JANUARY 22, 2018

Legaltech© news

ONLINE

An ALM Publication

Better SAPHE Than Sorry: Data Security in Document Productions

Introducing two specific opportunities providing greater protection in data productions, both of which could thwart some of the greatest ongoing cybersecurity threats.

BY FARRAH PEPPER AND MARC ZAMSKY

Cybersecurity is *so* hot right now, to borrow a phrase from Derek Zoolander, eponymous lead of the modern comedy classic "Zoolander." Phishing, hacking and ransomware—oh my—are all-too-familiar tactics engaged by the nefarious, making data protection top of mind for corporations and their counsel. Cybercriminals want your data and in response, companies are investing more than ever to ensure that their data is safe, secure and immune from attack.

Enter the lawsuit, where the exchange of information during discovery is a necessary evil. Suddenly, corporate data you valiantly protected now sits outside the firewall, beyond your control in your adversaries' environment or, worse, on a USB flash drive sitting on—or off—their desk.

Why this departure from data protection protocols? If one were to read the legal industry's mood ring on security in document productions, it might skew "complacent." Years of status quo production formats and methodology have been mutually accepted, even though unintended consequences can include broader exposure of client data to cyber threats and a lack of ongoing control after the data is produced. Nevertheless, neglecting client data vulnerability post-production is arguably at odds with ethical obligations and out of step with technology solutions already available, not to mention the general temperament in the market.

Why spend so much time, effort and energy protecting data when such efforts could ultimately be undermined by document productions? This article explores two specific opportunities providing greater protection in data productions—in terms of adopted standards for production hosting, and a new production format—both of which could thwart some of the greatest ongoing threats.

Rules of the Road

Keeping client data safe is not only sound business, but also ethically sound. In assessing the security framework for document productions, three roads converge—the Federal Rules of Civil Procedure (FRCP), the Model Rules of Professional Conduct and ABA Opinion 477R. Put together, they suggest a producing party's inherent right to data security coupled with counsel's ethical obligation to ensure confidentiality of client data.

Federal Rules of Civil Procedure: Physical productions under FRCP Rule 34 have become relatively routine, although, per Rule 34(b)(2)(D), a producing party still maintains the right to object to the form of production as requested. Courts often afford additional protections under Rule 26 by ordering production limitations, such as protective orders, confidentiality or "attorney-eyes-only" designation.

Model Rules of Professional Conduct: Now juxtapose Rule 34 with Model Rule of Professional Conduct 1.6(c) (adopted by 28 states and buttressed by California ethics opinions), which states that professional legal competence must encompass technical "know-how." Comment 18 to Rule 1.6(c) requires "a lawyer to act competently to safeguard information relating to the representation of a client" against unauthorized access or inadvertent or unauthorized disclosure.

ABA Opinion: ABA Formal Opinion 477R recently recognized that in a world where hacking and data loss are increasingly likely, the American Bar Association would adopt a requirement for counsel to "assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continuously updated in response to new developments," including an understanding of how client information is "transmitted and stored." This tracks with the ethics opinion issued by 19 states (and counting) that articulate a lawyer's duty to assess a cloud vendor for security protocols and its ability to safeguard client confidentiality. Together with ABA Model Rule 5.3 (Responsibility Regarding Non-Lawyer Assistance), there appears to be a nondelegable duty for counsel to ensure client data confidentiality, including when a lawyer engages a third party to host client data.

Keep Client Data SAPHE and Sound

Accepting the premise that there is an ethical obligation for counsel to ensure client data is protected, then the question becomes: What more can reasonably be done to ensure data protection beyond that which routinely occurs today via physical productions of data to requesting parties?

In "Zoolander," the titular lead character had a signature pose that made him a top model and, somewhat inexplicably, prevented an assassination and international incident. If only it could be that easy to "save the day" when protecting data from neglect or misuse in document productions. But, what if it could be that simple? Your authors submit the following straightforward yet novel ideas for consideration, which even a graduate of the Derek Zoolander School for Kids Who Can't Read Good should find compelling.

First, consider the adoption of new security standards for production hosting. Picture a new standard, specific to the legal industry, with a moniker such as "SAPHE" (pronounced "safe"), for Secure Access Production Hosting Environment. Receiving parties would then have to demonstrate that data would be hosted in a SAPHE-compliant location. In other words, keep it safe and in a SAPHE.

While many organizations have already developed their own internal security standards for third-party data hosting and the Association of Corporate Counsel (ACC) offered guidance on managing one's own vendors in 2017, it is high time that there be industry consensus on a minimum baseline level of data security in a hosting environment afforded to every production. SAPHE would include standards and protocols for data encryption, physical and logical data security, restricted access and password protocols, intrusion detection software and monitoring, along with penetration testing, adequate firewall protection and—so producing parties can maintain control of their data at the close of a matter—data destruction and return protocols. Data center controls exist in many forms, certifications and compliance levels, including SOC and SSAE, while regulatory mandates may require HIPAA, ITAR or GDPR compliance, and specific industries may require even heightened levels for certain data, such as PCI, ISO and FedRamp; so why not SAPHE for data productions?

Where ABA Formal Opinion 477R only issued broad "guidance," at least one organization, the Legal

Cloud Computing Association, has taken a first step of publishing cloud hosting standards for the legal industry, and others are likely to follow. While production hosting standards themselves may require some further deliberation to reach consensus—as well as whether SAPHE is best positioned as a third-party or self-certification model—everyone should at least be able to agree that the days of the "broom closet server" or the "lost thumb drive" for post-production data should be history.

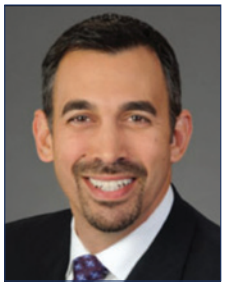
Second, corporate data subject to production can be "watermarked" such that data is identifiable as a production and traceable in the event of impermissible disclosure. Behold, we introduce the "Pepper Mark" (named for one of our authors and following in the footsteps of Edwin G. Bates, inventor of the Bates Stamp). Like the Bates Stamp adorning the footers of productions, the Pepper Mark would be a permanent watermark placed faintly and diagonally across the production page indicating, for example, the name of the requesting party, the production number, date and other identifying information.

The Pepper Mark then acts as a cybersecurity protection in two ways. First, by assigning personal accountability, it is a blatant deterrent to the receiving party to allow mishandling of data (a "Pepper Spray," if you will). Second, even if that deterrent failed and data were then published after a hack or leak, it could be traced to the source, and appropriate remediation could be pursued. (This may or may not include a trail of colleagues following the offender around, "Game of Thrones"-style, clanging bells and chanting "shame!") While a new concept for document productions, such watermarks are common in due diligence reviews, corporate board materials and, in a recent high-profile matter, a printer watermark even helped track down an NSA leaker. Let this article be a call to action to discovery software vendors to make the Pepper Mark an easily accessible feature for productions.

It is critical that corporate data is protected, not just internally, but when data productions are required outside the firewall. There is an inherent right for a company to control and protect its data and, further, to be able to remediate data in compliance with corporate policy when no longer needed. A reasonable approach, and one supported by both the rules and legal ethics, is to ensure document productions are marked and identified, and hosted in a secure, controlled and safe environment, where diligence against attack and theft is maximized and risk is minimized, without prejudicing receiving parties. This could readily be ensured without court intervention through artfully crafted language in an ESI agreement, along with the adoption of new standards.

Much like Derek Zoolander, who broke out of his rut when he discovered there was more to life than being "really, really, really, ridiculously good looking," it is time for parties to break the cycle of complacency with existing document production standards. Let us all open a dialogue about the best ways to protect our data in this new era of global cyber challenges.

Farrah Pepper *is an award-winning attorney with deep expertise in discovery, legal technology, data life cycle management and information governance. Pepper is experienced in building and leading in-house and law firm teams, including the GE Discovery COE in her role as GE's first Executive Counsel—Discovery and the e-discovery practice group at an international Am Law 100 firm.*



Marc Zamsky *serves as Chief Operating Officer of Compliance Discovery Solutions. Zamsky is responsible for leveraging Compliance's strong history in managed review and delivering eDiscovery Technology Services, including Compliance's revolutionary Discovery-as-a-Service, or "DaaS" Platform, built on Relativity, Nuix and Brainspace. Compliance is a division of System One Services.*