FOLEY HOAG LLP

Table of Contents

Introduction
By Martha Coakley

Trade Secret Theft Takes Center Stage
By Stephen Bychowski

The Changing Face of State Law and Enforcement
By Stephen Bartlett

HIPAA Compliance
By Jeremy Meisinger

Emerging Security Threats
By Erik Schulwolf

Energy & Security
By Christopher Cifrino

Changes Afoot in Federal Enforcement
By Christopher Escobedo Hart

About the Authors

Introduction

By Martha Coakley

Cybersecurity was a prominent factor in 2016 in all aspects of government, business and personal affairs. Russian and other foreign national hacking has the potential to spark a new form of cold (cyber)war with the United States. Breaches and cyber threats affecting tens of millions of individuals as well as companies are not only ubiquitous, they're the new normal.

As Massachusetts Attorney General in the last decade, responding to one of the first massive consumer data breaches at TJX Corporation, we saw the beginning of the world we now live in. With the state's then new statute and data privacy regulations, Massachusetts implemented robust means of protecting average consumers' personal confidential information.

As our "Cybersecurity – 2017" articles highlight, cybersecurity threats and harms have only continued to increase, as has the need to protect our consumers and businesses. Eric Schulwolf looks at some of the emerging threats, examining the increase in 2016 of the pernicious rise of ransomware and imagining what new security dangers 2017 will bring. Chris Cifrino turns his attention to the unique problems facing the energy grid and how energy companies should be thinking about cybersecurity. Jeremy Meisinger analyzes changes to HIPAA compliance, a vitally important question for those who must contend with HIPAA's dauntingly complex set of privacy regulations. Steve Bychowski takes time out from thinking about consumer information and examines the increasing threat to company trade secret information. Finally, Steve Bartlett and Chris Hart look at state and federal enforcement, respectively, in the face of changing political winds.

As our authors note, 2017 brings both challenge and opportunity in the realm of cybersecurity. The challenge is that the threats we face will overwhelm us, forcing stakeholders to remain permanently in a defensive crouch. But the opportunity remains to identify how the scaffolding of cybersecurity is changing, as well as to craft and model of preventive and mitigating solutions that will work now and in a rapidly changing future.

Trade Secret Theft Takes Center Stage

By Stephen Bychowski

When it comes to the issue of data privacy and security, especially among lawyers, the discussion generally concerns personally identifiable information.

This includes names, addresses, social security numbers, emails addresses, passwords, etc. of individuals. Beginning with California in 2002, states have been imposing privacy and security obligations on companies that store personally identifiable information. Now, fourteen years later, almost every state has laws protecting the personally identifiable information of its residents. Federal laws play an important role too. For instance, when you add medical information to the mix, it becomes protected health information governed by the Health Insurance Portability and Accountability Act (HIPAA). If the information is held by a financial institution, then Gramm-Leach-Bliley Act (GLBA) might apply.

These laws are generally designed to protect the sensitive information of individuals that companies maintain as part of their business. The laws can require companies to take reasonable steps to secure that data, stop it from being stolen or inadvertently disclosed, and in the event a breach occurs, to notify the effected individuals. All of this is unquestionably important. And part of the reason it is important is that an ever increasing number of nefarious individuals are attempting to steal the cache of personally identifiable information stored on the servers of businesses. Part of the incentive for such hacks is that this information can be sold on the black market and used to commit identify fraud and other criminal activities.

This is the world in which we live, and these laws and their implications are the mainstay of data privacy and security discussions. My prediction for 2017 is that the conversation will shift from the security of information about individual consumers to the security of sensitive business information. This is important because when hackers break into Yahoo and LinkedIn and steal millions of usernames and passwords, as was announced this year, the laws discussed above apply, and the effect on the individual consumers is the primary concern. But when hackers steal confidential financial information, secret formulas, ongoing research and development projects, confidential agreements with third parties, long-term business plans, etc., the state and federal data security and privacy laws discussed above generally do not apply. Yet these breaches can be utterly disastrous for a company. Once in possession of this data, hackers can make the information public, sell it to competitors, or use it for extortion. Thus, companies are well advised to develop strategies and policies focused on protecting their business information from such attack.

These breaches are common and appear to be on the rise. In fact, their prevalence could be much greater than it seems because, unlike data breaches affecting consumer information, data breach and security laws generally do not require public disclosure of breaches that only affect business information. One example is ransomware, which is becoming a prevalent form of such breaches. In a ransomware attack, malicious software takes control of the company's computers and encrypts all of the data, making the information inaccessible. The hacker then demands a payment in exchange for the decryption key necessary to unlock the data. Such an attack not only places sensitive business information into the hands of unknown hackers, but it also blocks the company from accessing its data. If the company does not have adequate back-ups, the ransomware attack could mean that the data is gone unless the company pays the ransom. But even when the victim pays,

sometimes the hackers still do not provide the decryption key. Moreover, paying the hackers only encourages similar attacks in the future, and the company could be unknowingly funding even worse criminal activities. A recent study found that 47% of U.S. companies have experienced a ransomware attack in the past year. The CEO of PhishMe, a cybersecurity company, recently reported: "Barely a year ago, ransomware was a concerning trend on the rise. Now, ransomware is a fully established business model and a reliable profit engine for cybercriminals …."

Cyberattacks by foreign governments and competitors are also on the rise. And when foreign governments and competitors attack, trade secrets and other sensitive business information are the likely target. For instance, back in April, U.S. Steel Corp. filed a trade complaint with the International Trade Commission alleging that the Chinese steel industry formed a cartel to set steel prices, and in collaboration with the Chinese government, stole U.S. Steel's trade secrets. Similarly, Chinese hackers were recently accused of perpetrating attacks on U.S. technology and drug companies seeking intellectual property and trade secrets, including designs and research for unreleased products. Finally, this time last year, Samsung announced that hackers attacked its network in an attempt to steal the technology behind its Samsung Pay service.

Because the data security laws discussed above are not designed to deal with theft of business information, victims need to pursue other avenues if they want to seek redress. One option is the Computer Fraud and Abuse Act, which generally prohibits accessing a computer without authorization and obtaining information from that computer. Critically, the act includes a civil cause of action. Another option is the recently enacted Defend Trade Secrets Act. This act creates the first federal civil cause of action for trade secret theft. The act also includes a controversial civil seizure procedure that allows a court "in extraordinary circumstances" to order the seizure of property in order to prevent the dissemination of trade secrets. State law can also provide viable causes of action. For instance, in the event of a cyberattack by a competitor, claims for torturous interference and unfair competition might be appropriate.

In the end, 2017 will certainly be an interesting year for data privacy and security. Massive hacks involving the theft of personally identifiable information will continue, if not increase. But I think we will also see the rise of attacks targeted at sensitive business information. Companies should ensure in the year to come that they have strategies and procedures in place to combat such attacks.

The Changing Face of State Law and Enforcement

By Stephen Bartlett

In the patchwork of state and federal law regulating the use and maintenance of personal confidential information, states play a significant role and can often be the most important regulator and law enforcement authority.

Recent events have signaled changes in how states interpret and enforce their data privacy standards — and thus how the baseline for understanding what is protected, and what is expected of businesses, might be changing. California, which has been at the forefront of the development of state data privacy laws, remains an important bellwether.

In that respect, a significant development is California AG Kamala Harris's release of a comprehensive data breach report in early 2016, to significant fanfare. The report included guidance on minimum privacy and security standards — which the report deemed a compliance "floor" — for custody of personal information by any entity in California collecting such information. The Attorney General's first recommendation was drawn from the Center for Internet Security's ("CIS") Critical Security Controls. AG Harris's report determined that the 20 CIS controls "define a minimum level of information security that all organizations that collect or maintain personal information should meet." As understood by AG Harris and the industry at large, CIS Critical Security Controls are a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks. CIS itself touts the baseline effectiveness of its standards. According to CIS, organizations that apply just the first 5 CIS controls can reduce their risk of cyberattack by around 85%; and implementing all 20 controls increases the risk reduction to around 94%.

Attorney General Harris did not simply suggest the CIS controls as a viable data security apparatus for California entities collecting and retaining information. Signifcantly, she instead presented the controls as *sub-regulatory guidance*. She noted that "the failure to implement the controls that apply to an organization's environment constitutes a *lack of reasonable security*" (emphasis added). Those words carry legal heft. California Civil Code § 1798.81.5 requires all businesses that collect personal information on California residents to use "*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" (emphasis added). In her report, Attorney General Harris signaled that California businesses must now comply with the CIS controls, or risk an enforcement action or lawsuit under § 1798.81.5. (To date, the California Attorney General's Office has not sued an entity for failure comply with the CIS controls.)

California's incorporation of a national institute's recommended standards as a baseline for data security measures potentially opens the door for other state Attorney's General to follow suit. If more states adopt, for example, CIS standards, that could encourage the creation of a harmonized network of state data privacy and security standards, where business expectations might differ little from state to state. At least six other states (Florida, Utah, Arkansas, Nevada, Maryland and Rhode Island) have adopted statutes requiring entities that collect and retain personal information from consumers employ *reasonable procedures* or *reasonable security measures* to protect such information. That said, there is as of yet no case law in these states directing what types of measures satisfy this "reasonability mandate," and little in the form of guidance from the Attorneys General of the respective states. 2017 might begin to flesh out the legal meaning of these concepts.

Business entities working across state lines would benefit from a more concrete and consistent definition of "reasonable procedures." Currently, such business entities must speculate as to what "reasonable" means in any given state, and develop

data privacy protections accordingly. This could lead to uncertainty and even confusion if businesses determine those standards differ greatly across state lines. Reliance on uniform national standards would be a prudent, but not necessarily sufficient way for businesses to satisfy the unstated requirements of these statutes. That will remain so until state Attorneys' General illuminate a common path to compliance.

Anticipating this future, Attorney General Harris explicitly called for adoption of some uniform standards in her 2016 report. A key recommendation in her report was that state policy makers (including state Attorneys General) should collaborate in seeking to harmonize state breach laws on some key dimensions. According to Attorney General Harris, such an effort could preserve innovation, maintain consumer protections, and retain jurisdictional expertise. A result of a collaborative effort to harmonize state breach laws would be to "minimize the number of patches" in the patchwork of state laws and give businesses a clearer path to compliance. The CIS Controls provide a functional platform for harmonization. Indeed, the National Governor's Association lauded the Controls as far back as 2013. The Association recommendation states "turn to the Critical Security Controls for a baseline of effective cybersecurity practices" and that the controls "provide states with a security framework that can strengthen their cyber defenses and ultimately protect information, infrastructure, and critical assets." While California is the first state to incorporate the CIS controls into formal guidance, continued calls for uniformity and standardization in state data privacy requirements indicate more states are likely to follow.

HIPAA Compliance

By Jeremy Meisinger

The year ahead promises to be a busy one for those with responsibility for HIPAA compliance, as the Office of Civil Rights (OCR), charged with enforcing HIPAA, continues to lean in to compliance initiatives and addresses new questions in the rapidly-evolving healthcare information technology environment.

OCR has explicitly identified two key areas for continued effort in 2017:

1. audits; and
2. modernizing HIPAA and supporting innovation in healthcare (as well as hinting at possible further updates based on changing technology).

Additionally, OCR has recently released guidance on cloud computing, signaling its interest in this fast-growing field.

The HIPAA Audit Program

OCR is currently in Phase II of its HIPAA audit program, in which OCR identified covered entities for audit in the summer and business associates in the fall. In early 2017, OCR is set to identify additional entities for audit.

OCR intends to identify a "broad spectrum of audit candidates," with such criteria as "size of the entity, affiliation with other healthcare organizations, the type of entity and its relationship to individuals, whether an organization is public or private, geographic factors, and present enforcement activity." With respect to the last of these, OCR will not audit entities that are currently under investigation or undergoing a compliance review by OCR.

The initial stages of Phase II focused primarily on "desk audits," essentially reviews of documents submitted by auditees. The 2017 stages of Phase II will move to onsite audits and will examine a broader scope of HIPAA requirements than did the desk audits. While OCR describes the audits as "primarily a compliance improvement activity," OCR has noted that serious issues identified in the audit process could lead to compliance reviews.

Modernizing HIPAA and Supporting Innovation in Healthcare

As HIPAA celebrated its twentieth anniversary in the past year, OCR has turned its attention to addressing aspects of medical privacy that were not anticipated at the time the law was enacted. OCR has specifically identified three major areas for "modernizing":

- Addressing cybersecurity risks. OCR particularly intends to implement the Cybersecurity Information Sharing Act (CISA) of 2015 by issuing guidance for cybersecurity management by covered entities and business associates. This guidance will incorporate the National Institute of Standards and Technology (NIST) Framework. OCR will also expand its investigation of cyber-attacks and breaches.

- Addressing big data. Like many observers, OCR sees both tremendous promise and considerable risk in the gathering of health data now possible due to the widespread adoption of electronic medical records and cloud computing. Accordingly, OCR is committed to creating "a more robust system for the collection, use and sharing of the personal health information and other data necessary" to fuel research reliant on big health data. This system will require "adequate protection for the privacy and security of [...] personal health information as well as [the] right to access the information and gain the benefits of the initiatives

underway." These are lofty aspirations, and it is not yet clear what OCR intends to do make these goals a reality.

- Addressing new questions. OCR notes that, because of the age of HIPAA and the rapid proliferation of data-producing devices in our daily lives — everything from wearable technology to internet-enabled refrigerators and electrical meters — there now exists data "beyond traditional medical records" that "encompass genomic, lifestyle, financial, environmental and other information." OCR's observation is as much a call for legislative action as it is a hint for future administrative change, as OCR acknowledges that HIPAA "may not extend" to covering all of these types of information. But the question remains where OCR will locate what it sees as the boundaries of permissible regulation.

Focus on Cloud-Computing

OCR's recently released guidance on cloud computing is an example of an attempt to tackle new technology, and indicates that OCR will be keeping a close eye on cloud services providers in the future. OCR maked clear that cloud services providers are business associates for the purposes of HIPAA once engaged to receive, maintain, and transmit electronically stored Protected Health Information (PHI). Accordingly, the relationship between a covered entity and a cloud services provider should be governed by a written, HIPAA-compliant business associate agreement.

Cloud services providers are subject to HIPAA as business associates even if they are unable to view PHI, such as in an arrangement whereby a business associate receives and stores encrypted data but does not have a decryption key. Encryption alone does not satisfy the security requirements of HIPAA but, the guidance makes clear, plays a role in apportioning responsibility for security. The guidance gives the example of a covered entity providing encrypted data but no decryption key, and states that where such a covered entity implemented its own appropriate user authentication controls, the cloud services provider would not be required to verify user authentication also. The guidance states that where a business associate agreement puts the lion's share of security responsibility on the covered entity, a cloud services provider would not be responsible for "compliance failures that are attributable solely to the actions or inactions" of the covered entity.

The guidance, beyond making specific recommendations, also signals that OCR will be taking a hard look at the activities of cloud services providers in the years to come.

Together, OCR's plans encompass both old and new. The audits, while not new, are envisioned by OCR to lay groundwork for a more permanent audit program. The march of technology too is not new to HIPAA, but the pace of change and sprawling, often consumer-facing nature of new technology is already posing challenges for interpretation of the two-decade old law. OCR seems to intend to meet these challenges head-on, and so must covered entities, business associates, and the attorneys who advise them.

Emerging Security Threats

By Erik Schulwolf

In 2016, new and alarming cybersecurity threats emerged, raising concerns in government, the business world, and elsewhere. Ransomware became the most profitable form of malware in history. A cyberattack using an army of "Internet of Things" devices caused major problems for websites such as Twitter and Netflix. The 2016 U.S. presidential election was consumed with allegations of previous cybersecurity lapses by one candidate and ongoing hacking in support of the other. Cybersecurity threats are unlikely to cede the spotlight in the coming year. Below I discuss some of the major cybersecurity threats to be aware of in 2017.

Ransomware Remains a Threat

Ransomware, a form of malicious software that infiltrates computer networks or systems and encrypts data or denies access until a ransom has been paid, has been the fastest-growing cybersecurity threat during 2016. According to the federal government, an average of more than 4,000 ransomware attacks per day occurred since the beginning of the year. Ransomware attacks have particularly targeted the health care sector, with several hospitals seeing their networks attacked over the course of 2016. Ransomware is delivered in a variety of ways, notably through phishing emails.

Ransomware attacks are not expected to abate in 2017. Indeed, some are estimating as much as a tenfold increase in ransomware attacks next year. One major concern is that the ransom amounts requested could increase dramatically as cybercriminals better understand the value of the data they are holding hostage. Some also predict an increase in denial of service (DoS) attacks, instead of encryption, to extort victims.

Businesses, especially in the health care sector, will have to be cognizant of federal guidance in protecting against ransomware and, if necessary, responding to ransomware attacks. In July, the HHS Office of Civil Rights (OCR) announced in guidance that ransomware attacks in many cases constitute breaches subject to the requirements of the HIPAA Breach Notification Rule. Federal Trade Commission Chairwoman Edith Ramirez stated in September that "A company's unreasonable failure to patch vulnerabilities known to be exploited by ransomware might violate the FTC Act." The United States Computer Emergency Readiness Team has also released detailed guidance relating to how to protect against and respond to ransomware. These federal agencies suggest measures such as workforce training and education, frequent backups, and application whitelisting to guard against ransomware attacks. Federal agencies such as the FBI do not support paying the ransom if attacked, but recognize that "executives, when faced with inoperability issues, will evaluate all options to protect their shareholders, employees, and customers."

Attacks in the Cloud

The trend of businesses and other organizations moving their data storage to the cloud has increased in recent years and shows no signs of slowing. The vast amount of data being stored in the cloud may make large public cloud providers such as Amazon Web Services, Microsoft Azure, and IBM "primary targets for hackers in 2017."

Every customer represents a potential security weakness for a cloud provider, highlighting the challenges faced by cloud providers. A hacker could infiltrate an organization with weak authentication protocols and passwords and then infiltrate the cloud provider through the organization. An enterprise's data stored on a cloud that suffers a hack can "provide a backdoor for hackers to access other enterprise systems."

Attacks on cloud providers could take the form of data breaches involving personal financial information, health information, trade secrets, and other data. DoS attacks on cloud providers[1] could create problems for the many businesses using that provider. The Cloud Security Alliance notes, however, that "[c]loud providers tend to be better poised to handle DoS attacks than their customers." Ransomware attacks on the cloud may also increase, as hackers may use the cloud as a "volume multiplier" for their attacks.

One particular concern is that organizations migrating environments to the cloud are relying[2] on the cloud providers alone to provide expanded security. It is important for organizations to note that moving data to the cloud will probably not relieve them of their obligations with regard to the privacy and security of personal information. Liability in the case of data breaches will often be an important point to negotiate in contracting with a cloud provider. One potential resource for businesses and other organizations is the National Institute on Standards and Technology's "Guidelines on Security and Privacy in Public Cloud Computing," although keep in mind that these date to 2011.

Threats from the Internet of Things

The Internet of Things (IoT) is the buzzword used in recent years for the connection to information networks of systems and devices with mainly physical purposes. This has potentially revolutionary implications in a variety of areas, from home appliances (imagine your alarm clock telling your toaster to begin making you breakfast) to urban management. It is predicted that 20.8 billion "connected things" will be in use by 2020.

However, as the Department of Homeland Security has noted, "the reality is that security [in the IoT space] is not keeping up with the pace of innovation." Only a month ago, a distributed denial of service (DDoS) attack on the cloud-based internet performance management company Dyn impacted websites such as Twitter, Netflix, and Reddit. Security experts determined that the attack was launched using internet connected devices such as security cameras that hackers took over using Mirai, a "self-spreading malware" that targets IoT devices. More attacks using the IoT could be on the horizon in 2017.

The IoT is a threat multiplier for a variety of reasons. First, it vastly increases the number of access points to networks that bad actors can exploit. Importantly, IoT devices are "by default . . . open and available to the Internet and come protected with default passwords." Moreover, "most IoT devices are considered throwaway devices and security patches are not issued." As Sean Gallagher notes in ArsTechnica, "even though consumer device manufacturers have become generally more serious about IoT security, there are still a vast number of devices on the Internet that are configured with default or permanent passwords—passwords that another botnet developer could easily add to a targeted library." Perhaps most worryingly of all, as more critical systems begin to rely on the IoT, the consequences of attacks may become more dire, especially in the healthcare space.

These vulnerabilities are prompting calls for regulators to address cybersecurity for the IoT. BeyondTrust predicts that in 2017 large-scale attacks making use of the IoT will drive new regulations. Within the past month, the Department of Homeland Security has released non-binding principles and best practices for securing the IoT. These include the creation of unique and difficult to crack user names and passwords for IoT devices, automatic application of patches, and applying tested cybersecurity practices to the IoT. In early 2015 the FTC released a report on privacy and security for consumer IoT devices. However, commentators continue to press for federal legislation in this area, notably amendments to HIPAA and the Gramm-Leach-Billey Act.

[1] Forcepoint 2017 Security Predictions Report, available at https://www.forcepoint.com/2017predictions.

[2] Forcepoint 2017 Security Predictions Report, available at https://www.forcepoint.com/2017predictions.

FOLEY HOAG LLP

Energy and Security

By Christopher Cifrino

In 2015, a sophisticated cyberattack hit six of Ukraine's energy providers simultaneously, causing a blackout for hundreds of thousands of Ukrainians.

The U.S. has thus far evaded similar attacks, but the energy sector remains of vital strategic importance. Because it has long been considered a prime target for cyber threats, from cybercriminals and foreign states alike, regulators, especially at the federal level, have shown particular attention to this sector. Below, I look back at developments in energy sector cybersecurity in 2016 and ahead to what 2017 may bring.

Federal Regulation Continues to Evolve

On the federal level, 2016 has seen the release of updated Critical Infrastructure Protection (CIP) requirements by the North American Electric Reliability Corporation (NERC), the non-profit empowered by the Federal Energy Regulatory Commission (FERC) with authority to oversee grid security. The CIP plan is a set of nine standards and some 45 requirements that cover a broad variety of cybersecurity protocols. Under the CIP plan, utilities are required to identify critical cyber assets and ensure they are protected by electronic security measures, such as encryption and two-factor authentication. They must develop plans for incident reporting and recovery, and train personnel on response plans. The CIP standards even govern physical security measures, such as security guards and visitor logs. Version 5 of the CIP standards is fully phased in on April 1, followed quickly by version 6 in July, but companies cannot afford to rest on their compliance laurels: version 7 drafting is already underway! Look for more CIP updates in 2017.

State Involvement on the Rise

Federal regulation gets most of the attention, but NERC's mandatory reliability standards only covers about 20% of the energy distribution grid (lines operating at 100 kV and above) – meaning the other 80% is left to be regulated at the state or local level. Thus the state-level response to increasing cyber threats is of vital importance. 2016 saw several states stepping in and offering more cyber regulations. Connecticut's Public Utilities Regulatory Authority, for example, established a new cybersecurity oversight plan for utilities in the state and created a yearly voluntary forum for industry and government personnel to confer on cyber threats and responses. Energy commissions in approximately a dozen other states have rules or orders of some sort addressing cybersecurity. That, of course, leaves a majority of states without any such regulation (at least by the relevant energy authority — state attorneys general can regulate through their consumer protection and privacy authority). It seems likely that 2017 will bring more organization and more regulation on the state level.

Will Voluntary Information-Sharing Take Off?

In December of 2015 Congress passed two pieces of legislation that were designed to encourage voluntary sharing of cybersecurity information among companies. The Fixing America's Surface Transport Act, or FAST Act, empowers FERC to define "Critical Energy Infrastructure Information." Such information will be exempt from FOIA disclosure and receive protection from dissemination by government personnel, on the theory that companies will be more likely to share sensitive information about cyber

threats with the government if they have assurances about who it will be shared with.

FERC finally issued regulations defining "Critical Energy Infrastructure Information" in November 2016, but the FAST Act's sharing provisions may already be obsolete. The Cybersecurity Information Sharing Act of 2015, covered here on the blog in February, has the same goal — encouraging data sharing and collaboration by providing mandatory protections for the disclosed information — but it applies to all industries and government agencies (not just the energy sector) and all "cyber threat indicators" (not just Critical Energy Infrastructure Information). The government is certainly on board, as all agencies are required under the statute to participate in information sharing by the middle of this month. But has the private sector followed suit? Will they in 2017? As of now, the answer is unclear.

As 2016 draws to a close, a cyberattack like the one that brought down Ukraine's electricity grid in 2015 has yet to materialize in the U.S. But it does not seem any less likely now than it was a year ago, either. Oh, and in addition to worrying about sabotage by foreign agents, energy companies, like any company, still have to be prepared to prevent and respond to "normal" threats such as data breaches or ransomware. The regulatory landscape and the cyber threats faced will continue to evolve in 2017 — and the energy sector, perhaps more so than any other sector, should be prepared to stay up-to-date, compliant, and protected.

Changes Afoot in Federal Law Enforcement

By Christopher Escobedo Hart

Fragmentation in U.S. data privacy and cybersecurity law is both peril and promise. The peril? Businesses must contend with uncertainty and the costs associated with pleasing many regulatory masters. The promise? Various regulatory bodies can compete for the most effective way of approaching cybersecurity, setting a path forward for others to emulate.

At the federal level, the primary enforcement actor has been, for some time, the Federal Trade Commission. Indeed, since the Third Circuit's decision in *FTC v. Wyndham*, the FTC's authority in this space has been largely affirmed (and generally unquestioned). Other federal agencies have also started to more forcefully enter the cybersecurity enforcement arena, including the Securities and Exchange Commission, the Consumer Financial Protection Bureau, and the Federal Communications Commission. Up until November 8, it seemed like those agencies would be competing in a would-be Clinton administration over enforcement turf. But after the unexpected election of Donald Trump, all bets appear to be off. Fragmentation and uncertainty might very well be the norm for years to come, and the potential for a Trump administration to emphasize de-regulation could have unexpected consequences. Let's take a look at where we've been and where we might be going.

A Look Back: Two Steps Forward?

2016 saw the FTC's self-defined increase in cybersecurity enforcement authority and the full-throated entry of the CFPB and SEC (as well as continued actions by the FCC) into the cybersecurity enforcement mix.

If one thing is clear, it's that the FTC has carved out an important and significant space in the field of data privacy, and everyone else is playing catch-up. Because of its broad power under federal statute (its "Section 5" authority in which the FTC is empowered to enforce against unfair and deceptive trade practices), the FTC has been uniquely positioned to alter the behavior of private market actors in the data privacy space, creating clearly-discernable parameters in how a company should act reasonably in its handling of personal consumer data and in its response to a breach event.

The FTC was not, however, content in 2016 to rest on its laurels. On July 29, the Commission published an order in the *FTC v. LabMD* case, articulating a much broader view of its powers than the Third Circuit had articulated in *Wyndham*. The Commission's decision overturned the decision of the Administrative Law Judge holding in LabMD's favor; the ALJ reasoned that the harm claimed by the FTC was both speculative and unlikely. (For our take on the ALJ's opinion, read our blog entry here.) The Commission made two principle holdings: first, that "privacy harm resulting from the unauthorized *disclosure* of sensitive health or medical information is in and of itself substantial injury under Section 5(n)," (emphasis supplied) even though as the ALJ had found there was no "tangible injury such as monetary harm or health and safety risk." In other words, the Commission found that disclosure of sensitive private information was an *inherent* harm over which the FTC had plenary enforcement authority.

In addition to this holding — that mere *disclosure* was an inherent harm – the Commission also determined that mere *exposure* of sensitive information (without evidence of disclosure to an unauthorized third party) was "likely to cause substantial injury," holding that "significant risk" of harm would be sufficient to meet this standard (in contrast to the ALJ's holding that this language required a "high probability" of harm, and thus that mere exposure

was insufficient to invoke the FTC's Section 5 authority). Both of these holdings present the possibility of significant expansion of FTC power, giving the FTC enforcement authority even where no tangible injury has taken place or is even likely to take place.

Compared to the FTC, every other agency has been and continues to be in a distant second place. However, activity in 2016 suggested that there was movement afoot. The SEC has been in possession of law enforcement authority over data security since 2011 (through Rule 30(a) of Regulation S-P, also known as the "Safeguards Rule,"), and began exercising that authority in 2015, when it brought and ultimately settled an action against R.T. Jones. This year, it settled with Morgan Stanley to pay a $1 million penalty relating to a data breach. But its enforcement activity is only now getting off the ground, and no federal court has defined the reach of the SEC's authority in this space.

The CFPB, a creature of the Dodd-Frank financial industry reform legislation, also jumped in to the enforcement arena, ordering online payment platform Dwolla to pay a $100,000 penalty and to change its data security practices, after the agency investigated the company and found that although Dwolla communicated to its customers that its data privacy standards exceeded industry standards, the company in fact (according to the CFPB) failed to maintain adequate standards. Importantly, the CFPB ordered this penalty and action even though Dwolla did not suffer a data breach.

Finally, the FCC joined in investigative efforts with the FTC on mobile device security updates. Although the FCC does not have the same kind of investigative authority as the FCC, it nevertheless requested from telecommunications carriers information regarding security updates, and called its investigation a "partnership" with the FTC, signaling its efforts to work with other agencies in cybersecurity efforts.

In all, these actions suggest continued and in some cases significant expansion of federal enforcement and regulation of cybersecurity and data privacy.

A Look Ahead: Three Steps Back?

But will that continued and significant expansion continue? Many signs point to "maybe not," including the following:

- Currently, LabMD has a pending appeal before the 11th Circuit; that court stayed enforcement of the FTC's order, discussed above, stating that "there are compelling reasons why the FTC's interpretation may not be reasonable." A decision is expected in 2017, and as of now there is reason to think that the 11th Circuit will balk at the FTC's interpretation of its own power.

- Additionally, the FTC will have two commission spots for President Trump to fill, and the Commission will have a 3-2 Republican majority for the first time in more than a decade.

- With Republicans in control of all three branches, both Dodd-Frank and the CFPB appear to be in danger. Aggressive pre-breach enforcement action like that taken by the CFPB in the Dwolla case might be unlikely in 2017.

- SEC Chair Mary Jo White will be stepping down, and President Trump will be appointing her replacement, signaling a potentially significant shift for agency enforcement priorities.

- In general, there are strong signs that Trump's administration, based on his cabinet picks, will be decidedly de-regulatory.

What does this all mean? To quote Yogi Berra, predictions are hard, especially about the future. But there are strong signs that the FTC's authority will be cabined by the 11th Circuit; that the CFPB will have at least some of its powers taken away, and that the SEC will not play a larger role if in fact de-regulatory impulses win the day.

But this does not necessarily mean that regulations will slacken. As we have noted in this space, states appear ready to pick up the leadership mantle and recraft their regulations in favor of consumers. And let's not count out the possibility that regulations concerning cybersecurity might be viewed differently, even by a pro-deregulation administration, than other kinds of regulations, especially given the end-of-year tumult brought by revelations of Russian attempts to meddle in the U.S. election through hacking and the disclosure by Yahoo! that up to 1 billion customer accounts were compromised in a hack that occurred years ago.

Perhaps the next year will be a year of pausing federal enforcement action in the cybersecurity realm, but expect that vacuum to be filled by other actors.

FOLEY HOAG LLP

About the Authors

Martha Coakley
Partner - *Boston*
p: 617 832 1115
e: mcoakley@foleyhoag.com

Stephen Bychowski
Associate - *Boston*
p: 617 832 1164
e: sbychowski@foleyhoag.com

Stephen Bartlett
Associate - *Boston*
p: 617 832 3007
e: sbartlett@foleyhoag.com

Erik Schulwolf
Associate - *Boston*
p: 617 832 3022
e: eschulwolf@foleyhoag.com

Jeremy Meisinger
Associate - *Boston*
p: 617 832 3029
e: jmeisinger@foleyhoag.com

Christopher Cifrino
Associate - *Boston*
p: 617 832 1734
e: ccifrino@foleyhoag.com

Christopher Escobedo Hart
Counsel - *Boston*
p: 617 832 1232
e: chart@foleyhoag.com

Colin Zick
Partner, Chair, Privacy & Data Security Practice - *Boston*
p: 617 832 1275
e: czick@foleyhoag.com