The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 1, Number 4 May 20, 2015

BREACH RESPONSE

After a Cyber Breach, What Laws Are in Play and Who Is Enforcing Them?

By Jenny A. Durkan and Alicia Cobb
Quinn Emanuel Urquhart & Sullivan, LLP

In recent years, the power and capability of intelligent devices has grown exponentially, as have companies' reliance on global cyber networks. Unfortunately, bad actors have innovated just as quickly and cyber risks threaten businesses, individual privacy and national security. Recent reports detail a breathtaking and unrelenting rise in cyber breaches, with five malware events occurring every second, and 60% of successful attackers able to compromise an organization within minutes.

But the law has not kept pace with technological innovation. There is no single uniform law protecting individual privacy, nor one that governs all of a company's obligations or liabilities regarding data security and privacy. As a result, any business that suffers a significant cyber breach almost certainly will face not only multiple civil suits, but multiple investigations by federal and state authorities.[1]

A single investigation by a federal or state regulator is a serious event for a company. Undergoing multiple simultaneous investigations, each with varying rules, requests and investigators, can overwhelm a company if not properly managed. There is no other area of the law where a victim of a crime faces such legal jeopardy and uncertainty.

Short of a new legal framework, the gamut will only get more difficult, as additional federal and state agencies assert authority in the field. Good legal preparation means having informed counsel ready to step in when a breach occurs to guide the myriad of investigations, and build work product and privilege protections.

A critical initial step for any company is to understand its legal landscape before a breach occurs, with a thorough inventory of applicable laws and regulations. This also means knowing which regulators have jurisdiction, what they expect, and what they might do in case of a breach. While the applicable regulators can vary by the type of data involved, by industry sector and by geographic location, the following are seven key players of which to be aware.

1) Federal Law Enforcement

Investigation, prevention and prosecution of cyber crime is one of federal law enforcement's top priorities. The two primary federal agencies charged with criminal enforcement are the FBI and the United States Secret Service. In addition, the Department of Justice has dedicated cyber resources in the Criminal Division, the National Security Division and in each of the United States Attorney's offices. These include prosecutors, investigators and forensic specialists. Federal resources are directed to the more significant threats. For example, the FBI prioritizes high-level intrusions, the largest and most pernicious botnets, state-sponsored hackers, and global cyber syndicates. The Secret Service works on similar investigations, and also plays a key role in coordinating and training local police through its Electronic Crime Task Forces. Together, the FBI, Secret Service and other federal entities coordinate through the National Cyber Investigative Joint Task Force.

Any significant data breach caused by criminal acts likely will be the focus of a Secret Service or FBI investigation. These investigations are by their nature very intrusive. Both agencies are mindful that the business entity is a victim, and increasingly attempt to coordinate with the business, IT and security needs of the impacted entity. However, law enforcement has a specific mission with exacting rules: get the evidence necessary to identify, disrupt and prosecute the bad actors, and gather all available intelligence. This means law enforcement will collect and image impacted computer devices, interview witnesses and require the production of sometimes voluminous information.

Much of this activity begins immediately upon learning of a breach, and often at the same time that a company itself is trying to identify the source, nature and scope of the problem, as well as a solution. But the company's goal to get business back online, and law enforcement's need to collect evidence and pursue a case can sometimes conflict.

For example, law enforcement may recommend delaying any third-party notification of a breach in order to prevent tipping off the malicious actors that they have been discovered. Moreover, because of restrictions on criminal or national security cases, the information law enforcement can share with companies is limited. Thus, open and regular communication with law enforcement throughout all steps of an investigation is imperative.

2) Securities and Exchange Commission

Traditionally, the SEC's involvement was contingent on whether the breach was a "material event" triggering disclosure obligations. However, in recent years, the SEC has increasingly flexed its muscles in the cyber arena by issuing guidance identifying risks and cybersecurity governance issues, conducting sweeps of companies to test readiness and, earlier this year, issuing a summary of its examinations. The SEC has also issued guidance to registered investment companies and advisers regarding cybersecurity.[2]

While no enforcement action has yet been commenced by the SEC in this arena, the agency has sent a clear message that it will act when appropriate, and SEC leadership, including Chair Mary Jo White, have been very outspoken on the importance of the issue. Such guidance documents provide a clear outline of the SEC expectations, and what it will examine should it take enforcement action. See "*The SEC's Two Primary Theories in Cybersecurity Enforcement Actions*," The Cybersecurity Law Report, Vol. 1, No. 3 (May 6, 2015).

3) Federal Trade Commission

Of all the federal civil enforcement agencies, the FTC has perhaps the deepest roots when it comes to protecting consumer information and privacy. Accordingly, it may assert itself in almost any significant breach event that exposes consumer personal information. Given that the FTC's core mission is to protect consumers from fraudulent, deceptive and unfair business practices, it has a variety of hooks for jurisdiction in this arena.

The FTC has broad authority to enforce a range of laws, including the Truth in Lending Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, the Telemarketing and Consumer Fraud and Abuse Prevention Act, the Children's Online Privacy Protection Act and laws against spam. Recently the FTC has brought claims arguing that a company's practices as to data security "taken together, failed to provide appropriate security for personal information on its computer networks," and that their practices exposed consumers to identity theft and disclosure of sensitive medical information, which amounted to "unfair . . . acts or practices."[3]

In addition, the Health Information Technology for Economic and Clinical Health (HITECH) Act grants the FTC jurisdiction over certain entities not covered by HIPAA that collect personal healthcare information. Under this authority, the FTC has imposed a Health Breach Notification Rule, violations of which are treated as an unfair or deceptive practice, 16 C.F.R. §318.7, and the FTC has followed up with robust guidance and enforcement. See FTC, "*Complying with the FTC's Health Breach Notification Rule*" (April 2010).

The FTC has vigorously asserted its jurisdiction on all fronts. It has confirmed it is investigating the Target breach, and reports that it has brought over 130 spamware and spyware cases and more than 40 general privacy lawsuits.[4] In 2014 alone, the FTC brought privacy enforcement actions against a wide

range of companies including Snapchat, online payday lenders, telemarketers, Wyndham Worldwide and Fandango.[5] Notably, in settlements it has required companies to agree to a jaw-dropping 20-year monitoring agreement.[6]

The forward-leaning posture is expected to continue. On May 6, 2015, the FTC appointed Katherine Race Brin as its Chief Privacy officer. Brin is a veteran of the FTC, steeped in its original core mission. She served as an attorney in the Division of Privacy and Identity Protection for seven years and has been acting in the CPO position since 2014.[7]

4) Federal Communications Commission

Until recently, it was unclear what role the FCC would play. Recent actions, however, leave no doubt that the FCC will assert jurisdiction over data breaches and will use its powers to enforce consumer interests. For instance, last month, the FCC entered a consent decree with AT&T relating to a breach in AT&T foreign call centers, which compromised the personal information of over 51,000 AT&T customers. AT&T not only agreed to pay a civil penalty of $25 million, it was required to develop and implement a compliance plan. See "*FCC Makes Its Mark on Cybersecurity Enforcement with Record Data Breach Settlement*," The Cybersecurity Law Report, Vol. 1, No. 2 (Apr. 22, 2015).

The compliance plan requirements signal the minimum protections the FCC will demand. AT&T must "ensure appropriate processes and procedures are incorporated into AT&T's business practices to protect consumers against similar data breaches in the future," and specifically must "improve its privacy and data security practices by appointing a senior compliance manager who is privacy certified, conducting a privacy risk assessment, implementing an information security program, preparing an appropriate compliance manual, and regularly training employees on the company's privacy policies and the applicable privacy legal authorities."[8]

5) State Attorneys General

Any significant breach involving private consumer information likely will draw the attention of multiple state attorneys general. Nearly every state has its own data protection and breach notification laws, and with the growing concern and visibility of the problem many state attorneys general have focused on data privacy. For example, the California Attorney General has made online privacy a key issue, and recently formed an "ECrime Task Force"[9] and the Connecticut Attorney General recently formed a Department on Privacy and Data Security.[10]

Similarly, the Massachusetts Attorney General has an established Cyber Crime Division and implemented a broad Cyber Crime Initiative.[11] Likewise, the New York Attorney General has proposed enhanced data security laws.[12]

Multiple state attorneys general have launched investigations in the wake of recent breaches, including breaches at Target, Home Depot, Neiman Marcus and Experian. Often, these are done through joint investigations and committees. See, e.g., Ill. Attorney Gen., "*Madigan: Federal Data Breach Law Should Not Weaken States' Consumer Protections*," Feb. 5, 2015; Mass. Office of the Attorney Gen., "*AG Coakley Joins Multi-State Committee to Investigate Target Data Breach*," Jan. 13, 2014; Mass. Office of the Attorney Gen., "*AG Coakley Investigates Potential Data Breach Involving Major Credit Reporting Company; Issues Consumer Advisory*," Apr. 22, 2014.

6) Key Health Care Information Regulators

Few sectors are subject to more regulation than the healthcare industry. Because of the sensitive nature of healthcare information, this regulation extends to breaches. As noted above, the HITECH Act gives the FTC jurisdiction in some cases. In addition, there are a number of entities that have regulatory authority.

The CYBERSECURITY LAW REPORT

www.cslawreport.com Volume 1, Number 4 May 20, 2015

U.S. Department of Health & Human Services, Office for Civil Rights

The U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules as to "covered entities" (including health insurance issuers) both by investigating complaints and by conducting compliance reviews.[13]

HIPAA sets forth certain security standards, and provides that covered entities will give notification of a breach to individuals, the media and the Secretary of HHS. In particular, covered entities are to provide notification to individuals and to the media "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach,"[14] and they are to provide notice to the Secretary "contemporaneously with the notice" to individuals.[15]

State Attorneys General

In addition to consumer protection powers discussed above, the HITECH Act gave state attorneys general the authority to bring civil actions on behalf of their state residents to enjoin conduct and/or obtain damages for violations of the HIPAA Privacy and Security Rules.[16]

The OCR website suggests that OCR will coordinate with the state attorneys general in such actions.[17] Moreover, the State is required to provide written notice of any such action to the Secretary of HHS. However, if the Secretary of HHS has initiated an action with respect to a violation of HIPAA the State may not bring such an action during the pendency of the Secretary's action.[18]

State Insurance Commissioners

When a major data breach occurs at an insurance company, state insurance commissioners may have and assert local authority to investigate the circumstances of the breach, and if necessary, take regulatory action. For example, after the recent breach of Premera Blue Cross, the Washington State Insurance Commissioner announced that Washington would be leading a multi-state market conduct examination of Premera, along with Oregon and Alaska. Others impacted by the "Blue Card" system (Premera's national provider network) may also join the exam team.[19]

The scope of such examinations conducted can be broad. In the Premera case, the Commissioner indicated the examination could involve multiple states and onsite reviews of an insurer's financial books, records, transactions and how they relate to a company's activities in the marketplace. The exact scope of Premera's exam also might include: all cybersecurity aspects of the breach; Premera's response to the breach and any corrective actions taken; and the financial impact of the breach on consumers, providers and Premera.[20]

7) Other Financial Regulators

In addition to investigations by the SEC, FTC and state attorneys general, entities in the financial industry face investigations or examinations by other entities. For example, at the end of 2014, the New York Department of Financial Services announced new targeted cybersecurity preparedness assessments. Letters sent to all regulated banks stated that a cyber preparedness review would become a standard part of bank examinations. It would include assessments of factors such as cybersecurity protocols and training, vendor security, insurance coverage and incident response readiness.[21] Similarly, last year FINRA launched a targeted examination of firms relating to cybersecurity, and then this year issued a Report on Cybersecurity Practices.[22] The report makes clear that FINRA will continue to emphasize cybersecurity in its examinations. It sets forth some principles and guidance for firms to improve security, including in the areas of governance, risk assessment and technical controls.[23] While FINRA states that it is not requiring any specific measures, it "expects firms to consider the principles and effective practices presented in this report as they develop or

enhance their cybersecurity programs. FINRA will assess the adequacy of firms' cybersecurity programs in light of the risks they face."[24] In other words, companies can expect future examinations to address the factors outlined in the report.

* * *

In short, the post-breach timeframe can be very perilous. On top of the significant financial costs associated with identifying, containing and remediating a large-scale breach and the potential for damage to a company's reputation, companies may face burdensome simultaneous investigations from numerous federal and state agencies. It is critical to conduct a thorough review to identify the laws and regulations applicable to the industry and geography, and to become familiar with the role and expectations of various regulatory bodies. A company's recovery after a breach is dependent upon its ability to successfully navigate simultaneous overlapping investigations by various regulators.

Jenny A. Durkan is a partner at Quinn Emanuel Urquhart & Sullivan, and the Global Chair of its Cyber and Privacy practice. She served as the U.S. Attorney in Seattle, chaired a key DOJ committee on cyber crime and testified before Congress on the issues. She handles a range of civil and criminal cases, and is a fellow in the American College of Trial Lawyers, with offices in Seattle and Washington, D.C.

Alicia Cobb is an associate in the Seattle office of Quinn Emanuel Urquhart & Sullivan. She has represented clients in structured finance, antitrust, class action, and white collar criminal litigation.

[1] This article addresses the legal framework within the United States. Increasingly, however, a significant breach can implicate obligations under foreign law, which can include far-reaching rights to individuals. For example in Europe, data privacy and security is governed not only by an E.U. privacy directive adopted in 1995, but by rights under the European Convention on Human Rights and the Council of Europe Convention. See, generally, European Union Agency for Fundamental Rights, "*Handbook on European Data Protection Law*" (2014). This penumbra of rights led to the decision declaring that individuals had the "right to be forgotten", and therefore the right to have personal information deleted from web search capabilities. See generally, European Commission, "*Factsheet on the 'Right to be Forgotten' ruling*". Moreover, in the 20 years since the E.U. Privacy Directive was adopted, member countries have interpreted and enforced the directive in differing ways, leading to "fragmentation and incoherence." European Commission, "*The Proposed General Data Protection Regulation: The Consistency Mechanism Explained*," Jun. 2, 2013. The E.U. is currently negotiating an updated law, with a more unified approach, but agreement and implementation could be years away.
[2] Guidance Update, April 2015.
[3] Order, Matter of LabMD, Inc., Dkt. No. 9357 (Fed. Trade Comm. Jan. 6, 2014).
[4] Federal Trade Commission 2014 Privacy and Data Security Update.
[5] Id.
[6] See, e.g., FTC Press Release, "*Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False*" May 8, 2014.
[7] FTC Press Release, "*Katherine Race Brin Appointed FTC Chief Privacy Officer*," May 6, 2015.
[8] In the Matter of AT&T, Order dated April 8, 2015.
[9] State of Cal. Dep't of Justice, Office of the Attorney General Cybersafety webpage, "*Attorney General Kamala D. Harris Announces New ECrime Unit Targeting Technology Crime*."
[10] Conn. Office of the Attorney Gen., "*Attorney General Jepsen Forms Permanent Department on Privacy, Data Security within Office of the Attorney General*," Mar. 11, 2015.
[11] Mass. Office of the Attorney Gen., The Cyber Crime Division.
[12] N.Y. Attorney Gen., "*A.G. Schneiderman Proposes Bill To Strengthen Data Security Laws, Protect Consumers From Growing Threat of Data Breaches*," Jan. 15, 2015.
[13] HHS, "*Health Information Privacy, How OCR Enforces the HIPAA Privacy & Security Rules*."
[14] 45 C.F.R. 164.404(b), 164.406(b).
[15] 45 C.F.R. 164.408(a), (b).
[16] 42 U.S.C. 1320d-5(d)(1); see also Pub. L. 111-5, Sec. 13410(e).
[17] U.S. Dep't of Health & Human Services, "*Health Information Privacy, State Attorneys General*."
[18] 42 U.S.C. 1320d-5(d)(4), (7).
[19] News Release, "*Washington to lead multi-state investigation of Premera*," Mar. 24, 2015.
[20] Id.
[21] Dep't of Fin. Servs. Press Release, "*NYDFS Issues Examination Guidance to Banks Outlining New Targeted Cyber Security Preparedness Assessments*," Dec. 10, 2014.
[22] FINRA, "*Report on Cybersecurity Practices*," Feb. 2015.
[23] Id.
[24] Id. at 2.