Skadden

PRIVACY & CYBERSECURITY UPDATE

FEBRUARY 2014

CONTENTS

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 11, or your regular Skadden contact.

SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP

Four Times Square
New York, NY 10036
212.735.3000

NIST RELEASES FINAL FRAMEWORK DOCUMENT

On February 12, the National Institute of Standards and Technology (NIST) issued its long-awaited "Framework for Improving Critical Infrastructure Cybersecurity."[1] The final Framework was a "key deliverable" ordered by President Obama a year earlier in his February 12, 2013, executive order 13636 and Presidential Policy Directive addressing the regulation of critical infrastructure network security. However, as discussed below, while the Framework is couched as a "final" document, it represents only the first phase in what will be an ongoing process aimed at improving the protection of the country's critical infrastructure industries.

The Framework closely mirrors the preliminary framework, released in October 2013, which we discussed at length in our October 25 "Privacy & Cybersecurity Update." We therefore provide here only an overview of the Framework and the differences between the preliminary framework and the final Framework.

Overall, the Framework is a voluntary guide that companies in designated critical infrastructure industries can use to evaluate their cybersecurity practices, develop a plan to reduce their risks and respond to security breaches.[2] While the final Framework does not propose new cybersecurity standards pursuant to the executive order, relevant regulatory agencies are now using the Framework as a basis for reviewing critical infrastructure cybersecurity within their sectors and determining whether they have the legislative authority to enact any regulations that might be required. Within 90 days of the publication of the Framework, agencies that conclude that they do not have sufficient powers must propose "prioritized, risk-based, efficient, and coordinated actions" to mitigate cyber risks.

In general, the Framework is composed of three parts — a Framework Core, the Framework Implementation Tiers and the Framework Profile. The Framework Core lists the five security functions that a cybersecurity-conscious organization should consider, then breaks each one into categories and subcategories that should be addressed. The Framework Implementation Tiers provide companies with different tiers of security they might fall into, depending, in part, on how proactive they are in assessing risk. In a statement accompanying the final Framework, NIST clarified that while organizations are encouraged to advance their Tier level, "successful implementation" is based on how well an entity achieves the outcomes in its specified Tier and not which Tier it advances to.

Finally, the Framework Profile is a tool organizations can use to apply the Framework Implementation Tiers to the functions presented under the Framework Core and

---

[1] *Available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf.

[2] Critical infrastructure industries include: chemical, commercial facilities, communications; critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture; government facilities, healthcare and public health, information technology, nuclear services, transportation systems and water systems.

develop a comprehensive cybersecurity strategy. Significantly, while the Framework, like its predecessor drafts, refers to existing security standards, it does not propose any specific standards that should be followed nor does it highlight any shortcomings in those existing documents. Instead, NIST has described the Framework as "a basic, flexible, and adaptable tool for managing and reducing cybersecurity risks." This lack of specific requirements also means that the Framework does not provide a safe harbor for organizations that implement it.

Although the Framework is designed to provide a roadmap for critical infrastructure companies to manage their cybersecurity programs, it also provides useful guidance to companies that are outside these industries but seeking such a framework.

KEY CHANGES FROM THE PRELIMINARY FRAMEWORK

In the final Framework, NIST made a number of revisions to the categories and subcategories within each of the five security functions. For example, the Framework:

- Clarified that access permissions should not just be "managed," but should be managed consistent with "the principles of least privilege and separation of duties"; and
- Added a subcategory under the category "Protect: Data Security" requiring that" [i]ntegrity checking mechanisms are used to verify software, firmware, and information integrity"

The latter is one example of several new cybersecurity subcategories added in the Framework, which also eliminates a few subcategories listed in the preliminary Framework. Other key examples of new subcategories include:

Protect, Information Protection Processes and Procedures: "A vulnerability management plan is developed and implemented";

- Respond, Mitigation: "Newly identified vulnerabilities are mitigated or documented as accepted risks"; and
- Recover, Communications: "Recovery activities are communicated to internal stakeholders and executive and management teams."

NIST added language on risk analysis and management to the Framework's guide to "Establishing or Improving a Cybersecurity Program." In particular, the revised guide splits the preliminary orientation step into two parts: one in which organizations identify "business/mission objectives and high-level organizational priorities" and another in which they identify "related systems and assets, regulatory requirements, and overall risk approach" and "threats to, and vulnerabilities of, those systems and assets" after they determine their cybersecurity programs.

Perhaps the most important change to the final Framework from the earlier versions relates to the Privacy Methodology that had been attached. As we reported in our January 2014 "Privacy & Cybersecurity Update," NIST signaled that it intended to make this change in response to considerable public comment as to how it was addressing privacy. In essence, NIST dropped its separate appendix that mapped privacy proposals to each cybersecurity category in favor of a more generic statement on privacy. The final Framework also removes a specific subcategory for data protection that had existed in earlier drafts. As NIST now notes, "[N]ot all activities in a cybersecurity program may give rise to" privacy issues, and it is the role of the government, not the private sector, to address civil liberty considerations. However, NIST did not adopt a key industry suggestion to limit the scope of personal information that Framework users should protect as private only to that information already controlled under existing laws (or voluntarily designated private). Instead, NIST left open the possibility that private personal information in this context might sweep in a broader set of personal information.

THE FRAMEWORK ROADMAP

In conjunction with the final Framework, NIST also issued a companion Roadmap that is equally informative and provides insight into NIST's approach.[3] The Roadmap sets forth, consistent with the executive order's mandate and based on input from stakeholders, "areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations." The nine such areas identified by NIST are:

- *Authentication:* Improving user authentication, such as through multi-factor authentication. This might require individuals to augment passwords ("something you know") with "something you have," such as a token, or "something you are," such as a biometric. Today, there is no real framework of authentication standards to promote security and interoperability.
- *Authomated Indicator Sharing:* Automated sharing of cybersecurity threat information between organizations so that they can detect and respond to cybersecurity events as they occur. NIST notes that standards are required so that organizations of different levels of capability and size can participate in, and take advantage of, information sharing.
- *Conformity Assessment:* Conformity assessment to show that a product, service or system meets specified requirements for managing cybersecurity risk. In this regard, NIST plans to work with private sector standards owners and those who manage conformity assessment programs to help stakeholders understand how these programs can be leveraged to demonstrate conformity with cybersecurity standards.
- *Cybersecurity Workforce:* Improving the size and capabilities of the cybersecurity workforce. According to NIST, there is a well-documented shortage of general cybersecurity experts, particularly of experts who appreciate the unique challenges posed to the critical infrastructure sector. NIST plans to continue its efforts to promote existing and future cybersecurity workforce development activities.
- *Data Analytics:* Using big data to analyze cybersecurity threats, but taking into account the potential privacy issues raised by such usage.
- *Federal Agency Cybersecurity Alignment:* Applying cybersecurity standards and guidelines across federal agencies that complement rather than duplicate or conflict with existing statutes, policies and standards. This includes determining how the Framework can be leveraged for such agencies.
- *International Aspects, Impacts and Alignment:* Considering globalization of cybersecurity issues and the fact that many governments are proposing and enacting strategies, policies, laws and regulations covering information technology for critical infrastructure as a result.
- *Supply Chain Risk Management:* Improving awareness of how supply chains are an essential part of the risk landscape and need to be considered as part of an organization's risk management programs. Companies need to focus on their interdependencies and the weakest link in their supply chains.
- *Technical Privacy Standards:* Addressing privacy issues while acknowledging that there are few identifiable technical standards or best practices to mitigate the impact of cybersecurity activities on individuals' privacy or civil liberties. In this regard, NIST notes that the Fair Information Practice Principles (FIPPs), which have been used as a basis for a number of laws, regulations and frameworks around the world, are process-oriented and do not define privacy in a way that has enabled the development of a risk management model.

---

[3] *Available at* http://www.nist.gov/cyberframework/upload/roadmap-021214.pdf.

THE DHS "C-CUBED" PROGRAM

In conjunction with the release of the final Framework, the Department of Homeland of Security (DHS) announced a new private-public initiative to encourage adoption of the final Framework by medium and small-sized companies: the Critical Infrastructure Cyber Community C3 (C Cubed) Voluntary Program.[4] The C3 Voluntary Program is designed to develop general and sector-specific guidance for the final Framework and to collect feedback on the final Framework. The website for this initiative can be found at http://www.us-cert.gov/ccubedvp.

NEXT STEPS

There are a number of significant next steps in the evolution of the Framework:

- Although the final Framework marks the end of this phase of NIST's work, NIST considers the final Framework to be a "living document" that "will continue to be updated and improved as industry provides feedback on implementation" and intends to respond to "new threats, risks, and solutions." Indeed, NIST already envisions a version 2.0 of the Framework. To that end, NIST has announced that it will receive and consider comments about the Framework on an informal basis and then issue a formal notice of revision to version 1.0.
- NIST also plans to promote the Framework though industry groups, associations and nonprofits and to help organizations understand and use the Framework. NIST will then specify areas in which it would like comments and specific deadlines for those comments with a goal of developing and publishing proposed revisions. As part of its review process, NIST plans to hold at least one workshop within six months so that organizations can share their actual experiences with using the Framework.
- DHS will now become a focal point of activity as the C3 Voluntary Program uses outreach to support adoption of the Framework and will effectively be a clearing house for Framework feedback.
- While NIST plans to continue its work on the Framework, it also envisions a point at which it will transition responsibility for the Framework to a non-government organization that has the capability of working closely with international organizations.
- NIST also will host a privacy workshop in the second quarter of 2014. The workshop will focus on the advancement of privacy engineering as a foundation for the identification of technical standards and best practices that could be developed to mitigate the impact of cybersecurity activities on individuals' privacy or civil liberties.
- Incentives remain a critical component of adoption of the final Framework. To that end, the executive order called for various agencies to make proposals regarding incentives for final Framework adoption. Upon release of the final Framework, the White House announced that these proposals will be released in the coming months.

---

[4] Available at http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program.

CALIFORNIA SUGGESTS UPPER TIME LIMIT ON "TIMELY" DATA BREACH NOTIFICATION

A recent complaint filed by the California attorney general suggests that there is an upper limit on how long companies can wait to provide data breach notification. In a complaint filed on January 24, the attorney general alleged that Kaiser Foundation Health Plan violated California unfair competition law by failing to notify consumers of a data breach quickly enough after the breach occurred.[5] Although a number of states specify a time period with which notice must be provided (such as Florida, which provides a 45-day window), many states, including California, simply require companies to notify individuals of data breaches "without unreasonable delay"[6] or in a timely fashion. In the past, companies had interpreted this clause to mean that they had some leeway to complete forensic testing, formulate a notice and communications strategy, and determine how to best minimize the public relations impact. The facts set forth in the Kaiser complaint suggest that the clock is ticking much faster than companies may have appreciated. The timeline is as follows:

- *September 24, 2011:* Kaiser learns that a hard drive containing unencrypted personal information, including social security numbers, of current and former Kaiser employees was purchased at a thrift store.
- *December 21, 2011:* Kaiser obtains possession of the external hard drive and begins conducting a forensic examination.
- *December 28, 2011:* Initial forensic examination of the hard drive is completed, revealing over 30,000 social security numbers and other employee information.
- *Mid-February 2012:* Kaiser completes its inventory and analysis of the hard drive.
- *March 19, 2012:* Kaiser mails letters to 20,539 California residents affected by the breach.[7]

As this timeline indicates, about one month passed between Kaiser's conclusion of the forensic examination and the actual notification. Indeed, many companies would look at this timeline and deem it perfectly reasonable. However, the Complaint asserts that Kaiser could have notified individuals "as early as December 2011," suggesting that Kaiser potentially should have begun notification even before completing the full inventory of the hard drive. Kaiser settled the case for a $30,000 penalty and $120,000 in legal fees, along with a promise to implement additional security-related procedures, including an agreement to implement more prompt notification for future breaches, employee training and review of its email encryption policy.[8]

PRACTICE NOTES

Although this case is applicable only to data breach notification required under California law, states with similar notification constructs may look to the Kaiser decision as informing what constitutes a reasonable time period. In addition, while some news reports have suggested that four months is now the "upper threshold" for notification in California, the complaint suggests that Kaiser should have commenced notification within days or a few weeks after its initial forensic study. A company suffering a data breach involving California residents should keep in mind two key points:

- The timeline for notifying customers of a data breach may be shorter than previously thought, meaning that companies may have to act quickly in order to avoid liability.

---

[5] Complaint, *California v. Kaiser Foundation Health Plan, Inc.*, No. RG14711370 (Cal. Supp. Ct., Jan. 24, 2014) (the Complaint)
[6] Cal. Civ. §1798.82.
[7] Complaint at 4-5.
[8] Marianne Kolbasuk McGee, Kaiser Plan Reaches Breach Settlement, "Health Care Information Security," (Feb. 3, 2014), http:// www.healthcareinfosecurity.com/kaiser-plan-reaches-breach-settlement-a-6471.

- Companies may no longer be able to claim that they waited to provide notification until such time that they had identified all victims of the breach. Rather, companies may be required to provide "rolling" notification to customers, with customers being notified shortly after they have been identified as victims of the breach.

FTC FINDS COMPANY RESPONSIBLE FOR DATA PRIVACY ACTIVITIES OF ITS VENDOR

On January 31, 2014, the Federal Trade Commission (FTC, or Commission) announced that GMR Transcription Services, Inc. (GMR) had agreed to settle FTC charges brought against the company for its failure to adequately protect its customers' personal information. The charges are notable because the alleged data breach actually occurred while GMR customer personal information was being processed by GMR's independent vendor, not by GMR itself. The FTC complaint therefore signifies a move by the FTC to hold companies responsible for the data activities of their vendors.

GMR transcribes digital audio files for individuals and businesses. After customers upload their audio files, GMR assigns those files to independent service providers to be transcribed. Between January 2009 and May 2012, GMR assigned medical audio files it received from customers to Fedtrans, an independent service provider located in India, which then assigned the files to individual typists for transcription.

GMR was unaware, however, that Fedtrans used an application that stored the medical audio files and transcripts in clear, readable text and which could be accessed online without authentication of any kind. As a result, between March 2011 and October 2011, a major search engine (not identified by the FTC) was able to access and index thousands of these medical transcripts, making them accessible to anyone using the search engine. These medical files contained highly sensitive personal information of GMR customers, including medical histories, medical examination notes and information about psychiatric disorders, alcohol and drug abuse, and pregnancy loss.

The FTC alleged that GMR "misrepresented that they maintained reasonable and appropriate practices to protect consumers' personal information from unauthorized access" and that the company failed to ensure that those transcribing the files complied with security and privacy requirements.[9] Specifically, the complaint alleged that GMR failed to require Fedtrans to implement, or confirm that it had implemented, security measures such as the use of antivirus software. For example, GMR had not entered into a contract with Fedtrans requiring the service provider to securely store and transmit the files (by, for example, encrypting the data) or that its typists go through an authentication process, such as the use of unique user credentials. GMR also did not request or review information regarding Fedtrans' security practices, including any audits of its computer networks.

The proposed FTC consent order, which is subject to public comment through March 3 (after which the FTC will consider making it final), prohibits GMR from misrepresenting the extent to which it protects the privacy and security of the personal information it collects from its customers. GMR, in its previous privacy policy, had stated that "each transcriptionist within the GMR community is required to sign a Confidentiality Agreement prior to working with us."[10] The order also requires GMR to establish a more stringent security program, including requiring GMR to develop "reasonable steps to select and retain service providers capable of

---

[9] Analysis of Proposed Consent Order to Aid Public Comment in *In the Matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekant Srivastava*, File No. 122 3095, Jan. 31, 2014, *available at* http://www.ftc.gov/system/files/documents/cases/140203gmranalysis.pdf.

[10] Complaint at §10, *In the Matter of GMR Transcription Services, Inc., Ajay Prasad, and Shreekant Srivastava.*

appropriately safeguarding personal information they receive" and requiring GMR to contract with these service providers to maintain those safeguards.

PRACTICE POINTS

The FTC's complaint highlights that a company's data security obligations extend to processes performed by its third-party vendors.

- Companies that use third-party vendors to process the personal information of its customers should enter into written contracts with those vendors that set out specific security measures. These security measures should include processes such as file encryption and authentication processes for the vendor's employees.
- Companies should take care to avoid any over misrepresentations, such as references to agreements that do not exist, in their privacy policies. As we have noted in prior mailings, the FTC has been actively pursuing companies based on what they claim in their security statements to customers.

FTC SIGNALS EXPANSION OF DATA SECURITY ENFORCEMENT AND CALLS FOR LEGISLATION

On February 5, in two very different venues, FTC commissioners publicly described the Commission's policy priorities in the area of data privacy and suggested a potential new avenue of FTC enforcement activity in the area of "unfair" (even if not deceptive) privacy practices.

CHAIRWOMAN RAMIREZ TESTIFIES BEFORE THE HOUSE

Testifying on behalf of the Commission, FTC Chairwoman Edith Ramirez appeared before the House of Representatives' Energy and Commerce Committee's Subcommittee on Commerce, Manufacturing and Trade. In her prepared remarks, she outlined the various privacy threats facing the public, with an emphasis on identity theft. According to the FTC, in 2012 7 percent of all U.S. residents aged 16 or older were victims of identity theft. With these threats in mind, she went on to describe the Commission's past enforcement efforts, the steps it has taken to educate businesses and consumers on privacy issues, and its legislative priorities.

Chairwoman Ramirez described the Commission's enforcement efforts as addressing two separate but related issues: (i) deceptive statements on data privacy and security, and (ii) unfair data practices. She characterized the cases the Commission brought under its deception authority as being based on companies' express or implied claims that they provide reasonable security for consumers' personal data. Chairwoman Ramirez explained that, in those cases, the Commission believed that, despite the companies' express or implied statements, they had failed to implement "available, cost-effective security measures to minimize or reduce data risks."

With respect to unfairness, the Chairwoman claimed that 20 of the 50 data cases the FTC had brought to date involved what the Commission viewed as unfair data practices, though she noted that many of those cases also had involved deception. In her testimony, she articulated the following standard for unfairness:

> [I]f a company's data security practices cause or are likely to cause substantial injury to consumers that is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers or to competition, those practices can be found to be unfair and violate Section 5 [of the FTC Act].

Notwithstanding the chairwoman's testimony, privacy practitioners had generally believed the FTC's enforcement activities were focused on misleading statements by companies. The unfairness doctrine that the chairwoman described appears to indicate that the FTC intends to expand its actions in the privacy area.

Overall, however, Chairwoman Ramirez emphasized that the FTC does not require perfect security but instead focuses on reasonableness. She explained that "a company's data security measures must be reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and address vulnerabilities."

With respect to policy issues, the chairwoman described the FTC's recent outreach efforts in the areas of mobile security, identity theft (including child identity theft and senior identity theft) and the "Internet of Things."[11] She also described the Commission's efforts to provide privacy and data security education resources for consumers and businesses.

Finally, Chairwoman Ramirez reiterated the Commission's longstanding desire for federal legislation on data security standards for companies and data security breach notification obligations. National data security standards, she explained, are important for protecting consumers against the increasing risk of identity theft. With respect to data breach notifications, she cited the diversity of state laws on the issue and explained that a single and consistent national standard would simplify compliance for companies.

COMMISSIONER BRILL ANSWERS QUESTIONS VIA TWITTER

On the same day that Chairwoman Ramirez testified before the House, FTC Commissioner Julie Brill (@JulieBrillFTC) engaged in an hour-long question-and-answer session via Twitter. The time and format constraints of the medium meant Commissioner Brill was only able to answer 16 questions (two of which came from Skadden attorneys), and her responses were limited to 140 characters and therefore short on detail, but she did provide some insights on the Commission's views on certain issues.

Commissioner Brill echoed Chairwoman Ramirez's suggestion that the FTC may expand its review of companies' data security practices beyond deception. A Skadden attorney asked whether the Commission was concerned that its pattern of punishing deceptive or misleading data security statements effectively discouraged companies from informing the public about their data security practices. Commissioner Brill responded by explaining that the Commission examined company statements and underlying data security practices, and considers *both* to be potentially deceptive and unfair.

The Commissioner also touched on other important data security and privacy issues:

- *Legislation.* The commissioner echoed the chairwoman's calls for U.S. federal legislation on data security and data security breach notifications.
- *U.S. Safe Harbor.* Commissioner Brill described the U.S. Safe Harbor program for EU privacy law compliance as providing important protections for U.S. and EU citizens, and affirmed the Commission's commitment to improving enforcement cooperation with the EU.
- *Priorities.* In response to a question from a Skadden attorney on what she viewed as the most pressing privacy issues for the FTC, Commissioner Brill suggested that the Commission will take an active interest in a broad array of privacy issues. She specifically listed the following: health, financial and other sensitive data, data broker practices, the "Internet of Things," mobile security, facial recognition issues, and the Children's Online Privacy and Protection Act.

---

[11] For more information on these efforts, see our January 2014 "Privacy & Cybersecurity Update," available at http://www.skadden.com/insights/privacy-cybersecurity-update-january-2014.

COMMON THEMES AND PRACTICE POINTS

Between Chairwoman Ramirez's testimony and Commissioner Brill's tweets, a few common themes and practice points are clear.

- *The FTC Will Look at Unfair Data Security Practices.* Both the chairwoman and the commissioner suggested that the FTC will focus its enforcement efforts not simply on misleading or deceptive statements but also on "unfair" data practices. Although neither explicitly said so in their statements, under this broader standard, it theoretically would be possible for the FTC to take action against a company that provided full, accurate disclosure of its data security practices if those practices were nevertheless seen as inadequate and therefore "unfair." Companies should therefore look beyond whether their public statements on data security are accurate and examine whether their practices meet the standard described by Chairwoman Ramirez in her testimony.
- *The FTC Will Continue to Take a Broad View of Its Privacy and Security Jurisdiction.* Chairwoman Ramirez's description of the FTC's enforcement and outreach efforts and Commissioner Brill's broad list of FTC priorities both suggest that the Commission will be active in a wide array of privacy and data security issues in the future. Companies should review their business activities closely to identify areas that could pose a risk to the privacy and security of consumer data.
- *The FTC Will Press for Federal Legislation on Data Security and Breach Notifications.* Both Chairwoman Ramirez and Commissioner Brill mentioned the FTC's desire for federal legislation on general data security standards and data breach notifications. Companies that collect or store personal information should keep abreast of these issues as they develop.

CHALLENGES TO THE FTC'S AUTHORITY – NEW DEVELOPMENTS

As we reported in our December 2013 "Privacy & Cybersecurity Update," Wyndham Hotels and LabMD each have challenged the FTC's authority over data security breaches in pending actions brought by the FTC. There have been new developments in each of these cases.

WYNDHAM HIGHLIGHTS THE FTC'S CALLS FOR CYBERSESECURITY LEGISLATION

In recent months, the FTC has walked a somewhat fine line, arguing on the one hand that its enforcement authority in the area of data security needs to be expanded while at the same time maintaining that it already has sufficient authority to pursue entities that did not provide adequate security. This tension has played out most prominently in the FTC's ongoing legal skirmish with Wyndham Hotels.

In April 2012, the FTC filed a complaint against Wyndham for alleged data security failures that led to three data breaches at Wyndham hotels. The FTC alleged that these failures led to fraudulent charges on consumers' accounts, millions of dollars in fraud loss and the export of hundreds of thousands of consumers' payment card account information to an Internet domain address registered in Russia. The crux of the FTC's complaint is that Wyndham engaged in "deceptive" practices by misrepresenting that they took "commercially reasonable efforts" to secure customers' payment card data and engaged in "unfair" practices, as their lax security measures failed to adequately protect this payment card data.

Wyndham moved to dismiss, asserting in pertinent part that the FTC lacked authority to file such a complaint since there is no established baseline security standard to which Wyndham

could be compared. Wyndham also argued that the FTC has suggested to Congress it does not have sufficient authority over data security. Oral argument on Wyndham's motion took place in November 2013.

The legislative reaction to the recent data breaches at Target and other retailers has given Wyndham additional arguments. In a recent letter to the court, Wyndham asserted that its position is supported by S. 1976, the Data Security and Breach Notification Act of 2014, introduced by Sen. Jay Rockefeller (D-W.Va.) and S. 1995, the Personal Data Protection and Breach Accountability Act, introduced by Sens. Richard Blumenthal (D-Conn.) and Ed Markey, (D-Mass.). According to Wyndham, since each of these bills requires the FTC to develop and issue data security rules (using its notice and comment procedures), no such rules currently exist, and therefore, Wyndham was held to a non-existent standard. The letter is the latest in a series of back-and-forth submissions by the parties since the November oral arguments. As Congress debates new data security legislation and the role of the FTC, the issue of the FTC's current authority will remain in question until the court renders a decision.

LABMD VOLUNTARILY DISMISSES ITS COMPLAINT AND STATES IT IS WINDING DOWN OPERATIONS

The FTC had accused LabMD of failing to implement reasonable and appropriate measures to prevent unauthorized access to consumers' personal health data when LabMD customers' personally identifiable health information became available on a peer-to-peer file-sharing network. In 2012, when LabMD failed to comply with the FTC's Civil Investigative Demand, the FTC filed suit in federal court in Georgia seeking to force LabMD to comply. The FTC prevailed and launched an administrative action against LabMD. The company responded by filing suit in the District of Columbia, challenging the FTC's authority to bring such a claim. LabMD also appealed the Georgia court's decision to the Eleventh Circuit. On February 18, the Eleventh Circuit said it lacked jurisdiction since the FTC had not issued a cease and desist order. LabMD subsequently voluntarily dismissed its District of Columbia action. In January, LabMD also announced it would be winding down its operations, citing the "debilitating effects" of the FTC's investigative practices.

CALIFORNIA TAKES STEP IN REGULATING THE "INTERNET OF THINGS"

California recently enacted A.B. 1274, entitled "Privacy of Customer Electrical or Natural Gas Usage Data," a law that (i) prohibits a business from sharing, disclosing or otherwise making available to any third-party a customer's electrical or natural gas usage data without disclosing the intended third party recipient and purpose of the disclosure and obtaining the express consent of such customer to the disclosure, and (ii) otherwise requires that businesses implement safeguards to protect such usage data. The law applies to electrical and gas corporations and to any other businesses that have access to such usage data. Customers may bring a private right of action seeking actual damages of up to $500 for each willful violation of the law. The law went into effect on January 1 of this year.

This new law is in response to privacy concerns posed by so-called "utility smart meters," which can provide energy and cost savings to consumers, but which also generate data that allow for certain of such consumers' behavior to be tracked, including the hours someone is typically at, or away from, home. More broadly, A.B. 1274 can be seen as an early example of a state law regulating the so-called "Internet of Things," a term used to describe products and other devices that are connected to wireless or wired networks and capable of generating and transmitting data without human input or interaction. The Internet of Things can be used to describe a wide-range of products and devices, including traffic sensors, home alarms,

advanced pacemakers, retail loyalty cards and GPS locators; in fact, the term can attach to any technology that has access to or can accumulate data unique to an individual and is capable of autonomously transmitting such information over a network.

As lawmakers focus more on how devices can store, use and generate personal data, they will likely consider the privacy implications of such data sharing. The new California smart meter law may be an important first step in the introduction of new legislation in this area or the expansion of existing laws. Significantly, if A.B. 1274 is any indication, lawmakers may be inclined to consider (and write laws around) individual "Internet of Things" devices on a case-by-case basis. If this holds true, it is possible that these devices may become subject to a patchwork of state laws across several jurisdictions. Such a patchwork could one day pave the way for broader federal legislation that either implements privacy rules specific to certain types of smart devices on a national level, or more broadly attempts to regulate the "Internet of Things."

SEC TO EXAMINE ASSET MANAGER'S CYBERSECURITY PROGRAMS

Jane Jarcho, the national associate director for the Securities and Exchange Commission's investment adviser exam program, recently announced during a presentation to compliance officers that the National Examination Program (NEP) would be evaluating asset manager policies and practices on cybersecurity as they relate to training, vendor access and vendor due diligence. This review will be conducted as part of the agency's routine examinations of investment advisers and investment companies.

SKADDEN CONTACTS

STUART D. LEVI
Partner / New York
212.735.2750
stuart.levi@skadden.com

JAMES S. TALBOT
Counsel / New York
212.735.4133
james.talbot@skadden.com

JOSHUA F. GRUENSPECHT
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com