Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | October 2017

In this month's issue, Stephen Claeys (one of our newest colleagues) writes about the emerging Asia-Pacific Economic Cooperation (APEC) cross-border rules (part of the increasing complexity of international data privacy laws). Matthew Gardner, Megan Brown, and Michael Diakiwski review one of the most recent Federal Trade Commission (FTC) privacy settlements (in contrast to the FTC's more typical data security cases) related to the recent Lenovo enforcement activity. Megan also reviews recent U.S. Department of Justice (DOJ) developments related to the Internet of Things (IoT) and surveillance. Lastly, Megan summarizes a report that Wiley Rein co-authored with the U.S. Chamber of Commerce, which focuses on the key principles of IoT security.

As always, please let me know if you have questions or comments on any of these topics. Also, if there are topics you would like to see addressed in future issues of *Privacy in Focus* – or if you have a need for a privacy or data security speaker at your event – please let me know. I can be reached at 202.719.7335 or knahra@wileyrein.com. Thank you for reading. ■

APEC's Cross-Border Privacy Rules System: Privacy Protection for the Asia-Pacific and Beyond

By Stephen J. Claeys

ALSO IN THIS ISSUE

Most consideration of international privacy rules focuses on the U.S.-EU Privacy Shield and the EU's General Data Protection Regulation (GDPR). Often overshadowed is the fact that there is also a system of privacy rules for the much more economically dynamic Asia-Pacific region. As this system expands, the benefits for companies certified under the system will likewise grow.

The CBPR System

The Cross-Border Privacy Rules (CBPR) system was established under the auspices of the Asia-Pacific Economic Cooperation (APEC), which consists of 21 member economies along the Pacific Rim. Members

continued on page 2

The Lenovo-FTC Settlement Highlights Risks of Certain Data Analytics Practices

By Matthew J. Gardner, Megan L. Brown, Michael Diakiwski

On September 5, 2017, the Federal Trade Commission (FTC) announced it had entered a no-fault settlement with Lenovo, Inc., over allegations that the company preinstalled ad software which compromised customers' online security and privacy.[1] The FTC's complaint, originally filed in 2014, alleged that certain consumer laptops sold in the United States came pre-installed with a "man-in-the-middle" adware program developed by a company called Superfish, Inc. According to the FTC, this adware operated without the users' knowledge or consent, intercepted users' web traffic, accessed sensitive customer data, and created security vulnerabilities.[2]

When the FTC settlement with Lenovo was announced, Acting FTC Chairman Maureen Ohlhausen told reporters that the settlement "sends a very important message" to companies that "everyone in the chain really needs to pay attention" to data security. Companies, including manufacturers, software and technology providers, and companies that used third-party vendors to interact with or manage

continued on page 3

APEC's Cross-Border Privacy Rules System: Privacy Protection for the Asia-Pacific and Beyond *continued from page 1*

range from the United States and Chile to Singapore and Russia, and represent about 54% of the global economy. APEC generally operates on a consensus-based approach to develop voluntary standards. Despite this approach, APEC members often adopt APEC standards as binding, and APEC standards are frequently the foundation for later established global standards.

APEC members established the CBPR system in 2011 with the goal of establishing meaningful protection for the privacy and security of personal information, while ensuring the free flow of personal information across borders. The CBPR system does this by requiring APEC members wanting to join to: 1) demonstrate that the CBPR system's principles are enforceable under national law; 2) identify the domestic authority that can enforce the CBPR system; and 3) identify an APEC-recognized third-party certifying organization. Once an APEC member joins the CBPR system, that APEC member's companies can participate in the CBPR system by having their privacy policies and practices reviewed and certified by the third-party certifying organization as meeting the CBPR system's requirements. Once a company is certified, the CBPR becomes enforceable against that company. Thus, the CBPR system is similar to the U.S.-EU Privacy Shield by providing for self-assessment, compliance review, recognition and enforcement.

The CBPR system does not replace national law, nor does it require an APEC member to recognize another member's privacy system as adequate based on the other

continued on page 5

continued from page 2

customer data, should closely monitor the collection of user data. Missteps could result in FTC enforcement, restrictive settlements, widespread state consumer protection claims, and class action litigation.

Brought under Section 5 of the FTC Act, the FTC's complaint alleged unfair and deceptive acts. Specifically, the FTC charged Lenovo with one count of deceptive failure to disclose, for not disclosing to consumers how the adware would operate. It also charged Lenovo with two counts of unfairness for (1) unfair preinstallation of man-in-the-middle software, "without [providing] adequate notice or [obtaining] informed consent" from users; and (2) unfair security practices, for Lenovo's failure "to take reasonable measures to assess and address security risks created by third-party software preinstalled on its laptop...."[3]

Under the FTC's Consent Order, Lenovo is prohibited from misrepresenting any features of preinstalled software related to consumer Internet browsing-based advertising. In addition, Lenovo must obtain affirmative user consent before installing such software on its laptops, provide instructions for how the consumer may revoke consent to the covered software's operation, and provide reasonable and effective means for consumers to opt out, disable, or remove all the covered software's operations, including uninstallation. Further, for a period of 20 years, Lenovo is required to implement a comprehensive software security program for most preloaded software, which is subject to third-party audits. The FTC may also seek monetary fines if Lenovo fails to abide by the Consent Order.[4] In a separate agreement, Lenovo agreed to pay $3.5 million to settle charges brought by the State Attorneys General under state consumer protection laws.[5]

How the Superfish Adware Worked

In 2014, Lenovo partnered with Superfish to sell new Lenovo laptops preinstalled with Superfish-created adware called VisualDiscovery. Superfish specializes in visual search technology that can analyze a picture or video and determine what object is featured in that image. Using that technology, VisualDiscovery generates advertisements with links for products that are similar to what the user is searching for and observing on their laptop's screen. These targeted ads are inserted into a user's web browser and appear as if they were part of the website the user was visiting.

In order to encrypt web traffic, browsers and web servers use Hypertext Transfer Protocol Secure (HTTPS). Using HTTPS, a server sends a public certificate to the user's browser through which the user's browser can verify the identity and authenticity of the website. The public certificates for these HTTPS connections are issued by a handful of trusted certificate authorities, such as Symantec. After verification using the certificate, the browser and server are able to generate an encryption key for the communication session, allowing each party to encrypt and decrypt the communications.

According to the FTC's Complaint, the Superfish adware on Lenovo laptops interrupted this process. Instead of communicating directly with a website using HTTPS, a user on a Lenovo laptop first communicates with VisualDiscovery, which operated as a proxy. The adware installed a root certificate that replicated the root

continued on page 4

continued from page 3

certificate that would normally be supplied by a trusted website. Using its own root certificate, the adware verified to the user's browser that it was communicating with a trusted website. From the user's point of view, the transaction appeared to be a normal, encrypted HTTPS transaction.

The adware, however, decrypted the user's web traffic and analyzed it to generate targeted ads. VisualDiscovery then re-encrypted the traffic and forwarded it to the website the user requested. The FTC referred to this as a man-in-the-middle attack because both the user and the website were unaware that a third party (in this case, Superfish) had intercepted their communication.

Beyond legal and privacy concerns, many data security experts argued that the Superfish adware was a security disaster, because of vulnerabilities in the way the adware encrypts and decrypts information.[6] Superfish used the same root certificate and the same password to decrypt the private key on every Lenovo laptop, which hackers could have used to easily imitate a trusted website or decrypt all traffic sent using an adware-installed Lenovo laptop.[7]

Class Action Lawsuits

Beyond the FTC and state charges, multiple plaintiffs' attorneys filed class action lawsuits against Lenovo and Superfish. Among a variety of claims, plaintiffs alleged that the defendants violated the Computer Fraud and Abuse Act (CFAA).[8] The CFAA is broad in scope and generally prohibits knowingly accessing a computer without authorization or exceeding authorized access and causing harm.[9] The CFAA provides both criminal and civil sanctions and was designed to prevent traditional hacking attacks. It has also been used in a wide variety of contexts beyond traditional hacking, and federal courts often struggle to define what conduct violates the CFAA.

In June 2015, a federal multidistrict litigation panel consolidated some of the Lenovo lawsuits in the Northern District of California. In January 2016, Lenovo filed a motion to dismiss. Judge Whyte issued an order in October 2016, granting Lenovo's motion to dismiss in part. The court dismissed the claims under the federal Electronic Communications Privacy Act as well as several related state claims.

However, with respect to the CFAA claim, and several other statutory unauthorized access and consumer protection claims, Lenovo's motion to dismiss was denied. In denying Lenovo's motion, the court stated "Lenovo entered into an agreement with Superfish to preinstall VisualDiscovery on several laptop models and 'share in any revenues that flowed from the partnership.'" Further, plaintiffs alleged that Lenovo executives were provided with demonstrations of the VisualDiscovery adware, and "some [executives] expressed concerns" about the SSL decoder programs and how the adware may negatively impact Lenovo laptops. As of October 2017, the case, In re: Lenovo Adware Litigation, remains active.

Why This Matters

Technologies are changing rapidly, and the application of decades-old laws like the Wiretap Act and the CFAA to these new technologies is not straightforward and has resulted in ambiguity about whether certain technologies and practices are legal. With

continued on page 5

The Lenovo-FTC Settlement Highlights Risks of Certain Data Analytics Practices

continued from page 4

more companies monetizing ad revenue and leveraging big data, businesses need to be aware that the FTC will scrutinize not only their use and handling of consumer data, but also the practices of third-party vendors with access to that data. Hardware manufacturers, like Lenovo, may receive scrutiny for software preinstalled on their products.

These claims are highly fact-dependent but typically turn on two primary issues: first, whether the user has given consent to a business to use their personal data; and second, the nature of the technical arrangement between the user, the business, and any third-party vendors. For companies that are evaluating the legality of a new data collection practice, the analysis should include a detailed understanding about how the technology works and what notification will be provided to consumers. ■

For more information, please contact:

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Michael Diakiwski
202.719.4081
mdiakiwski@wileyrein.com

[1] FTC, Lenovo Settles FTC Charges it Harmed Consumers With Preinstalled Software on its Laptops that Compromised Online Security (Sept. 5, 2017), *available* **here** .
[2] *In the Matter of Lenovo (United States) Inc.*, Complaint, FTC File No. 152 3134 (Sept. 2017), *available* **here**.
[3] *Id.*
[4] *See Lenovo Consent Order.*
[5] *See, e.g.* Press Release, Cal. Dep't of Justice, Attorney General Becerra Announces $3.5M Settlement with Lenovo for Preinstalling Software that Compromised Security of its Computers (Sept. 5, 2017), *available* **here**; *see also* Press Release, N.J. Dep't of Law & Pub. Safety, Attorney General Announces $3.5 Million Multi-State Settlement with Lenovo over Hacker-Vulnerable Software (Sept. 5, 2017), *available* **here**.
[6] *See* U.S. Computer Emergency Readiness Team, Alert (TA15-051A) Lenovo Superfish Adware Vulnerable to HTTPS Spoofing, (Feb. 20, 2015), *available* **here**.
[7] *See* Aditi Jhaveri, "Superfish software on Lenovo notebooks: What you can do," FTC Consumer Info. (Feb. 27, 2015), *available* **here**.
[8] 18. U.S.C. §§ 1030 *et seq.*
[9] *See* 18 U.S.C. § 1030(a).
[10] *In re: Lenovo Adware Litigation*, No. 15-md-02624, 2016 WL 6277245 (N.D. Cal. Oct. 27, 2016).
[11] *In re: Lenovo Adware Litigation*, 2016 WL 6277245, at *6.

APEC's Cross-Border Privacy Rules System: Privacy Protection for the Asia-Pacific and Beyond

continued from page 2

member having joined the CBPR system. Instead, it provides harmonization in privacy protection systems and establishes minimum standards for privacy protections. The CBPR system bridges across differences between domestic privacy approaches by applying commonly agreed-upon principles and rules. Having more harmonized privacy protection systems that meet minimum standards in turn helps facilitate data flows between CBPR members. Companies can also market certification under the CBPR system to customers and business partners as an indicator of reliability and compliance.

continued on page 6

Status and Prospects

So far, the United States, Canada, Mexico and Japan have joined the CBPR system. South Korea was recently formally approved to join, and Singapore have submitted an application. The Philippines, Thailand, Vietnam, Thailand, Australia, Taiwan and Hong Kong have also expressed interest in participating. Thus, while the CBPR system may have started slowly, it is moving toward a critical mass of APEC members. Commerce Secretary Wilbur Ross stated on October 17 that he is seeking to expand the CBPR system to more APEC members. U.S. companies certified under CBPR include Apple, HP, IBM, Cisco Systems, Lynda.com, Merck, and Box.

The benefits of the CBPR system are expected to further expand. First, though not required to, APEC members may begin to recognize companies' certification under the CBPR system as meeting that member's domestic privacy requirements. This already happened when Japan recently amended its Protection of Personal Information Act (PPIA) to allow data transfers out of Japan to companies certified under the CBPR system. This is particularly important for U.S. companies given that the Japanese government recently indicated that it does not plan to give the United States a blanket designation of providing adequate data protection.

Second, the CBPR system could become the basis for a global privacy protection system, or at least become interoperable with other systems. There is an ongoing effort between APEC and the EU to explore the interoperability between the CBPR system and the EU's GDPR. A meeting between APEC and EU working groups was held last August, and the agreed goal is to develop a joint work plan by 2018. Commerce Secretary Ross also recently said that Commerce is exploring how to make the CBPR system and the EU's regime compatible. ■

For more information, please contact:

Stephen J. Claeys
202.719.7425
sclaeys@wileyrein.com

Wiley Rein Welcomes Stephen J. Claeys

Stephen J. Claeys recently joined Wiley Rein LLP as a partner in our renowned International Trade Practice. Steve assists clients on a variety of international trade law and policy matters, including bilateral and multilateral trade agreements, trade remedies and safeguards, foreign market access barriers, e-commerce and digital trade, agriculture trade, and customs enforcement. He has 25 years of experience advising members of Congress, senior White House and U.S. Department of Commerce officials, and clients on international trade law and policy, and supervising the enforcement of the U.S. trade remedies laws. He most recently served as trade counsel for the U.S. House of Representatives, Committee on Ways & Means, Subcommittee on Trade.

In his prior congressional role, Steve also served as House Ways and Means Committee staff lead on all areas of the Trans-Pacific Partnership agreement negotiations, as well as advising on other trade agreement negotiations. He drafted and helped secure passage of legislation on Trade Promotion Authority, amendments to the U.S. trade remedies law, reauthorization and restructuring of U.S. Customs and Border Protection, the U.S.-Panama Free Trade Agreement, and Permanent Normal Trade Relations with Russia.

Prior to his six years on the Hill, Steve served as Deputy Assistant Secretary for Antidumping/Countervailing Duty Operations at the U.S. Department of Commerce, Import Administration, and served as a National Security Affairs Special Advisor to the White House, Office of the Vice President (Richard B. Cheney). Steve can be reached at 202.719.7425 or sclaeys@wileyrein.com.

The DOJ Addresses The Internet of Things, National Security and Surveillance

By Megan L. Brown

On October 10, Deputy Attorney General Rod Rosenstein, the No. 2 official at the U.S. Department of Justice, delivered **remarks** expressing concern about the Internet of Things. He made clear that the federal government remains committed to getting electronic data to solve crimes, and observed that the tech community must be prodded to strike a different balance: "Technology providers are working to build a world with armies of drones and fleets of driverless cars, a future of artificial intelligence and augmented reality. Surely such companies could design consumer products that provide data security while permitting lawful access with court approval."

A few areas stand out for the IoT and the tech industry.

continued on page 8

continued from page 7

First, Mr. Rosenstein expressed serious concerns about IoT security. In describing the **2016 Mirai botnet attack**, he found "especially worrisome" that the attack "used simple Internet-connected devices, such as cameras and digital video recorders. Those so-called 'Internet of Things' devices" he said, "are easily susceptible to control by hackers because of the widespread use of default passwords and other failures to secure them." From that attack and others, DOJ has drawn the lesson that "our digital infrastructure … can be hijacked and used against us as an attack vector. The possibilities for such attacks will grow. Estimates reveal that 6.3 billion Internet-connected devices were used in 2016. The total may reach 20.4 billion by 2020. Imagine the possible attack vectors if all of those devices employed default passwords." This sentiment is consistent with prior federal government observations that raise concerns about the broad security implications from IoT devices' widespread use.

Second, the Deputy Attorney General observed that innovation may outpace law and be inconsistent with public safety. "The digital infrastructure is not always constructed with adequate regard for public safety, cybersecurity, and consumer privacy," Mr. Rosenstein said. He also observed that "the tools we use to collect evidence run up against technology that is designed to defeat them," including but not limited to encryption and corporate decisions to store "evanescent" data overseas.

Third, he characterized the interests and behavior of tech executives as counterproductive. "Technology companies operate in a highly competitive environment. Even companies that really want to help must consider the consequences." This is true, given litigation risks, challenges in protecting shared information from public disclosure, and the possibility of public criticism here and abroad. The Deputy Attorney General laments that "the government's efforts to engage with technology giants on encryption generally do not bear fruit. Company leaders may be willing to meet, but often they respond by criticizing the government and promising stronger encryption." He predicts that "[t]echnology companies almost certainly will not develop responsible encryption if left to their own devices. Competition will fuel a mindset that leads them to produce products that are more and more impregnable."

The private sector should be attuned to DOJ's views on these issues as they develop innovative products and services, knowing that they may be called on to assist the government. As DOJ made clear in its **litigation against Apple for help unlocking an iPhone**, it will not shy away from using all the tools at its disposal to promote its view of public safety. At the same time, DOJ, as well as state and local law enforcement, should consider how to engage and find common ground with the private sector on these tough issues. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

New Chamber White Paper on IoT Security

Wiley Rein partner Megan Brown and several firm associates collaborated with the United States Chamber of Commerce to develop a white paper on security in the Internet of Things (IoT), with the goal of helping policymakers evaluate and consider whether and how to address privacy and security in the IoT. It highlights the incredible potential of the IoT for consumers and nations in the developed and developing world. We concluded that when it comes to security, attempts to regulate today may well be outdated tomorrow. Flexible approaches to collaboration and cooperation to address shared threats have significant advantages over national regulation, which may fragment the global economy. Ten key principles emerge from the **report**.

1. Any approach to IoT security should be data-driven, based on empirical evidence of a specific harm, and be adaptable both over time and cross-border.

2. Security demands should never be used as industrial policy to advance protectionism or favor national economic interests.

3. National boundaries need not become arbitrary obstacles to the movement of devices or data, or to the offering of IoT-related services.

4. Global standards work is the best way to promote common approaches and technology solutions. Such standards should be open, transparent, and technology-neutral.

5. Any government IoT strategy should promote technical compatibility and interoperability to the maximum extent possible.

6. Everybody is vulnerable, so cyber threats must be met with global information sharing and collaboration to improve and safeguard the IoT ecosystem.

7. End users need to be educated about their roles and responsibilities in this digital age.

8. Manufacturers and vendors should be encouraged to routinely evaluate and improve endpoint security.

9. The international community must collectively condemn criminal activities that infect and exploit the openness and connectivity of the Internet and our digital future.

10. Governments must work together to shut down illegal activities and bring bad actors to justice. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Events & Speeches

Privacy Bootcamp for Security Professionals

Kirk J. Nahra, Speaker

IAPP's Privacy. Security. Risk. 2017 Conference

October 16, 2017 | San Diego, CA

I'm a Lawyer: How Can I Advise on Data Security Issues?

Kirk J. Nahra, Speaker

IAPP's Privacy. Security. Risk. 2017 Conference

October 17, 2017 | San Diego, CA

Security @ San Francisco 2017

Matthew J. Gardner, Speaker

HackerOne

October 24, 2017 | San Francisco, CA

The Litigation Jungle; panel on litigation risks facing technology and the Internet of Things

Megan L. Brown, Speaker

U.S. Chamber of Commerce 2017 Legal Reform Summit

October 25, 2017 | Washington, DC

Health Care Delivery and Payment Reform: Global Payment and Measurement

Kirk J. Nahra, Moderator

AUWCL and ASLME Presents: Next Steps in Health Reform 2017

October 26, 2017 | Washington, DC

Legal Panel

Megan L. Brown, Speaker

API Cybersecurity Conference & Expo

November 7, 2017 | Houston, TX

We've Been Breached: Now What? How to Effectively Work with Law Enforcement and Regulators

Kirk J. Nahra, Speaker

Healthcare Security Summit

November 14, 2017 | New York City, NY

How HIPAA Can Address Cyber Risk Prevention

Kirk J. Nahra, Speaker

Cyber Security Risk Management in Healthcare

February 7-8, 2018 | London, UK

Privacy Bootcamp for Security Professionals

Kirk J. Nahra, Speaker

IAPP's Global Privacy Summit

March 27-28, 2018 | Washington, DC

The Path Towards a New and Complete Consumer Health Regulatory Structure

Kirk J. Nahra, Speaker

Twenty-Seventh National HIPAA Summit

March 27, 2018 | Arlington, VA

continued on page 11

Events & Speeches

continued from page 10

Privacy and Security Enforcement Highlights

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association National Summit

May 2018 | Orlando, FL

Top Ten Privacy and Security Developments for the Health Care Industry

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association National Summit

May 2018 | Orlando, FL

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Stephen J. Claeys	202.719.7425	sclaeys@wileyrein.com
Michael Diakiwski	202.719.4081	mdiakiwski@wileyrein.com
Matthew J. Gardner	202.719.4108	mgardner@wileyrein.com
Bruce L. McDonald	202.719.7014	bmcdonald@wileyrein.com
Kirk J. Nahra	202.719.7335	knahra@wileyrein.com