Wiley Rein LLP

PRIVACY IN FOCUS®

Developments in Privacy and Information Security Law | April 2018

In this month's issue, we address potential security practices for mobile and connected devices, the recent Clarifying Lawful Overseas Use of Data Act (CLOUD) legislation, and the firm's hosting of an event with the Director of the Office for Civil Rights at the U.S. Department of Health and Human Services.

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. ■

— Kirk Nahra, Privacy & Cybersecurity Practice Chair

Security, Standards, and IoT: Will Connected Devices Flourish Under Prescriptive Regimes?

By Megan L. Brown and Michael L. Diakiwski

Security for Internet-connected devices, the "Internet of Things" (IoT), is critically important. Now, more than ever, it is top of mind for device manufacturers, network operators, consumer advocates, lawmakers, and government regulators – domestically and internationally. In the face of recent attacks, government authorities and consumer advocates have proposed legislation, frameworks, certifications, and labeling schemes.

A sense of urgency to act must not threaten the efficacy of IoT devices or stymie innovative applications with premature or oversimplified approaches. Below we explore some of the proposals to enhance IoT security and underscore key principles, which should be followed to ensure that the marketplace continues to produce innovation beneficial across the globe.

Greater Use, Greater Threat

In 2017, worldwide demand for IoT devices skyrocketed. Networked devices have become, to a large degree, essential in many respects. It is estimated that more than 8.4 billion devices were

continued on page 2

ALSO IN THIS ISSUE

2 CLOUD Act Passes Omnibus Spending Bill, Impacting User Data Stored Overseas

7 HHS Office for Civil Rights Director Roger Severino Leads Discussion on Health Care Regulation and Cybersecurity

10 Wiley Rein Welcomes Back Former FEC Chairman Lee Goodman

8 Events & Speeches

CLOUD Act Passes in Omnibus Spending Bill, Impacting User Data Stored Overseas

By Megan L. Brown, Matthew J. Gardner, and Shawn M. Donovan

On March 23, 2018, President Trump signed a $1.3 trillion spending package that will keep the government funded through the end of September. The Omnibus bill includes the Clarifying Lawful Overseas Use of Data Act (CLOUD Act or Act), a bill proposed in February that will allow U.S. law enforcement to access citizens' data stored overseas and clarify the legality of similar requests coming from foreign law enforcement agencies for data on their citizens stored in the United States.

The Act may have significant implications for companies that receive requests from U.S. or foreign law enforcement for user data. While issues about data localization will continue – indeed, it may be impossible for a single government to resolve those issues – the Act takes steps to clarify the ability of U.S. law enforcement and certain foreign governments to obtain user data across borders.

Domestic Law Enforcement Requests for User Data Stored Overseas

The CLOUD Act amends the Stored Communications Act (SCA), a 1986 law enacted long before the advent of cloud computing and the construction of storage centers around the world. The CLOUD Act makes clear that U.S. law enforcement can reach user data stored overseas, adding the following section to the SCA:

continued on page 6

Security, Standards, and IoT: Will Connected Devices Flourish Under Prescriptive Regimes? *continued from page 1*

in use in 2017, which was more than a 30% increase from the year before.[1] Every hour, a million new IoT connections are made and future predictions are even more staggering.[2] Ericsson estimates that between 2015 and 2021, the number of IoT-connected devices will grow by 23% each year.[3]

"Smart" devices will have profound impacts on our daily lives, with medical devices identifying diseases earlier and enhancing patient treatment, sensors improving efficiencies in farming and agriculture, controls monitoring and conserving energy use, and consumer devices simplifying everything from seamless global communications to residential security and entertainment.

But this explosion of connected devices comes with security implications. Unsecured devices can become infected with malicious code and be redirected without the knowledge of end users. This type of infected network, called a "botnet," can be used to launch distributed denial-of-service (DDoS) attacks, which can overwhelm networks and systems, causing them to fail.

In 2016, the largest DDoS attack to date, called the Mirai botnet, was launched against a major domain name system provider. This global botnet targeted the service provider, leading some of the most popular destinations on the Internet to go down. Other attacks target specific "devices" – such as connected vehicles and medical devices – and can result in a "hijacking" of the device, with the user or operator losing control of the device itself.

continued on page 3

Draft Legislation Aims to Tackle IoT Security

Some lawmakers feel the need to act. 2017 saw the introduction of a multitude of bills in Congress, aiming to enhance IoT security and end-user awareness.

For example, last October, the Cyber Shield Act of 2017 was introduced in the House and Senate.[4] The Act would direct the U.S. Department of Commerce to create a voluntary self-certification program that would independently identify, verify, and label compliant IoT devices with strong cybersecurity standards. Companies that meet the standards could display a compliance label on their products. The labels may be in the form of different "grades" that indicate the extent to which a product meets "industry-leading cybersecurity and data security benchmarks." The bill is discussed in more detail **here**.

Last summer, a group of U.S. Senators introduced the Internet of Things (IoT) Cybersecurity Improvement Act of 2017,[5] which would require companies selling connected products to the government to make commitments about security and expand device support. It would also create guidelines for each agency to impose vulnerability disclosure requirements. A description of the bill can be found **here**.

Another bill, the IoT Consumer TIPS Act,[6] would require the Federal Trade Commission (FTC) to develop guidance to help consumers improve their cybersecurity practices with respect to connected devices. It is discussed further **here**.

Additionally, the FTC has confirmed that it will be vigilant about IoT security and released **updated guidance** about compliance with the Children's Online Privacy Protection Act (COPPA),[7] confirming that COPPA **does apply** to IoT devices.

Calls for IoT "Standards" and Labeling Persist

Domestically and internationally, efforts are underway to establish minimum standards, certifications, or labeling schemes related to IoT security. Privacy and consumer advocates are developing proposals to reshape the certification and labeling of consumer devices.

In March 2017, *Consumer Reports* announced its "Digital Standard,"[8] "an ambitious ... effort to shape the digital marketplace in a way that puts consumers' data security and privacy needs first."[9] The Digital Standard was developed by privacy and consumer rights advocates "to encourage industry to design and produce safer products for consumers." It is far from perfect, however. It has prescriptive security requirements and seeks to alter private industry security designs, without first getting industry feedback in the Standard's development. In March 2018, a year after its initial release, groups associated with the Digital Standard announced they would be seeking feedback from companies and other stakeholders to encourage broader adoption.[10] Yet the prescriptive nature of this standard may limit its broad application.

Consumer labels and disclosures about security are complex and should be carefully studied. Nuanced and variable information about technology attributes, security choices, end-user behavior, updates, and third-party activity is not the sort of binary or objective data we are used to seeing on labels. Software lifecycle management is not like calorie information, and consumers may need more education about cyber hygiene than what fits on a label.

And the rest of the world is not sitting idly by.

continued on page 4

In September 2017, the European Commission (EC) introduced a "Cybersecurity Package," which includes a stringent certification scheme for connected devices.[11] In the "Cybersecurity Act," the EC would establish rules to create certification schemes for particular Internet-connected devices and services. Presently, European Union member states may have varying requirements, and this framework seeks to coalesce around a more uniform certification. Under the proposal, the certification schemes would be voluntary, "unless otherwise provided in Union legislation laying down security requirements [for] products and services."

Among other proposals in the EC Cyber Package, a joint Commission and industry initiative would seek to define a "duty of care" principle to help reduce the risk of product and software vulnerabilities and promote "security by design."

In 2016, the Government of Japan released a "General Framework for Secure IoT Systems,"[12] which "aims to clarify the fundamental and essential security requirements for secure IoT systems." Japan's efforts to build upon this General Framework, enhance security more generally, and collaborate internationally remain ongoing.

Diffuse efforts around the world introduce additional complexity into the marketplace, with the prospect of compliance with multiple standards and regulatory requirements. Governments should support international standards work that harmonizes varied approaches to regulating technology.

Core Principles for IoT Security Policy

Flexible approaches to collaboration on shared threats have significant advantages over national regulation or labeling schemes, which can fragment the global economy and limit technological innovation. Manufacturers and vendors of connected devices should be encouraged to routinely evaluate and improve endpoint security.[13]

Security should be risk-based. The consequences for compromised or failed devices vary significantly based on the environments in which they operate. A television at home may not need to meet the same rigorous standards of a system control regulating the flow of water or electricity. Risk models differ, and so too should approaches to diverse devices.

Approaches to IoT security should be data-driven, based on empirical evidence of a specific harm. Security policy should be adaptable both over time and across borders. This counsels against ossifying technical requirements in regulation or law. And any government IoT strategy should promote technical compatibility and interoperability, here and abroad.

This is an international threat that no one nation or actor can solve alone; the international community must collectively condemn criminal activities that exploit the openness and connectivity of the Internet. Governments must work together to shut down the criminal networks that threaten the resilience of the Internet and IoT ecosystem.

Finally, public education about the threats and best practices in this space is essential. Because unsecured devices can threaten the broader ecosystem, end users need to be educated about their roles and responsibilities.

Conclusion

With so many ongoing and overlapping efforts, there is a danger of premature, ill-considered, and conflicting requirements and obligations.

continued on page 5

Standardized requirements, certifications, and labeling schemes are not practical in an ecosystem of billions of devices, each with varying use-cases, risk profiles, and applications across industries. Indeed, labeling or security "ratings" can breed a false sense of security, contribute to over-warning, and generate needless consumer litigation.

Inflexible or prescriptive requirements, such as those proposed in the Digital Standard, do not serve to drive advancements related to security or innovation. The pace of change in technology is only mirrored, in some cases, by the threats and risks that develop. Security, as it relates to technology, is evolving constantly. For this vast ecosystem, in a rapidly developing and expanding marketplace, security must be risk-based and non-prescriptive. This will allow the many opportunities and benefits that IoT devices bring to our society to be felt across the globe. ■

This article was originally published in CircleID and can be found **here**.

For more information on these or other IoT issues, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Michael L. Diakiwski
202.719.4081
mdiakiwski@wileyrein.com

[1] Press Release, Gartner, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016* (Feb. 7, 2017), **https://www.gartner.com/newsroom/id/3598917**.

[2] i-SCOOP, *The Internet of Things (IoT) — essential IoT business guide*, **https://www.i-scoop.eu/internet-of-things-guide**.

[3] Ericsson, *Ericsson Mobility Report – On the Pulse of the Networked Society*, at 3 (June 2016), **https://www.ericsson.com/assets/local/mobility-report/documents/2016/ericsson-mobility-report-june-2016.pdf**.

[4] S. 2020, 115th Cong. (2017), **https://www.congress.gov/115/bills/s2020/BILLS-115s2020is.pdf**. H.R. 4163, 115th Cong. (2017), **https://www.congress.gov/115/bills/hr4163/BILLS-115hr4163ih.pdf**.

[5] S. 1691, 115th Cong. (2017), **https://www.congress.gov/115/bills/s1691/BILLS-115s1691is.pdf**.

[6] S. 2234, 115th Cong. (2017), **https://www.congress.gov/115/bills/s2234/BILLS-115s2234is.pdf**.

[7] FTC, Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business (June 2017), **https://www.ftc.gov/tips-advice/business-center/guidance/...**.

[8] The Digital Standard, **https://www.thedigitalstandard.org/the-standard**.

[9] Consumer Reports, *Consumer Reports Launches Digital Standard to Safeguard Consumers' Security and Privacy in Complex Marketplace* (Mar. 6, 2017), **https://www.consumerreports.org/media-room/press-releases/2017/03/...**.

[10] Inside Cyber, *Advocates seek input on 'Digital Standard' for IoT devices* (Mar. 16, 2018).

[11] European Commission, *Cybersecurity Act*, COM (2017)477 (proposed Sept. 13, 2017), **https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en**.

[12] National Center of Incident Readiness and Strategy for Cybersecurity, General Framework for Secure IoT Systems (Aug. 26, 2016), **https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf**.

[13] For more principles and a broader discussion, see Principles for IoT Security, United States Chamber of Commerce, available at **https://www.uschamber.com/IoT-security**.

> "A provider of electronic communication service or remote computing service shall comply with the obligations of this chapter to *preserve, backup, or disclose the contents of a wire or electronic communication* and any record or other information pertaining to a customer or subscriber within such provider's *possession, custody, or control*, regardless of whether such communication, record, or other information is located within or outside of the United States." (Emphasis added.)

The Act also gives providers the right to apply for a motion to quash or modify legal process if the provider reasonably believes the subscriber is not a U.S. person and that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government. It also requires a court to conduct a comity analysis in the event of a motion to quash.

Modified Procedures for Handling Foreign Law Enforcement Requests

Congress recognized that communications-service providers sometimes face conflicting legal obligations when a foreign government orders production of electronic data that United States law may prohibit providers from disclosing. To address these conflicts, the CLOUD Act creates a mechanism whereby Congress, working with the U.S. Departments of Justice and State, can enter into an "Executive Agreement" with approved foreign governments. Under the Act, communications service providers are permitted to respond to certain requests from foreign governments that are covered by an Executive Agreement.

Executive Agreements will only be approved "if the Attorney General, with the concurrence of the Secretary of State," determines that:

- The country has "robust substantive and procedural protections for privacy and civil liberties in light of the data collection and activities of the foreign government that will be subject to the agreement" (to be determined by reference to a comprehensive list of human rights and rule of law standards);
- The foreign government has adopted minimization procedures regarding information concerning U.S. persons; and
- The agreement has protections to prevent the foreign government from targeting or collecting information about U.S. persons or persons located in the U.S., and to prevent the U.S. government from requesting the foreign government to use the agreement as a runaround on current restrictions on data collection.

Orders issued under the agreements must relate only to serious crimes and meet a number of other requirements. For example, Orders must provide a "reasonable justification based on articulable and credible facts, particularity, legality, and severity regarding the conduct under investigation"; be "subject to review or oversight by a court, judge, magistrate or other independent authority"; and cannot be used "to infringe freedom of speech," among other limitations.

United States v. Microsoft Corp.

The Act clarifies issues that have led to years of litigation, most notably the recent dispute between U.S. law enforcement and Microsoft. In October 2017, the Supreme Court of the United States granted certiorari in *United States v. Microsoft Corp.* to address whether an email service provider must comply with a warrant supported by probable cause under the SCA when the email records are

continued on page 7

CLOUD Act Passes in Omnibus Spending Bill, Impacting User Data Stored Overseas *continued from page 6*

stored outside of the United States. The SCA authorizes the government to obtain email records when it has a warrant supported by probable cause to believe a crime is being committed.

In *Microsoft*, a federal judge issued a warrant, which was served on Microsoft at its headquarters in Redmond, Washington. The warrant required Microsoft to disclose information about an email account that the government believed was being used for drug trafficking. Microsoft refused to comply, arguing that the SCA did not apply because the emails were stored in Ireland. The trial court disagreed with Microsoft, but the U.S. Court of Appeals for the Second Circuit reversed and refused to enforce the warrant because of what it found to be an extraterritorial effect. The Supreme Court heard argument in February, and the case is now pending.

Passage of the CLOUD Act is likely to moot the case, and Microsoft supports the Act. The Court took up the case to determine whether the SCA was intended to cover data controlled by U.S. companies but held overseas. The CLOUD Act amends the SCA to require production of user data overseas, likely resolving that question. ■

For more information, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Matthew J. Gardner
202.719.4108
mgardner@wileyrein.com

Shawn M. Donovan
202.719.7293
sdonovan@wileyrein.com

HHS Office for Civil Rights Director Roger Severino Leads Discussion on Health Care Regulation and Cybersecurity

On March 28, Wiley Rein hosted a roundtable, "Outlook on Cyber: Health Care Regulation and Cybersecurity," featuring Roger Severino, Director of the U.S. Department of Health & Human Services (HHS) Office for Civil Rights (OCR), along with Timothy Noonan, Acting Deputy Director for Health Privacy at OCR, and Kathryn Marchesini, Chief Privacy Officer at the Office of the National Coordinator for Health Information Technology.

The discussion was moderated by Megan Brown, a partner in Wiley Rein's **Telecom, Media & Technology** and **Privacy & Cybersecurity** practices. It was designed to encourage government officials and health care professionals to share ideas and collaborate on cybersecurity and privacy challenges. The government guests highlighted future regulatory action and public engagement.

During the event, panelists touched on a variety of topics, including the types of enforcement cases OCR is most likely to pursue; interoperability challenges; initiatives to remove the government as a barrier between physicians and patients; efforts to clarify and reform the Health Insurance

continued on page 8

HHS Office for Civil Rights Director Roger Severino Leads Discussion on Health Care Regulation and Cybersecurity *continued from page 7*

Portability and Accountability Act (HIPAA) in light of the opioid crisis and recent school violence; use of open application program interfaces for app developers; and potential compensation for victims of data breaches. Participants touched on the importance of remembering that companies suffering a data breach are themselves victims of crimes, as the FBI Director recently noted. Given the cyber challenges facing the private sector, partnership and collaboration are vital.

To keep up-to-date with the latest cybersecurity tips and threats, the panelists recommended subscribing to the **OCR Cyber Newsletter**, and advised attendees to consult the Cyber-Attack Quick Response **infographic** for a succinct overview of responding to and reporting cyber-related security incidents. The National Institute of Standards and Technology (NIST) has resources available as well. Additionally, the panelists encouraged application developers to visit OCR's health app developer **portal**, which allows developers to engage with OCR on privacy and security issues in mHealth design and development.

Wiley Rein's multidisciplinary privacy and cybersecurity practice addresses a wide range of sectors and areas, including telecommunications, technology innovators, government contractors, mobile health (mHealth) applications, and health data security. ■

For more information on these issues, please contact:

Megan L. Brown
202.719.7579
mbrown@wileyrein.com

Kirk J. Nahra
202.719.7335
knahra@wileyrein.com

Events & Speeches

Lawyering in Tech | A Discussion with Women General Counsels

Megan L. Brown, Moderator

Women's High-Tech Coalition & Wiley Rein

April 17, 2018 | San Francisco, CA

Wiley Rein Reception with HackerOne

RSA Conference

April 18, 2018 | San Francisco, CA

Cyber Defense of American Companies: Can "Operational" Partnerships Work?

Megan L. Brown, Speaker

RSA Conference

April 18, 2018 | San Francisco, CA

"The Exchange" Data Privacy and Cybersecurity Forum

Matthew J. Gardner, Co-Chair

Today's General Counsel Institute

April 24, 2018 | Boston, MA

Events & Speeches (cont'd)

Identifying, Understanding and Limiting Your Legal Vulnerabilities

Edward R. Brown, Speaker

Cyber Sector Risk Critical Infrastructure

April 25, 2018 | New York, NY

The Urgency of Cyber Threats to U.S. & Global Critical Infrastructures

Megan L. Brown, Speaker

Cyber Sector Risk Critical Infrastructure

April 25, 2018 | New York, NY

Privacy and Security Enforcement Highlights

Kirk J. Nahra, Speaker

Blue Cross Blue Shield Association National Summit

May 1-3, 2018 | Orlando, FL

Top Ten Privacy and Security Developments for the Health Care Industry

Kirk J. Nahra, Speaker

BCBSA National Summit

May 1-3, 2018 | Orlando, FL

Managing Your Big Data

Kirk J. Nahra, Speaker

BCBSA National Summit

May 3, 2018 | Orlando, FL

Securing the Insecure: Cybersecurity in a Connected World

Megan L. Brown, Speaker

Third Internet of Things (IoT) National Institute

May 9, 2018 | Washington, DC

Plenary Session 1: Success Stories in International Coordination – IoT

Megan L. Brown, Speaker

6th Annual Conference on Governance of Emerging Technologies and Science: Law, Policy and Ethics

May 16, 2018 | Washington, DC

Ready or Not, GDPR is Here. Kirk J. Nahra, Speaker

Bloomberg Law Leadership Forum **May 23, 2018 | New York, NY**

Privacy Bootcamp

Kirk J. Nahra, Speaker

IAPP Privacy. Security. Risk. 2018

October 17, 2018 | Austin, TX

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

Kirk J. Nahra, Moderator

IAPP Privacy. Security. Risk. 2018

October 18-19, 2018 | Austin, TX

Wiley Rein Welcomes Back Former FEC Chairman

Wiley Rein LLP welcomes **Lee E. Goodman**, former Chairman and Commissioner of the Federal Election Commission (FEC), back to the firm as a partner in our renowned **Election Law & Government Ethics Practice**. Nationally recognized for his experience in close elections, recounts, and election administration, Mr. Goodman rejoined the firm in February and advises clients on laws regarding political activities and free speech.

Mr. Goodman was presidentially appointed to the FEC on October 21, 2013, after the U.S. Senate confirmed his nomination by unanimous consent. He served as Chairman of the FEC in 2014 and Vice Chairman in 2013. During his years on the Commission, Mr. Goodman promoted free speech on the Internet; vigorous free press rights, including for new media; and practical deregulation of political parties.

Prior to joining the FEC, Mr. Goodman was in private practice, including two stints at Wiley Rein. He advised several presidential campaigns, and served as general counsel of the Republican Party of Virginia from 2009 to 2013. His prior government service includes four years as legal counsel and policy advisor to the Governor of Virginia, and three years as counsel and special assistant to the Attorney General of Virginia. He also served as chief advisor to the Chairman of the Congressional Advisory Commission on Electronic Commerce.

Mr. Goodman has authored several articles on election law, including a chapter on regulation of political speech on the Internet in the book *Law and Election Politics – The Rules of the Game*, and frequently lectures on election law topics. He has served on the boards of several political, educational, and cultural nonprofit organizations. He received his B.A., with highest distinction, from the University of Virginia, and his J.D. from the University of Virginia School of Law, where he served as articles editor for the *Journal of Law & Politics*.

Contributing Authors

Megan L. Brown	202.719.7579	mbrown@wileyrein.com
Michael L. Diakiwski	202.719.4081	mdiakiwski@wileyrein.com
Shawn M. Donovan	202.719.7293	sdonovan@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