

INFORMATION LAW JOURNAL

A Publication of the Information Security and IoT Committees
ABA Section of Science & Technology Law

AUTUMN 2017 VOLUME 8 ISSUE 4

EDITOR/FOUNDER: THOMAS J. SHAW, ESQ.

The Horde is Over the Gates and in the Tower: Defending Against a Discovered Zero-Day

By [Christopher Land](#)

Just over two years ago as summer was taking hold in Cape Cod, the Woods Hole Oceanographic Institution ("WHOI") uncovered a coordinated attack by a foreign entity; a so-called advanced persistent threat ("APT" for short) had breached its network and infiltrated sensitive research files. WHOI (pronounced [Read more](#)

How Knowledge Integration Platforms, AI and Machine Learning Help the Duty to Preserve

By [Daniel Meyers](#), [Salim Elkhoul](#), and [Joseph Pochron](#)

The IT infrastructure of businesses today is no longer limited to behind-the-firewall servers and enterprise appliances from traditional providers like Microsoft and IBM. Modern employees demand the ability to access their workspace and collaborate with colleagues in dynamic, diverse environments that can be [Read more](#)

Addressing the Evidentiary Challenges in Proving the Authenticity of Digital Records

By [Tim Reiniger](#)

Distinguishing authentic digital records from those that are forged is a central evidentiary challenge in the digital environment. This concern is complicated by the untestable and ephemeral nature of digital data, the ease and pervasiveness of copying digital information, and ubiquity of network access to digital documents. [Read more](#)

New York Quietly Relaxes In Camera Review Requirement for Social Media Discovery

By [Joseph Francoeur](#) and [Sean Geary](#)

Why should the courts have to undertake the burden of evaluating *in camera* a party's social media account to determine what information is relevant and discoverable? New York's Appellate Division, First Department asked that very question in 2015. In *Forman v. Henkin*, the majority responded to the dissent's [Read more](#)

Lessons and Practical Guidance from the Target Data Breach AG Settlement

By [Aldo Leiva](#)

On May 15, 2017, Target Corporation executed the Assurance of Voluntary Compliance¹ ("Settlement Agreement") with the Attorneys General of 47¹ states and the District of Columbia, thereby settling all civil claims that had been brought against Target by the Attorneys General, arising out of the Target Data [Read more](#)

****Editor's Message****

We are concluding the eighth full year of publishing the *Information Law Journal* each quarter, continuing to welcome authors and readers from across the ABA. This issue again presents articles focusing on various aspects of leading-edge domestic and international practice in information, Internet, and emerging technologies law. Nearly 200 authors have written for the *Information Law Journal* and its antecedents. Six authors are writing here for the first time.

Our next issue (Winter 2018) is scheduled to be published in December 2017. All readers of the *Information Law Journal* may share their experiences and knowledge with their fellow professionals by writing an article. Every qualified submission within the scope and requirements as explained in the [Author Guidelines](#) will be published. The issue following the next issue (Spring 2018) is scheduled to be published in March 2018.

The Horde is Over the Gates and in the Tower: Defending Against a Discovered Zero-Day Cyber-Attack While Protecting Your Intellectual Property and Research and Academic Integrity

By Christopher Land



Just over two years ago as summer was taking hold in Cape Cod, the Woods Hole Oceanographic Institution (“WHOI”) uncovered a coordinated attack by a foreign entity; a so-called advanced persistent threat (“APT” for short) had breached its network and infiltrated sensitive research files. WHOI (pronounced “who-ee” by those who know and love it) was not the first, and definitely will not be the last victim in the international intrigue of cyberwars. Countries such as Russia and China are seeking intellectual property, trade secrets, government information, and research data on global hotspots. This attack occurred just as the US government declared cyberattacks a national threat and emergency. Executive Order 13694 of April 1, 2015. Attacks that are growing in size, sophistication, and number of victims.

Universities and academic research institutions are key targets of these attacks. They comprise a perfect storm of vulnerability and valuable information: great minds and big projects working under a strong and respected tradition of open academic process, and often with individualized networks without centralized IT control. Balancing the demands of an open access and transparent academic organization, while protecting national security interests, takes careful coordination, planning, and oversight. This article will provide suggestions on how to develop an action plan, how to roll it out, and how to weigh the competing needs and interests of an academic institution pulled into an international cyberwar.

When—not if—your company, research organization, or university has a significant cyber breach, planning and organizing the counterpunch will be your key priority. Assessing the damages can be done after the fact. For a private research and scientific organization such as WHOI, knowing what was accessed was secondary to knowing the extent of the breach, planning to stop and plug it, and then developing a solid rollout plan for recommended remediation and media fall-out. An attack from an APT is no mere “Nigerian bank” spam attack; an APT is a highly skilled hacker or team of hackers, sometimes sponsored by foreign governments, foreign military, and/or intelligence services. An APT intruder tries to get into your network, avoids any detection software system/s, and quietly lurks around creating back doors, new means of access, and rewriting codes to hide its footprints on how it may extract information. An APT can lie hidden, slowly moving around your system, trying not to trip any network security alerts by only having occasional and small extractions of data, while it explores and builds its own infrastructure in your network. Like a ninja, slowly building traps, hidden back doors, and holes in your organization without you knowing. It is insidious and menacing.

The attack on WHOI was a so-called zero-day vulnerability by an APT. A zero-day is an unknown threat to your software, hardware, or network that can create complicated and systemic breaches before anyone realizes something is wrong. It is a breach, from a sophisticated attacker, that is not yet publicly known or patched. WHOI was subject to a zero-day attack by an APT located in China. They were highly sophisticated and knew what they wanted and how to navigate the system. The attack resulted in significant media coverage and attention from local media, as well as NBC, Fox News, and the online Quartz magazine. See, *Woods Hole Oceanographic Institution Says Hack Linked to China*, NBC online (10/16/2015); *Woods Hole Oceanographic Institution targeted by cyberattack*, Fox 25 Boston News online (10/19/2015); *One of America's premier research institutions was hacked—and the signs point to China*, Quartz (10/16/2015). If you suffer a zero-day attack or have a network vulnerability exploited by an APT, here I provide the steps and the questions we asked and suggest this might provide a framework for any entity.

Legal Take the Lead - Upon receiving notice from the head of WHOI's IT, I brought the entire project under the command and auspices of the General Counsel's office, with day-to-day management left to the head of IT and IT's cybersecurity team. Changing a team's project report structure can be no small matter depending on a company's culture. But besides making certain action discussions subject to attorney-client privileges, it also provides gravitas to the issue, and third-party oversight that reduces the chances of an internal IT team hiding past mistakes, and a solid structure for mixed-asset, cross-team collaboration.

Know Your Response Team - The next call was to outside counsel who had experience in cybersecurity and national security matters. Luckily when I was still at a firm, I had worked with a partner with such experience, Gus Coldebella. Gus ran a task force on cybersecurity in the Department of Homeland Security before going into private practice. The point here is, know your cybersecurity team before "it" happens. Gus and I were on the phone five minutes after I got my initial call, and we were all meeting in my office the Monday morning after. Also, know your IT team; I try to meet with WHOI's IT and the cybersecurity team once every two or three months to review security issues and developments.

Cyber Insurance: Buy It – According to one survey, less than 30% US companies have bought cyber policies, despite the increased assaults in the two to three years. *Cyber Insurance Market Watch Survey*, The Council of Insurance Agents and Brokers (10/26/2016). That 70% of American companies are exposed seems staggering considering the major news worth attacks on companies such as Target, Sony Pictures, Penn State, and the list goes on. There are plenty of good articles on the best cyber policies, and this is a still largely unsettled field of insurance that continues to quickly develop. Further, there are numerous options on such policies, and much the topic of options requires a much more involved review than can be addressed here in this article. Whatever your policy covers, however, make sure that it includes expenses for hiring outside IT consultants, a response team, cyber legal experts, and maybe even public relations firm. WHOI had not yet placed such coverage, for various reasons including cost, coverage was very unclear in 2014, we did not hold or retain third-party

Personally Identifiable Information, and therefore exposure and liability was unclear. As such, when the breach was discovered, we were scrambling to hire a third-party consultancy firm. If you have a policy in place already, then you should establish a rapport with the IT cybersecurity experts early, have regular calls, and see what proactive assistance they can provide. Despite not having a policy, our IT team worked quickly – within days – to get a cybersecurity consultant firm on site.

Stay Dark and Assess the Threat – Within days, the project task force team met to lay out our plan. With an advanced and sophisticated threat, we were advised not to begin remediation until the threat was known and uncovered completely; only then should we shed light on it. This process of knowing and uncovering the depth and level of the attack may take a couple of weeks. This means your system remains vulnerable.

Therein lies the risk balance. If the APT is not fully understood, back doors into your network could be left open and exploited when you think the system has been protected. But if the APT is left in your system while you hunt for it, you could be left vulnerable to extraction of more data and IP. We balanced this by leaving our system running, not indicating we had found the intruder, and watched the APT movements. We had protocols in place to shut down if the threat was after key data. In our case, if the APT set sights on Personally Identifiable Information (“PII”), or Sensitive Personal Information (“SPI”), or accessed sensitive intellectual property, we would take the risk and shut down the APT and any transfer of data immediately. WHOI develops cutting-edge robotics systems and autonomous vehicles, and data and research are our crown jewels of our IP and a hot industry. A thief could not be allowed to walk out the door with them.

To successfully manage this risk of loss of key data requires having a solid plan and protocol in place on when to stop the APT, due to the value or legal risk of the data being compromised compared to the risk of the APT knowing you have located them before you have completed remediation readiness. While pulling up the drawbridge too soon has the risk that not all backdoors have been located, you have to know when that risk weighs less than your property value or potential liability.

Loose Lips Sink Ships (as does email and voicemail audio files) – At the initial assessment we knew what we did not know: how many systems, files, directories, databases, and email systems were compromised. So, we initiated drastic secrecy security protocols. No emails about the project. No phone messages. Almost all communication was conducted via voice phone or encrypted systems with added security precautions.

In addition, we also kept to a minimum those who needed to know about the attack and the remediation plan. The bare minimum. We informed the Chairman of the Board and the Chair of the Audit and Risk committee, but no other board members. Internally only the project team (composed of IT, legal, and facility security), the Vice President overseeing IT, and the President of the Institution

were informed. No other VPs, departments, or leadership levels were briefed (except for two others carefully chosen, described below). The risk was too great.

This did carry some independent internal risk. As an academic research institution, the department heads (who head the various divisions) form the primary deliberative body of the Institution. In other words, while the Vice Presidents implement strategy and day-to-day management, strategy itself is typically bottom-up and driven by the researchers and scientists. Leaving them out of the process, thereby risking alienating the key constituent body who makes most institutional decisions, could again threaten levels of trust, but also undermines a successful rollout plan. To mitigate that risk, however, we briefed two senior researchers whose departments were at risk and apparently targeted in the breach (from what our initial IT assessments could indicate) and who had security clearances. This seemed like the best-balanced approach, given the situation. It was important to keep the circle small but include leadership who could be affected and who could add value and insight in perfecting a rollout plan that could affect the researchers. As with any new process, getting the thoughts on how a process – before it is actually implemented – could impact those it was directed at is invaluable. The hypothetical issues raised by these department chairs and researchers were key in making a plan that worked.

While IT Assesses, You Plan – During our weekly meetings (which did not appear on our Outlook calendars or were given a false project name), IT and our IT consultants briefed us on what they learned and had been working on, and then we developed what our public rollout and remediation strategy would look like. This was no easy task for a research institution with scientists, engineers, students, and researchers in the field around the world. We had to overcome significant coordination hurdles to execute a major remediation event on one single day, globally, and within a few short hours. That was deemed necessary by the consultants because if a single user failed to update the systems or passwords properly and timely, the APT could re-enter the system. This required taking the entire network offline, with no warning, for six to twelve hours. Imagine being the person responsible for taking your organization's entire network offline with no warning to any of its departments, divisions, workers, or researchers. You will want that to go smoothly.

IT developed a careful technical schedule for the offline remediation, laying out the steps to be taken, and when. But the technical aspects are just a small part of the problem; you also have the risk of a general panic and major disruption of operations. When remediation starts, there cannot be long wait and a busy signal for the help desk, unknown deadlines will be on that day and so the system has to be back up and running fast. Not only would a failure disrupt operations for potentially days or weeks, it could also destroy trust between operations and the program team. At WHOI, that damaged trust would be among our researchers and scientists, and it would not be quickly or easily repaired. Doing it right will be easier. We developed and prepared a number of actions/initiatives to be deployed at zero-hour:

- Staffed additional IT professionals (both from WHOI and with the contractor).
- Added operators and a phone bank to take calls and run people through the process of updating passwords.
- Developed procedures to confirm employees were validated and authentic.
- Created an internal landing page that would direct people to validate and then update passwords.
- Prepared a short but cryptic message for outside users attempting to access the internal the system.
- Drafted a media statement and media plan.
- Posted pre-printed informational flyers throughout the campus.

Coordinate with Federal Authorities – To many general counsels, inviting federal law enforcement or other interested entities may seem fraught with other risks. But this is an area where their expertise, assistance, experience, and knowledge can be a great help. You can balance to what extent you let them under the curtain if there is potential for compliance, liability, or regulatory issues, but some level of discussion or coordination is advised.

In the end, despite many worries that it would be a disaster, the remediation plan worked nearly flawlessly and with little concern or complaint. We have, by all accounts, successfully excised the APT and updated our systems, and we continue to monitor and upgrade. Less than two months after WHOI's remediation efforts in October 2015, Chinese nationals were arrested for attacks on the federal government's office Personnel Management. *Chinese government has arrested hackers it says breached OPM database*, Ellen Nakashima (Washington Post, 12/5/2015). And just this month, China's Ministry of Education announced plans to further build its cyber expertise that would result in a so-called "Cyber Army." *'Cyber Army': Beijing Raising a New Generation of Digital Wizards* (Sputnik, 8/18/17). The cyber threat is never-ending, ever evolving, and only growing, but we hope that with good preparation, solid forecasting from leadership, and vigilance, we are even better prepared to deal with future threats.

Some other key takeaways I might share:

- **Turn attack into opportunity.** This is a good time to invest in needed cyberinfrastructure or changes. If your legal department has been pushing for increased IT infrastructure, IT security experts, or insurance coverage, use this as your cudgel. If there is a problem

department or area resistant to change, this can be the motivation and the argument for that change.

- **Coordinate at base level of the organization.** We brought in all lead supervisors of the administrative assistants the day before zero-hour to brief them and answered questions. We met at 4 p.m. the day before the rollout to mitigate the risk of an inadvertent leak; however, it also allowed them to know what was happening, to inform their teams, and to help roll out the program.
- **Tabletop and meet.** Running a breach exercise and discussion of these issues with your likely project team is priceless. Bring in your outside experts to do the exercises with you, it is worth the investment, to do it then and do not first meet in an emergency.

Christopher Land is General Counsel and the Vice President for Legal Affairs at the Woods Hole Oceanographic Institution. As General Counsel, he provides advice, opinions and representation on all areas of law affecting the Institution. Among his duties are engaging in institution strategy and business development; providing counsel and advice concerning compliance with federal and state statutes and regulations affecting research and higher education organizations; and negotiating, drafting and reviewing contracts.

He is responsible for providing proactive counsel on a broad array of critical, strategic, and public policy issues to WHOI's Board of Directors, the Director and President, and all senior managers in their WHOI roles and positions. The size, complexity, scope, and diversity of the WHOI community generate a range of complex, cutting edge legal issues. Many, such as academic freedom, sponsored research, shared governance, and student rights and obligations, are unique to a research and academic environment. WHOI also has the added complexity of being a large maritime operator of oceangoing vessels, maritime crew, longshoremen, a number of small craft, AUVs and ROVs, and the resulting Admiralty Law and Jones Act issues. He also manages WHOI's Risk Management and Compliance system.

Chris received a BA from San Francisco University and is a 2002 graduate; Order of the Coif and Cum Laude, of Tulane Law School. Mr. Land has been a senior attorney with the firm Goodwin Procter of Boston, where he represented clients in various industries, including pharmaceutical and medical device manufacturers, power and energy companies, and academic and research institutions, including WHOI.

How Knowledge Integration Platforms, Artificial Intelligence and Machine Learning Help Satisfy the Duty to Preserve, Access and Manage Digital Information across Disparate Data Sources

By Daniel Meyers, Salim Elkhoul, and Joseph Pochron



The IT infrastructure of businesses today is no longer limited to behind-the-firewall servers and enterprise appliances from traditional providers like Microsoft and IBM. Modern employees demand the ability to access their workspace and collaborate with colleagues in dynamic, diverse environments that can be

accessed from the road, from mobile devices and through the cloud. A dizzying array of platforms have arisen to meet this demand. The result is that present-day productivity means discussing projects on one platform (HipChat, Slack, etc.), collaborating on documents through another (Confluence, SharePoint), and managing client relationships through a third (Salesforce, Zendesk, Jira). And that's not to mention corporate emails, text messages, social media accounts and accounting/finance databases.

While this panoply of data sources is a boon to operational efficiency and employee satisfaction, it presents a nightmare for legal, compliance, information governance and data protection/privacy professionals. Traditional forensic collection tools and records management strategies are difficult (if not impossible) to apply to this diversity of environments. Working through the data collection capabilities integrated into these varied platforms also falls short because they generate inconsistent outputs requiring tremendous manual labor to normalize, search and analyze on a consolidated basis.

In the context of a litigation or investigation, the negative consequences are clear. Attorneys struggle to find the information they need to assess exposure and strategy in the early stages of the dispute. Worse yet, collection and preservation failures have resulted in significant sanctions and public chastising for both the client and its attorneys.

Disparate information sources also create challenges for compliance and records management. The ability to readily access documents consistent with regulatory requirements and track the implementation of retention schedules is severely undermined by the sheer volume of data sources being utilized today. Nowhere is this need felt more keenly than in Europe where the forthcoming GDPR (and its enhanced enforcement mechanisms) not only require businesses to rapidly respond to data subject access requests, but more generally to understand and control what categories of information are stored on what platforms and how to securely store and access them upon demand.

Fortunately, tech-forward platforms have also arisen to alleviate these tech-forward pain points. This article explores how knowledge integration platforms utilize an array of connectors, artificial intelligence and machine learning to empower companies to access, search and manage data across the many platforms used by employees. Such tools provide hope for an efficient, defensible, compliant future.

The Legal Requirement to Preserve and Access Data Wherever it Resides

Modern businesses are subject to an array of legal requirements concerning how they process, store, access and remediate documents. While technology evolves at a lightning pace, legal evolution is slow. Thus, many laws that were designed in the context of a paper world are still being applied in the digital age. Even more modern, technology-focused legal requirements – and laws that have received a technology-focused makeover – contemplate digital platforms that have evolved materially or even become outright stale by the time the law is in effect. The result is that lawyers working in the data management space must remain vigilant in understanding how creative solutions, outside the box thinking and technological advancements in data management are integral to a successful legal and compliance program. This is true not only for lawyers in the niche fields of e-discovery, information governance, and privacy/security, but more generally for in-house counsel and compliance professionals.

Data Preservation Obligations

A litigant's obligation to preserve potentially relevant documents once a litigation (or governmental investigation) is reasonably anticipated is well-settled. In October 2003, the seminal U.S. decision was issued on "the scope of a litigant's duty to preserve electronic documents and the consequences of a failure to preserve documents that fall within the scope of that duty."¹ In *Zubulake IV*, Judge Scheindlin explained:

Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a "litigation hold" to ensure the preservation of relevant documents. As a general rule, that litigation hold does not apply to inaccessible backup tapes (e.g., those typically maintained solely for the purpose of disaster recovery), which may continue to be recycled on the schedule set forth in the company's policy. On the other hand, if backup tapes are accessible (i.e., actively used for information retrieval), then such tapes would likely be subject to the litigation hold.²

While the issue before the court in *Zubulake IV* was the duty to preserve one particular category of electronically-stored information (back-up tapes), the reasoning and holding contained therein has

¹ *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 214 (S.D.N.Y. 2003) ("*Zubulake IV*").

² *Id.* at 218.

regularly been applied across evolving sources of ESI. The resulting line of cases is a veritable breadcrumb trail of new digital platforms and how the failure of attorneys to stay ahead of the technology has resulted in significant, case-altering sanctions.

For example, in *In re Pradaxa*,³ the defendants were sanctioned almost \$1,000,000 for failing to preserve text messages. The court held that “the duty to preserve is not a passive obligation; it must be discharged actively” and thus “[t]he defendants had a duty to ensure that their employees understood that text messages were included in the litigation hold.” But in truth, back in 2012, when the duty to preserve was first triggered in that case, not all lawyers recognized that text messages had become a common source of business “documents.” In that light, the failure to proactively preserve such data sources may be viewed with a more forgiving eye than the court cast.

The consequences of failing to preserve data stored on cloud-based platforms was felt keenly by the defendants in *Brown v. Tellermate*.⁴ In Tellermate, to support their age discrimination claim, plaintiffs requested that defendant produce information from Salesforce.com, a cloud-based website that the defendant used to track employee sales performance (sales performance, of course, was the lynchpin of the defendant’s affirmative defense that plaintiffs were terminated not because of their age, but because of their performance).

Tellermate’s counsel, however, refused to produce Salesforce data, arguing that defendant lacked the ability to collect data directly from the platform and that plaintiffs would instead need to subpoena Salesforce itself.⁵ After an evidentiary hearing exposed the factual and technological fallacy of that argument, the court admonished counsel, noting that it had demonstrated a “basic inability to appreciate” the nature of its client’s electronic data and fell “far short of their obligation to examine critically the information which Tellermate gave them [about the company’s IT infrastructure].”

The court emphasized that “as discoverable information becomes progressively digital, e-discovery including e-mails and other electronic documents, plays a larger, more crucial role in litigation.”⁶ The “failure to appreciate” the nature of Tellermate’s ESI not only led to a “corresponding failure to take steps to preserve that information” at the time the duty to preserve was triggered, but more alarmingly, led to a total loss of that information because under Tellermate’s license, Salesforce itself only retained information for expired accounts (such as plaintiffs’) for up to six months.⁷

As a sanction for defendant’s preservation failure, the court not only awarded plaintiffs all their costs and attorney fees incurred in connection with the preservation dispute, but also issued an order that

³ *In re Pradaxa (dabigatran Etxilate) Prods. Liab. Litig.*, MDL No. 2385, 2013 WL 648692 (S.D. Ill. Dec. 9, 2013), *rev’d in part on other grounds*, 745 F.3d 26 (7th Cir. 2014).

⁴ *Brown v. Tellermate*, No. 2:11-cv-1122, 2014 WL 2987051 (S.D. Oh. July 1, 2014).

⁵ 2014 WL 2987051, at 1, 5.

⁶ *Id.* at 10.

⁷ *Id.* at 9.

defendant not “be entitled to present or rely upon evidence that it terminated [plaintiffs’] employment for performance-related reasons.”⁸ Thus, the court effectively eviscerated defendants’ core defense to the merits.

The takeaway from these cases is simple: the duty to preserve ESI containing potentially relevant information is triggered at the time that a litigation or governmental investigation is reasonably foreseeable. The duty – and the court’s expectations – apply irrespective of the platform upon which such information resides.

Data Access Obligations

The duty to preserve potentially relevant data is, of course, far from the only legal obligation that disparate and cloud-based data sources render more difficult to satisfy. Various regulatory requirements also mandate that companies be able to locate, access and retrieve certain categories of information upon demand.

For example, under the Securities Exchange Act of 1934, registered members, brokers and dealers must store broad categories of books and records “in an easily accessible place.”⁹ To the extent such books and records are stored on “electronic storage media” – i.e., “any digital storage medium or system” – the member, broker or dealer must “at all times have available, for examination by the staffs of the Commission and self-regulatory organizations of which it is a member, facilities for immediate, easily readable projection or production of micrographic media or electronic storage media images and for producing easily readable images.”¹⁰ Indeed, “the member, broker, or dealer must maintain, keep current, and provide promptly upon request by the staffs of the Commission or the self-regulatory organizations of which the member, broker, or broker-dealer is a member all information necessary to access records and indexes stored on the electronic storage media.”¹¹

Thus, simply put, when companies registered with the SEC utilize varied and cloud-based data repositories to run their operations (and thus store their books and records), there is an obligation to be able to quickly identify, access and present such books and records on an ongoing basis and in response to any regulatory inquiry.

Likewise, under Article 15 of the European Union’s forthcoming General Data Protection Regulation (effective May 2018), data subjects will not only have the right to “obtain from the [data] controller confirmation as to whether or not personal data concerning him or her are being processed,” but also the right of “access to the personal data” and “a copy of the personal data undergoing processing.” Such information (and copies of the data) must be provided “without undue delay and in any event

⁸ *Id.* at 18.

⁹ See 17 C.F.R. §240.17a-4.

¹⁰ *Id.* (emphasis added).

¹¹ *Id.* (emphasis added).

within one month of receipt of the request,” although that “period may be extended by two further months where necessary, taking into account the complexity and number of the requests.”¹²

Accordingly, where information concerning a data subject is stored within and across various platforms, data controllers have, at most, three months from the receipt of the access request to search, identify and delivery a copy of the data to the requester. This complex task is made all the more demanding by the fact that the controller also must identify whether the resulting data contains personal information about other data subjects, in which case it must be redacted as well.

The Growing Complexity of Corporate IT Infrastructures

The legal requirements to preserve and access data impose substantial burdens on the modern business. Computer forensic technicians in the e-discovery industry are first-hand witness to the remarkable proliferation of data sources across a typical enterprise’s digital landscape. The core responsibility of such forensic specialists is to map the company’s data sources and perform forensically-sound collections from each source that contains information potentially relevant to the underlying dispute or investigation (and thus, preserve the data).

Ten years ago, the digital topography of a typical corporation was comprised of (a) network servers containing shared file folders, (b) email servers, (c) back-up tapes or alternative archiving solutions to store legacy documents, (d) database servers for customized systems typically utilized by accounting and/or finance departments and (e) desktop/laptop computers. To forensically collect from these environments, a technician could rely on a single collection tool, such as FTK Imager (AccessData) or EnCase Imager (Guidance Software). Only the most progressive companies at that time were providing mobile devices to their employees for corporate use or had installed applications such as SharePoint on their servers.

By five years ago, the IT landscape had shifted. Mobile devices, Instant Messaging (IM) platforms and online repositories and collaboration sites such as SharePoint and Dropbox had become common data sources to be collected. And, of course, social media platforms had become everyday reality for private parties and businesses alike. Thus, the forensic technician’s toolbag suddenly needed a lot more tools for specialized environments, such as mobiles (Cellebrite) and social media (X1). But still, “cloud computing” was a term largely known only to the tech sector and was rarely part of a company’s sanctioned IT infrastructure.

As noted in the introduction to this paper, the corporate IT ecosystem today is far more varied. Most companies have overcome their security-driven fear of cloud environments (recognizing that the security investments of cloud infrastructure providers often surpasses that of corporate firewalls). In turn, a forensic examiner routinely is asked to collect not only from yesteryear’s digital platforms, but

¹² See GDPR Article 12(3).

also from an ever-increasing laundry list of corporate solutions like JIRA, Slack, Confluence, Salesforce, Zendesk, etc.

This constantly evolving digital landscape has created significant challenges to a cost-efficient, defensible and compliant process to forensically acquire and preserve, let alone even access, data. The technician's toolbag can only contain so many tools and the cost of licensing new generations of collection software is cost-prohibitive. While many new platforms have integrated their own collection capabilities, the outputs are as varied as the platforms themselves, thus requiring substantial manual labor to normalize the exported information in a manner that is useful to the legal team or other end-user. Fortunately, fire has been met with fire; cutting-edge technology platforms that connect to and integrate this multitude of new data environments offer hope for a streamlined, defensible future.

Knowledge Integration Platforms use Artificial Intelligence and Machine Learning to Create the Future Norm

Knowledge integration platforms connect directly to a wide variety of data sources used by organizations to enable real time search across and within each platform simultaneously. These tools use the different source's APIs to continuously collect the files in native format along with all related metadata. Understanding a source's API is key to being able to collect all relevant information. Integrations can also be limited by what the source's API allows in terms of collection calls or available metadata.

Data can now be collected simply and in a defensible manner by going through a short authentication procedure to give permissions to the knowledge integration platform. Once authentication is established, the platform can begin collection directly from the source. Collecting and exporting from tomorrow's cloud platforms need not be a pain as long as you've identified a knowledge integration platform that understands how to manage multiple APIs and can rapidly add integrations.

When collecting the files from these sources, such platforms can also automatically process and index the data (with some platforms, this can be achieved on an automated, continuous basis established through administrative settings). During processing, the platform uses AI to identify types of documents, perform sentiment analysis and identify language based on the context of the files. During the processing phase AI can also be used to extract features embedded on images, identify relationships between files, making sure that metadata remains intact. The result is a smarter and up to date database of company information, where everything is automatically searchable and eDiscovery ready.

Such knowledge integrators create real-time expectations for identifying and retrieving relevant data from multiple sources, even in the most complex of IT infrastructures. They are ideal for the targeted preservation and continual, up to date access of electronically stored information. The value of these tools should not be understated. The availability of data will become the norm in e-discovery and data

access demands alike. They allow attorneys and information managers to focus on other tasks and issues, not driving up costs with time spent on information-gathering and consolidation.

Conclusion

In the race between technological development and legal evolution, the law will always lag behind. For professionals tasked with managing progressive IT infrastructures in a compliant manner, the legal lag can equate to potentially significant violations, sanctions and other forms of exposure. Fortunately, tech-forward solutions can be applied to address tech-forward problems. Knowledge integration platforms are a perfect example of this cycle, empowering companies to access, search and manage data across disparate platforms through an array of connectors, artificial intelligence and machine learning.

Daniel Meyers is the President of TransPerfect Legal Solutions (TLS) Consulting & Information Governance divisions. Dan advises clients on e-discovery best practices and motion practice, litigation readiness plans, defensible data disposition programs, and data privacy concerns, with a particular emphasis on cross-border data transfers. His clients range from financial institutions and multinational corporations to start-ups and small-to-medium businesses. Dan is certified as an E-Discovery Specialist (ACEDS) and an Information Privacy Professional (CIPP/US). Prior to joining TLS, Dan was a Commercial Litigation Partner at an Am Law 100 law firm and the Founder and Chair of the firm's E-Discovery & Information Governance practice group. Dan's commercial litigation practice covered a wide range of complex business disputes before federal and state courts, including cross-border, corporate governance, bankruptcy, securities, breach of contract, and business tort cases

Salim Elkhoul is the founder and CEO of Onna, a platform for real-time search across multiple repositories that aids in eDiscovery and finding high-value items across legal departments. Onna integrates with major services and storage repositories, such as G Suite, Office 365, Dropbox, and Slack, to ensure data is collected defensibly and can be exported in standard eDiscovery format for review. Onna was recently named as one of Gartner's Cool Vendors in AI for Legal Affairs. Prior to Onna, he was the founder of ESTET, a litigation support services firm that creates custom technology solutions to enhance the litigation strategy of corporations, AmLaw 100 firms, and boutique law firms. Since its founding, ESTET has garnered numerous awards, such as being named on the Inc. 500 | 5000 list of fastest growing companies and on Deloitte's Technology Fast 500 list, as well as being named one of the Best Places to Work in Los Angeles.

Joseph Pochron is a digital forensics examiner and high-technology investigator with more than 12 years of experience. He is a retired law enforcement Detective for the Lehigh County District Attorney's (LCDA) Office where he conducted both reactive and proactive investigations pertaining to crimes involving digital evidence. He also served as the commanding officer of the LCDA Computer Crimes Task Force. Joseph is active in the digital forensics community and professional organizations, and holds several industry-recognized certifications. Joseph has also accumulated considerable teaching experience, serving several years as an adjunct professor and designing a digital forensics curriculum at both the undergraduate and graduate levels for DeSales University. Joseph has presented on several digital forensic related topics at local, state, and national conferences, and has conducted training on

digital forensics techniques and best practices for hundreds of industry professionals. Joseph currently serves as the director of the west coast region within the Forensic Technology & Consulting division at Transperfect Legal Solutions.

Addressing the Evidentiary Challenges in Proving the Authenticity of Digital Records

By Tim Reiniger



Distinguishing authentic digital records from those that are forged is a central evidentiary challenge in the digital environment.¹ This concern is complicated by the untestable and ephemeral nature of digital data, the ease and pervasiveness of copying digital information, and ubiquity of network access to digital documents. In particular, electronic signatures and seals need the capability to link persons to actions and thereby provide a necessary immutable reference for proving the authenticity of digital information over time.² Online notarization and eWill laws reflect an emerging approach that leverages virtual presence.

The Electronic Signature as a Foundation of Digital Evidence – Proof Challenges for Practitioners as Described in Stephen Mason’s Newly Reissued Treatise *Stephen Mason’s Electronic Signatures in Law* (4th ed) Treatise

Signature law has historically been the primary method by which law links acts to human intent and identity in establishing the authenticity of records. Hence, evidentiary analysis of the various technological methods for creating electronic signatures necessarily assumes a central role in establishing and resolving such links in the digital information realm.

Stephen Mason’s updated analysis of electronic signatures – *Electronic Signatures in Law* (4th ed) (2016)³ – provides timely and essential insights that have been influential in the creation of new legal techniques for enabling the testability and proof of the authenticity of electronic signatures and digital records. In this analysis and critique of electronic signature forms and laws as they are developing around the world, Stephen Mason explains the evidentiary purposes of electronic signatures and their historical antecedents in signature law generally.

The new edition improves upon the prior version in three significant ways. First, explanation and review of the current legal treatment of the various forms of electronic signatures has been expanded from two chapters to nine. Second, the chapter on the electronic signature directive in the European Union has been updated and expanded to cover the new Regulation on electronic identification, signatures, and trust services, including electronic seals. Third, relevant caselaw and statutory updates have been added throughout the book with special attention given to the evidentiary proof challenges

¹ GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE xxvi (“Society must come to grips with whether it currently has an ability to learn the truth about everyday communications, agreements, transactions, and indeed all types of records of digital information. . . . [W]e currently exist in a regime of untestability.”); George L. Paul, *The “Authenticity Crisis” in Real Evidence*, PRAC. LITIGATOR, Nov. 2004, at 45–46.

² STEPHEN MASON, *ELECTRONIC SIGNATURES IN LAW* 10 (Institute of Advanced Legal Studies 4th ed. 2016).

³ Available for free at: <http://ials.sas.ac.uk/digital/humanities-digital-library/observing-law-ials-open-book-service-law/electronic-signatures>.

posed by biodynamic manuscript signatures, which many of us encounter with the use of credit cards at stores.

The ability to test the authenticity of digital records rests on gathering sufficient reliable facts regarding the identity of the originators or actors, the integrity or immutability of the information, and time information relating to the records.⁴ And proving the authentication of an act of pushing a computer button or affixing a private key as that of a specific person is the main evidentiary concern of the electronic signature. Mason argues that, whatever the form it takes, the electronic signature should be configured to capture reliable evidence of intent, identity, integrity, and time.⁵ “Proof is central to the question.”⁶ Therefore, the practitioner must be alert to the evidentiary strengths and weaknesses of each type of electronic signature technology. And, for the purposes of the book, Mason treats the term “electronic signature” as encompassing all forms currently in use.⁷

Establishing the authenticity of an electronic signature in any form poses three evidentiary challenges of which lawyers need to be aware:

1. The difficulty of authenticating identity in digital or online environments as compared with the traditional paper environment. “The function of attaching an electronic signature to a document or message is not understood in the same way as the use of manuscript signatures, partly because the signature can be applied to the document without any action by the individual to whom the signature is attributed, or without their knowledge.”⁸
2. Electronic signatures and networked communications are challenged by a lack of direct evidence in proving who clicked the button or caused the particular electronic signature to be made and when.⁹
3. The difficulty in establishing authorization for the use of the electronic signing technology over time. “[T]he recipient cannot determine whether the sending party authorized the use of the digital signature; this is also true of any other form of electronic signature.”¹⁰

⁴ For a detailed discussion of the evidentiary criteria for testing the authenticity of digital records, see PAUL, *supra* note 1, at 34-36.

⁵ MASON, *supra* note 2, at 9-10.

⁶ *Id.* at 209.

⁷ *Id.* in Chapter 6, Mason discusses how “electronic signatures” can appear in many forms, including as digital signatures, smartcards, typed names, box clicks, email names, Personal Identification Numbers (PINs), electronic sounds, electronic seals, biometrics, and biodynamic versions.

⁸ *Id.* at 306.

⁹ *Id.* at 189. “[I]n the digital context, the moment of authentication may not be when the person actually types in their name or adopts the signature text at the end of the email or put in automatically when a new email is begun where the program is set up to include a signature at the end of the email.”

¹⁰ *Id.* at 318.

It is crucially important for a relying party to be able to trust the origin and integrity of the sender's electronic message, including the electronic signature. "The process of authentication is between software protocols, not between human beings and it is not clear whether the authentication relates to the origin of the data, or acts to verify the identity of a person or entity."¹¹

Electronic signatures must be issued with clear and unambiguous management policies regarding password control, unique number identifiers, hashing capabilities, and public revocation lists. Afterwards, relying parties anywhere in the world can have confidence that the individual's credential-based signature is being used by the actual electronic signature owner and not an imposter. "The most important point to be aware of is this: the private key of a digital signature is only as good as the password that protects it."¹²

Mason provides detailed arguments for practitioners looking to challenge a particular digital certificate or digital signature process in court. "Befuddled by technicians, many politicians have been misled into the false promise that only digital signatures can be the legal equivalent of a manuscript signature, mainly because of the incorrect assurances that digital signatures are secure and safe from interference."¹³

For Mason, machine or system-made evidence should be neither automatically deemed more reliable than human testimony, nor given evidentiary presumptions.¹⁴ "One presumption that may apply to computers is the presumption that a machine is presumed to be in working order. In the context of digital evidence, however, it is pertinent to be aware of the imperfections inherent in the way computers function, and how digital evidence is prone to alteration. Evidence derived from a computer must be admissible, authentic, accurate and complete in the same way as any other form of evidence."¹⁵

Mason's book is strongly recommended for any legal practitioner, policy maker, or judicial officer who needs to assess the deployment and use of electronic signatures and electronic seals.

Online Notarization Laws and Virtual Presence: The Virginia Model Gains Traction

Effective July 1, 2012, the Commonwealth of Virginia became the first state in the United States to authorize the notarization function to be fulfilled by use of two-way audio-video conference. Virginia's Electronic Notaries Act of 2011¹⁶ authorizes online notarization by treating audio-video teleconferencing that meets certain standards to be treated the same as a traditional "in person" presence. In effect, the law allows for a direct, personal electronic presence to be treated the same as

¹¹ *Id.* at 152.

¹² *Id.* at 318.

¹³ *Id.* at 116.

¹⁴ *Id.* at 386.

¹⁵ *Id.* at 385-86.

¹⁶ Chapter 731, available at <http://leg1.state.va.us/cgi-bin/legp504.exe?111+ful+CHAP0731>.

a direct, personal “molecular” presence. As a result, a signer who is located anywhere in the world can personally appear online before a duly commissioned Virginia notary via audio-video conference technology. To enable this connection, both the signer and the notary must have a computer with a webcam and audio capability so that the signer and notary can both see and hear each other in accordance with Virginia Supreme Court standards.

Personal appearance serves as the fundamental manner in which a principal invokes the jurisdiction and authority of a notary public as a public officer. (*See, e.g., Colburn v. Mid-States Homes, Inc.*, 266 So.2d 865 (Ala., 1972), *Commonwealth v. Haines*, 97 Pa. 228 (Pa. 1881), *Humble Oil & Refining Co. v. Downey*, 183 S.W.2d 426 (Tex. 1944), and *Yates v. Ley*, 92 S.E. 837 (Va., 1917).) Thus, an authorization for notaries public to use audio-video communication technology represents the provisioning of an alternative to physical presence as a means for a signer to invoke the notary public’s jurisdiction and authority.

Videoconference technology has been deemed trustworthy and reliable in many criminal and civil proceedings.¹⁷ With the Virginia model, the standards governing appearance by two-way electronic audio and video communication in Virginia courtrooms require that the parties must be able to “simultaneously see and speak to one another” using a live, real-time signal that is secure from unlawful interception.¹⁸ Where such audio-video conference technology is available, the use of this technology constitutes an “appearance” before “a magistrate, intake officer or, prior to trial, before a judge” and these officers “may exercise all powers conferred by law and all communications and proceedings shall be conducted in the same manner as if the appearance were in person.”¹⁹

While a notarized document carries strong presumptive evidentiary value, it is not the physical appearance of the signer before the notary that provides this value. Rather, it is the notary’s authority, conveyed by his/her signature and seal properly affixed to the underlying document that provides the evidentiary presumption courts rely on. In other words, we trust the notary, not the signer. A notary binds a signer to a document by presumption that is very difficult to overcome. The online notarization law relies on the presumption that the self-authenticating function of a notary can be fulfilled by audio-video conference technology as easily as it can be by physical appearance.

With respect to identity, the multi-factor procedures for online notarization under the Virginia model actually ensure that online signing is more reliable and resistant to fraud and manipulation than traditional notarization. The online notary must *confirm*²⁰ the identity of the signer gained through

¹⁷ See Louisiana Chapter 406 (2017) available at: <https://www.legis.la.gov/legis/ViewDocument.aspx?d=1052576>. Note also the discussion of the use of video conferencing for criminal arraignments and parole hearings by the Michigan state correctional facilities in Elaine Pittman, *Virtual Justice*, GOVERNMENT TECHNOLOGY, January 10, 2011, at 34-5.

¹⁸ *See, e.g.,* VA. CODE ANN. § 19.2-3.1 (B). Note also that, pursuant to VA. CODE ANN. § 47.1-13 D, the online notarial acts are deemed to have taken place in Virginia and under Virginia law.

¹⁹ VA. CODE ANN. § 19.2-3.1 (A).

²⁰ VA. CODE ANN. § 47.1-2.

inspection of a government issued identification document by (1) personal knowledge of the signer (including the testimony of a credible witness under oath who has personal knowledge of a signer), (2) reliance on prior (antecedent) in-person proof of identity (such as a series of knowledge-based questions provided by a credit information company),²¹ or (3) reliance on the signer's use of a digital certificate that is authenticated either by a biometric or a high-security smartcard such as a nonfederal issued PIV-I card.²² By contrast, in paper notarization, a notary identifies a signer by viewing the signer's identity document (in the United States, typically a driver's license). The notary, of course, has no means to determine if the identity document is itself forged.

With respect to the capability later of testing the integrity of the records, including the notary's electronic signature, the Virginia model requires that the notary's electronic signature and electronic seal be affixed in a manner that renders the document tamper-evident.

Perhaps most significantly, the Virginia law requires a notary to adhere to a duty of care evidenced by an electronic record. Every online notary transaction must be captured in an accompanying electronic record that contains important data about the signer and the transaction, including the date and time.²³ In addition, every electronic record must include a digital recording of the entire video and audio conference between the signer and the notary. These electronic records of electronic notarial acts must be maintained for a period of at least five years from the date of the transaction, although notaries (or parties relying on the record) may elect to keep the records in perpetuity.

To ensure trust in the evidentiary presumptions given to documents certified by notaries as public officers, the Virginia online notarization model requires that the online notary keeps sole control over his or her notarial electronic signature, e-seal, and record-keeping. The online notary is prohibited from allowing others from using these tools. And relying parties must be able to independently verify that the notary's electronic signature and seal have been used only by the named notarial officer.²⁴

Currently, there are three variations of the Virginia model of online notarization: Virginia, Montana, and the Uniform Law Commission's Amendment to the Revised Uniform Law on Notarial Acts (RULONA) (2016). In 2015, following Virginia's lead, Montana became the second state to enact online notarization.²⁵ While the Virginia model authorizes out-of-state signers to invoke the jurisdiction of the

²¹ As an example, a signer must undergo a series of challenge/response questions when asserting his identity online, and the use of independent third-party database checks to confirm identity markers (such as a social security number, a residence address, etc.) is used to cross-reference the signer's identity assertion responses. For a description of antecedent in-person proofing' see FPKIPA – CPWG Antecedent, In-Person Task Group, *FBCA Supplementary Antecedent, In Person Definition*, (see fn. 4).

²² For a description of PIV-I, see Federal CIO Council, *Personal Identity Verification (PIV) Interoperability For Non-Federal Issuers*, v1.0.0 (May 2009) available at www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf.

²³ VA. CODE ANN. § 47.1-14 C.

²⁴ Timothy S. Reiniger, *Evidentiary Requirements for Electronic Notarization and the Legalization of Certified Electronic Documents*, in PAUL, *supra* note 1, at 212–13.

²⁵ See MONT. CODE ANN. § 1-6-603(7) and § 1-6-615).

commissioning state notary, the Montana version limits the applicability to Montana residents and property transactions and court proceedings in Montana. As another approach, the RULONA limits online notarization applicability to United Citizens traveling outside of the United States.²⁶ This year, Ohio²⁷, Nevada²⁸ and Texas²⁹ have followed Virginia in authorizing out-of-state signers.

Like both Virginia and Montana, the Nevada and Texas online notarization laws 1) permit out-of-state signers to invoke the authority of an online notary by means of audio-video communication, 2) favor the use of multi-factor authentication for confirming the identity of the signer, 3) require real-time, interactive, and secure audio-video communications, 3) require the online notary's electronic signature and electronic seal to render the underlying document tamper-evident, and 4) require sole control by the online notary of the notary's electronic signature, electronic seal, and audio-video conference recordings.

First Online e-Closing of a Property Transaction

On July 28, 2017, the first online e-Closing of a home mortgage refinance to be electronically signed and notarized online involved a husband and wife who were physically located in Illinois and who needed to finalize the transaction in Chicago, Illinois with a Michigan-based lender. The transaction was insured by Stewart Title. The online notary, a commissioned Virginia electronic notary using the Notarize³⁰ audio-video conference and signing technology, was physically located in Virginia.

The signers and the online notary logged in and viewed the document simultaneously in the Notarize signing platform. The signers showed a picture identification that was based on a prior antecedent event and successfully completed a knowledge based questioning procedure³¹ to fulfill the identity confirmation requirement, and then electronically signed the document by affixing digital signatures. The signers then verbally acknowledged their intent to sign the document to the online notary. The online notary counter-signed the document by affixing a digital signature and an electronic official seal that includes the jurisdiction, notary's full name and title, commission number, and date of commission expiration. The electronically notarized document for the home refinance then proceeded to completion with routine electronic recording of the document among the land records at the Cook County, Illinois Recorder of Deeds. The recording of the document was formally accepted on August 2,

²⁶ Available at: http://www.uniformlaws.org/shared/docs/notarial_acts/2016_ARULONA_Final%20Act.pdf.

²⁷ See HB 49 available at: <https://www.legislature.ohio.gov/legislation/legislation-summary?id=GA132-HB-49>.

²⁸ See Chapter 511 (2017) (AB413) available at: https://www.leg.state.nv.us/Session/79th2017/Bills/AB/AB413_EN.pdf.

²⁹ See 85(R) HB 1217 available at:

<http://www.capitol.state.tx.us/tlodocs/85R/billtext/pdf/HB01217F.pdf#navpanes=0>.

³⁰ Information about Notarize is available at: www.notarize.com.

³¹ For example, a signer must undergo a series of challenge/response questions when asserting his identity online, and the use of independent third-party database checks to confirm identity markers (such as a social security number, a residence address, etc.) is used to cross-reference the signer's identity assertion responses. This process, which is well understood and applied in the banking industry, also is subject to the guidelines set forth in the *FBCA Supplementary Antecedent, In Person Definition* (16 July 2009) available at http://www.idmanagement.gov/fpkpa/documents/FBCA_Supplementary_Antecedent.pdf.

2017, which makes the electronically signed and notarized document part of the permanent public record.

This online e-Closing builds on the first public recording of an online deed in the United States that had taken place on June 6, 2013 and involved the sale of a property in Alexandria, Virginia, signers physically located in France, and an online notary in Richmond, Virginia.³²

First Online eWill Law

The first online eWill law in the United States was enacted in Nevada this year.³³ Joined with the online notarization law, this law amends Nevada's existing eWill law to authorize the use of audio-video conference technology to be used by testators, settlors, witnesses, and notaries in the creation of valid wills and trusts. The new position of a Qualified Custodian is created to function as the record-keeper of the electronic will and trusts. Recognition is also given to paper printouts for admission in probate court as authoritative originals of eWills and eTrusts.³⁴

Lessons

The following observations can be made about the emerging legal frameworks for testing and proving authenticity of digital information:

1. Online notarization and online eWills provide stronger capabilities for capturing evidence of signer intent, identity, integrity, and time that exist in the paper world.
2. In light of the first online eClosing, the online notary may soon be at the vanguard of enabling trust relations in the digital network-based economy. Digital data and ubiquitous connectivity now render impractical, undesirable and even obsolete requirements for physical appearance in many contexts.
3. Online notarization laws reflect the reality that, with cloud-based services and storage, electronic documents and their signers now can act virtually more easily than ever before. Signers located outside of the physical presence (as traditionally understood) of the online notary in Virginia, Montana, and Ohio, and, next year, in Nevada and Texas using common and easily understood software and hardware.

³² For a description of the first online deed, see Phillip Marson and Timothy Reiniger, *The Deed is Done*, 10 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE AND LAW REVIEW 144 (2013) available at: <http://journals.sas.ac.uk/deeslr/article/view/2034>.

³³ See Chapter 511 (2017) (AB413) available at: https://www.leg.state.nv.us/Session/79th2017/Bills/AB/AB413_EN.pdf. Note that similar legislation this year, Florida HB 277, was vetoed by the Florida Governor, available at: <https://legiscan.com/FL/text/H0277/id/1615662>.

³⁴ *Supra* note 33, Nevada Chapter 511 (2017) (AB413), section 21.

4. With digital networks and cloud computing, there is no longer a geographically-limited bound physical connection between the document and the signer. Therefore, the logic of requiring a signer to physically appear in 'molecular form' before a notary in order to attribute a particular person to a particular document no longer applies. A direct personal appearance in electronic form may suffice.

Conclusion

Stephen Mason's treatise on Electronic Signatures in Law continues to be the leading text on the subject. His emphasis on the need for electronic signatures to collect evidence of intent, identity, document integrity, and time information has directly impacted the development of online notarization and eWill laws in the United States.

Online notarization and eWills bring the notary into the stream of electronic commerce in a manner never before possible. Online notaries are poised to serve as identity agents for individuals and trust framework providers, identity credential enrollment agents, document certifiers, fact verifiers, and information governance and assurance professionals generally to a wide variety of public and private parties.

Using an online notarization, digital identity users now may take advantage of all the conveniences of online transaction processing, including greater speed, efficiency, security and electronic archiving. Relying parties also can place greater trust in the trustworthiness of these transactions due to the stringent identity confirmation and authentication of signers, and the notary's electronic record-keeping, which includes a real-time recording of the notarial act itself that is subject to statutory protections regarding third party access.

Timothy Reiniger is a licensed attorney in California and Washington DC. He leads the Timothy Reiniger LLC advisory practice from Cape Elizabeth, Maine and is the founder of The Cybernotary Society. He is an author of the Virginia online notarization law as well as the Virginia Digital Identity Management Law. He contributed a chapter on electronic notarization in George L. Paul's Foundations of Digital Evidence (ABA, 2008). As a nationally recognized expert on the notary office and identity policy, he has testified before the U.S. House Judiciary Committee, and The Hague Conference on Private International Law, and has served as an ABA Advisor to the Uniform Law Commission Committees on Identity Management and Online Notarization. He currently serves on the Advisory Board of the European Commission's LIGHTest Project. tim@reinigerllc.com

New York Quietly Relaxes In Camera Review Requirement for Social Media Discovery

By Joseph Francoeur and Sean Geary



Why should the courts have to undertake the burden of evaluating in camera a party's social media account to determine what information is relevant and discoverable? New York's Appellate Division, First Department asked that very question in 2015. In *Forman v. Henkin*,¹ the majority responded to the dissent's criticism of the rule requiring in camera review, noting that it is not a rule at all but discretionary, though this is the first time it so held in the social media context. The majority further

noted that *stare decisis* would prevent a change in course after the matter has been consistently decided. However, in a telling dissent Judge Saxe observed that social media case law is not so well developed as to enjoy *stare decisis* treatment as the issues were admittedly still evolving. Judge Saxe noted "this Court has required that an *in camera* review be performed so that the defendant is not made privy to non-relevant content."

The majority disagreed with the dissent's position that precedent established that *in camera* review was *always* required and rather it was left to the discretion of the trial courts; yet it cited two cases finding *in camera* review was discretionary but neither involved the social media context. The issue was not resolved in *Forman* because neither party challenged the *in camera* review on appeal.

Two years passed, and on June 20, 2017, the First Department in *Flowers v. City of New York*² quietly did just that – relaxed *stare decisis* and removed the *in camera* burden on the courts in the social media context. Understanding social media's effect on litigation has once again been shown to be a moving target.

The Prior Rule on Discoverability of Social Media

Generally, courts have been reluctant to allow discovery of social media data, recognizing privacy concerns of the individual. Courts have denounced blind requests for access to social media accounts as impermissible "fishing expeditions." Litigants have been able to convince courts to allow social media with an evidentiary showing that the request was not blind at all. However, to protect the privacy of the party, the court would then undertake an *in camera* review to determine the relevancy of the social media data. This two-step approach became known as the "factual predicate" approach.

While discovery obligations traditionally lay squarely on the parties, in the social media context courts have demonstrated a willingness to stray from the traditional discovery approach and instead delve

¹ 134 A.D.3d 529, 538 (1st Dep't 2015)

² 151 A.D.3d 590 (1st Dep't 2017)

into parties' personal lives and attempt to gauge one's expectation of privacy prior to release. As federal judges have recognized, "postings on Facebook and other social media present a unique challenge for courts, due to their relative novelty and their ability to be shared by or with someone besides the original poster."³ However, in their efforts to adapt to the unique challenge, courts have unwittingly assumed the discovery burdens traditionally borne by the parties.

The factual predicate approach was introduced in *McCann v. Harleysville Ins. Co. of N.Y.*⁴ In *McCann*, the defendant sought photographs and the use of the plaintiff's Facebook account. The court ruled that a party seeking social media content must establish "a factual predicate with respect to the relevancy of the evidence." Notably, the court indicated that the application of a "factual predicate" test would guard against the proverbial fishing expedition that could result from a defendant's unfettered access to an opposing party's social media account.

The *McCann* ruling is mirrored by the decisions in *Romano v. Steelcase, Inc.*,⁵ and *Kregg v. Maldonado*.⁶ In *Romano*, the trial court permitted discovery of opposing party's private profile only after satisfaction of the threshold burden. The court found it reasonable to infer from the limited postings on the plaintiff's public social media profile pages that the plaintiff's private pages might contain material that was relevant to the claims at hand and that "preventing defendant from accessing plaintiff's private postings" would be in "direct contravention to the liberal disclosure policy of New York State." In *Kregg*, defendants requested disclosure of the content of a social media account established for an injured party subsequent to the injury. Relying on *McCann*, the court in *Kregg* explained that the request for the review of the account was too broad and therefore denied the motion without prejudice, allowing defendants to resubmit a more narrowly tailored request.

The two-pronged procedure was utilized in *Patterson v. Turner Constr. Co.*⁷ When the threshold burden was deemed met, the trial court conducted an *in camera* review, and on appeal the court remanded for an additional review to determine relevancy. Relying on *Patterson*, in *Tapp v. New York State Urban Dev. Corp.*,⁸ the court concluded that merely having a Facebook account does not establish a factual predicate for discovery of private material posted to a Facebook page and therefore there was an "insufficient basis to compel plaintiff to provide access to the account or to have the court conduct an *in camera* inspection." The *Tapp* court explicitly rejected the argument that a social media posting may reveal daily activities that contradict or conflict with certain claims and instead required the review under the "factual predicate" or threshold model to determine if access should be granted to the private postings on an account.

³ *Orr v. Macy's Retail Holdings, Inc.*, 2016 U.S. Dist. LEXIS 147573 citing *Higgins v. Koch Dev't Corp.*, 2013 U.S. Dist. LEXIS 94139.

⁴ 78 A.D.3d 1524 (4th Dep't 2010)

⁵ 30 Misc. 3d 426 (N.Y. Sup. Ct., 2010)

⁶ 98 A.D.3d 1289 (4th Dep't 2012)

⁷ 88 A.D.3d 617 (1st Dep't 2011)

⁸ 102 A.D.3d 620 (1st Dep't 2013)

Change Is Foreshadowed in 2015

As late as June 2015, the First Department continued to employ the two-prong rule requiring factual predicate and *in camera* review. In *Spearin v. Linmar, L.P.*,⁹ the First Department found that defendants established the predicate when they located on plaintiffs public Facebook page a picture of the plaintiff at a piano, which contradicted the claim that as a result of the injuries plaintiff could no longer play the piano. The trial court ordered the plaintiff to provide an authorization for access to all Facebook account records without any review for relevancy. However, the First Department reversed and ordered that the trial court conduct an *in camera* review to identify relevant information.

A few months later in December 2015, the First Department decided the *Forman v. Henkin* matter. In *Forman*, the plaintiff fell from a horse and alleged that the stirrup leather attached to the saddle broke, causing her to lose her balance and fall to the ground. The plaintiff claimed the defendant was negligent in preparing the horse. The defendant sought an order compelling unlimited authorization to obtain records from the plaintiff's Facebook account. The trial court granted the defendant's motion with some limitations. The plaintiff appealed. The First Department reversed, finding the "defendant has failed to establish entitlement to either plaintiff's private Facebook photographs [or messages]."

The First Department cited to "well-established case law governing disclosure [requiring] some threshold showing before allowing access to a party's private social media information." The court cited to *Richards v. Hertz Corp.*,¹⁰ which addressed the trial court's granting of the plaintiffs' motion for a protective order striking a demand for authorizations seeking access to all postings to the plaintiffs' Facebook account. The plaintiffs were injured in an automobile accident and plaintiff McCarthy testified that her injuries prevented her from playing sports and that she experienced pain in the cold. Defendants' counsel found on plaintiff McCarthy's public Facebook page pictures of the plaintiff skiing after the accident. The trial court ordered the plaintiff to review her Facebook account and produce all pictures of her "participating in a sporting activity."

On appeal, the Second Department found that the defendants had met their burden by making "some showing that at least some of the discovery sought will result in the disclosure of relevant evidence." However, the Second Department reversed the ruling directing plaintiff to review the account and produce relevant photographs and instead ordered that the trial court must conduct an *in camera* inspection of the entire Facebook profile.

In its decision in *Forman v. Henkin*, the First Department declined to rule on the issue of *in camera* review as it was not raised on appeal. However, as noted above, clearly the First Department wrestled with the issue *in dicta* and in the dissent, teeing up the issue for another day.

⁹ 129 A.D.3d 528 (1st Dep't 2015)

¹⁰ 100 A.D.3d 728 (2nd Dep't 2012)

The New Rule: Factual Predicate Required, But Not *in Camera* Review

Judge Saxe in the dissent in *Forman v. Henkin* took issue with both prongs of the requirements to allow discovery of social media, finding the New York Civil Practice Law and Rule (CPLR) obligates parties to produce all relevant information, and this he believes includes social media. As a result, neither the predicate nor the *in camera* review are necessary or prudent requirements.

Recently, on June 20, 2017, the First Department quietly departed for the first time from its requirement of *in camera* review in the social media context, but it retained the requirement of a factual predicate. In *Flowers v. City of New York*,¹¹ the plaintiff brought an action for wrongful arrest and prosecution, and denied at his deposition ever using any aliases or nicknames, including “Moe.” The City brought a motion to compel seeking the plaintiff’s Facebook data, offering the factual predicate of the plaintiff’s public Facebook pages wherein the plaintiff had several pages using some form of the word “Moe.” In addition, one of these pages included a picture of the plaintiff’s nephew. The trial court denied the motion, but the First Department reversed.

The First Department found that “the City made a threshold showing that examination of the above Facebook accounts will result in the disclosure of relevant evidence bearing on the claim” and cited to three decisions as authority, including *Forman* and *Richards*. However, in a major break from the past the First Department did not require *in camera* review. Instead, the First Department – apparently following the recommendation of Judge Saxe in his dissent in *Forman* – merely required the plaintiff to review the social media and produce what is relevant. The Court directed the plaintiff “to review and provide or permit access to those Facebook and associated Messenger accounts, including their messenger components, and any deleted materials which contain any information connecting plaintiff to the accounts in question, connecting him to any variation of the nickname ‘Moe.’”

Impact of the *Forman* and *Flowers* Decisions on Social Media

The First Department seems to have reached a compromise with regard to the changes suggested by Judge Saxe’s dissent in *Forman*. Judge Saxe suggested that both the predicate and *in camera* review should be replaced by simply enforcing the CPLR requirements to provide relevant information. In *Flowers*, the First Department departed from the practice of ordering *in camera* review in the social media context and instead adopted the Saxe approach under the CPLR.

However, the decision in *Flowers* begs the question of why the factual predicate is required at all. The purpose of the predicate was to protect parties from unwarranted fishing expeditions into their Facebook accounts without some showing. While the requirement seemed to make sense, if parties are now required to review their social media and produce relevant material in accordance with the CPLR and are no longer required to give unfettered access to such accounts via an “authorization” to

¹¹ 151 A.D.3d 590 (1st Dep’t 2017)

the other side, then why require the predicate at all? If the courts merely order parties to review their own accounts as opposed to giving blanket authorizations, then there simply is no need to provide a predicate. Looking at this from the other direction, should parties be excused from the CPLR requirements to produce relevant social media merely because they were smart enough not to post pictures on their public page of themselves playing piano, skiing or using nicknames that contradict their cases? Such a result is truly absurd. Litigants should be made to search their social media for relevant materials, just as they would be required to search their document files for relevant documents. After counsel receives such assurances that a search was done, but public social media reveals the search to be inadequate or never actually done, then and only then will unfettered access be granted.

This relevancy approach to discoverable social media content has already been applied in other jurisdictions. For example, in *Mailhoit v. Home Depot*¹² the Central District of California found that a request for social networking communications between the plaintiff and current or former Home Depot employees was relevant. But rather than limit the whole request due to an unsatisfied threshold requirement, the court denied the request on grounds that it was not reasonably particular. In *Davenport v. State Farm Mut. Automobile Ins. Co.*¹³ the Middle District of Florida specifically noted that “social networking content is neither privileged nor protected by any right of privacy” but nonetheless discovery requests must be “tailored to seek information that is reasonably calculated to lead to the discovery of admissible evidence.”¹⁴

In light of *Flowers*, parties in New York should be on notice that they will be responsible for reviewing their social media accounts and producing relevant information in accordance with the CPLR. If the First Department has not expressly said so yet in *Flowers*, clearly this day is near.

Joseph Francoeur is a partner in Wilson Elser’s New York City office. In addition to practicing in many areas of the law including professional liability defense, federal statutory litigation, commercial disputes, employment and labor and insurance coverage matters, he also is experienced in emerging issues in e-discovery and social media.

Sean Geary is an associate in Wilson Elser’s New York City office. He focuses his practice on professional liability defense defending lawyers, law firms, insurance agents, brokers, and other professionals in individual cases in courts, before regulatory bodies or in arbitration and mediation.

¹² 285 F.R.D. 566 (C.D. Cal. 2012)

¹³ 2012 U.S. Dist. LEXIS 20944 (M.D. Fla. 2012)

Lessons and Practical Guidance from the Target Data Breach AG Settlement

By Aldo M. Leiva



On May 15, 2017, Target Corporation executed the Assurance of Voluntary Compliance¹ ("Settlement Agreement") with the Attorneys General of 47² states and the District of Columbia, thereby settling all civil claims that had been brought against Target by the Attorneys General, arising out of the Target Data Breach that was first disclosed by Target to authorities on December 19, 2013. Following Target's disclosure, authorities initiated an investigation and determined that the breach occurred between November 27, 2013 and December 15, 2013 and involved portions of Target's computer system that processed payments at its retail stores, as well as portions that stored consumer contact information, affecting up to 110 million Target customers whose credit card and debit card information were compromised.³

The investigation also determined that hackers had successfully gained unauthorized access to a third party vendor's network and had stolen credentials that were used to access the Target customer database.⁴ Based on the investigation, Attorneys General in 47 states and the District of Columbia ultimately filed civil claims against Target, pursuant to various Consumer Protection Acts, Personal Information Protection Acts, and Breach Notification Acts from states where affected Target consumers resided. The settlement with the Attorneys General is the largest multi-state data breach settlement to date, requiring payment of \$ 18.5 Million to the participating states.

Prior to this settlement, Target had already settled a civil action instituted by Visa, with a payment of up to \$ 67 Million to Visa and its card issuers.⁵ More recently, the Eighth Circuit Court of Appeals had reversed⁶ a District Court's approval of a \$ 10 Million settlement in a consolidated class action arising from the data breach, and remanded it to the District Court for further consideration, on the grounds that the Order approving the settlement was perfunctory and did not include the required rigorous analysis in support of the settlement. However, in May 2017, the District Court again approved the

¹ The Target Assurance of Voluntary Compliance document is available for review at https://ag.ny.gov/sites/default/files/nyag_target_settlement.pdf

² Alabama, Wisconsin, and Wyoming were not part of the settlement.

³ "Target: Hacking Hit Up To 110 Million Customers," Chris Isidore, CNN Money, January 11, 2014, accessed on July 20, 2017 at <http://money.cnn.com/2014/01/10/news/companies/target-hacking/>

⁴ "Target to Pay \$ 18.5 Million to 47 States in Security Breach Settlement," Rachel Abrams, New York Times, May 23, 2017, accessed on July 30, 2017 at <https://www.nytimes.com/2017/05/23/business/target-security-breach-settlement.html>

⁵ "Target Reaches Deal With Visa Over 2013 Data Breach," Shan Li, Los Angeles Times, August 18, 2015, accessed July 30, 2017 at <http://www.latimes.com/business/la-fi-target-breach-settlement-20150818-story.html>

⁶ See Eighth Circuit Court of Appeals Order, In re: Target Corporation Customer Data Security Breach Litigation, February 1, 2017, <http://media.ca8.uscourts.gov/opndir/17/02/153909P.pdf>

settlement of the class action lawsuit.⁷ All told, the settlement sums to date approach \$ 100 Million, exclusive of additional legal fees, forensic expert costs, and notification costs, which demonstrates the significant impact that this breach has had on Target.

In addition to payment of \$ 18.5 Million to the Attorneys General, the Settlement Agreement also sets forth specific administrative and technical measures that are to be adopted by Target in order to safeguard consumer information and address the system vulnerabilities that the Attorneys General concluded played a role in the Data Breach. Given the potential liability and risk that a data breach represents, a review of such measures provides useful insight and guidance⁸ to counsel for any businesses and entities that collect, store, maintain, and transmit consumer data on computer systems, and which operate under U.S. jurisdiction, whether they are large and complex entities or not.

Consumer Protection, Personal Information Protection, and Data Breach Notification Assurances

The Settlement Agreement consists of assurances by Target that it will adopt or improve upon certain security measures, as specified by the Attorneys General. Among the assurances required of Target in the Settlement Agreement, is the ongoing requirement to comply with Consumer Protection Acts and Personal Information Protection Acts of any U.S. States in which it operates, in relation to its collection, maintenance, and safeguarding of Personal Information. Under the terms of the Settlement Agreement, "Personal Information" is defined as any information pertaining to a consumer and containing such data elements as a Social Security number, driver's license number, state-issued identification card number, or financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to the consumer's financial account.⁹ Target is also prohibited from making any misrepresentations relating to the extent to which it maintains and safeguards the privacy, security, confidentiality, or integrity of any Personal Information collected from its customers. It is also required to comply with all Security Breach Notification statutes in regard to any future security breach involving unauthorized access to or acquisition of Personal Information, and was also expressly required to provide notice¹⁰ to the Attorneys Generals of New Mexico and South Dakota, until such time as these states enact data breach notification statutes, at which point Target would act in compliance with these new laws.

⁷ "Minnesota Judge Again Approves Certification of Target Data Breach Class Action," Jessica Karmasek, May 18, 2017, Legal NewsLine, accessed on July 30, 2017 at <http://legalnewslines.com/stories/511117410-minnesota-federal-judge-again-approves-certification-of-target-data-breach-class-action>

⁸ In fact, Connecticut Attorney General stated at the time that the Settlement would "serve to inform other companies as to what is expected of them in terms of the security of their consumers' information." See "AG Jepsen: Conn. Leads \$18.5M Settlement with

Target Corporation over 2013 Data Breach," State of Connecticut Attorney General Press Release, May 23, 2017, accessed on July 30, 2017 at <http://www.ct.gov/ag/cwp/view.asp?A=2341&Q=593122>

⁹ Or, as otherwise defined under applicable state law.

¹⁰ Such notice will not be required if, upon reasonable determination by Target, there is no reasonable likelihood that harm to a consumer will result from the data breach.

Written Information Security Program

As part of the Settlement, Target is also required to develop, implement, and maintain a comprehensive Written Information Security Program (“WISP”) that is “reasonably designed” to protect the security, integrity, and confidentiality of Personal Information collected from consumers. The WISP must include administrative, technical and physical safeguards commensurate with Target’s size and complexity of operations, scope of activities, and the sensitivity of the consumer Personal Information that will be collected. It must also be designed and implemented to ensure “appropriate handling and investigation” of any security incidents involving Personal Information. Target’s WISP may be adapted from any existing policies that meet the above criteria, and it must be implemented by an executive/officer with the appropriate background or experience in information security, who is also charged with advising the Chief Executive Office and Board of Directors of the company’s security posture, security risks, and security implications of its decisions. The Settlement Agreement mandates that any such information security officer must receive the resources and support reasonably necessary to ensure that the above functions are carried out.

Administrative Safeguards and Technical Safeguards

Target is required to develop and implement policies and procedures for auditing third party vendors’ compliance with Target’s WISP. This particular requirement likely stems from the source of the Target Data Breach, which arose when a third party HVAC contractor’s computer system was compromised by hackers, who were then able to gain access to Target’s system and access the payment and personal information of customers¹¹. Target must make reasonable efforts to maintain and support software used on its networks, while assessing any impacts that software updates will have on business/network operations, as well as the necessary resources to address end-of-life software issues.

Encryption protocols and policies are also required. Specifically, such measures must be reasonably designed to encrypt Personal Information stored on desktops pertaining to cardholders, with mandatory encryption of data elements, as well as any other data elements required by state law to be encrypted, and which is stored on laptops, portable devices, and/or which are transmitted wirelessly or across public networks. These encryption measures are intended to make the information useless if stolen. Target is also responsible for complying with the Payment Card Industry Data Security Standard in regard to consumers’ credit card information, and must also reasonably manage the review and, as appropriate, adopt industry-accepted payment card security technologies, such as chip and PIN technology.

Segmentation of credit card information from the rest of Target’s computer network is required, and Target must also take “reasonable, risk-based steps” to map data flows and connections between its

¹¹ “HVAC Vendor Eyed As Entry Point For Target Data Breach,” Gregory Wallace, CNN Tech, February 7, 2014, accessed on July 30, 2017 at <http://money.cnn.com/2014/02/06/technology/security/target-breach-hvac/index.html>

payment data systems and the rest of its computer network, in order to identify and assess potential penetration vulnerabilities. It must also develop and implement a risk-based penetration testing program to identify, assess, and remedy vulnerabilities within its network. Target must take steps to maintain the separation of development and production systems. Target is also required to evaluate and, as appropriate, restrict or disable all unnecessary network programs that provide access to credit card information or which it reasonably believes would impact security.

In addition to the above technical requirements, Target must develop and implement strong passwords, password-rotation policies in regard to individual accounts, service accounts, and vendor accounts, as well as two-factor authentication for individual accounts, administrator accounts, and vendor accounts.

On-going file-integrity monitoring is also now required, consisting of deployment of controls designed to notify Target personnel of unauthorized modifications to critical applications or operating system files relating to credit card data. Point-of-sale terminals and in-store point-of-sale servers must also be secured via technical controls, such as application whitelisting solutions, to detect and prevent execution of unauthorized applications. Target must also collect logs and monitor network activity and implement, to the extent technically feasible, reasonable controls, such as firewalls and authentication controls. Policies and procedures relating to the management and documentation of changes to the network must also be developed and implemented.

Interestingly, the above administrative and technical safeguards are to remain in effect for a minimum of five (5) years from the effective date of the Settlement Agreement. Although such a time period is presumably imposed to ensure that Target will develop an ongoing and consistent compliance and implementation program, the Settlement Agreement also expressly provides that Target will, of course, be required to comply with all applicable Consumer Protection, Personal Information Protection, and Data Breach Notification at all times. For these reasons, and given that the administrative and technical safeguards are consistent with cybersecurity guidelines (such as the Cybersecurity Framework promulgated by the U.S. National Institute of Standards and Technology¹²), Target will likely retain the safeguards beyond the five (5) year term.

Third Party and AG Assessment of Target Compliance with Settlement Terms

Several terms in the Settlement Agreement provide further insight as to how ongoing compliance with such settlement agreements will be implemented by authorities against companies facing enforcement actions or civil suits. The primary method of ensuring compliance by Target with the terms of the Settlement Agreement is the requirement that a Third Party Assessor conduct an assessment and issue a report to the Connecticut Attorney General's Office within one (1) year of the execution of the Settlement Agreement. The Third Party Assessor must be certified as a Certified Information Systems

¹² See Cybersecurity Framework at NIST website, <https://www.nist.gov/cyberframework>

Security Professional (“CISSP”), or as a Certified Information Systems Auditor (“CISA”), or must hold similar qualifications, and have at least five (5) years of experience in evaluation of the security of information systems.

The report must address the following components of Target’s compliance status: (1) administrative, technical, and physical safeguards adopted and maintained by Target, (2) appropriateness of such safeguards in light of Target’s size and complexity, nature and scope of activities, and sensitivity of Personal Information maintained by Target, (3) explain the extent to which such safeguards have been implemented, and (4) identify the Security Assessor responsible for ensuring PCI compliance by Target.

If any of the participating Attorneys General determine that Target has failed to comply with any of assurances/terms of the Settlement Agreement, Target shall receive written notification, and Target must submit a written response including the following information: (1) a statement explaining why Target believes it is fully complying with the Settlement; or (2) a detailed explanation of how the alleged violation(s) occurred, and corresponding statements establishing that the alleged violation has been addressed and how, or that the alleged violation cannot be reasonably addressed within thirty (30) days from receipt of the notice. Under this second scenario, however, Target is not excused from complying with the terms of Settlement Agreement, and must provide an additional written statement establishing that Target: (1) has initiated corrective action to address the alleged violation, or (2) is pursuing such corrective action with reasonable diligence, and (3) has presented a reasonable timetable to address the alleged violation.

Target’s strategies in responding to and managing the aftermath of its massive data breach provide a great deal of insight to counsel advising data collectors/processors of consumer data in the United States. Its decision to enter into the Settlement Agreement presumably saved Target additional costs, fees, and penalties by avoiding prolonged litigation or adverse judgments. It also created a compliance template for Target that is intended to further strengthen its cybersecurity and privacy protections for consumers. Target’s latest actions contrast with its early response to the data breach. Although notifying authorities within days of discovering the data breach, Target actually delayed issuance of the disclosure, resulting in news of the data breach initially being released to the news media as rumors by third parties in the cybersecurity field.¹³

From a practical and public relations perspective, this cost Target the opportunity to shape the narrative and assume responsibility and accountability for the breach before the breach has been leaked to the press. From a legal perspective, undue delay in issuing the disclosure may have placed Target at risk of violating data breach notification statutes in the subject states. In any case, the

¹³ “Target Confirms Point-of-Sale Data Breach, Announces It Exposed 40 Million Credit Card Numbers,” posted by John Biggs, December 19, 2013, TechCrunch.com, accessed on July 30, 2017 at <https://techcrunch.com/2013/12/19/target-confirms-point-of-sale-data-breach-announces-it-exposed-40-million-credit-card-numbers/>

continuing consequences of the 2013 data breach to Target are instructive for business entities and the terms and measures imposed upon Target in the Settlement Agreement provide a basic template for counsel, information officers, and business executives to assess and improve upon their cybersecurity efforts.

***Aldo M. Leiva, Esq.**, chairs the Data Security and Privacy Practice at Lubell Rosen, and is based in the firm's Miami office. Any questions regarding CADRA or this article can be sent to Mr. Leiva via email at aml@lubellrosen.com*