Skadden

PRIVACY & CYBERSECURITY UPDATE

JANUARY 2015

CONTENTS (click on the titles below to view articles)

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 14, or your regular Skadden contact.

SUMMARY OF PRESIDENT'S RECENT PROPOSALS FOR CYBERSECURITY LEGISLATION

President Obama has proposed a variety of legislative initiatives that would overhaul U.S. cybersecurity and privacy policy.

As we noted in a recent *Privacy & Cybersecurity Update*,[1] President Barack Obama released in January several new legislative proposals aimed at implementing a comprehensive overhaul of U.S. cybersecurity and privacy policy. The proposals were initially announced by the president at speeches given at the Federal Trade Commission (FTC) and the National Cybersecurity and Communications Integration Center (NCCIC), and the president reiterated the importance of these measures to national security during his State of the Union address on January 20, 2015. In his speech, Obama alluded to recent high-profile cybersecurity attacks as evidence of the need for reform and called on Congress to implement his changes to better protect American citizens while still allowing the country to prosper from the benefits provided by technology and the Internet.

We have outlined below the key components of each piece of legislation: a federal data breach notification law, information sharing legislation, modifications to existing law enforcement legislation, the Student Digital Privacy Act and the Consumer Privacy Bill of Rights.

FEDERAL DATA BREACH LEGISLATION

There is perhaps no area of law that seems more in need of a uniform federal standard than the area of data breach notification. Today, 47 states and the District of Columbia have their own data breach notification requirements. While there is considerable overlap between the laws, there are enough differences that companies facing a multistate data breach must spent considerable time and money trying to comply with each state's laws.

The President's proposed Personal Data Notification & Protection Act (the Data Notification Act, or Act) seeks to remedy this multistate quagmire through a single federal law that would preempt all state laws. Under the Data Notification Act, any entity engaged in or affecting interstate commerce that uses, accesses, transmits, stores or collects sensitive, personally identifiable information about more than 10,000 individuals must notify affected individuals of any unauthorized access to their information. While the proposed law uses the term "sensitive" personal information, it includes the basic approach of many statutes today. Under the law, such information would include name plus two other items from an enumerated list, including address or phone number, mother's maiden name, birth date, social security number and financial account information, among others. The proposed law also is broader than many state laws in that the list includes unique biometric data such as fingerprints and retina or iris images.

[1] See *Privacy & Cybersecurity Update: President Announces Cybersecurity Legislative and Regulatory Proposals*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Update_President_Announces_Cybersecurity_Legislative_and_Regulatory_Proposals.pdf.

The obligation to notify is triggered when an individual's sensitive, personally identifiable information has been, or is reasonably believed to have been, accessed or acquired. However, notice is not required if the business conducts a risk assessment and determines there is no reasonable risk that the unauthorized access has resulted, or will result, in harm to the individuals whose information was subject to the access. For example, a company may conclude that the data was encrypted in a manner that cannot reasonably be deciphered. By adopting this approach, the Data Notification Act sides with those states that only require notice when there is a risk of harm. This is in contrast to those states that require notice for any unauthorized access, even when the company is confident no harm resulted. Businesses must report the results of their risk assessments and their decision not to notify individuals to the FTC. The risk assessments must adhere to generally accepted practices and include logging data for a period of six months prior to the risk assessment. Companies that process data on behalf of third parties must inform the third party in the event of a breach.

One of the largest criticisms of the state-by-state approach is the different timeframes for notice that are required, with many states simply requiring notice "without unreasonable delay." The Data Notification Act would create a single standard of "without an unreasonable delay following a security breach," but also setting an outside date of 30 days after the breach is detected. A company may receive an extension of this time period from the FTC and may delay notice if so required by law enforcement.

Notice under the proposed federal law can take place via written notification, telephone or, if an individual previously consented, email. If the number of individuals to be notified exceeds 5,000 people, then the business may use the media to reach affected individuals. In addition, if more than 5,000 individuals must be notified or the database accessed contained more than 500,000 individuals nationwide, businesses must notify agencies designated by the Department of Homeland Security. The Act will be enforced by the FTC, and any violation will be deemed an unfair or deceptive practice under the Federal Trade Commission Act.

The Act will supersede all state laws relating to data breach notification, though states may separately decide whether notification content should include information about state specific victim protection assistance. The Act does permit state attorneys general to bring civil actions to enjoin practices violating the Act, enforce the Act or seek civil penalties against a violating entity up to $1,000 per individual and a maximum of $1,000,000 per violation, unless the violation was willful or intentional. Therefore, while the Act acknowledges the role state AGs play in data breach notification, the federal legislation clearly intends to bring data breach notification laws within the federal arena. It remains to be seen what room, if any, states will have to continue to legislate in the area.

INFORMATION SHARING LEGISLATION

The information sharing aspect of the president's legislative proposal is designed to encourage the private sector to share identified "cyber threat indicators" with both the NCCIC and other private sector entities, as well as to facilitate real-time information sharing from the NCCIC to other federal agencies and Information Sharing and Analysis Centers (ISACs) developed and operated by the private sector. A central provision of the information sharing legislation is the definition of "cyber threat indicator," as the rest of the legislation relates directly back to that term. The proposed statute defines "cyber threat indicator" (CTI) as information:

(A) that is necessary to indicate, describe or identify:

  (i) malicious reconnaissance, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cyber threat;

  (ii) a method of defeating a technical or operational control;

(iii) a technical vulnerability;

(iv) a method of causing a user with legitimate access to an information system or information that is stored on, processed by or transiting an information system inadvertently to enable the defeat of a technical control or an operational control;

(v) malicious cyber command and control; or

(vi) any combination of (i)-(v); and

(B) from which reasonable efforts have been made to remove information that can be used to identify specific persons reasonably believed to be unrelated to the cyber threat.

The proposed legislation authorizes any private entity to disclose lawfully obtained CTIs to NCCIC and ISACs and protects those entities from civil or criminal liability (in both federal and state court) for their voluntary disclosure or receipt of any lawfully obtained CTIs, as long as such disclosure or receipt is consistent with the statute. However, in order to address concerns about privacy and civil liberties, the proposal requires private entities disclosing or receiving CTIs to "take reasonable efforts to minimize information that can be used to identify specific persons and is reasonably believed to be unrelated to a cyber threat, to safeguard information that can identify a specific person from unauthorized disclosure, and to comply with reasonable restrictions that another private entity places on further disclosure of a [CTI] to a third-party private entity." Furthermore, the proposed legislation directs certain administrative agencies (including the Privacy and Civil Liberties Oversight Board) to develop policies and procedures to govern the use and disclosure of information under the statute, and to identify a private entity that would develop a set of "best practices" for the industry to use when dealing with CTI disclosures.

Finally, the statute directs federal agencies, particularly the secretary of Homeland Security and the NCCIC, to ensure that CTIs are shared with appropriate federal authorities in as close to real time as possible. The proposed legislation also explicitly preempts any state or local law that is inconsistent with its terms.

The president's proposal in many ways tracks the Cyber Intelligence Sharing and Protection Act (CISPA), a bill that Congress has debated, on and off, since 2012. While most consider information-sharing a critical component of enhancing private and public sector cybersecurity, the president's proposal will likely face the same key challenge as CISPA — namely, balancing the liability protection that companies require against civil liberty concerns about the disclosure of information to the government.

LAW ENFORCEMENT LEGISLATION

The president's proposed legislation also provides significant updates to law enforcement's authority to pursue and prosecute cybercriminals. First, the proposed legislation adds certain cybercrimes to preexisting categories of offenses, allowing increased and easier prosecution of those crimes. For example, the statute would add offenses committed in violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030) to the list of racketeering activities that can be prosecuted under the Racketeering Influenced and Corrupt Organizations Act (RICO). Similarly, the legislation adds existing laws criminalizing the sale, distribution and advertising of surreptitious interception devices to the list of predicates for bringing money laundering charges. This change would allow law enforcement to bring money laundering charges against defendants who conceal profits from the sale of such surreptitious interception devices, in addition to any other charges that can already be brought.

The proposed legislation also revamps the penalties for violations of several cybercrime statutes. The act would amend the Computer Fraud and Abuse Act (CFAA) to enhance its effectiveness against insider attacks on computers and computer networks, allowing prosecution against persons who intentionally access a protected computer without authorization and who

intentionally exceed their authorized access of a protected system. Further, the definition of "exceeds authorized access" would be updated to include accessing a computer with authorization and then using such access to alter or obtain information that the accesser knows he is not authorized to alter or obtain. The proposal also criminalizes the sale of a "means of access" to commit cybercrimes, such as a botnet, and reduces the mental state required for prosecution for the use of botnets from "intent to defraud" to "willful." The legislation also empowers courts to issue injunctions to shut down or disrupt botnets. Further, it expands law enforcement authority to prosecute overseas sale of stolen U.S. financial information and to deter the sale of spyware used to stalk or commit identity theft.

However, the proposed legislation also would reduce or eliminate the criminal penalties for inadvertent acts by employees, so that such acts would not become subject to a criminal violation. For instance, under the amended CFAA, in order for an individual to be prosecuted: (i) the information obtained must exceed $5,000; (ii) the offense must be committed in furtherance of a felony; or (iii) the protected computer must be owned or operated on behalf of a governmental entity. Finally, the proposed legislation also would expand law enforcement's ability to seek civil and criminal forfeiture of proceeds and property obtained by and used in cybercrimes.

Most have hailed the president's proposals in this area as much needed changes to help strengthen law enforcement's ability to prosecute cybercrimes. Some have nonetheless expressed concern that the CFAA amendments will expose employees to criminal liability who overstepped their access authority and viewed information that they were not supposed to obtain.

STUDENT DIGITAL PRIVACY ACT

The Student Digital Privacy Act would prevent companies from selling student data to unrelated third parties or using student data for discriminatory means. The bill is modeled on the California Student Online Personal Information Protection Act, and ensures that data collected in the educational context can be used only for educational purposes. The rationale behind this proposal is to allow parents and educators to feel comfortable taking advantage of technology to enhance teaching and learning opportunities without the risk that student data will be sold or used to students' detriment. The legislation also would prohibit entities from using student data to engage in targeted advertising. According to the president, 75 companies already have agreed not to engage in collecting student data for targeted advertising purposes. Finally, the legislation would prohibit the use of students' data for any kind of profiling that would put certain students at a disadvantage as they move through their educational careers. However, the act does allow student data to be shared for research initiatives and to improve the educational process.

While legislation that protects students will likely find broad, bipartisan support, the Student Digital Privacy Act would be another step towards a sector-specific approach to privacy regulation (adding to laws protecting financial information, health information and information about children). Such an approach may make compliance difficult for companies that collect and process a variety of different types of information.

CONSUMER PRIVACY BILL OF RIGHTS

The final piece of the president's proposed legislation, the Consumer Privacy Bill of Rights (Bill of Rights), was first proposed by the Obama administration in January 2012. While the text of this particular iteration of the bill has not yet been released, the White House has outlined what this proposed legislation will contain.

The goal of the bill is to create a baseline national standard for collecting and processing data that banks, retailers and other companies that handle consumer data would have to follow.

The three main consumer rights the bill is expected to protect are the rights to:

- decide (not just know) what types of personal information are collected about them;
- know and control how their personal data is used; and
- have their information stored safely and securely.

The administration expects to release the text of the proposed Bill of Rights within the next few weeks.

As with many other proposals in the area of consumer data privacy, it is unlikely that a full consumer bill of rights will be enacted. There remains too much tension and uncertainty as to the proper balance between an individual's right to privacy and the many benefits that individuals gain by sharing their information, such as access to free content or services. Indeed, many people cannot even describe where they want this balance to be struck. While consumers would, in theory, want to evaluate each use of their data on a case-by-case basis, they also do not want to face the annoyance of constantly being asked about whether they approve the use of their data.

Return to Table of Contents

NEW YORK ATTORNEY GENERAL PROPOSES NEW APPROACHES TO DATA SECURITY

The New York AG has called for legislation that would require minimum cybersecurity standards and a Safe Harbor for companies who meet a higher standard.

New York State Attorney General Eric T. Schneiderman has proposed significant changes to New York's privacy and data security legislation through the enactment of a new Data Security Act (the DSA). The proposal, coming on the heels of Obama's announcement of the White House's legislative agenda, highlights the tension that will likely arise between the federal and state governments as states work to maintain their authority in the area. Given the number of trend-setting privacy laws enacted by California, the DSA represent New York's attempt to also be known as a state with cutting-edge thinking in this area.

The DSA would require entities that own, maintain or possess private information to meet certain standards to safeguard private information. Although details of these standard have not yet been released, the New York AG's statement indicated that the law would include: (1) administrative safeguards to assess risks, train employees and maintain safeguards; (2) technical safeguards to identify risks and detect, prevent and respond to attacks; and (3) physical safeguards, such as special disposal procedures, and intrusion detection. Entities that certify with independent third-party auditors would enjoy a rebuttable presumption in litigation that they have reasonable data security. The challenge with such a law will be defining appropriate standards that have binding legal effect (as opposed to suggested guidance like that provided by the NIST Cybersecurity Framework). The requirements would have to be specific enough that they have real meaning, but general enough that the state is not advocating a specific cybersecurity approach for all companies.

The DSA also would incentivize companies to adhere to an even higher standard of security by offering immunity from data breach liability. As with the baseline standard, it will be challenging to establish a legally binding heightened standard. Privacy advocates and other stakeholders also will likely balk at blanket immunity if a company followed certain proscribed steps.

In addition to implementing minimum data security requirements, the attorney general also proposed a more mundane change to New York's existing data breach notification law:

"Private information" would be expanded to include both the combination of an email address and password, and an email address in combination with a security question and answer. California's data breach notification law was recently amended with a similar change. The definition of private information would include medical information, including biometric information, and health insurance information

The proposed New York law also would incentivize companies to share forensic reports prepared as a result of data breaches with law enforcement officials by ensuring that such sharing does not affect any privilege or protection. This proposal would address a concern that many companies have that sharing such a report with any outside parties, including law enforcement, could affect the attorney-client privilege of such reports.

Return to Table of Contents

DELAWARE DATA DESTRUCTION LAW TAKES EFFECT

Delaware joins the ranks of states requiring secure destruction of personal information when it is no longer needed.

On January 1, 2015, two new Delaware laws relating to the destruction of personal information no longer needed by an entity went into effect.[2] Through these new laws — one of which applies to employee data, the other to consumer data — Delaware joins the growing number of states that have passed laws mandating the secure destruction of personal information.

BACKGROUND

Among the many issues confronting information security policymakers and organizations is the high cost of disposing of personal information in a secure manner such that it cannot be misappropriated during or after the disposal process. Given the concern that companies may look to cut corners in this important area, over 30 states, now including Delaware, have enacted legislation mandating how personal information can be destroyed.

DESTRUCTION REQUIREMENT

Companies that are subject to the new laws have to take "reasonable steps" to destroy (or arrange for the destruction of) consumer and employee data when the information will no longer be retained by the company. These steps include using a mechanism such that the data becomes "entirely unreadable or indecipherable through any means."

TO WHOM DOES THE LAW APPLY?

The new Delaware laws apply to Delaware employers and companies that do business in Delaware. The laws do not apply to entities covered by other data privacy laws (*e.g.*, HIPAA, Gramm-Leach-Bliley), but otherwise apply to all other entities, regardless of size, revenue or charitable status. It is not yet clear whether the new laws will apply to companies that are incorporated in Delaware but do not have information about Delaware citizens. Given the number of companies incorporated there, however, it is likely the plaintiff's bar will assert that the law applies to these companies.

WHAT PERSONAL DATA DOES THE LAW COVER?

The laws impose requirements on data that include personal identifying information, whether it is stored in hard copy or electronic format. "Personal identifying information" is defined as a

[2] Del. Code tit. 6 § 5001C to -5004C, tit. 19 § 736.

consumer's full name or first initial and last name combined with any of the following elements (when either the name or one of the following elements is not encrypted):

- signature;
- date of birth;
- Social Security number;
- passport number, driver's license or state identification card number;
- insurance policy number;
- bank account or financial services account number;
- credit or debit card number;
- any other financial information; or
- personally identifiable confidential health care information.

RIGHTS OF ACTION AND POSSIBLE TREBLE DAMAGES

Both laws create a possibility of substantial liability for violations, including both private and public causes of action, and successful civil suits can result in an award of treble damages. While the laws do not create any specific statutory damages, each record that is disposed of in a way that does not comply with the law is a separate violation. In addition, the laws grant the Division of Consumer Protection of the Delaware Department of Justice authority to bring an action in law, and the Division of Consumer Protection may bring an administrative enforcement proceeding.

PRACTICE POINTS

While Delaware is not the first state to enact such a law, it serves as an important reminder that companies should:

- review their current retention and disposal policies to ensure that information is not retained longer than needed and disposed of securely; and
- ensure that employees and vendors are educated about the new requirements.

Such actions are good business practice, even if the company does not have a legal obligation to comply.

Return to Table of Contents

COURT DISMISSES VIDEO PRIVACY PROTECTION ACT CLAIMS AGAINST DOW JONES

A Georgia federal court declines to expand the meaning of "personally identifiable information" under the Video Privacy Protection Act, thereby limiting the types of claims that can be brought.

In *Locklear v. Dow Jones & Co.*,[3] a federal judge in Georgia granted Defendant Dow Jones' motion to dismiss plaintiff's putative class action based on defendant's alleged violation of the Video Privacy Protection Act, 18 U.S.C. § 2710 (the VPPA) with respect to disclosures of plaintiff's alleged personally identifiable information (PII) to mDialog, an analytic and advertising company. The *Dow Jones* ruling continues a trend of district courts dismissing claims under the VPPA on the grounds that PII is "information *which must, without more*, itself link an actual person to actual video materials."

[3] No. 1:14-CV-00744-MHC (N.D. Ga. Jan. 23, 2015).

BACKGROUND

Dow Jones is an international media company that publishes a variety of newspapers and magazines. It also offers media to consumers in other mediums, including the free, on-demand *Wall Street Journal Live Channel* on Roku, a digital media-streaming device that delivers videos, news and other content to consumers' televisions via the Internet. In order to view specific television shows or video clips on their Roku devices, users must download and install the application called "channel" from the Roku Channel Store.

Plaintiff alleges that she downloaded and began using the WSJ Channel on her Roku in November 2012, and that each time she viewed a video clip using the WSJ Channel, Dow Jones disclosed her Roku device serial number and video viewing history to mDialog. Plaintiff alleges that her Roku serial device number and video viewing history constitute PII under the VPPA and that Dow Jones' disclosure of such PII violated the VPPA.

The primary question addressed by the court was whether the information transmitted by Dow Jones to mDialog constituted PII under the VPPA.

THE COURT'S RULING

The court rejected Dow Jones' argument that plaintiff failed to allege any "injury in fact" sufficient to satisfy the requirements for Article III standing. The court held that the alleged violation of a statutorily created right creates standing, even if no injury would have existed without the statute. Because plaintiff alleged the violation of her right to privacy under the VPPA, the Court held that she had sufficient standing to maintain the case.

The court also rejected Dow Jones' argument that plaintiff was not a "consumer" of Dow Jones or WSJ Channel under the VPPA because she paid no money to watch the WSJ Channel. The court held that the term "consumer" under the VPPA included a "renter" or "subscriber," both of which are not defined under the statute. The court followed the reasoning of other courts that the term "subscriber" in the VPPA did not necessarily imply payment of any money. Accordingly, plaintiff's allegation that she downloaded and used the WSJ Channel and her Roku serial number and viewing history were transmitted to mDialog qualified her as a "subscriber" and therefore a "consumer" under the VPPA.

However, the court agreed with defendant that plaintiff's anonymous Roku serial number and video viewing history, without more, is not PII. The court distinguished the facts in the case from those in the *In re Hulu Privacy Litig.*[4] because Hulu had disclosed its users' Facebook user IDs, which personally identified Facebook users and was more than a unique, anonymous identifier. Instead, the court held the facts to be akin to those in *Ellis v. Cartoon Network, Inc.*,[5] where the defendant Cartoon Network transmitted to data analytics company Bango the user's video history and Android ID. In *Ellis*, the court dismissed plaintiff's VPPA claim, holding that the Android IDs did not constitute PII under the VPPA because Bango had to take extra steps to connect the information disclosed by the Cartoon Channel to an identity. Here, although plaintiff alleged that mDialog could identify her and attribute her video records to her, she admitted that mDialog could only match the Roku number to plaintiff after it obtained *additional* demographic data linked to a Roku serial number from *other sources*.

---

[4] No. C 11-03764 LB, 2012 WL 3282960, at *8 (N.D. Cal. Aug. 10, 2012).
[5] No. 1:14-CV-484-TWT, 2014 WL 5023535, at *2 (N.D. Ga. Oct. 8, 2014).

PRACTICE POINTS

The court's sensible approach in rejecting plaintiff's invitation to expand the definition of PII under the VPPA is in keeping with the trend of district courts since the *Hulu* opinion. The common law seems to be evolving to provide more certainty for media companies that work with analytics and metrics companies to analyze their subscribers' preferences.

Return to Table of Contents

RUSSIA'S NEW DATA LOCALIZATION LAW: WHAT COMPANIES NEED TO KNOW

A new Russian law requires "data operators" who process data about Russian citizens to keep a copy of such data within the Russia Federation by September 1, 2015.

In July 2014, Russian President Vladimir Putin signed into law new legislation regarding so-called "data localization."[6] The somewhat vague Data Localization Law requires "data operators" who process data about Russian citizens to keep a copy of that data within the Russia Federation. While the head of the upper chamber of Russia's parliament has stated that the law is designed to best protect personal data, many feel that the law really was enacted to give Russian law enforcement better access to personal data, especially since only one copy (as opposed to every copy) must be retained in Russia. *Although originally slated to go into effect in September 2016, the Russian government has changed the mandatory compliance date to September 1, 2015*. The acceleration of the compliance date was in response to a general perception that companies saw the original date as so far out in the future that no steps would be necessary for some time. A plan to accelerate the compliance date to January 1, 2015, was shelved when companies complained that compliance by that date was not possible.

The key sentence of the Data Localization Law states that "operators processing data of Russian citizens, whether collected online or offline, are obliged to record, systematize, accumulate, store, update, change and retrieve such data in databases located within the territory of the Russian Federation." Both "data" and "processing" are defined broadly under Russian law. For example, processing includes a variety of types of manipulating data such as gathering, recording, storage, verification, use, deletion and transfer. Personal data also is generally interpreted more broadly than in other countries. In effect, the law requires data processors to maintain a copy of all data within Russia. "Data operators," although not defined under the Data Localization Law, is generally understood to cover both data controllers and data processors.

Given the law's breadth, many are waiting for official guidance from the Roskomnadzor, the Russian Data Protection Authority. In November, the Roskomnadzor made a number of unofficial statements regarding the law, including that it likely applies to employees working within Russia. There is still no official word on whether the law will apply to data collected prior to September 1, 2015, or to companies located outside of Russia that hold data about Russian citizens. Nonetheless, companies should begin preparing for the broadest interpretation of the law.

PRACTICE POINTS

Any company that controls or processes any data about individuals living in Russia should commence plans to have a copy of that data stored within the Russian Federation if it is not already doing so. Companies also should pay particular attention to any guidance from the Russia government or the Roskomnadzor regarding the breadth of the law.

---

[6] Federal Law No. 242-FZ.

LabMD LOSES ANOTHER ROUND IN FIGHT WITH FTC OVER DATA SECURITY AUTHORITY

The medical testing company suffers another setback in its challenge to the FTC's authority over information security matters.

On January 20, Georgia-based medical testing company LabMD lost another around in its ongoing dispute with the FTC arising out of data security breaches experienced by the company. The Eleventh Circuit Court of Appeals upheld a lower court's May ruling that it lacked jurisdiction over the Commission's case against the company until a parallel administrative proceeding was complete. This decision presents yet another setback for the company in its challenge to the FTC's authority over information security matters.

BACKGROUND

As we have previously reported,[7] the FTC brought an administrative proceeding against LabMD based on two separate data breaches affecting information belonging to approximately 10,000 consumers. The first breach was uncovered in 2008 when a file with billing information for more than 9,000 customers was found on LimeWire, a P2P sharing site that had been installed on a billing computer. The second breach was uncovered in 2012 when law enforcement officers in Sacramento, California, found documents containing information for approximately 500 LabMD customers in the possession of identity thieves.

The FTC's initial complaint, filed in August 2013, alleged that LabMD's failure to implement security measures sufficient to prevent a 2012 data breach violated Section 5 of the FTC Act's prohibition of "unfair" business practices. After the FTC initiated its administrative action, LabMD challenged the FTC's authority on two key grounds. First, the company asserted that the Commission lacks a general authority to enforce information security standards under the FTC Act. Second, the company argued that even if the FTC has such general authority, it lacks specific authority over this particular set of circumstances because the information that was breached is already subject to the Health Insurance Portability and Accountability Act and the Health Information Technology for Economic and Clinical Health Act.

ELEVENTH CIRCUIT DECISION

The Eleventh Circuit did not address LabMD's arguments against FTC jurisdiction, even though the district court's ruling had rejected them. Instead, the court ruled that it did not have jurisdiction over the case until the administrative proceeding resulted in a final determination.[8] It did not accept LabMD's argument that a January 2014 order, which rejected LabMD's positions on FTC jurisdiction, was sufficiently final to confer subject-matter jurisdiction to the federal court system. "The FTC complaint and order are not sufficiently definitive, cleanly legal or immediately burdensome so as to require our review at this stage," a panel of the court wrote.

Instead, the court explained that it had consistently found that, when the facts of a case are "inescapably intertwined" with the legal questions being presented, it is imprudent for a court to interfere with an agency process. The FTC's agency process, explained the court, "is best suited to develop the factual record, allow [the FTC] to continue to evaluate its positions on the issue and apply its expertise to complete the proceeding. All of this will allow for more robust appellate review by this court when the action concludes."

---

[7] *See, e.g., Privacy & Cybersecurity Update, December 2013*, available at http://www.skadden.com/newsletters/Privacy_Cybersecurity_Alert_December_2013.pdf.
[8] The Eleventh Circuit's ruling is available at http://media.ca11.uscourts.gov/opinions/pub/files/201412144.pdf.

NOT THE END

LabMD's dispute with the FTC has followed a complex path, and this ruling by the Eleventh Circuit is unlikely to be the end of the matter. Indeed, the administrative proceeding is scheduled to resume on March 3. However, as the company has shut down most of its operations — citing the burden of defending the FTC action — it remains to be seen how far it will go to defend this claim. The company is one of only two (the other being Wyndham Worldwide Corporation) that have, to date, challenged the FTC's authority in this area in court. When and if a final ruling is issued in this case, the decision could have far-reaching consequences in the information security space.

Return to Table of Contents

STATEMENTS BY FTC CHAIRWOMAN AND NEW REPORT HIGHLIGHT FTC FOCUS ON THE 'INTERNET OF THINGS'

The FTC underscores its concerns about the privacy risks presented by devices that are connected to the Internet.

In January, the FTC took two steps that highlight its focus on the Internet of Things, an area the FTC touted in 2014 as a major subject of concern. A significant address by Chairwoman Edith Ramirez at the International Consumer Electronics Show (ICES) was followed by the release of the FTC's in-depth staff report on this issue. As we have noted in prior newsletters, the Internet of Things refers to the growing number of physical devices that collect information and transmit it over the Internet. These so-called IoT devices include heart monitors that post information to social media, thermostats that collect information on consumers' use of their home in order to better regulate heat and air conditioning use, and road sensors that collect and transmit traffic that information to transportation agencies. Estimates suggest that in 2015 there will be approximately 25 billion connected IoT devices, many of which transmit sensitive data pertaining to an individual's movements, habits and private activities.

ADDRESS BY CHAIRWOMAN RAMIREZ

On January 6, 2015, Ramirez opened a panel at ICES by discussing privacy and policy issues that the Internet of Things poses for consumers and society. Reiterating the FTC's concerns about how data is collected, secured and used, Ms. Ramirez called for companies to take key measures to adequately protect consumers in an age of interconnected devices increasingly embedded into everyday life.[9] The mere presence of the FTC chairwoman as a keynote speaker at this trade show demonstrates the growing importance of the Internet of Things and the FTC's strong focus on this area of privacy protection.

As Ramirez pointed out, the Internet of Things has the potential to change the world in ways both beneficial and dangerous: "The Internet of Things could improve global health, modernize city infrastructures, and spur global economic growth … [but connected devices] are also collecting, transmitting, storing, and often sharing vast amounts of consumer data, some if it highly personal, thereby creating a number of privacy risks." The chairwoman highlighted several aspects of the Internet of Things of particular concern, such as ubiquitous data collection, by which even minute individual choices and actions leave a digital residue. Pieced together, such information provides what Ramirez called a "deeply personal and startlingly complete" individual profile. The IoT devices also raise concerns about unexpected uses of consumer data, particularly in connection to companies selling customer data to third parties. Finally, the Internet of Things raises

[9]The full text of Ramirez's remarks can be found at: http://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf.

the specter of security breaches. Any device connected to the Internet is vulnerable to attack, and the proliferation of such devices increases the number of potential points intruders may exploit. To address these risks, Ramirez reiterated the FTC's recommendation that companies prioritize security in each phase of an IoT's development, minimize data collection, and implement transparent notice and choice policies to better inform customers about collection and uses of their data.

The FTC has previously addressed concerns about privacy and security issues arising in the Internet of Things. Although it claims a more general authority to enforce privacy and information security standards through its mandate to address unfair or deceptive trade practices under the FTC Act, it is actively encouraging Congress and relevant industries to adopt strict consumer privacy regulations, as well as to stringently enforce their own policies. As we have previously reported, the Commission for some time has been recommending that companies developing IoT products take security and privacy issues seriously in their products.

THE FTC STAFF REPORT

On January 27, the FTC issued a staff report on the Internet of Things. The report, *Internet of Things: Privacy and Security in a Connected World*, highlights the FTC's concerns in this area, and makes clear that the subject will likely be a focus of enforcement action in the future. The report follows a November 2013 workshop the FTC held on this topic and focuses on the following key areas:

- *Security* – The FTC noted that there is a widespread agreement that IoT products should implement reasonable security, taking into account the amount and sensitivity of data collected and the costs of remedying any security vulnerabilities. To that end, the FTC encouraged companies to make security a priority though a "privacy by design" approach including by:
  - conducting a privacy or security risk assessment;
  - minimizing the data they collect and retain; and
  - testing security measures before launching an IoT product.
- Best practices also include training employees about this issue and making sure such security issues are addressed "at the appropriate level of responsibility within the organization." When companies identify a security risk, they are encouraged to implement a defense-in-depth approach. Under this approach, security measures are implemented at several levels (*i.e.*, not just merely relying on a consumer's password to protect security). Companies also should limit those who have access to a consumer's device, data and network, and engage in ongoing monitoring, patching vulnerabilities as they become known.
- *Data Minimization* – According to the FTC Report, companies should limit the data they collect and retain on IoT devices, and then dispose of the data once it is no longer needed. This approach, the FTC has stated, minimizes the risk of a cybersecurity attack (as possessing less data makes the company a less attractive target), while also minimizing the risk the company will use the data in ways that the consumer could not have reasonably anticipated. Some have argued that this proposal, while seemingly non-controversial, could hamper the benefits of IoT devices by limiting how companies can innovate in this area.
- *Notice and Choice*. One of the key challenges with an IoT device is that, since these devices often lack a consumer interface, there is often no practical way to provide consumers with notice of applicable privacy policies or the choice of opting out. The FTC Report acknowledges this challenge but nonetheless stresses the need for meaningful notice and choice if data is going to be used other than to provide the direct service the consumer expects. Options suggested by the FTC include video tutorials, affixing QR codes on devices and providing choices at points of sale, within set-up wizards or in privacy dashboards. The FTC's key point is that notice should not be buried within other documentation. The FTC Report also indicates that choice would not be necessary if the data has been anonymized. As with the data minimization requirement,

some have expressed concern that a notice and choice requirement would hamper innovation with respect to new uses of data. These groups advocate a "use-based" approach under which some data usage would always be allowed, and some usage prohibited. The FTC Report acknowledges the potential for such an approach in the future but notes that this framework does not exist today.

- *Legislation.* One of the most anticipated pieces of the FTC Report was the position that the FTC would take on IoT legislation. To the relief of many in the IoT field, the FTC Report states that legislation in this area would be premature. The FTC did , however reiterate its call for Congress to enact "strong, flexible, and technology-neutral federal legislation to strengthen its existing data security enforcement tools" and for federal data breach notification. Similarly, the FTC called for broad-based (as opposed to IoT-specific) privacy legislation that would address requirements for consumer choice and data usage.

A DISSENTING VOICE

The difference of opinion on regulating the development of IoT devices is perhaps best reflected in the fact that one FTC commissioner, Joshua Wright, dissented from the report. According to Wright, the FTC made a number of proposals without any empirical evidence that consumer welfare would be improved if they were adopted. As one example, he critiqued the proposals on data minimization, noting that the FTC failed to undertake any cost-benefit analysis of the adverse impact on innovation before determining that data minimization should be encouraged. Wright also asserted that the workshop format did not provide the FTC with sufficient information to issue specific recommendations.

PRACTICE POINTS

The FTC Report and Commissioner Ramirez's remarks at the leading consumer device conference reaffirm that the privacy and information security risks posed by the Internet of Things is an issue of great importance to the Commission. Companies that operate in this space should take these recommendations into consideration as they develop new products. Further, in light of the Commission's increasing enforcement efforts relating to privacy and security matters, companies should be prepared to provide evidence of their efforts to address these issues.

Return to Table of Contents

CALIFORNIA ASSEMBLY ESTABLISHES COMMITTEE ON PRIVACY AND CONSUMER PROTECTION

California establishes a Committee on Privacy and Consumer Protection at the state Assembly, demonstrating its growing focus on this area.

California, a state that has long led the country in enacting privacy and cybersecurity legislation, has established a Committee on Privacy and Consumer Protection at the state Assembly. The committee will be chaired by Assemblyman Mike Gatto (D-Los Angeles), the longest serving member in the Assembly. Gatto gained considerable publicity in recent months with his efforts to "crowdsource" privacy legislation. Under his plan, citizens can help draft and edit privacy legislation via an online Wiki. Gatto has committed to introducing the legislation after a consensus emerges. Speaker of the Assembly Toni Atkins (D-San Diego) described the new committee as "the one to watch" heading into 2015. Given California's leading role on these issues, and the growing importance of privacy and cybersecurity issues, Atkins is likely correct.

Return to Table of Contents

Attorney contacts appear on the next page.

SKADDEN CONTACTS

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Cyrus Amir-Mokri
Partner / New York
212.735.3279
cyrus.amir-mokri@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@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

Return to Table of Contents

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000