# The internet of things: Attempts to regulate the vast and unknown

**By Michelle L. Dama, Esq., and Adrienne S. Ehrhardt, Esq.**
***Michael Best & Friedrich***

Put simply, the "internet of things," or IoT, is a network of internet-connected objects able to collect and exchange data using embedded sensors.

The IoT can be seen all around us: in connected cars, smart homes, smart appliances, healthcare devices, supply chains and logistics, and smart manufacturing, just to name a few.

And the future of the IoT is only growing. Some estimate that the number of IoT devices is expected to reach 50 billion by 2020.[1]

The benefits of these innovations are self-evident (Who doesn't want their car to slow down or stop to prevent an accident or drive them to their destination?), but the data these devices collect also create new risks.

Put simply, the "internet of things," or IoT, is a network of internet-connected objects able to collect and exchange data using embedded sensors.

Change in this area is occurring at an exponential rate. And technological change, by its very nature, causes uncertainty — including legal uncertainty.

Consumers, developers, manufacturers and innovators of IoT products or applications ask the same set of questions: Are the products and applications useful? Do they work? Can I trust them?

For consumers, trust can be the delineating factor. And WikiLeaks' recent release of Vault 7 — documents that allegedly came from the CIA — has reinvigorated an important question: How vulnerable am I?

The Vault 7 documents demonstrated how, by using IoT technology, hackers can target, infect, extract and control a variety of devices and their data, including smartphones, smart TVs and even cars.[2]

According to the WikiLeaks report, the CIA exploited Samsung's smart TV functions to place "the target TV in a 'Fake-Off' mode, so that the owner falsely believes the TV is off when it is on. In 'Fake-Off' mode the TV operates as a bug, recording conversations in the room and sending them over the internet to a covert CIA server."

The CIA apparently also pursued the ability to infect vehicle control systems found in cars and trucks.

**Michelle L. Dama** (L), a partner with **Michael Best & Friedrich** in Madison, Wisconsin, focuses her practice on litigating commercial and intellectual property disputes, including issues concerning privacy and data security. She can be reached at mldama@michaelbest.com. **Adrienne S. Ehrhardt** (R), who is also a partner in the firm's Madison office, focuses her practice on complex aspects of privacy and data management matters. She can be reached at asehrhardt@michaelbest.com.

Despite these revelations, the challenge with any of the legal issues surrounding IoT is to keep consumer data private and secure without stifling innovation.

## REGULATORY ENVIRONMENT IS POTENTIAL MIXED BAG

No current regulations specifically address the IoT.

Rather, a patchwork of existing laws and regulations cover issues that arise.

This framework is complicated by the fact that government regulatory agencies largely operate in silos.

The Federal Trade Commission protects consumers; the U.S. Food and Drug Administration regulates medical devices; and the Federal Communications Commission regulates interstate radio, wire, satellite and cable communications.

Comparatively, IoT devices and products are a system of integrated objects and networks that span a variety of industries. As a result, they do not neatly fall under one agency for regulation.

Moreover, the pace of innovation in the IoT ecosystem, with new products coming out daily, is much faster than the pace of notice-and-comment rulemaking from agencies.

Congress is making attempts to add structure and clarity to the regulatory environment via legislation addressing the IoT.

But the bills are vague in their directive, reflecting the amorphous nature of what they are attempting to regulate.

In April 2016 a House committee introduced a bill titled Developing Innovation and Growing the Internet of Things Act, or the DIGIT Act, which required the Department of Commerce to create a working group of federal stakeholders to provide a report and recommendation regarding the IoT.[3]

According to the bill, the working group must:

- Identify federal laws and regulations, grant practices, budgetary or jurisdictional challenges and other sector-specific policies that inhibit IoT development.
- Consider policies or programs that encourage and improve coordination among federal agencies with IoT jurisdiction.
- Implement recommendations from the steering committee.
- Examine how federal agencies can benefit from, use, and prepare for the IoT.

The exploratory nature of the directive illustrates how far away Congress is from implementing IoT regulations.

Congress knows that regulation may hinder innovation. It cautioned in the DIGIT Act that "IoT policies should maximize the potential and development of the IoT to benefit all stakeholders, including businesses, governments, and consumers."

The only apparent progress on the DIGIT Act seems to be in the Senate, which introduced the same bill in January.[4]

On March 2 another IoT bill, the Securing the Internet of Things Act of 2017, was introduced in the House. That bill tasks the FCC to work with the National Institute of Standards and Technology to develop standards for radio frequency device certification that "address cybersecurity throughout the lifecycle of the equipment, including design, installation, and retirement."[5]

While more specific in naming an agency and creating a partnership with the NIST, the potential regulations that could stem from this bill, and the range of products and technology it could affect, is relatively open-ended.

Rather than giving individual agencies jurisdiction over IoT devices, some experts surmise that IoT laws may largely take an industry-specific approach, but be overseen by a variety of agencies.

Some have loosely compared the IoT to the airline industry — the Federal Aviation Administration handles flight safety, the Transportation Security Administration screens passengers and the National Transportation Safety Board investigates accidents — a patchwork of policies that all center around a single industry.

However, this approach may lead to inconsistent standards. Additionally, with this approach no one agency develops expertise.

## CHILD'S TOY SHOWS SECURITY CONCERNS

An example of the ad hoc approach to regulating new technologies that create potential unintended security issues can be seen in the action the FTC took with respect to two children's toys.

In December 2016 the Electronic Privacy Information Center and other consumer protection and children's privacy groups filed a complaint with the FTC against Genesis Toys and Nuance Communications Inc. related to their interactive, internet-connected toys.[6]

Genesis manufactures and sells the My Friend Cayla doll and i-Que Intelligent Robot. Both toys contain a Bluetooth microphone and speaker that enable connection to the internet via a downloadable mobile application.

Once these toys are connected, children can talk and interact with them using software provider Nuance's voice technology. The technology converts kids' spoken words into text and allows the toy to respond after searching online for appropriate responses.

EPIC's complaint alleges that the toys record children's communications and upload the sound recordings to Nuance's cloud-based servers, in violation of the Children's Online Privacy Protection Act. That law restricts the collection of personal data about children.

The complaint also invokes the FTC's Section 5 authority to regulate unfair and deceptive acts and practices.

The purpose of collecting these recordings, according to Genesis Toys' terms of service, is to "enhance and improve the services for the toys and for other services and products."

However, it has been alleged that Nuance's clients include military and intelligence firms and that the dolls amount to childhood surveillance.

Of particular note is the fact that Germany banned the toys as an espionage device.[7] According to German officials, the dolls are prime targets for hackers, who can use the toy's technology to watch kids and spy on families.

The FTC complaint illustrates the piecemeal and reactive approach that currently exists in the U.S. to address IoT legal issues. U.S. laws of general application can and are being adapted to regulate IoT.

## WHAT ARE POTENTIAL GUIDEPOSTS?

Given this uncertainty in regulation, how can IoT businesses manage legal risks?

Although not specifically for IoT, the following guidelines and regulations already touch on IoT issues: Fair Information Practice Principles, privacy by design, the Children's Online Privacy Protection Act, the NIST Cybersecurity Framework, and the General Data Protection Regulation, or GDPR, for European citizens.

> The challenge with any of the legal issues surrounding IoT is to keep consumer data private and secure without stifling innovation.

### *Fair Information Practice Principles*

The FTC has developed guidelines that represent accepted principles for the collection, use, transfer and protection of personally identifiable information. The core principles are:

- Transparency.
- Individual participation.
- Purpose specification or articulating the purpose for which the information is intended to be used.
- Data minimization or only collecting data necessary to accomplish specified purpose.
- Use limitation.
- Data quality or ensuring that information is accurate and timely.
- Security or using appropriate safeguards against loss or unauthorized use.
- Accountability.

### *Privacy by design*

Privacy by design is an approach to building privacy within systems and products. The seven fundamental principles of privacy by design are:

- Taking a proactive or preventative approach, not a reactive or remedial approach — think about data privacy at the beginning of the process, not after a breach.
- Make privacy the default setting — giving consumers the maximum privacy protection as a baseline.
- Embed privacy into the design of the system and test for vulnerabilities.
- Make privacy a positive-sum game rather than a zero-sum game, meaning privacy need not be a tradeoff to revenue and growth.
- Full lifecycle protection — end-to-end security that should follow data wherever it goes.
- Visibility and transparency — information about your privacy policies should be readily available to build trust with customers.
- Respect user privacy — consumers own their data and are the only ones who can grant and revoke consent.

### *Children's Online Privacy Protection Act*

COPPA imposes restrictions on operators of online services directed to children under 13 and on operators of general audience online services that have actual knowledge that they are collecting personal information online from a child 13 or younger.

The term "online service" broadly covers any service that is available over the internet or connects to the internet or other type of computer network. The law gives parents control over what information websites can collect from their children.

### *NIST cybersecurity framework*

The National Institute of Standards and Technology, or NIST, established a framework for managing cybersecurity risk. It provides a flexible and scalable framework that is technology neutral and can accommodate global cybersecurity standards for evaluating cybersecurity risk.

### *General Data Protection Regulation*

The EU Parliament adopted the General Data Protection Regulation in April 2016 as the EU's omnibus data protection law.

For companies or entities that seek to collect and process personal data, the GDPR requires consumers to give their consent with a clear, affirmative act that indicates specific and informed permission.

It also requires that consent be as easy to withdraw as it is to give, and it has additional requirements for notifying consumers about data breaches.

The GDPR has expanded territorial reach and applies to data controllers or processors located outside of the EU if their activities relate to the offering or goods or services to, or monitoring the behavior of, EU data subjects.

It has a two-year transition period and will not directly apply until May 25, 2018.

## THE WORLDVIEW OF REGULATING IOT

The IoT presents a common challenge in other parts of the world.

In 2016 the Global Privacy Enforcement Network conducted a study on the IoT. Twenty-five data protection regulators from around the world reviewed over 300 IoT devices, ranging from smart electricity meters to health monitoring devices.[8] The results showed in these international jurisdictions:

- 59 percent of devices failed to adequately explain to customers how their personal information was collected, used and disclosed.
- 68 percent failed to properly explain how information was stored.
- 72 percent failed to explain how customers could delete their information off the device.
- 38 percent failed to include easily identifiable contact details if customers had privacy concerns.

This study highlights the issues created by IoT devices globally.

Moreover, the increasing interconnectedness of the world along with IoT devices will create additional complications.

Canada's privacy commissioner has voiced his support for a global approach to addressing these issues, saying the study showed the commitment of privacy regulators to work together.

Similarly, the head of the United Kingdom Information Commissioner's Office, Steve Eckersley, has suggested an international approach to enforcement.

"By looking at this internationally, we've been able to get an excellent overview on this topic," he said. "We'll now be building on that, working with the industry and looking specifically at companies who might not have done enough to comply with the law."[9] WJ

> IoT devices and products are a system of integrated objects and networks that span a variety of industries. As a result, they do not neatly fall under one agency for regulation.

## NOTES

[1] Dave Evans, The Internet of Things: How the Next Evolution of the Internet is Changing Everything (2011), http://bit.ly/1LgfMSb.

[2] Press Release, Wikileaks, Vault 7: CIA Hacking Tools Revealed (Mar. 7, 2017), http://bit.ly/2nal1ld.

[3] H.R. 5117, 114th Cong. § 2(b) (2016), http://bit.ly/2okdMPK.

[4] S. 88, 115th Cong. (2017), 2017 CONG US S 88 (Westlaw).

[5] H.R. 1324, 115th Cong. (2017), 2017 CONG US HR 1324 (Westlaw).

[6] Complaint, *In re Genesis Toys & Nuance Commc'ns* (F.T.C. Dec. 6, 2016), http://bit.ly/2gNpdOb.

[7] Amanda Erickson, *This Pretty Blond Doll Could Be Spying on Your Family,* Wash. Post, Feb. 23, 2017, http://wapo.st/2okpk5D.

[8] Michael Maguire, *2016 GPEN Privacy Sweep, Internet of Things: Participating Authorities' Press Releases,* Global Privacy Enforcement Network (Sept. 28, 2016, 2:30 PM), http://bit.ly/2nywp5w.

[9] Press Release, Office of the Privacy Comm'r of Canada, Global Internet of Things Sweep finds connected devices fall short on privacy (Sept. 22, 2016), http://bit.ly/2ojROOE; Press Release, Information Comm'r's Office, Privacy regulators study finds Internet of Things shortfalls (Sept. 22, 2016), http://bit.ly/2cW9tq7.