INFORMATION LAW JOURNAL

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

WINTER 2015 VOLUME 6 ISSUE 1 EDITOR: THOMAS J. SHAW, ESQ.

Hacking Back In Self-Defense: The Parameters of Active Defense

By David Willson

In the not so distant past, when asked about cyber security, most companies and firms believed that data breaches would not happen to them, they are too small or don't have anything the hackers want. This attitude is quickly changing with the recent very high profile breaches like JP Morgan, Target, Home Depot, Neiman Marcus, Sally Beauty Supply, and many healthcare organizations. The reality is the threat has been present for many years; the breaches are just becoming more public. A lot of small and medium size businesses have already been breached but those breaches didn't make the news. In many cases businesses that have been breached still don't know it. *Read more*

E-Discovery Challenges in White Collar Investigations

By David A. Kronig, Alexander B. Hastings and Edward H. Rippey

As the number and scope of large-scale white collar investigations continues to grow, the e-discovery challenges associated with these matters are becoming more acute. While many of the considerations associated with e-discovery in the civil context map to the realm of white collar investigations, several unique issues warrant particular consideration. This article aims to identify some of the primary challenges in fulfilling discovery obligations in a white collar investigation. Many of the unique issues with e-discovery in the white collar context arise from the inherent imbalance of power between *Read more*

Stopping the FTC's Unreasonable Data-Security Rampage

By Hillard M. Sterling and Christina M. Liu

Hackers are thriving and staying steps, indeed miles, ahead of the companies they target (pun intended). Social media has become the hackers' main platform, where phony links and web pages plant highly sophisticated malware into cell phones and other mobile devices, for eventual transmission into corporate America's computer systems. It has become increasingly true that there are two types of companies: those that know they have been hacked, and those that don't. The government now states that it is here to help, and, as famously observed *Read more*

Beware of Visual Hacking: Are You Protecting Client Confidences?

By Mari J. Frank

Have you considered who might be viewing and collecting information about your clients and cases without your awareness? Many of us are tethered to our smart phones, tablets, laptops, and other engaging electronic devices. Instantaneously, we connect to our office, clients, opposing counsel, the court, the cloud, and more from myriad places including restaurants, airplanes, trains, the beach, or just about anywhere where connection is available. This mobility allows for flexibility, quick connectivity, and creativity. But mobile technology also exposes our clients' sensitive information to increased privacy and confidentiality vulnerabilities. *Read more*

2014 (4Q) Information Law Updates: Cases, Statutes, and Standards

By Thomas J. Shaw

In the fourth quarter of 2014 and the end of the third quarter, there have been many developments in U.S. and international information law, especially information security, privacy, and cloud computing cases, statutes, and standards. These include international and U.S. state and federal laws and regulations passed or coming into force. It also involves civil and criminal cases and enforcement actions brought by regulators. And it encompasses the new standards, guidelines and legal ethics opinions in this area. But it does not attempt to track legislation that has not yet been passed. *Read more*

Hacking Back In Self-Defense: The Parameters of Active Defense

By David Willson

In the not so distant past, when asked about cyber security, most companies and firms believed that data breaches would not happen to them, they are too small or don't have anything the hackers want. This attitude is quickly changing with the recent very high profile breaches like JP Morgan, Target, Home Depot, Neiman Marcus, Sally Beauty Supply, and many healthcare organizations.

The reality is the threat has been present for many years; the breaches are just becoming more public. A lot of small and medium size businesses have already been breached but those breaches didn't make the news. In many cases businesses that have been breached still don't know it.

So, if breached, what are your options? Typically, hire a company to help you clean up, do some damage control, contact law enforcement, and determine what happened. Unfortunately in many instances, depending on where you are and how serious the breach is, law enforcement may be too busy to assist or not have the technical expertise. Beyond this, there is not much you can do.

What if the breach is not a single incident but your company or firm is under persistent attack? You continue to suffer denial of service (DoS) attacks, or your intellectual property, client data, or proprietary data is constantly walking out of the door. Can you legally defend yourself? Depending on the facts and circumstances, yes.

Many people, though, will tell you no, it is illegal to defend yourself; they claim you will start a war with China, or, you will impact an innocent bystander. The legality of self-defense is certainly something to discuss, but the other two arguments are just ridiculous. Starting a war with China is not even worth addressing. As for impacting an innocent bystander, the company that was hacked and is now being used to attack my company may be a victim like me, but is in no manner an innocent bystander. Consider the movie with Harris Ford, "Firewall." His family was kidnapped and he was forced to break into the bank he was responsible for securing. Certainly he was in a tough position and had a tough decision to make. But, he was not an innocent bystander. Yes, a victim, but not innocent, he had a choice. The analogy is not perfect, but, the company whose server is being used to attack others must accept some culpability. Their security may not be up to par or there could be a number of other factors that allowed them to be hacked and now used as a weapon.

Legally, the issues include the Computer Fraud and Abuse Act (CFAA), and similarly various state computer crime laws, and then there is the theory of self-defense. To clarify, the CFAA makes it unlawful to gain unauthorized access to another's computer. The term computer under the CFAA includes any computing device connected to the Internet. This therefore includes, servers, PCs, laptops,

smartphones, etc. Many state computer crime laws follow the example of the CFAA and also include data privacy rules.

Self-defense is the defense of person and property. The key to claiming self-defense that that the attack must be imminent, in progress or continuing. For instance, if someone punches you in the face and runs away, self-defense does not apply if you chase that person down to retaliate. The same applies if someone breaches your network. If he/she attacked and is now gone, self-defense is not an option. If the attack, though, is imminent, ongoing or persistent, why shouldn't you be able to defend your property?

If you are going to track down and go after your attacker you will most likely have to access the computer network of other users and companies. This is because only an extremely dumb hacker would hack from his computer directly into your business. Good hackers will typically compromise a number of networks bouncing from network to network to hide their tracks and then use the server of a compromised business to attack, or utilize a botnet. When attempting to follow the hacker's tracks you will more than likely end up in the network of that not-so innocent bystander. If you decide to block the attack, hack back, employ active defense, or just track down your intruder, will likely impact the owner (so-called innocent bystander) of the compromised server.

Here is the key: Business owners must take a proactive planned approach. This cannot be the IT department hiding in the basement trying to stay under the radar or doing some recreational hacking at night or on the weekends. Information must be collected and decisions made by the company leadership at various points. I have spoken to and heard many stories of the employee who goes home and tries to track the hacker on his own, or the IT department who decides to take matters into their own hands, and finally, the company leadership who loves the idea but tries to create a buffer and act like they had no knowledge if all goes bad.

The leadership must make decisions based upon legal issues and whether the potential risk of the activity outweighs the loss or damage the company is suffering from the breaches. Business owners must understand that at some point they may be called to account and at that point they should be comfortable with the decisions they made in self-defense of their company and be able to justify each and every decision.

Here is how this would work. Once a breach is detected, a team of experts must be called in. The experts would include people to conduct malware analysis, online intelligence gathering, network analysis, traceback analysis and techniques, a public affairs person to help with messaging and reputation if needed, programmers who can develop the necessary tools and techniques for whatever courses of action are chose, and an attorney who can provide legal and risk management support throughout the operation. There may be others but this is a start. Incidence response, malware analysis, some Intel collection and interviews would be conducted to begin gathering as much information as possible.

The goal is to be able to provide the leadership with the data necessary to make well-informed decisions. The leadership will have to decide at various points whether to move forward with a particular course of action, cease all operations, or gather more Intel prior to moving ahead. As stated above, the decision must be made early on that the attacks are persistent and ongoing. If searching for stolen data, then self-defense is not an issue since this would be akin to retribution, and so the primary focus here would be steps to identify where the data is and how to retrieve. This would be more of an Intel exercise versus a hacking back or active defense exercise. Both are viable options.

Let's say your Intel identifies the server that attacks are being launched from. If you can identify who owns the server and where it is, then contact the owner and explain that he has been compromised and work with him to take action. If he ignores you or refuses to acknowledge any culpability, then it is game on. The leadership will have to decide is the damage being suffered great enough to proceed. If yes, then utilizing an escalated approach, take the steps necessary to block the server from being used to attack you. If this results in a lawsuit your counterclaim would be that the plaintiff was provided notice that he was being used to attack you and refused to take action forcing you to take unilateral action and you are now countersuing him for all the damage you have suffered due to his lack of or inadequate security. Chances are if you tell the server owner that his server is not just attacking you but 100 other companies and you will proceed to inform them, he will be more likely to cooperate.

If on the other hand you cannot identify the server and its owner, the decision must be made, based on the Intel available, whether or not to take action, what action, and whether the continuing damage outweighs the potential damage of taking action. At various points the leadership must be presented with the facts and asked to make a decision. Companies make risk decisions all the time and have to decide whether the benefit outweighs the risk.

As for the CFAA, much of the activity engaged in to collect the Intel, traceback, and even block an attack or identify data may be automated. For example, let's use a scenario, you may or may not find realistic, just to prove my point: you have been persistently attacked and are constantly suffer DDoS attacks or are constantly losing valuable data. You have attempted to clean up but the bot in your network is persistent, regenerates and is difficult to remove. You develop your own code, attach it to the "phone home" function of the bot, and when the bot reaches out to speak to its CnC server your code is dumped on the server and blocks the communication path. Now, have you violated the CFAA, gained unauthorized access to the server? The server of the so-called "innocent bystander" has gained unauthorized access to your network by placing and/or providing instructions to the bot. Also, how is your code any different from that of adware, cookies, spam, and a dozen other programs that run automatically on the Internet and load themselves up on your machine without your consent or knowledge? With the exception of spam, are these illegal? No.

CEO's have a fiduciary responsibility to protect the company. Doing nothing may be the best choice after a cyber-attack, but should not be the only choice. The decision to employ active defense should not be considered criminal by anyone, to include the Justice Department or courts. That is like saying

you cannot defend yourself if someone is beating on you or else we the police will arrest you. This is a civil issue if anything, and therefore must be well-documented and the leadership must be comfortable with their decisions and ready to defend them in court, before shareholders, clients, and the media if necessary.

David Willson *is a licensed attorney in NY, CT and CO, and focuses on risk management, cyber security, reputation protection and the law. He is the owner of Titan Info Security Group, a risk management and cyber security law firm. He holds the CISSP & Security + certifications and has two LLM's in International Law and in Intellectual Property law. He is a member ISSA and InfraGard. He is also on the Board of Advisors with Cylance.*

David is a retired Army JAG officer. During his 20 years in the Army, in addition to over eight years of litigation, he provided legal advice in computer network operations (CNA, CND, CNE), information security and international and operational law, and intelligence oversight, to the DoD, NSA, the Army, various combatant commands, and other agencies to include DNI, DTRA, JTF-GNO/DISA, INSCOM/1st IO, DIA, STRATCOM, and was the legal advisor to the IOTC, NASS, then JFCC-NW (now CYBERCOM).

E-Discovery Challenges in White Collar Investigations

David A. Kronig, Alexander B. Hastings and Edward H. Rippey



As the number and scope of large-scale white collar investigations continues to grow, the e-discovery challenges associated with these matters are becoming more acute. While many of the considerations associated with e-discovery in the civil context map to the realm of white collar investigations, several unique issues warrant particular consideration. This article aims to identify some of the primary challenges in fulfilling discovery obligations in a white collar investigation.

A. The Government's Broad Subpoena Power

Many of the unique issues with e-discovery in the white collar context arise from the inherent imbalance of power between the government and a company or individual under investigation. In general, civil litigation involves counterparties with equal power to compel discovery and who often (although not always) share a concern for minimizing e-discovery costs. However, in a white collar investigation, the government has broad authority to compel discovery, often without the need to consider costly reciprocal requests. This authority can lead to broad subpoenas that request wide swaths of data, such as "all documents related to" a subject area over many decades or copies of everything on certain custodians' hard drives.

However, this broad subpoena power is somewhat tempered by the reality of limited resources. For instance, the Department of Justice ("DOJ") has explained that its investigators should avoid collecting information that they lack the resources to review and should encourage producing parties to propose ways of narrowing the scope of discovery.[1] These limited resources are an important consideration in narrowing the scope of an investigation and the amount of material that must be produced.

B. Planning Discovery & Communicating with the Government

To minimize the scope, cost, and length of an investigation, counsel should develop a discovery plan as early as possible. After a subpoena is served or an investigation is otherwise underway,[2] counsel should issue the appropriate document preservation notices and begin collecting initial information in

---

[1] *See* Tracy Greer, *Electronic Discovery at the Antitrust Division: An Update* (October 15, 2014), *available at* http://www.justice.gov/atr/public/electronic_discovery/281388.pdf.

[2] Of course, discovery obligations may begin before a subpoena is served. Similar to civil litigation, a duty to preserve may arise when there is a reasonable anticipation that the government will begin an investigation or bring charges. *See, e.g.*, Sarbanes-Oxley Act, 18 U.S.C. § 1519 (imposing criminal liability on individuals who destroy information in "contemplation of" a federal investigation); *United States v. Kernell*, 667 F.3d 746 (6th Cir. 2012).

preparation for a discovery plan. Such information includes: (1) the number of potential custodians; (2) the estimated number of total documents and pages; (3) the number of gigabytes or terabytes of data; and (4) the number of hours it would take to review that data, both for relevance and privileged material. This information both establishes the resources required to respond to the investigation and sets the government's expectations as to what is practical and reasonable in terms of timing of productions and the scope of review.

Armed with this information, counsel should begin discussions with the government as soon as possible. While there is no criminal corollary to Federal Rule of Civil Procedure 26(f)'s requirement that parties meet and confer to discuss discovery issues, communication with the government should be an essential part of counsel's strategy. Indeed, once counsel has gathered the information described above, it may be strategically beneficial to present the government with a proposal that, among other things: (1) describes any relevant document retention policy; (2) establishes a time period for which documents will be collected; (3) lists proposed custodians and search methodology; (4) sets out the order of custodians for review and production; and (5) proposes the form of production. Depending on the circumstances of the investigation, it may not always be in the client's best interests to present such a proposal—but, doing so can frequently help set a cooperative tone and define reasonable parameters for productions. A "hit report," which is a test of the proposed search terms on a handful of custodians, can be a useful tool to demonstrate to the government that the discovery plan strikes the appropriate balance—that is, that it casts a broad enough net for the government to conduct an effective investigation, while not producing mountains of irrelevant data.

Early communications with the government should also address whether certain technologies can be used to ease the burden on both the producing party and the government. For instance, predictive coding can reduce the cost for the producing party, while also satisfying the government's potential desire for quick productions. Other solutions such as deduplication and e-mail threading should be considered, as they can reduce the amount of material that must be reviewed by both the producing party and the government. Indeed, the DOJ's Antitrust Division recognizes these advantages and has negotiated agreements allowing producing parties to use these approaches to reduce the cost and scope of production.[3]

During these negotiations, the government may inquire about a client's IT systems, document retention policies, and the various servers and other devices on which potentially relevant information may be stored, such as personal telephones or computers. The government may also have specific requirements concerning metadata and the format of the production. As a result, it is often advantageous to involve IT professionals from both sides who are familiar with the government's needs and the producing party's IT systems. Often-times, communication between members of the IT staffs can identify and resolve potential issues at the outset before they become serious and costly problems down the road.

---

[3] *See* Greer, *Electronic Discovery at the Antitrust Division: An Update*, *supra*.

Granted, circumstances vary from case to case. But in general, the early and continued communication with the government in developing and implementing the discovery plan is critical because it can lead to a significantly narrower and less burdensome review process. Moreover, transparency with the government throughout the discovery process fosters a more cooperative tone, giving the government more comfort that it is receiving the information it needs to conduct an effective investigation and making it less likely that the government will subsequently challenge the data collection efforts. All this, of course, can lead to a less costly, less disruptive, and shorter investigation. That said, it is advisable that counsel keeps detailed records of collection efforts throughout the investigation to ensure that, should the need ever arise, the data collection efforts are defensible.

C. Electronic Storage Devices

In addition to issuing subpoenas that seek production of all documents related to a broad subject area, the government has started to seek production of electronic storage devices ("ESDs"), such as computer hard drives. These requests are becoming more common, especially in light of the Securities and Exchange Commission's ("SEC") new forensics lab, which enhances the agency's ability to recover modified or deleted ESI from ESDs. However, counsel must be sensitive to the fact that these devices often contain information that is far outside the scope of the investigation and/or potentially privileged. While the authority of the SEC to subpoena ESDs remains largely untested, requests for ESDs are being made and, therefore, solutions to mitigate the risks associated with this broad production must be considered.

One such solution (at least with respect to privilege concerns) lies in Federal Rule of Evidence 502 ("Rule 502"). Under Rule 502(b), disclosure of privileged material does not result in a waiver so long as the disclosure was inadvertent and the holder of the privilege took reasonable steps to prevent disclosure and to rectify the error. Further, the government may be given access to the ESD pursuant to a "claw-back" or "quick-peak" agreement, which generally protects against waiver and requires the return of privileged material that is produced. Some agencies may also be willing to use "clean teams"—teams of attorneys who are walled off from the underlying investigation—to review materials for potential privilege issues. However, while Rule 502(e) ensures that such agreements are binding on the signatories to the agreement, it may be advantageous to seek a court order under Rule 502(d) providing that production of privileged documents does not result in waiver in other federal or state proceedings. Of course, while such an order could protect against waiver in subsequent civil proceedings or other investigations, it may not be practical to seek one in light of certain time constraints and the status of the investigation.

D. Sanctions and the Dangers of Spoliation

Those versed in the area of e-discovery are well aware of the threat of sanctions for spoliation. While these sanctions in the civil context can be severe, the stakes are often even greater in white collar investigations. Explaining to the government that spoliation has occurred will likely make investigators less trusting of the discovery plan and may cause them to prolong the investigation and expand its scope. Moreover, should an investigation reach the trial stage, the same range of sanctions for spoliation are available as in civil litigation, but there are also a host of consequences that are much more severe than civil penalties. Most dramatically, the government can prosecute a range of obstruction of justice charges and may even choose to abandon the underlying investigation and instead pursue obstruction charges that could be easier to prove.[4]

Therefore, it is crucial that counsel consider early and often the ways to prevent spoliation. In particular, special care must be taken when issuing document preservation notices in light of the sensitive issues involved in a white collar investigation. Counsel should consult with IT professionals and potentially a forensic expert to ensure that data is preserved. While not necessarily required or warranted in every instance, counsel may also consider taking a forensic imagine or "snap shot" of key ESDs, such as an important custodian's hard drive. Of course, while these steps may be important in protecting data, they should not unduly delay the issuance of a preservation notice. Moreover, after a preservation notice has been issued and data collection is set to begin, special consideration should be given to whether self-collection is appropriate in certain situations, especially where custodians may be reluctant to comply with discovery obligations.

E. Cross-Border Concerns

Similar to civil litigation, counsel must be aware of cross-border concerns that can arise during a white collar investigation. Indeed, investigations involving the Foreign Corrupt Practices Act are particularly prone to cross-border issues because they often focus on overseas conduct and involve documents located abroad. Unlike discovery rules in the United States that generally allow for discovery of relevant material, many countries have strict data-privacy laws that limit the collection, processing, and transfer of "personal data." Many countries broadly define "personal data" to include a host of electronic data, including e-mail.[5] Further, some data-privacy statutes broadly define the notion of processing to include any operation that is performed on personal data.[6]

---

[4] *See, e.g.*, *Kernell*, 667 F.3d at 756 (affirming obstruction of justice charge under 18 U.S.C. § 1519 when defendant deleted information in anticipation of an investigation).

[5] *See, e.g.*, European Union Data Privacy Directive, 94/46/EC, ch. I, art. 2(a) (providing that "'personal data' shall mean any information relating to an identified or identifiable natural person").

[6] *See, e.g.*, European Union Data Privacy Directive, 94/46/EC, ch. I, art. 2(b) (providing that "'processing of personal data' . . . shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction").

These broad definitions often mean that simply the preservation of data (much less its collection and review) raises data privacy concerns because the implementation of a litigation hold can be viewed in some countries as data processing. However, preservation of foreign material may be crucial because, although government investigators may not be able to compel discovery abroad through their subpoena power, they can require the production of foreign material through a Mutual Legal Assistance Treaty—a bilateral treaty that provides for the exchange of evidence and information between signatory nations. Therefore, to the extent a country's data privacy requirements are unfamiliar, local counsel should be consulted to ensure that any collection or processing of data complies with the law. In addition, when a government investigation potentially implicates foreign discovery, counsel should advise the government as soon as practicable that certain data is located overseas and thus may be inaccessible or take longer than usual to produce.

F. Conclusion

Every white collar investigation involves unique twists and turns. Throughout any investigation, though, counsel should remain attuned to potential e-discovery issues. The two keys to resolving many issues that may arise are (1) to cultivate an early and thorough understanding of the universe of the client's data, and (2) to maintain ongoing, candid communication with the investigating entity. With these principles in mind, counsel will be well positioned to guide their clients to an efficient and favorable resolution of any investigation.

David Kronig *(dkronig@cov.com) a graduate of the Georgetown University Law Center, is a litigation law clerk and in the E-Discovery Practice Group at Covington and Burling, LLP.* ***Alexander Hastings*** *(ahastings@cov.com) is a government contracts and litigation associate and a member of the firm's E-Discovery Practice Group.* ***Edward Rippey*** *(erippey@cov.com) is a partner at the firm, handles complex commercial litigation, and is Chair of the E-Discovery Practice Group.*

Stopping the FTC's Unreasonable Data-Security Rampage

By Hillard M. Sterling and Christina M. Liu


Hackers are thriving and staying steps, indeed miles, ahead of the companies they target (pun intended). Social media has become the hackers' main platform, where phony links and web pages plant highly sophisticated malware into cell phones and other mobile devices, for eventual transmission into corporate America's computer systems. It has become increasingly true that there are two types of companies: those that know they have been hacked, and those that don't.

FTC's Aggressive Enforcement Actions

The government now states that it is here to help, and, as famously observed by Ronald Reagan, those words are indeed terrifying. The Federal Trade Commission has been flexing its muscles and requiring businesses to implement "reasonable" data-security measures. What does "reasonable" mean? Well, the FTC does not say, at least not before a breach. After a business has been hacked, and someone steals sensitive data, the FTC may decide that the protective measures were "unreasonable," and then sue.

Where does the FTC get this authority? Accordingly to the FTC, it can regulate data security, and require reasonableness, under Section 5 of the 100-year-old FTC Act, which empowers it to regulate "unfair" or "deceptive" practices. According to the FTC, stolen data is "unfair" to consumers, who are "deceived" if companies state or imply that their systems are secure.

What about fairness for the businesses who somehow must predict which data-security protections are "reasonable," hence mandatory? The FTC's guidance on that front, unfortunately, is scant at best. The FTC has issued or endorsed certain guidelines, but most are vague and offer few discernable industry-specific data-security standards. Worse, those guidelines are no shield against litigation by the FTC, since "reasonableness" may require something more than the guidelines, depending on the unique factual circumstances under which businesses receive, store, transmit, and protect data.

These ex-post-facto actions appear to be quintessential examples of punishing the victims. Courts typically serve as a bulwark against such draconian exercises of overbroad regulatory power. Academically, the FTC's muscle-flexing looks like an ideal candidate for a legal challenge based on violations of constitutional principles of procedural fairness and due process. The practical reality, however, is to the contrary. When the FTC sues, the natural inclination is to settle. Otherwise,

businesses face the unsavory specter of protracted and expensive litigation, compounded by enormous risks of bad publicity and a black eye in the marketplace.

Most businesses, in fact, are settling rather than litigating. One recent review observed that, "[u]sing the deception prong, the FTC has brought and settled more than 30 cases challenging the companies' claims about the security they provide for consumers' personal data and more than 20 cases alleging that a company's failure to reasonably safeguard consumer data was an unfair practice."[1] The terms of these settlements often are confidential, but they invariably involve substantial fines, as well as ongoing compliance standards that are enforced through regular audits. The resulting costs and burdens are staggering.

Recent FTC Challenges

However, there are two pending cases in which companies are resisting and challenging the FTC's assertion of generic authority to regulate data security. After getting sued by the FTC in New Jersey federal court, Wyndham Worldwide Corporation fought back and filed a motion to dismiss, arguing that the FTC lacked such authority to regulate data security and demand amorphous "reasonable" measures. Although Wyndham's arguments were compelling, in her April 7, 2014 order, Judge Esther Salas rejected them, denied the motion, and declined to limit the FTC's authority in any manner.[2] Judge Salas specifically held that the FTC can bring data-breach actions under the "unfairness" prong without first issuing standards.[3]

Monday-morning quarterbacks criticized Wyndham for filing the dismissal motion, which was panned by some as a strategic blunder that only emboldened the FTC. However, Wyndham may be vindicated after all. On June 23, 2014, Judge Salas permitted Wyndham to seek an interlocutory review of portions of the April 7, 2014 opinion. In particular, Judge Salas ordered the following questions to be certified for interlocutory review by the Third Circuit: (1) "Whether the Federal Trade Commission can bring an unfairness claim involving data security under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a);" and (2) "Whether the Federal Trade Commission must formally promulgate regulations before bringing its unfairness claim under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a)."

Wyndham has filed its appellate brief, arguing that the FTC does not have authority to regulate businesses' data-security as "unfair" or "deceptive," and that extending the definition of "unfair" to cover cybersecurity was too much of a stretch. Wyndham also attacked the sufficiency of FTC's complaint as failing to allege "sufficient injury" that is "not reasonably avoidable by consumers

---

[1] Gina Stevens, "The Federal Trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practices (UDAP) Authority," September 11, 2014, Congressional Research Service, available at http://fas.org/sgp/crs/misc/R43723.pdf.

[2] *FTC v. Wyndham Worldwide Corp*., 2014 BL 94785, D.N.J., No. 2:13-cv-01887, 4/7/14.

[3] *Id*.

themselves," who arguably could have avoided injury by, for example, accepting Wyndham's offer to reimburse the fraudulent charges.

In another recent case, in an FTC-friendly administrative action, the FTC filed a claim against LabMD, alleging a failure to protect consumer health data in two instances in 2008 and 2012. LabMD has wrapped up operations since the complaint, citing the "debilitating effects of the FTC's investigative practices and litigation." [4] Nevertheless, the legal battle continues and creates another rare but potentially important challenge to the FTC's assertion of expansive data-security authority. Specifically, in March 2014, LabMD fought the FTC and filed a lawsuit and a motion for a preliminary injunction in the Northern District of Georgia. The federal court dismissed LabMD's suit as nonjusticiable, and LabMD then appealed to the Eleventh Circuit.

In its appeal, LabMD argued that the FTC lacked authority under Section 5 to regulate personal health information data-security practices because: (1) HIPAA and HITECH provide the sole regulatory schemes applicable to healthcare data-privacy practices, and, as Wyndham has argued, and (2) the FTC's enforcement action violated due process because of the absence of any administrative guidance regarding what could be considered "unfair" data-security practices under Section 5.

However, LabMD also included two highly unusual arguments in its appeal that may increase the odds that the case will end up in front of the U.S. Supreme Court.[5] First, LabMD argued that the appellate court had jurisdiction to rule prior to the administrative proceedings, which were a foregone conclusion given the consistently favorable rulings for the FTC. Given that LabMD's administrative case is still pending, there are long odds that the Eleventh Circuit would deem this case ripe. If the Eleventh Circuit did side with LabMD, the risks of destabilizing administrative law and federal agency oversight are especially high. Courts are generally hesitant to make bold moves on justiciability. LabMD also invoked the First Amendment, arguing that the FTC's investigation tactics and monitoring stifled LabMD CEO Michael Daugherty's free-speech rights. This argument has a higher chance being appealed to the Supreme Court, due to the Supreme Court's penchant towards those arguments in recent opinions.

The Wyndham and LabMD cases may lead to a split of authority on the core issue of whether the FTC has authority to regulate data-security under Section 5 of the FTC Act. If that occurs, the issue may be teed up for Supreme Court review. Those cases, however, also may be decided on their unique issues, such as LabMD's arguments based on the arguably exclusive jurisdiction of HIPAA and HITECH over health care data.

---

[4] Press Release, "FTC Actions force LabMD to Wind Down Operations." January 28, 2014, available at http://michaeljdaugherty.com/2014/01/29/labmd-winds-operations/.

[5] "LabMD May Struggle at 11th Circuit, Positioning itself for Supreme Court, Lawyers Say," September 29, 2014, Warren's Washington Internet Daily," available at http://www.drinkerbiddle.com/files/ftpupload/PORTAL/Warren_Washington.pdf.

Given the absence of clarity to the FTC's requirement of data-security reasonableness, many businesses are waiting with bated breath for these appellate rulings. But clarity may be a long way off. Even if Wyndham and LabMD won their appeals, other trial and appellate courts across the country may endorse the FTC's authority. Perhaps the authority issues may reach the Supreme Court in several years. In the meantime, businesses are faced with the ongoing risk that their data-security protections may be challenged by the FTC as unreasonable and deficient.

Turning to Congress for Clarity

Although this sounds like wishful thinking and counterintuitive in today's political climate, the ball is in Congress's court to bring clarity here. Although there have been multiple competing data-security bills that have gone nowhere in the past several years, the costs of inaction and gridlock are intolerable. There seems to be a bipartisan consensus on the obvious reality that the status quo is unacceptable. Moreover, there are several potential key areas of additional bipartisan compromise.

First, both parties should find common ground on the need for specificity in data-security standards. Senator Rockefeller (D-W.Va.) has proposed a bill granting the FTC authority to write and enforce rules requiring specific data-security measures. Although the natural inclination for Republicans and industry groups is to oppose yet another governmental regulatory monolith, they also cannot find comfort in the FTC's boundless self-declared mandate to sue companies for unreasonableness.

With agreement on the need for specificity, the parties would need to confront the vexing issue of who defines the specifics. The FTC has been angling to expand its power. In recent FTC testimony before Congress, the agency has advocated for legislation that would: (1) strengthen its existing authority governing data-security standards on companies and (2) require companies to provide notification to consumers where there is a data-security breach. In both those areas, the FTC seeks the power to impose fines and to issue governing rules.[6] A number of Senate bills are pending that would increase and strengthen the FTC's regulatory reach over data security.[7]

However, the FTC appears uniquely unqualified to detail specifics over data-security for the entire economy. There simply is little if any data-security mastery there, certainly not for the wide spectrum of affected industries. Also, to mandate nationally applicable data-security standards makes no sense. Businesses face distinct security challenges depending on their respective industries, the types of data they handle, to whom they transmit their data, from where they receive their data, and a host of additional factors.

It makes much more sense, therefore, for industry groups to serve a central role in the development and preparation of the rules governing how businesses should protect their data. The need for negotiated rulemaking has been a hot topic for years, and data security appears to be an ideal area to

[6] See supra n. 1 at 12.
[7] *Id.*

bring industry groups into the governmental fold as a central part of the rulemaking process. The draft rules, of course, still would be subject to public review and comment. The result would be industry-specific standards prepared by knowledgeable businesses and constituencies, and based on real-world cost-benefit calculi that are far outside the government's capabilities.

But negotiated rulemaking, alas, does not appear to be in the cards. Congress's various bills, instead, have focused on providing (and often enhancing) governmental authority in this area (often through the FTC), and/or implementing more modest measures such as nationally uniform notification requirements. Policy experts are hopeful that a united Republican Congress will more favorably view to at least one piece of federal legislation: the Cybersecurity Information Sharing Act (CISA). CISA would allow the government and private sector to share cyber-threat indicators protected from certain disclosures and lawsuits.[8] This could be a sign of more legislation to come, but an agreed and bipartisan approach on the substantive principles governing the regulation of data security, or the FTC's authority to enforce those principles, seems far away. And even farther away, given today's climate, is the prospect of a meaningful set of industry-specific data-security standards developed with the true involvement of the businesses that must abide by them.

Conclusion

Data security has placed businesses between a rock and a hard place. On the one hand, they are fending off armies of increasingly sophisticated hackers. On the other, they face daunting risks of a post-breach governmental challenge for failing to act reasonably. It is time for clarity and specificity. Although these aspirational objectives may be agreed by most, their realization appears remote unless the judiciary or Congress acts promptly and meaningfully to stop the FTC from attacking victimized businesses for having failed to implement "reasonable" preventive measures.

Hillard M. Sterling *is managing partner of Winget, Spadafora & Schwartzberg, LLP's Chicago office. Mr. Sterling regularly represents a broad array of professionals in litigation, including attorneys, architects & engineers, accountants, agents and brokers, and real-estate professionals, among others. Mr. Sterling also represents directors & officers in a variety of business disputes. Mr. Sterling's practice also focuses on technology and cyber disputes and issues, bringing 25 years of experience in the entire range of technology cases, such as disputes related to systems implementation, software development and licensing, and IT intellectual property. In addition, Mr. Sterling counsels clients on developing and implementing best practices before, during, and after data breaches and incidents. Mr. Sterling has served as an expert commentator in print and broadcast media, and regularly speaks and presents, on various technology topics.*

Mr. Sterling's practice also extends to other types of commercial matters, including shareholder and partner disputes, intellectual property, employment, securities, antitrust, the False Claims Act, and products liability. Mr. Sterling is a 1986 graduate of Northern Illinois University, where he received his

[8] Cory Bennett, "Cyber bill Advocates pin hopes on GOP Congress." November 9, 2014, The Hill, available at http://thehill.com/policy/cybersecurity/223442-cyber-bill-advocates-pin-hopes-on-gop-congress.

B.A., summa cum laude. He received his J.D. in 1989, magna cum laude, and Order of the Coif, from Georgetown University Law Center, where he was an Executive Editor of its flagship law review, the Georgetown Law Journal. Mr. Sterling is admitted to practice law in Illinois and Washington, D.C., and various federal courts including the trial bar of the Northern District of Illinois.

***Christina M. Liu** is an associate at Winget, Spadafora & Schwartzberg, LLP's Chicago office. She focuses her practice on civil litigation with an emphasis on representing insureds in a wide range of business disputes including the defense of professionals, directors, and officers in a wide range of business disputes. Prior to joining Winget, Spadafora & Schwartzberg, LLP, she gained substantial experience at a boutique firm where she litigated and managed high-profile cases, took and defended over eighty depositions, argued at a multitude of hearings, and served as trial counsel. Ms. Liu also served as an Assistant General Counsel at the Illinois Department of Insurance in Chicago. During her time in-house, Ms. Liu gained first-hand administrative, regulatory, litigation, counseling, contract review, and legislative experience.*

Ms. Liu is a 2003 graduate of Columbia University, where she received her B.A. in Political Science. She received her M.Sc. in Law, Anthropology and Society in 2004, with Merit, from the London School of Economics and Political Science. She received her J.D. in 2007 from the University of Miami School of Law. During law school, Ms. Liu served as a judicial intern for the Honorable Donald L. Graham, U.S. District Court in the Southern District of Florida, as a legal and policy intern at the United Nations: Office of the Global Compact, and as a trainee at Majmudar & Co., a national law firm in Mumbai, India. Ms. Liu is admitted to practice law in Illinois, the District of Columbia and New York, as well as the trial bar of the Northern District of Illinois.

Beware of Visual Hacking: Are You Protecting Client Confidences?

By Mari J. Frank

Have you considered who might be viewing and collecting information about your clients and cases without your awareness? Many of us are tethered to our smart phones, tablets, laptops, and other engaging electronic devices. Instantaneously, we connect to our office, clients, opposing counsel, the court, the cloud, and more from myriad places including restaurants, airplanes, trains, the beach, or just about anywhere where connection is available. This mobility allows for flexibility, quick connectivity, and creativity. But mobile technology also exposes our clients' sensitive information to increased privacy and confidentiality vulnerabilities.

Those dangers, discussed in *The Visual Data Breach Risk Assessment Study* (released in December 2010), conducted by People Security and commissioned by 3M, revealed that two thirds of employees expose sensitive data outside the workplace, some even exposing highly regulated and confidential information. The study also found that the majority of businesses do not have visual privacy policies or measures in place to protect sensitive information from computer screen snooping when employees are working in public places. To download the studies, go to http://www.3Mscreens.com/whitepapers.

Lawyer professional responsibility rules require us to protect our clients' personal information and keep their confidences. Yet sensitive information is in jeopardy when client data is viewable by unauthorized persons. New technology allowing for storage of huge amounts of data in minute computerized electronic gadgets makes securing confidences challenging. To assure confidentiality of all communications, including private documents, financial statements, and other restricted client data which should not be seen or captured without consent, we must be vigilant. Our clients have a reasonable expectation that their private communications will be kept top secret and securely maintained. Confidentiality in conjunction with privacy has always been the hallmark of the attorney client privilege and the heart of our trusted relationships with our clients.

Although distinct concepts, privacy and confidentiality go hand in hand. Confidentiality is an ethical principle regarding safeguarding communications between lawyers and those we serve. The information is "privileged" and may not be divulged to third parties without client permission. In conjunction with confidentiality, data privacy denotes the right of our clients to control what personal information they may reveal about them, and how it is accessed, viewed, acquired, stored, shared, heard, and safeguarded. Ethically, we have a duty to be watchful and transparent about collecting, sharing, protecting, and securing data and private information. Permission is mandatory to share

privileged communications, and when we no longer need to use the data, we must safely store it for a reasonable period of time, or return or destroy it completely when discarding.

The America Bar Association Rules of Professional Conduct (revised August 6, 2012) address the issues of confidentiality and privacy with its relation to electronic age as stated below:

Rule 1.6 Confidentiality of Information

(a) A lawyer shall not reveal information relating to the representation of a client

unless the client gives informed consent…….

(c) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Inadvertent or unauthorized disclosures are menacing. An enormous threat to confidentiality is ***visual hacking,*** or the act of viewing or capturing sensitive, confidential and private information for unauthorized use. It is often overlooked when protecting client hard copy information and electronic data. Visual privacy deals with our ability to protect sensitive information as it is displayed on an electronic device screen or hard copy documents in an open environment. Given the vast digitization of sensitive information, the proliferation of remote viewing technology, and the ease of capturing data with tiny cameras, video surveillance, drones and smart phones, visual privacy breaches are an under recognized danger.

Consider if your office is exposed to these ***visual hacking*** risks:

Do you or your staff:

- Leave hard copy files out on desks and conference tables unattended after hours
- Forget to lock hard copy cabinets when not in use
- Fail to use shredders and locking bins when discarding confidential copies
- Disregard the use of encryption for sensitive documents in transit or at rest
- Ignore using secured electronic vaults for sharing documents
- Neglect to password protect sensitive data and confidential attachments via email
- Fall short with regard to limiting access to only those people who need know
- Allow staff to keep computer and electronic device screens unprotected without passwords and time outs

- Fail to use privacy filters for computers, smart phones, and other electronic devices.

To assess risk, take a walk around your office and record a visual privacy audit. Ascertain if your office is implementing reasonable on-line and off-line procedures to protect client confidences.

Our law offices have a duty to safeguard private, confidential information from prying eyes, and curious ears! When transmitting any sensitive client communication, whether by smart phone, text, or email, we are required to take *reasonable* precautions to prevent confidential information from disclosure of any kind to unintended recipients. Although it is daunting to keep up with new laws and cases, software and hardware technology, run a practice, get paid, and employ best practices for privacy and confidentiality strategies, these multifaceted tasks indicate lawyer *competenc*y under the ABA and state Rules of Professional Conduct.

Rule 1.1 Competence

A lawyer shall provide competent representation to a client. Competent representation

requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for

the representation.

To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the ***benefits and risks associated with relevant technology****, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.*

Aside from our professional responsibility standards, we also are obligated to comply with state and federal laws regarding data privacy and security.

For example:

California Civil Code 1798.81.5 states:

(a) . . . *the purpose of this section is to encourage businesses that own or license personal information about Californians to* ***provide reasonable security for that information.***

(b) A business that owns or licenses personal information about a California resident ***shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure****.*

1798.82. (a) *Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, s****hall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.***

Law offices collect "personal information" such as the Social Security number, the driver's license number, bank account numbers, health insurance information, etc. Although there is no federal security breach law, attorneys in the 47 states that have passed security breach laws, must disclose security breaches just as any other business when unencrypted personal computerized information is acquired by an unauthorized person. California and other states have interpreted *computerized* information to also include printed documents that were derived from a computer, therefore expanding the disclosure requirement to hard copies printed from devices.

We hear daily about massive security breaches by hackers acquiring millions of records of sensitive consumer data. But security breaches are also accomplished in less remote ways. For example, there are unscrupulous employees who remove and sell electronic records on thumb drives; and there are negligent staff who inadvertently allow access to their computers through social engineering, or through plain *visual hacking.*

A *visual data breach* is the result of close range or remote *visual hacking.* It can be accomplished when an unauthorized person views or captures confidential information from the open, active screen of a computerized device or visual misappropriation of sensitive data from hardcopy documents that may be left at unattended desks, workstations, fax machines, easily accessible file cabinets, unlocked trash bins, etc. Many unreported breaches occur because of low-tech privacy intrusions rather than high tech weaknesses.

With handy mobile gadgets available to use in almost any public place, we may easily become distracted and oblivious to snooping eyes around us. Even in our offices, how aware are we of visual displays of confidential data when clients, visitors, temporary employees, and repair people are on the premises during the day? And who has access to our offices after hours and on weekends? We must be conscious in the office and when working remotely as to what is visible to unauthorized persons.

To address the privacy vulnerabilities while you are working at the office or remotely, take proactive steps to protect your clients and your practice. Here are some tips to protect your clients' private and confidential information:

1. Create a visual privacy policy for the office. Then train, test, reward, and enforce best practices.

2. Use privacy filters and privacy screen protectors for smart phones, computers, tablets, and other electronic devices. (For example, 3M manufactures removable privacy screens for computers and all electronic devices that black outside views and only allow the user to see the screen. Nosy neighbors will only see a blank screen. You can use traditional privacy filters, and, (or) the 3M ePrivacy Filter, a facial recognition software which alerts users to onlookers, for visual privacy from virtually every angle.) Your privacy policy should require that privacy screens on devices be utilized at least while working in public places and where unauthorized persons can view screens.

3. Utilize passwords or secret design codes on your smart phone and other devices. Change your passwords often and after every instance of using public kiosks, in the event you could have been shoulder surfed. Be aware of your surroundings and where you are accessing sensitive information. Position your hands, body, and devices to avoid intrusive onlookers.

4. Institute "timeouts" for computers and electronic devices and implement privacy settings. Lock electronic devices when not in use, activate screen savers, and set up a secure vault for remote access. Set up devices so that you may remotely erase them in case of loss or theft.

5. Implement encryption for sensitive data and utilize dual or multiple authentication practices for decryption. All parties must have the "key" to authenticate. Redact the information that needs to be secured before distribution.

6. Make sure you have shredders issued to all attorneys and personnel and place them next to copiers, fax machines, scanners. They also should be a prerequisite for all who qualify to telework or qualify to use secure remote network access

7. Attach visual exposure security warning labels to all low threat tech and tech-related devices such as scanners, printers, file cabinets, waste containers, video conferencing equipment, etc.

8. Operate on a strong "need to know only" policy when replicating or distributing information that needs to be secured. Adopt a "Not in Plain View" policy for desktops, conference rooms, mobile settings, teleworkers, and remote activities.

Our clients depend upon us to safeguard their confidences and protect their private information from being seen by the wrong persons. Sensitive data displayed on a screen is vulnerable to viewing, either by "shoulder surfing" or by advanced optics used by sophisticated hackers. Technology is rapidly improving. The result will be more powerful mobile devices capable of containing mega confidential data easily accessible in public areas and facilities. Visual privacy is a crucial concern and sensitive data on screens and in plain view must be protected from risk of exposure by passers-by. Visual privacy controls, such as privacy filters on computers and mobile electronic devices, along with visual privacy policies outlining specific actions, procedures, and best practices are vital to protecting confidences in the evolving practice of law.

Mari J. Frank, Esq. *CIPP is an attorney–mediator, Certified Information Privacy Professional, radio host, and author in private practice in Laguna Niguel, California. She s a Fellow with the Ponemon Institute, a Board Member of the Privacy Rights Clearinghouse, and a member of the Visual Privacy Advisory Council. Her testimony has been accepted in Congress, the California legislature, the Social Security Administration, the Federal Trade Commission, and she is a qualified privacy expert in state and federal courts. Some of her books include: Safeguard Your Identity; From Victim To Victor: The Guide To Ending the Nightmare of Identity Theft; The Complete Idiot's Guide To Recovering From Identity Theft. Her radio Show Privacy Piracy airs on Monday mornings at 8 AM Pacific time on 88.9 FM in Irvine streaming also at kuci.org. Her PBS TV Special: Protecting Yourself in the Information, and her many other TV appearances aired nationally. Visit* www.kuci.org/privacypiracy; www.identitytyeft.org; www.MariFrank.com

2014 (4Q) Information Law Updates: Cases, Statutes, and Standards

By Thomas J. Shaw

In the fourth quarter of 2014 and the end of the third quarter, there have been many developments in U.S. and international information law, especially information security, privacy, and cloud computing cases, statutes, and standards. These include international and U.S. state and federal laws and regulations passed or coming into force. It also involves civil and criminal cases and enforcement actions brought by regulators. And it encompasses the new standards, guidelines and legal ethics opinions in this area. But it does not attempt to track legislation that has not yet been passed. To briefly summarize the major developments in this area of law and practice, each significant development is presented with a brief analysis after it. Deeper analyses of these developments can be found in other articles in this publication and in writings and presentations by various members of the committees.

These recent developments are categorized as:

- Statutes and Regulations – U.S.
- Statutes and Regulations – International
- Cases – Civil and Criminal
- Cases – Regulatory
- Standards and Guidelines

Statutes and Regulations – U.S.

State Laws[1]

Delaware passed a law addressing the digital assets of deceased persons. Modeled on the NCCUSL's Uniform Fiduciary Access to Digital Assets Act, this law gives the fiduciary over the assets (e.g. trustee, guardian, personal representative) the same rights in the digital assets such as email accounts as the deceased account holder had. The account's custodian (e.g. an Internet email provider such as Google) needs to allow access, copying or deletion of the account within 30 days of receiving a "valid written request" from the fiduciary. Custodians who do not comply are subject to both court orders and damages, while those who reply in good faith are immune to liability.

[1] Delaware, HB 345, An Act To Amend Title 12 Of The Delaware Code Relating To Fiduciary Access To Digital Assets And Digital Accounts (Aug. 2014); Cal. SB 1177, An act to add Chapter 22.2 (commencing with Section 22584) to Division 8 of the Business and Professions Code, relating to privacy (Sept. 2014).); Cal. AB 1442, An act to add Section 49073.6 to the Education Code, relating to pupil records (Sept. 2014); Cal. AB 1710, An act to amend Sections 1798.81.5, 1798.82, and 1798.85 of the Civil Code, relating to personal information privacy (Sept. 2014); Cal. AB 2643, An act to add Section 1708.85 to the Civil Code, relating to privacy (Sept. 2014); Cal. AB 2306, An act to amend Section 1708.8 of the Civil Code, relating to privacy (Sept. 2014).

California has enacted several laws protecting the privacy of K-12 students. The Student Online Personal Information Protection Act prohibits website, online services, or mobile apps providers from creating a profile of students, advertising to the students, or selling or disclosing their information, in addition to requiring reasonable security, protecting student data from disclosure, and deleting the data if requested. Another law signed the same day requires third-parties used to gather information on students from social media to use data only within the purposes of their contract with a school/school district and to delete the data upon completion of the contract or age attained by the student. Also, the data gathered must only be concerned with student or school safety and the student has a right to know what data has been gathered.

California has also amended its existing data protection laws to require that any identity theft prevention services offered after a data breach be for twelve months and at no cost to the consumer, to require reasonable security practices of any business that maintains personal information about a California resident (previously required for those who owned or licensed such data), and to prohibit the sale of SSNs. Other privacy enhancements to California laws include private rights of action for victims of "revenge porn" that also allow for equitable relief and the use of pseudonyms in filing the suits and making it an offense to use any type of recording device (including drones) to capture another engaged in personal or family activities where there is a reasonable expectation of privacy.

Chip and Pin Executive Order[2]

To increase the security of financial transactions, the Obama administration has issued an executive order requiring that government payment processing terminals and payment cards utilize enhanced security features including chip-and-PIN technology, stating by January 2015. Within 18 months, federal agencies making personal data available through digital means are required to implement multi-factor authentication and "an effective identity proofing process." Other steps to assist with the remediation of identity theft were directed, including the forwarding of compromised credentials and the identification of federal agency resources to assist victims of identity theft.

Statutes and Regulations – International

UK Employers and Social Media[3]

Similar to a number of laws passed by individual states in the U.S. to deal with employers who require employees or job candidates to sign in to social media sites to view postings made, the UK has decided to begin enforcement of section 56 of its Data Protection Act. This provision does not allow employers or potential employers to require employees or job candidates to produce a "relevant record" utilizing the data subjects' right of access.

---

[2] Obama Administration Exec. Order 13681, Improving the Security of Consumer Financial Transactions (Oct. 2014).

[3] UK, Ministry of Justice, Data protection guidance, *Update on commencement of Section 56 of the Data Protection Act* (DPA) 1998 (Sept. 2014).

Hong Kong Bank Data Protection Guidance[4]

The office of the personal data protection commissioner in Hong Kong has published guidance for banks. It first reviews the data protection principles in the Hong Kong privacy statute. Each is shown with practical examples of together with a list of the cases that they have handled. In addition, the guidance reminds banks of the need to adhere to the commissioner's Code of Practice for Consumer Credit Data. New measures added to privacy laws in 2012 are reinforced, such as the right of consumers to opt-out of direct marketing. Cases studies are introduced to provide advice, for the personal information collection statements banks must provide to its customers, personal identifiers, retention of customer data, intra-group sharing of customer data, and transfer of customer data outside Hong Kong. On the latter point, noting that despite the section prohibiting the transfer of personal data outside Hong Kong is still not in force, other related provisions must still be met. Also covered is transferring of data to law enforcement or regulators, use for debt collection, e-banking security, and privacy policies and practices.

Cases – Civil and Criminal

Nguyen v. Barnes & Noble[5]

The Ninth Circuit has ruled on the validity of browserwrap agreements and found them wanting under the facts of this case. The plaintiff filed suit after he his online order was cancelled due to lack of inventory and he was compelled to purchase another more expensive one. The defendant wanted to have the case heard in arbitration, as required under the terms of use. The terms of use were accessible to the plaintiff by a link shown on each webpage presented in the online ordering process. The court held that the conspicuous links on each webpage were not sufficient notice to the purchaser of the agreement he was entering into, given that there was no indication of mutual assent to the agreement and the system did not require an affirmative action of consent. Quoting a prior case, it stated that "validity of the browserwrap contract depends on whether the user has actual or constructive knowledge of a website's terms and conditions." Even though the links were proximate to buttons that had to be pressed to complete the order, this was not sufficient to provide constructive knowledge to the plaintiff. As such, the court ruled that the arbitration clause should not be enforced.

<u>CFAA Standing Cases</u>

Ferring Pharmaceuticals v. Watson Pharmaceuticals[6]

A district court in New Jersey has ruled that there was harm under the CFAA sufficient to create standing. This was a Lanham Act false advertising case involving a webcast presentation given by a

[4] Hong Kong SAR, Office of the Privacy Commissioner, *Guidance on the Proper Handling of Customers' Personal Data for the Banking Industry* (Oct. 2014).
[5] *Nguyen v Barnes & Noble, Inc.,* Case No. 12-56628 (9th Cir. Aug. 2014).
[6] *Ferring Pharmaceuticals, Inc. v. Warren Pharmaceuticals, Inc.*, Case No. Civ. No. 2:12-cv-05824 (D.N.J. Aug. 2014).

paid consultant for one pharmaceutical company comparing its product versus its rival's product. The defendant had counterclaimed violations of the CFAA for gaining access to its webcast-streaming servers, as the plaintiff "either evaded the password protections, or induced an individual who was invited and was provided with a password to exceed their authority and provide the password protected webcast" to the plaintiff. While the court said that the second scenario might not be actionable as an unauthorized access, the first scenario would be under the CFAA. The court ruled that there was sufficient loss from the costs to respond to, investigate, and remediate the actions of the plaintiff's incursion into defendant's servers to create standing and so refused to dismiss the CFAA counterclaim.

Pine Environmental v. Charlene Carson[7]

A district court in Massachusetts has ruled that a computer no longer used in interstate commerce is not subject to the CFAA. A former employee took the plaintiff's computer with her after resigning and joining a competitor. She had it returned several months later, after having accessed its information on customers of her former company and installing and utilizing software to delete relevant data on it. While her access to her former company's computer would have been unauthorized, the fact that she did not use it to access the former company's servers or network meant that it was no longer being used in interstate commerce. As such, it was no longer a "protected" computer and not subject to protection under the CFAA. So, the various claims arising from the actions of the defendant could only be pursued under state law.

Data Breach Standing Cases

Adobe Systems Privacy Litigation[8]

A district court in California has ruled that the risk of future harm is sufficient to give Article III standing. In this class action based on the defendant's 2013 data breach, the plaintiffs all alleged injury as either "(1) increased risk of future harm; (2) cost to mitigate the risk of future harm; and/or (3) loss of the value of their Adobe products." The court looked to the 2010 *Krottner v. Starbucks Corp.* decision where the Ninth Circuit ruled that possible future injury could confer standing when the plaintiff is "*immediately* in danger of sustaining some *direct* injury as the result of the challenged conduct." It distinguished the 2013 *Clapper v. Amnesty International USA* Supreme Court decision as not actually changing the Article III standing analysis and not overruling cases based on a substantial risk of harm requiring plaintiffs to incur costs to minimize or avoid them. Also, while the plaintiffs' risk of future harm in *Clapper* was highly attenuated and speculative, in the present case the risk of harm is "immediate and very real," as some of the data from the breach has already appeared on the Internet. The motion to dismiss for lack of Article III standing was denied.

---

[7] *Pines Environmental Services, LLC v. Charlene Carson and Fines Environmental and Survey, LLC*, Case No. 14-cv-12830 (D. Mass. Aug. 2014).

[8] *In re Adobe Systems, Inc. Privacy Litigation*, Case No. 13-cv-05226 (N.D. Cal. Sept. 2014).

Rejimas v. Neiman Marcus[9]

A district court in Illinois has ruled that the risk of future harm is not sufficient to give Article III standing, based on a different analysis and the precedents in that circuit. Of three recent cases in the Seventh Circuit, two did not allow for Article III standing based on the threat of future harm and one did. The two that did not focused on the "certainly impending" standard in the *Clapper* case. The one that did rationalized that *Clapper* had not overruled circuit precedence that any increased risk in future harm created sufficient injury in fact, but was a very strict reading of standing required by the national defense and constitutional questions. The court in the present case noted that of the 350,000 affected individuals, over 9,000 had already suffered fraudulent charges and likely more would. The court granted that the injuries would satisfy the "imminent" prong. But the fact that the fraudulent charges were reimbursed meant that these claims failed the "concrete" injury prong. The court felt that the threat of future harm from identity theft was not proved based on the data breach alone. For that reasons, time and money spent to prevent these were also not considered sufficient injury for standing. The court also did not accept that the theory that plaintiffs overpaid for the products purchased, as part of the purchase price was for information security that was clearly not implemented, as information security costs were "extrinsic" to the products purchased. Nor did the court accept the theory based on loss of control over personal information, because of the lack of concrete injury. The motion to dismiss for lack of Article III was granted.

_____

Ellis v. Cartoon Network[10]

Under a different statute, the VPPA, a Georgia district court found that the plaintiff had standing to bring a privacy claim. This was based on the statute allowing for redress, which itself gives an aggrieved plaintiff standing, even if there would not have been an injury without the statute. The plaintiff claimed that the defendant had disclosed his mobile phone app video viewing habits along with his Android ID to a third –party analytics company, without his consent. The analytics company used other information to reverse engineer the Android ID to determine his identity. But the court ruled that the Android ID which was disclosed was not personally identifiable information, as it took additional steps by the analytics company (the reverse engineering) to derive the personally identifiable information. There was no VPPA violation because the defendant did not disclose PII.

U.S. v. Akbar[11]

The federal government has charged a defendant under the ECPA with creating, advertising, selling, and disseminating a mobile phone software app that intercepts wire and electronic communications and conspiring to do so. Marketed primarily at those who suspect their partner of infidelity, the app StealthGenie is alleged to require a single installation by the purchaser and then it runs in the background unknown to the mobile phone user, while surreptitiously intercepting and recording

[9] *Rejimas, et al. v. Neiman Marcus Group LLC*, Case No. 14 C 1735 (N.D. Ill. Sept. 2014).
[10] *Mark Ellis v. The Cartoon network, Inc.*, Case No. 1:14-cv-484 (N.D. Ga. Oct. 2014).
[11] *U.S. v. Hammd Akbar*, Case No. 1:201414-cv-01273 (E.D. Va. Oct. 2014).

calls and surroundings and monitoring email, texts, voicemails, contacts, photos, videos, and appointments. The intercepts are then allegedly made available online for the purchaser to review.

Boston v. Athearn[12]

The state court of appeals in Georgia has determined that a jury should be able to hear the case against the parents of a boy who created a false Facebook account of a classmate and then filled it with distorted photos and racist and homophobic comments and invited others to view it. The suit is for the parents' lack of supervision and control of their child in allowing the defamatory material on the website to remain online for nearly a year after its initial publication, knowing it was causing injury to the targeted child.

Wyndham Derivative Suit[13]

A shareholder has unsuccessfully tried to bring a suit against the board of Wyndham Worldwide based on the same data breaches for which the FTC has started an enforcement action. The derivative suit stated that the board of directors had acted improperly in refusing his previous demand that they bring a lawsuit against corporate officials for failing to implement adequate data security and disclosing the data breaches timely. The defendants of this suit (the board) based their defense on the business judgment rule, failure to state a claim for which relief can be granted, and speculative and unripe damages. The court noted that the board had met and discussed this matter over a dozen times, had brought in external expertise, had seen that their recommendations were implemented, and had replied to the plaintiff's prior requests. Because the plaintiff could not overcome the high threshold required to defeat the business judgment rule (bad faith or unreasonable investigation), the motion to dismiss was granted.

Negro v. Santa Clara County[14]

In a case with a significant procedural trail, a court in Florida ordered discovery of Gmail documents from Google in California, based on the constructive or implied consent of the account holder, the defendant in litigation in Florida. The appeals court in California rejected this ability for a court to imply such consent, while at the same time affirming the ability of the court to order, for example through discovery sanctions, the party to consent to the production of such emails. This would allow Google to produce the emails, as an exception to the SCA restrictions placed on its ability to deliver such materials absent voluntary consent of a party to the communications. The California court held that the judicially-required consent did meet the requirements for voluntary consent under the SCA, as the defendant had the ability to refuse to comply with the Florida court order and then deal with the discovery sanctions in Florida. The court also rejected Google's arguments that it had a blanket exemption under the SCA to not produce documents for civil discovery purposes and

[12] *Boston v. Athearn*, Case No. A14A0971 (Ga. Ct. App. Oct. 2014).
[13] *Palkon, derivatively on behalf of Wyndham Worldwide Corp v. Wyndham Worldwide Corp., et al.*, Case No. 2:14-cv-01234 (D. N.J. Oct. 2014).
[14] *Negro v. Sup Ct. Santa Clara*, Case No. 1-13-CV239634 (Cal. Ct. App. Oct. 2014).

that even with account holder consent, its response to a discovery subpoena was merely voluntary. The court then directed the production of the emails for discovery in Florida litigation.

Walgreen v. Hinchy[15]

A state court of appeals in Indiana has upheld the verdict against an employer for the HIPAA privacy violations of its employee. In this case, a pharmacist had accessed and revealed to her boyfriend the prescription history of the plaintiff, his ex-girlfriend. This action arose from issues surrounding the subsequent pregnancy of the ex-girlfriend and the boyfriend contracting a STD. An internal investigation of the employer found a HIPAA/privacy violation and required the pharmacist to take a HIPAA course. The court of appeals did not find reversible error in the trial court's jury instructions regarding the respondeat superior liability of the employer for this privacy violation (filed as a state invasion of privacy claim due to the lack of a HIPAA private right of action) and so did not need to review the instructions given regarding negligent retention and supervision.

Byrne v. Avery Center[16]

The state supreme court in Connecticut has upheld the use of HIPAA as the standard of care for negligence claims in a health information disclosure lawsuit. The trial court had dismissed the plaintiff's claims based on common law negligence and NIED as HIPAA private actions in disguise, that HIPAA preempted state law in this area, and that it was without subject matter jurisdiction over such claims. The court ruled that HIPAA and the Privacy Rule do not preclude state law actions based on violations of state statutes or common law and based on other cases it reviewed, that "several have determined that HIPAA may inform the relevant standard of care in such actions." The court reversed the trial court, holding in the state that "HIPAA and its implementing regulations may be utilized to inform the standard of care applicable to such claims arising from allegations of negligence in the disclosure of patients' medical records pursuant to a subpoena."

Cases – Regulatory

FCC and Verizon[17]

The FCC has reached a settlement with Verizon over the use of new customers' personal information to conduct marketing campaigns and lack of notification of opt-out options. Over 2 million customers were not told of their privacy rights under the Communications Act, including that they could refuse to have their personal information used in marketing campaigns by opting-out and so could not give their consent. In addition to a fine of more than $7m, Verizon will notify customers on each of their invoices (instead of just the first one or the welcome letter) of the ability to opt-out of marketing campaigns.

---

[15] *Walgreen Co. v. Hinchy*, Case No. 49A02-1311-CT-950 (Ind. Ct. App. Nov. 2014).
[16] *Emily Byrne vs. Avery Center for Obstetrics and Gynecology*, Case No. SC 18904 (Conn. Nov. 2014).
[17] *In the matter of Verizon,* FCC File No. EB-TCD-13-00007027 (Sept. 2014).

FCC and Marriott[18]

The FCC has reached a settlement with Marriott over its blocking the use of personal Wi-Fi hotspots. Marriott admitted its employees in engaged in these acts, even though the customer's hotspot did not pose any threat to the Marriott network or the security of its customers. The FCC alleged that this was done so that the customers would instead use the hotel's Wi-Fi services. At the same time, Marriott and others in the hospitality industry have filed a petition with the FCC to address this issue of personal hotspots at their facilities.[19] The petition looks for a ruling that use of FCC-authorized equipment by the operator of a hotel properties' Wi-Fi network that interferes with the personal Wi-Fi networks is not a violation of statutes or FCC rules.

FCC and TerraCom[20]

The FCC has issued a notice of apparent liability for forfeiture against the defendant telecom providers. The FCC alleges that the wired and wireless providers collected personal and sensitive information from low-income Americans and stored the date on the Internet in folders without implementing any password protections or encryption. The charges included that, in violation of the Communications Act and FCC rules, the companies: "failed to properly protect the confidentiality of consumers' personal information; failed to employ reasonable data security practices to protect the personal information; engaged in deceptive and misleading practices by representing via their privacy policies that appropriate technologies to protect consumers' personal information were being deployed; and engaged in unjust and unreasonable practices by not fully informing consumers that their personal information had been compromised by third-party access." When discovered by a news agency, the companies claimed they were victims of a data breach. Based on records of over 300,000 people exposed at $29,000 per day of exposure, plus additional amounts for the deceptive practices, the proposed fine amounted to $10m.

FTC and Google[21]

The FTC has settled with Google over in-app billings generated during children's use of the apps buy billing the adult without their consent. The apps from Google Play Store allowed the parents credit card to be charged for in-app purchases sometimes without requiring a password or when the password was prompted for and entered, allowed unlimited in-app purchases for up to 30 minutes. The FTC alleged that many of the apps blurred the line between virtual in-app money and real money, that using virtual money would cost real money to the parents without their consent, thereby constituting an unfair practice not outweighed by the countervailing benefits to the consumer. Google agreed to pay at least $19m in refunds to those so charged.

---

[18] *In the matter of Marriott International, Inc. and Marriott Hotel Services, Inc.,* FCC File No. EB-IHD-13-00011303 (Oct. 2014).
[19] *In the matter of Petition of American Hotel & Lodging Association, Marriott International, Inc. and Ryman Hospitality Properties for a Declaratory Ruling to Interpret 47 USC § 333, or, in the Alternative, for Rulemaking* (Aug. 2014).
[20] *In the matter of TerraCom, Inc. and YourTel America, Inc.,* FCC File No. EB-TCD-13-00009175 (Oct. 2014).
[21] *In the matter of Google, Inc.,* FTC File No. 122-3237 (Sept. 2014).

FTC and Yelp / FTC and TinyCo[22]

The FTC has reached two settlements for violations of COPPA with mobile app providers. The settlement with Yelp was for its mobile app that did not provide the same age verification check as did its website. As such, it registered children who indicated that they were under 13 years of age and proceeded to collect personal information from them, without verifiable consent from their parents. This was contrary to their privacy policy and COPPA requirements. The settlement with TinyCo concerned their mobile apps that the FTC's complaint alleged were targeted at children, such as Tiny Pets, Tiny Zoo, Tiny Village, and Tiny Monsters. The complaint said that the company did not provide notice on its website or app or directly to parents of its online data collection practices from children, nor obtain verifiable consent from parents before using this information.

NLRB and Three D[23]

The NLRB has upheld the ruling of an administrative law judge that the dismissal of two employees for a Facebook discussion was improper. The employees had used Facebook as a forum to discuss with under-withheld taxes by the employer that they subsequently became liable for. One of the dismissed employees actively engaged in the online discussion with other employees about what to do about their tax withholding issues while the other merely "liked" one point of the conversation. The judge found that these were protected concerted activities and did not hold these two employees responsible for disparaging or defamatory comments made by other employees. The respondent has appealed this decision to the circuit court.

NLRB and Richmond District Neighborhood Center[24]

The NLRB has ruled against two employees of a non-profit youth organization whose Facebook discussion was determined not to be protected concerted activity. The board determined that the discussion advocated insubordination against management of the organization. The administrative law judge had determined that the employer was not required to wait and find out if the employees, who had been invited back to their positions, would carry out their threats and could rescind the offers to both of them based on their Facebook conversation. As such, the complaint was dismissed.

NLRB Social Media Disclaimer[25]

In an advice memorandum from the General Counsel's office to a region, the requirement that employees who identify themselves as employees of a company can be required to disclaim that their opinions do not necessary represent that of their company. The personal blogging and social networking policy of U.S. Security Associates, Inc. stated in part the following "Employees must make clear that the views expressed by them are their own and do not necessarily represent the

---

[22] *U.S. v. Yelp Inc.*., Case No. 3:14-cv-04163 (N.D. Cal. Sept. 2014); *U.S. v. TinyCo, Inc.*., Case No. 3:14-cv-04164 (N.D. Cal. Sept. 2014).

[23] *Three D, LLC d/b/a Triple Play Sports Bar and Grille and Jillian Sanzone*, NLRB Case No. 34–CA–012915 (Aug. 2014); *Three D, LLC d/b/a Triple Play Sports Bar and Grille and Vincent Spinella*, NLRB Case No. 34–CA–012926 (Aug. 2014).

[24] *Richmond District Neighborhood Center and Ian Callaghan*, NLRB Case No. 20–CA–091748 (Oct. 2014).

[25] NLRB Office of the General Counsel Advice Memorandum, Case Nos. 4-CA-66069, 2-CA-65325, 22-CA-63206 (Aug. 2014).

views of USA [a] *If you identify yourself anywhere on a web site, blog, or text as an employee of USA, make it clear to your readers that the views you express are yours alone and that they do not necessarily reflect the views of the company. To reduce such possible confusion, we require that you put the following notice in a reasonably prominent place on your site: "The views expressed on this web site/blog are mine alone and do not necessarily reflect the views of my employer, U.S. Security Associates, Inc.*" The Counsel's office found this lawful, because it did not unduly burden section 7 rights while furthering the employer's legitimate interest in protecting against authorized postings.

FTC and TRUSTe[26]

The FTC has reached a settlement with True Ultimate Standards Everywhere (TRUSTe) over re-certifications of its privacy seal certifications. TRUSTe requires annual recertification but in over a thousand cases cited by the FTC in its complaint, the company allegedly did not perform the required annual re-certifications. Also, the FTC alleged that the company, which changed from a non-profit to a for-profit organization in July 2008, was not insisting that seal holders update their references to acknowledge that fact.

Under the settlement, TRUSTe agreed to not misrepresent:

- The steps it takes to evaluate, certify, review, or recertify a company's privacy practices
- The frequency with which it conducts any such evaluation, certification, review, or recertification of a company's privacy practices
- Its corporate status and independence
- The extent to which the person or entity is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any of its sponsored privacy programs

FTC and PaymentsMD[27]

The FTC has settled actions brought against an online medical payments portal and its former CEO. The FTC complaint alleged that the after the payment capability was established, the company launched Patient Portal to allow consumers to view their history of payments and possible future payments. The company then started development a product to allow patients to view their health records through the Patient Portal application. To populate the records for this new service, the company solicited health insurance providers and pharmacies but did so without the knowledge or consent of the Patient Portal consumers. The complaint charged the lack of permission or the obscure ways the company tried to gain authorization from consumers were deceptive business practices, and in addition to changing its practices, all sensitive data gathered must be destroyed.

[26] *In the matter of True Ultimate Standards Everywhere, Inc. dba TRUSTe, Inc.*, FTC File No. 1323219 (Nov. 2014).
[27] *In the matter of PaymentsMD, LLC*, FTC File No. 132 3088 (Dec. 2014); *In the matter of Michael C. Hughes*, FTC File No. 132 3088 (Dec. 2014).

Standards and Guidelines

ICO Privacy Seals[28]

The UK's ICO has issued a document that provides a framework for privacy seal schemes that it may endorse. These schemes must be new, have data protection and privacy at their core and "demonstrate a positive approach to the adoption of good practice in information rights, rather than just compliance with the letter of the law." Proposals have to cover the scope and objectives of the scheme, incentives for organizations to become certified, the sustainability of the scheme, transparency and accountability of the scheme operator, an initial assessment process of the scheme, minimum standards for audit and review of the scheme, how to handle complaints about certification, the cost of certification, a contingency plan if the endorsement of ICO is revoked, and a linkage to other standards and schemes. Schemes must first be accredited with the UK Accreditation Services.

Article 29 WP and Internet of Things[29]

The Article 29 Data Protection Working Party has issued its opinion on the Internet of Things. Because these devices are deployed outside traditional IT infrastructures and have the same security techniques built in, security and privacy challenges arise. These include "Data losses, infection by malware … unauthorized access to personal data, intrusive use of wearable devices, or unlawful surveillance." The opinion looks not only at the risks but how these are addressed within the EU legal framework, before providing recommendations for manufacturers, data and social platforms, and standards organizations. The opinion focuses on wearable technologies, quantified self (devices that record information about one's own habits and lifestyle), and home automation.

The data protection and privacy challenges discussed:

- Lack of control and information asymmetry
- Quality of the user's consent
- Inferences derived from data and repurposing of original processing
- Intrusive bringing out of behaviour patterns and profiling
- Limitations on the possibility to remain anonymous when using services
- Security risks: security vs. efficiency

NIST SP 1108[30]

NIST has published the third release of its framework for smart grid interoperability, including its cybersecurity strategy. Changes in technological advances such as wireless-communication power

[28] UK ICO, *Framework criteria for an ICO endorsed privacy seal scheme* (Sept. 2014).
[29] Article 29 Working Party, *Opinion 8/2014 on the on Recent Developments on the Internet of Things* (Sept. 2014).
[30] NIST, SP 1108r3, *Framework and Roadmap for Smart Grid Interoperability Standards* (Sept. 2014).

meters and new standards pushed the release on this new version. It references such documents as the recently finalized multi-volume set of guidelines for assessing smart grid cyber security.[31]

FDA Medical Device Cybersecurity Guidance[32]

The FDA has issued this guidance to manufacturers of medical devices for consideration of the design and development of the devices' cybersecurity. After appropriate risk assessment procedures, the cybersecurity core functions were recommended as: Identify, Protect, Detect, Respond, and Recover. This includes limiting access to trusted users and trusted content, both the data and the software/firmware used on the device and ensuring that the critical functionality is protected, even when cybersecurity is compromised. Premarket submissions should include the lists of cybersecurity risks that were considered and controls that were implemented and the matrix connecting the two, how patches will be provided to the device over its lifecycle, how devices will not be compromised after leaving the manufacturer, and how the device will use cybersecurity controls in its intended environment.

NIST SP 800-150[33]

To further develop guidance from its security incident handling publication (SP 800-61), NIST has issued a draft on the sharing of cyber threat information. The guide recommends that organizations develop an information inventory and an understanding as to when it could be shared with others. It recommends sharing not only threat intelligence but also tools and techniques. After laying out both the benefits (e.g. greater defensive ability) and challenges (e.g. legal and organizational restrictions) of such sharing, the publication discusses the cyber-attack lifecycle and architectures for information sharing, it describes how to establish, use, and maintain information sharing relationships.

OECD Digital Asset Products[34]

The OECD has published guidelines for policies regarding consumer purchase and use of digital content. It addresses issues with the following areas: digital content product acquisition, access, and usage conditions, privacy and security, fraudulent, misleading and unfair commercial practices, children, dispute resolution and redress, and digital competence.

FFIEC Cybersecurity Assessments[35]

The FFIEC recently piloted cybersecurity assessments at over 500 financial institutions and published it observations on those assessments, although these general views fall short of actual guidance. These looked at the institutions' inherent risk, defined as "activities and connections, notwithstanding risk-mitigating controls in place." These activities and connections included the

[31] NIST, IR 7628r1, *Guidelines for Smart Grid Security: Vol. 2, Privacy and the Smart Grid* (Sept. 2014).
[32] FDA, *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices* (Oct. 2014).
[33] NIST, SP 800-150, *Guide to Cyber Threat Information Sharing* (Oct. 2014).
[34] OECD, *Consumer Policy Guidance on Intangible Digital Asset Products* (Oct. 2014).
[35] FFIEC, *Cybersecurity Assessment General Observations* (Nov. 2014).

types of connections, the products and services offered, and the technologies used. The assessment also looked to preparedness, in the categories of: Risk management and oversight, Threat intelligence and collaboration, Cybersecurity controls, External dependency management, and Cyber incident management and resilience.

NIST SP 800-171[36]

Following on from a 2010 executive order, NIST has released it direction for contractors handling controlled unclassified information (CUI) on their non-federal government systems. Such systems must comply with FIPS publications 199 and 200 and NIST special publications 800-53 and 800-60, with the base understanding that the confidentially impact value of CUI is no lower than moderate. The security requirements for protecting CUI include base security requirements from FIPS 200 and derived security requirements from NIST SP 800-53. Compliance is then found by performing security assessments, such as in NIST SP 853A. Basic and derived security requirements are then presented across 14 areas: access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, physical protection, personnel security, risk assessment security assessment, system and communications protection, and system and information integrity.

Thomas J. Shaw, Esq. *is a globally-located attorney at law, CPA, CRISC, CIP, CIPP, CISM, ERM*[P]*, CISA, CGEIT and CCSK and author of the 2014 book* World War I Law and Lawyers – Issues, Cases, and Characters*, author of the 2013 book* Cloud Computing for Lawyers and Executives - A Global Approach, Second edition*, author of the 2013 book* World War II Law and Lawyers – Issues, Cases, and Characters*, author of the 2012 book* Children and the Internet – A Global Guide for Lawyers and Parents*, author of the 2011 book* Cloud Computing for Lawyers and Executives – A Global Approach*, and editor/lead author of the 2011 book,* Information Security and Privacy – A Practical Guide for Global Executives, Lawyers and Technologists*, author of several forthcoming legal books, and editor/founder of this publication and its antecedents. He can be reached at thomas@tshawlaw.com.*

[36] NIST, SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (Nov. 2014).

Editor's Message

With this issue, we are starting the sixth year of publishing each quarter the *Information Law Journal* (previously published separately as the *Information Security and Privacy News* and the *EDDE Journal*). This issue presents articles from lawyers and technologists focusing on various aspects of leading edge domestic and international practice. The first article was written by David Willson of the Titan Info Security Group, discussing hacking back as an active defense. The second article is from the team at Covington & Burling LLP led by Edward Rippey, covering the e-discovery issues in white-collar investigations. The third article is by first-time contributors Hillard Sterling and Christina Liu of Winget, Spadafora & Schwartzberg, LLP, explaining the FTC's approach to data security enforcement. The fourth article is from frequent contributor Mari Frank, analyzing the risks of visual hacking. The fifth article describes recent changes globally to information law and technology statutes and regulations, caselaw, and standards and guidelines.

Thank you to all of the authors. I continue to ask that all readers of the *Information Law Journal* to share with their fellow professionals and committee members by writing an article for this periodical. Our next issue (Spring 2015) will come out in March 2015. There are many of you who have not yet been able to share your experience and knowledge by publishing an article here but please consider doing so to widen the understanding of all of our readers. Every qualified submission meeting the requirements explained in the Author Guidelines will be published, so please feel free to submit your articles or ideas, even if you are not quite ready for final publication. The issue following after Spring (Summer 2015) will be published in June 2015. As always, until then… and Merry Christmas.