Skadden

Privacy & Cybersecurity Update

Pending LabMD Case May Limit Enforceability of FTC Act in Data Breach Matters

In the most recent development in the long-running battle between LabMD and the FTC, the 11th Circuit has delayed enforcement of the FTC's order against LabMD, finding that the FTC had misinterpreted the level of harm to consumers required to support an FTC enforcement action.

An 11th Circuit panel issued an order earlier this month delaying enforcement of the Federal Trade Commission's (FTC) order against LabMD,[1] finding that the company would be irreparably harmed without a stay because of the costs LabMD would incur in complying with the FTC's order, and that LabMD's data security practices may not have been unfair within the meaning of the FTC Act.

Background

As previously reported,[2] LabMD — a now defunct Atlanta-based cancer detection company — suffered two separate data breaches during which personal health data belonging to approximately 10,000 consumers was disclosed, with one uncovered in 2008 and the other in 2012. Employees of a data security firm, Tiversa Holding Company (Tiversa), uncovered the LabMD data files on a peer-to-peer network while conducting a search for exposed sensitive data in an attempt to generate demand for its security services. Tiversa gave LabMD's name to the FTC as part of a list of companies with allegedly poor information security infrastructure after LabMD refused to use Tiversa's security services.

In August 2013, the FTC filed an action against LabMD under Section 5 of the FTC Act alleging that LabMD's failure to implement appropriate data protection measures likely would cause substantial harm to consumers and constituted an unfair business practice under the FTC Act. An administrative law judge dismissed the complaint due to lack of proof that anyone aside from Tiversa had ever accessed the sensitive files, therefore concluding the breach was unlikely to be a source of harm to consumers. The

[1] *LabMD, Inc. v. Federal Trade Commission*, case number 16-16270, in the U.S. Court of Appeals for the 11th Circuit.

[2] See our previous article on the matter here.

FTC reversed and issued a final order requiring LabMD take certain remedial measures, including ordering the company to implement an information security system, obtain biennial assessments by an outside auditor and notify patients affected by the data leaks. Citing the burden of the FTC case, LabMD announced in January 2014 that it was winding down its operations but continued to battle the FTC's claims. LabMD requested a stay of the final order and appealed to the 11th Circuit in September 2016 after the FTC denied its request.

Appeal to the 11th Circuit

The 11th Circuit found that "there are compelling reasons why the FTC's interpretation [of the unfairness prong of the FTC Act] may not be reasonable" and, as such, LabMD is likely to succeed on the merits. The court doubted that the FTC Act encompasses intangible emotional or reputational harms to consumers arising from the disclosure of sensitive data. In addition, the court found that the FTC's interpretation of "causes or is likely to cause substantial injury to consumers," a requirement for enforcement under the unfairness prong of the FTC Act, was not reasonable, as the FTC interpreted this to mean "significant risk," based on the sensitive nature of the data, rather than "probable risk." In other words, the mere fact that sensitive data was exposed is not sufficient to show that consumers are likely to be harmed.

The 11th Circuit also found that LabMD proved it would be irreparably harmed without a stay, citing the fact that the costs of complying with the order to implement remedial measures would exceed the less than $5,000 cash the company currently had on hand. The court also found that there would be no substantial injury to other parties since LabMD is no longer operating, and thus, that there is no current risk of breach.

Next Steps

The appeal will now proceed on the merits, but the fact that the court granted a stay suggests that the 11th Circuit may be receptive to LabMD's arguments for reversal of the FTC's order. The outcome of the case could limit the FTC's ability to enforce the FTC Act with regard to data breaches where the harm to consumers is intangible, or risk of harm to consumers is low, even in cases where the data at issue is sensitive in nature.

Return to Table of Contents

NIST Guides Industry Players in Effort to Secure the Internet of Things

The National Institute of Standards and Technology has issued a framework for securing devices connected to the internet that focuses on the engineering necessary to help prevent system compromises, recover from cyberattacks and protect the personal data collected by such devices.

The National Institute of Standards and Technology (NIST) has released detailed guidance on securing devices connected to the internet. Recent cyberattacks have spurred increased attention on the nascent industry and what can be done to secure the devices that constitute the fast-growing internet of things.

Background

On November 15, 2016, NIST, part of the Department of Commerce, released 257 pages of guidance that it has developed over four years regarding incorporation of strong security features into devices connected to the internet.[3] The Department of Homeland Security recently released a similar document, which focuses on higher-level security issues, while the NIST guidance concentrates on more granular implementation strategies. One driver for the release of this guidance is that products, and the software within them, are growing more interconnected and complex, and some projections indicate that the breadth of the internet of things could reach 50 billion devices by 2020. As part of this growth, more issues related to hacking, service disruption and data leaks are likely to emerge.

The release of the NIST publication was moved up in the aftermath of a massive distributed denial-of-service (DDoS) attack in late October 2016 that blocked access to many popular web destinations, including Netflix, Amazon and Twitter. The attack exposed how easy it can be to hack millions of devices and how much damage attacks can cause if left unchecked by more aggressive security protocols. The October attack was carried out using tens of millions of internet protocol addresses linked to webcams and DVRs around the world and was targeted at the domain service provider, Dyn. The webcams and DVRs were infected with malware known as Mirai, which exploited the fact

[3] A copy of the guidance can be found here.

that many such systems use default usernames and passwords that do not need to be changed by end users. This intrusion demonstrated that the threat posed by an unsecured internet of things goes beyond that of exposed data to a destabilized internet infrastructure.

Important Aspects

Titled "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," the NIST guidance aims to provide a framework to secure the plethora of devices connecting to the growing internet of things. Though these guidelines are voluntary, the implementation of a standards-based structure is aimed at altering the status quo and increasing investment in securely engineered systems.

The document focuses on the engineering that is necessary to (i) help prevent system compromises, (ii) recover from cyberattacks and (iii) protect the personal data that is increasingly stored in internet of things devices. As such, this guidance goes beyond mere "cyber hygiene," which includes building firewalls and patching systems. It includes 30 technical standards and security principles that aim to guide the construction of a fundamental architecture and design that contributes to overall security. The goal is to build security safeguards directly into the products and remain aware of security at every stage of the product life cycle and, to this end, the framework offers guidance on the complete product life cycle: Agreement Process, Organizational Project-Enabling Process, Technical Management Process and Technical Process. By taking this approach, NIST essentially has provided a preventative maintenance handbook that tries to avoid the pitfalls inherent in addressing problems only as they surface. NIST has taken into account that all organizations and systems are unique, and as such the guidance is intended to be flexible enough to fit many companies' needs.

Implications for Companies

Many experts believe that the threat from cyberattacks, like those carried out against Dyn, will remain substantial into the future, and this guidance may help to prevent similar problems if manufacturers embrace stronger security protocols while the internet of things is still in its infancy. This publication and the conversation surrounding the recent cyberattacks against Dyn present an opportunity for companies to reassess cybersecurity systemwide.

Not only will companies face technological challenges from this evolving landscape, but potential legal and regulatory pitfalls are evident for those who do not properly address security flaws. For example, though the guidance is voluntary, because it sets out generally applicable standards, those standards may become common practice in the industry. If companies do not comply with common practice, companies may find themselves facing potential liability from regulators or private litigants. In addition to the specter of legal liability, there are implications for companies' insurance policies, as underwriters may look to this framework in gauging risk when offering insurance products related to cybersecurity for manufacturers of these devices.

Return to Table of Contents

New Chinese Cybersecurity Law May Have Far-Reaching Impact on Foreign Business

A controversial Chinese cybersecurity law presents new obstacles for multinational companies conducting business in China. The new law includes data localization requirements for both personal and business data, and obligations to submit to government security reviews.

On November 7, 2016, the Standing Committee of China's National People's Congress, the top legislative body of the People's Republic of China, approved a new cybersecurity law that grants the Chinese government increased centralized power to "ensure network security, to safeguard cyberspace sovereignty, national security and the societal public interest."[4] The law was first published as a draft in July 2015 and has since garnered criticism from the international business community and rights organizations throughout its drafting process. Despite persistent pushback from overseas critics, the law will go into effect on June 1, 2017. The law will apply to the construction, operation, maintenance and use of information networks in China, as well as supervision and management of network security within China.

Corporate critics of the cybersecurity law have focused on the breadth of key provisions, suggesting that parts of the new law will make it difficult for multinationals to operate in China, or, at the very least, make it significantly more expensive for them to do so. Analysts also have suggested that the law's vagueness indicates that the Cyberspace Administration of China will have broad latitude to direct how the law is interpreted and enforced.

The new law places increased obligations on three types of entities conducting business in China: (i) critical information infrastructure operators, (ii) network operators, and (iii) network products and services providers. The obligations imposed on each are briefly outlined below.

[4] An official English version of the new law has not yet been released by the Chinese government. An unofficial English translation can be found here.

Obligations Imposed on Critical Information Infrastructure Operators

The law imposes a number of new requirements on entities that are critical information infrastructure operators. However, the definition of such entities is vague, making those new requirements applicable to any number of companies. Under the terms of the new law, critical information infrastructure includes "public communication and information services, power, traffic, water, finance, public service, electronic governance and other critical information infrastructure that if destroyed, losing function or leaking data might seriously endanger national security, national welfare and the people's livelihood, or the public interest, on the basis of their tiered protection system."

As provided in Article 37, companies deemed critical information infrastructure operators are required to store within mainland China any personal information and "other important data" — currently undefined by the new law — gathered or produced during operations. The law provides one exception to its data localization requirement, namely where a business requirement to share such data outside of China is "truly necessary." However, what qualifies as "truly necessary" remains undefined, and companies seeking reprieve under this exception would still have to submit to a security assessment, which some have noted may require companies to disclose sensitive information to the government. An earlier draft of the law suggested that disclosure of source code would be required as part of the security assessment, but the reference was removed following protests from other countries.

Obligations Imposed on Network Operators

Under the new law, broad obligations are placed on network operators, which are defined as "network owners, managers and network service providers." A network "refers to systems comprised of computers or other information terminals and related equipment that follow certain rules and procedures for information gathering, storage, transmission, exchange and processing." Network operators are expected to adhere to social mores, commercial ethics and to "accept supervision from the government and public." What is meant by "supervision from the government" is currently unclear.

Moreover, network operators that provide "network access and domain registration services for users, phone network access or provide users with information publication or instant messaging services" must require their users to provide "real identity information." If a user refuses to provide such information, network operators must refuse to provide them with relevant services. Pursuant to Article 28, network operators also should be prepared to provide "technical support" to public security and state security organizations to aid in their efforts to preserve national security and investigate crimes. The law has not defined what is contemplated by "technical support." However, some have speculated that this support obligation could mean turning over personal data or encryption keys to the Chinese government.

Network operators additionally are obligated to perform a series of security protection duties, which include: (i) formulating internal security management systems; (ii) adopting preventative cybersecurity technological measures; (iii) adopting monitoring and recording technological measures, including retaining logs for at least six months; and (iv) classifying and encrypting data .

Finally, the new law offers increased protection to data subjects, at least as such protection relates to their internet service providers, if not the Chinese government. Absent data subject consent, network operators must not provide personal information to third parties, unless the data subject is "unidentifiable and cannot be recovered." Under the new rules, data subjects have the ability to correct flawed personal information and may have such information deleted if the network operator "violated the provisions of laws, administrative regulations or agreements between the parties to gather or use their personal information."

Obligations Imposed on Providers of Products and Services

Providers of network products and services must inform users and "competent departments" whenever a security flaw or vulnerability is discovered. The new law specifically highlights "critical network equipment" and "specialized network security products," which either must meet certification standards or meet safety inspection requirements before being sold on the Chinese market. The law does not specify such standards or requirements.

Penalties for Non-Compliance

The law provides for a number of enforcement mechanisms that can be invoked against companies and individuals for violating the law, depending on the nature of the violation. Regulators can shut down websites, freeze assets and revoke business licenses, and, in some cases, individuals may be detained for up to 15 days. Fines also may be imposed on companies or management personnel; fines against companies range from approximately $7,500 to $150,000, and fines against individuals range from approximately $750 to $15,000.

Key Takeaways

Given the law's broad definitions of entities to which it applies, companies that typically may not identify themselves as critical information infrastructure operators, network operators, or network product and service providers may nonetheless find

themselves subject to the requirements of the new law. Companies that may fall within these definitions and that consider China a significant part of their business model should compare their current practices with the requirements of the law and identify any changes that would need to be implemented to comply by June 1, 2017. It is anticipated that Chinese government agencies and industry organizations will issue more detailed implementing regulations and standards prior to the June effective date, which should provide further guidance to companies seeking to comply with the new law.

Return to Table of Contents

Russian Court Allows Communications Agency to Block LinkedIn

Russia has blocked access to LinkedIn, citing the company's violation of a Russian data protection law that requires personal data of Russian users to be stored on servers located in Russia.

On November 18, 2016, Russia blocked access to LinkedIn, the world's largest professional social network, after a Moscow court paved the way for the ban. The court upheld a decision to block LinkedIn within Russia after the company was alleged to have violated a Russian data protection law. The law, passed in September 2015, requires online service providers to store the personal data of Russian users on servers within the country's borders. The controversy with LinkedIn marks the first time Russia has enforced this data localization law.

Background

In August, the Russian communications agency Roskomnadzor, which is responsible for matters in the telecom, information technology and mass communications fields, filed a complaint against LinkedIn in the Tagansky District Court. That court ruled in favor of Roskomnadzor, concluding that LinkedIn violated the Russian data protection law on two counts. First, it ruled that LinkedIn did not store personal information about Russian users within the country, and second, that the company processed information about individuals who were not registered on the site and had not agreed to the company's user agreement. LinkedIn appealed the ruling, but a Moscow court upheld the lower court on November 10, 2016, allowing Roskomnadzor to block the website.

Ramifications for Other Worldwide Internet Service Providers

Russia has said the purpose of the law is to protect citizens' personal data, but skeptics view it as a threat to foreign social networks and a means for Russia to gain control over the internet and user data. However, other countries, such as Germany, have passed similar laws, requiring technology companies to store users' information on local servers, without facing similar skepticism.

Some have speculated that LinkedIn was targeted as a means of sending a message to other companies. According to Roskomnadzor, other large U.S.-based online service providers have already started to move personal data storage to Russia in compliance with the law. In the aftermath of this court decision and subsequent ban, it is unclear whether other global technology companies will comply with the law or risk having their services banned in Russia. In light of these developments, companies that process the personal data of Russian citizens, and that consider Russia an important component of their business models, should evaluate their compliance with the data localization law.

Return to Table of Contents

(Attorney contacts appear on the next page.)

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

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

James R. Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian W. Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David C. Eisman
Partner / Los Angeles
213.687.5381
david.eisman@skadden.com

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

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

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

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

Richard J. Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Amy S. Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

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

Ivan A. Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

David E. Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

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

Jennifer L. Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

Helena J. Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

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

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@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