variety of security enhancement tools exists, specifically designed to prevent these malicious actors from easily gaining unauthorized access to sensitive data.

Two-Factor Authentication ("2FA") is an additional security step that makes it very difficult, or nearly impossible to access your protected account without access to a secondary security token. Although there are different types of 2FA tokens, the types of 2FA tokens that are more commonly used are: (1) a text message to your phone; (2) a random number generated by an "authenticator" app on your phone (e.g., Google Authenticator, LastPass, Authy); or (3) a push notification requiring your approval to your phone via an installed app on your phone (e.g., Google app, Microsoft Authenticator, or the built-in 2FA features of iOS).

The simplest type of 2FA requires that you input a numerical code that is text-messaged to you when you are logging in. This ensures that the only persons who can access your email account are those who have physical access to your password-unlocked phone. This is a good form of 2FA, but isn't foolproof, as there have been high-profile cases of hackers getting cellular phone providers to transfer your phone number to their control to bypass this added layer of security afforded by 2FA. While this is an extremely unlikely occurrence, it is not outside the realm of possibility. This is a great layer of security, but not the best.

A stronger type of 2FA is available from many service providers including Google (Gmail), Microsoft (Office, Teams, etc.) and involves an authenticator app installed on your phone. This authenticator app, once set up correctly, generates random numbers as "onetime passcodes," which are only valid for a brief period of time (20 seconds or so), and serve as a secondary password in order to get into your account. The use of an authenticator app has an added security advantage over SMS-based authentication in that a malicious actor who might hijack your phone account from your wireless carrier would nonetheless be denied access to the contents of one's authenticator app residing securely and password-protected on their mobile phone.

Using an authenticator app from Microsoft or Google also allows you the option, once enabled in the applicable settings, to allow for a push notification every time a new device attempts to log in to your account. This feature is convenient in that it does not require the extra step of typing in the random numbers generated by your authenticator app, but rather, just allows you to click a popup notification on your phone which asks if you want to allow access.

Arguably, the most secure type of 2FA is a hardware security key from companies such as Yubico, Titan, or Thetis. The use of a hardware key has an advantage over use of software apps in that they are more secure and less susceptible to being exploited by malicious actors. Instead of clicking on a notification popup or entering in a generated number, the physical key acts just like a key that you would use for your home or office: you insert the physical USB key into the

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
March 2021

computer that you are using to access the service. Newer offerings from Yubico allow NFC, or wireless, communication from the physical key to a phone. This option is the best for journalists, or activists concerned about surveillance by authoritarian governments. The downside, however, is that if you lose your hardware key(s), you may be locked out of, an email account for example, forever. If you are being monitored by government spies, using a physical token may be a necessity. For everyone else with business secrets to keep and confidences to maintain, using an authenticator app, or SMS 2FA, will likely be amply sufficient.

In the avoidance of doubt, enabling 2FA will protect your email from 99.99% of malicious actors trying to gain access to your privileged communications in order to gain an unfair advantage in litigation or engage in other nefarious activity. The only people able to access a 2FA-enabled email account will have to: (1) know the correct password; and (2) have physical access to a phone associated with the account that has been separately password-unlocked.

Who are the bad actors?

There are two types of bad actors that 2FA seeks to block access to. The first type are those who use infected links in emails (or Facebook messages, etc.) or virus-laden attachments in order to steal login credentials. These bad actors will generally use the compromised email account to spam others with infected links via email. This is the most common type of bad actor, and the one we hear about the most, usually by a colleague sending a follow-up email saying, "I was hacked, don't click on the link I sent you yesterday." This compromised email user, all but certainly, did not have 2FA enabled on their email account. By not enabling 2FA, a third party inevitably obtained the user's password through one of various hacking methods in order to gain control of the account and ultimately attempt to further propagate the email compromise campaign. The motivation behind this type of campaign is solely short-term financial gain.

The second type of bad actor is the scariest one. These bad actors are not directly motivated by financial gain, but rather by having access to an attorney's confidential communications. You will not hear about these types of intrusions very often because the intrusion depends on surreptitiousness and avoiding detection. The longer the intrusion goes undetected, the more serious the breach and the bigger the payoff for the intruder in terms of access to proprietary information. If one hasn't changed their email password for a long time (6 months or more) and does not presently have 2FA enabled, one would be totally unaware that the entirety of their email traffic is being externally monitored. While there are other tools that email providers offer to try to mitigate this risk, such as showing the locations and/or IP addresses of recent logins, there is no substitute for good password (changing) policies and having 2FA in play.

How to set up 2FA

(1) 2FA requires minor setup. However, most providers make enabling and implementing 2FA incredibly simple, largely because they benefit from reduced customer service resource expenditure in the event of account breaches. Setup takes a few minutes and will usually require the installation of an authenticator app on your phone. Setup protocols vary, but not by much.

(2) 2FA requires that you log in to your service anew at least once every 30 days. This login will require that you provide a number generated by your authenticator app (or sent to you via SMS, if your provider utilizes this protocol), or click on a notification popup on your phone, if you have set up this feature.

(3) Signing in from a new device will require that you use 2FA to gain access to the account, to ensure that you are the one signing in from the new device. But really, it is inaccurate to characterize this as a "downside," when in fact restricting logins from new devices is really the primary purpose of using 2FA to begin with. Someone initiating unauthorized access to your accounts will all but certainly be doing so from a new device.

In reality, the added inconvenience occasioned by 2FA is minimal to the point of being nearly inconsequential in light of the layer of added security that it provides; in fact, the duties of confidentiality inherent to legal representation both as a concept and a practice, make the use of 2FA with email accounts almost a requirement. As technological threats to the attorney-client privilege continue to evolve, it is the interests of the client that are paramount and the long-term habits of their counsel should be secondary in comparison.

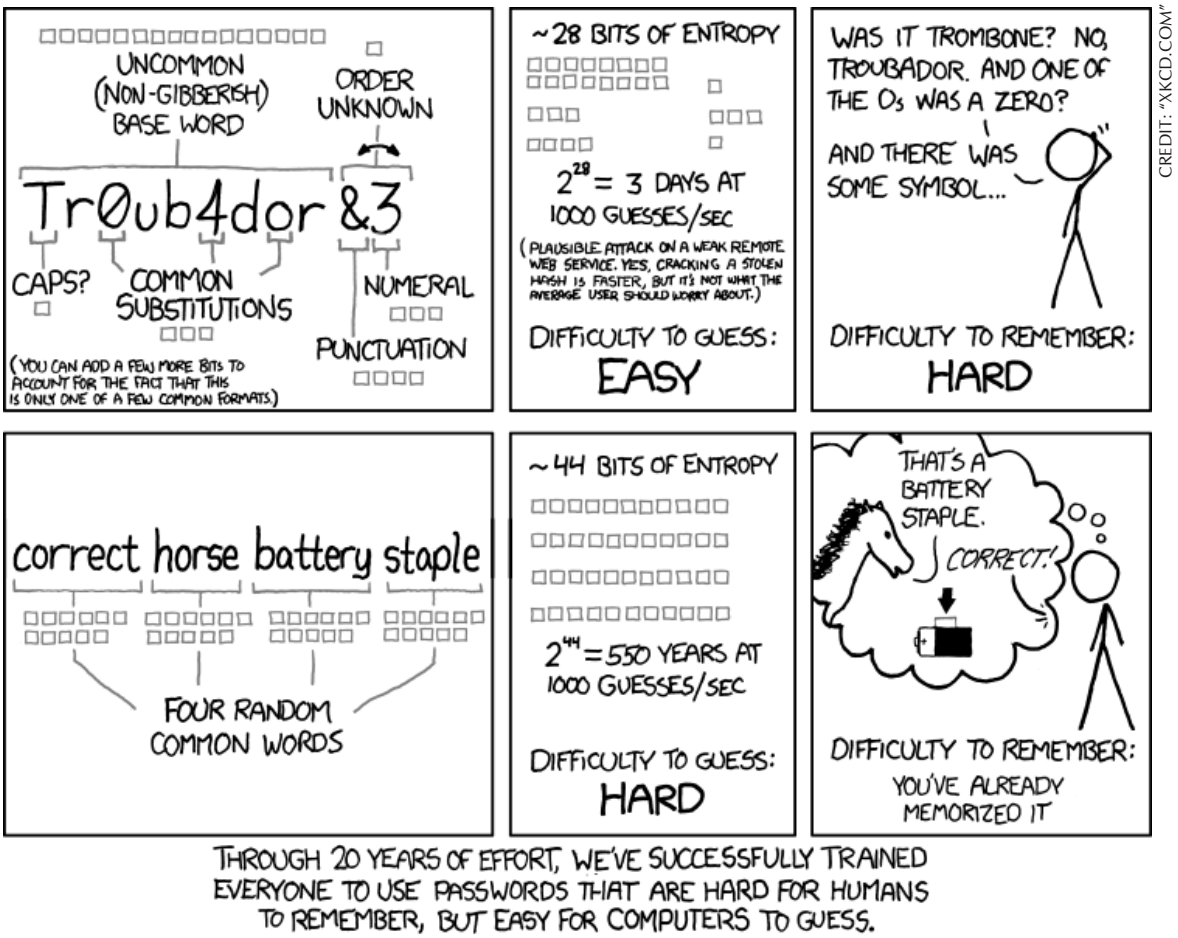
Enabling 2FA on your important email, banking, cloud storage, webhosting, and domain name registrar services will add a tremendous layer of security and help prevent very bad things from happening. Luckily, many financial institutions already require 2FA (call or SMS) for added security.

Using password managers to create and manage complex passwords

Password managers are one of the easiest and most trusted ways of turning your CCI trove into a hardened target. Password managers can be accessed via a browser, an app on a phone, or as a plugin in your usual web browser. A password manager requires you to remember one complex master password, and when entered, provides you access to a library of all your stored login credentials and password for other sites. This is incredibly useful as the user is no longer required to remember passwords for different sites, instead automatically storing long passwords of randomized characters.

This has the benefit of not only increasing the complexity of passwords, but maintains good password hygiene by avoiding the reuse of passwords across different webservices. While this may sound cumbersome in the abstract, once you begin using a password manager like LastPass, Dashlane, or 1Password, you will wonder how you survived without it. Website login credentials will be automatically saved once you install the browser extension, and login info will be

Journal of Consumer Attorneys Associations for Southern California
ADVOCATE
March 2021



CREDIT: "XKCD.COM"

automatically populated once you revisit the site, resulting in the closest you will get to a seamless experience while maintaining a reasonably high degree of security. Adding additional security measures such as 2FA, or biometric access (on the phone app or on a compatible workstation) will only serve to increase the level of CCI security exponentially.

Conclusion

Times are changing, and they are getting more and more dangerous for our clients, whose CCI we are entrusted with. With digital storage technology becoming more and more ubiquitous in our practices and our lives, it is important that we achieve and maintain technical competence with the various programs and data storage media that tend to blend so seamlessly into our practice of law. It is this seamlessness that begets complacency, which makes our "reasonable efforts" to protect CCI data so much more critical in the new practice of law. Educating oneself as to the relative risks and benefits of various programs and (cloud) storage media is no longer optional in the current threat environment.

The good news is that the utilization of simple, user-friendly security tools such as 2FA, password managers, biometrics, and remote device management will drastically reduce the likelihood of a data breach. Encryption tools, which were once the exclusive purview of the military and academia, are now freely available on consumer grade computers (e.g., Microsoft BitLocker included with Windows 10 Pro). In the data arms race, as threats have evolved, so have the defenses. And as many of the best defenses now require very little technical expertise to deploy, there are no good reasons to not integrate one or more of the robust security tools herein discussed into your new, more secure, virtual law practice.

Alan Romero is the principal of Romero Law, APC, *an employment litigation firm located in Pasadena. His practice focuses primarily on representing whistleblowers against government entities and the litigation of Lab. Code § 1102.5 and FEHA claims. Alan is a graduate of Southwestern Law School's SCALE program and was a CAALA 2020 Trial Lawyer of the Year finalist. The author can be contacted directly at ajr@romerolaw.com.*