The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2018
PHILADELPHIA, TUESDAY, JULY 24, 2018 VOL 258 • NO. 16 An ALM Publication

CYBERSECURITY

The Internet of Things: Are Government Regulation Efforts Too Little, Too Late?

BY GWENN B. BARNEY
Special to the Legal

Almost 20 years have passed since technology pioneer Kevin Ashton first coined the phrase Internet of Things (IoT) in a 1999 presentation for Procter & Gamble (Kevin Ashton, *Beginning the Internet of Things*, Medium (March 18, 2016). The Internet of Things consists of physical items that collect information through sensors or chips and then share that information with other devices through the Internet or other networks. Since the introduction of the term, the growing network of these connected devices (expected to reach 30 billion devices by 2020) (Internet of Things (IoT) connected devices installed base worldwide from 2015-2025, Statista, (last accessed May 28) has created tremendous possibilities. Today, we have phones that provide limitless information at our fingertips, health care devices that can instantly share a patient's vital statistics to save precious response time, and we are on the cusp of self-driving cars that promise mitigation, if not elimination, of human driving error. Yet, each device added to the internet creates opportunity for a malicious attack or hacking.

The state of IoT regulation is patchwork at best. Although most applicable federal regulations are enforced by the Federal Trade Commission (FTC), there are no comprehensive regulations or laws for IoT devices. The lack of clear and unambiguous standards to govern IoT security leaves IoT innovators wrestling to identify what standards should be achieved. This, in turn, can lead to security shortfalls. Congress is considering three pieces of legislation to help solve this dilemma. However, as discussed below, while each bill addresses some problems, none resolves all of the issues.

GWENN B. BARNEY *is an associate at White and Williams where she practices in the areas of cyber, general corporate, transactional and securities law. Contact her at barneyg@whiteandwilliams.com and 215-864-7063.*

> *"Some believe that time is of the essence to ensure that security measures are put in place for the IoT.*

THE PENDING LEGISLATION

Two of the three pending bills propose voluntary regulatory programs. The Cyber Shield Act of 2017 (S. 2020, 115 Cong. (2017)) proposes a voluntary program where manufacturers of IoT devices adhere to certain IoT security protocols and in return are given government certification that their devices are secure. This bill would task the secretary of commerce to create an advisory committee to administer the program comprised of covered products industry representatives, cybersecurity experts, public interest advocates, and federal employees with expertise in certification, covered devices or cybersecurity. The certification is expected to manifest as a sticker that manufacturers can place on their device.

Another bill, the Internet of Medical Things Resilience Partnership Act of 2017 (the Medical Things Act) (H.R. 3985, 115 Cong. (2017)), would establish "a working group of public and private entities led by the Food and Drug Administration to recommend voluntary frameworks and guidelines to increase the security and resilience of Internet of Medical Things devices."

The voluntary nature of the Cyber Shield Act and the Medical Things Act helps assuage concerns held by opponents of government IoT regulation that Congress intends to over-regulate the IoT and consequently stunt its development. The idea is that companies will participate in a voluntary program because of the consumer goodwill generated by the Cyber Shield certification or compliance with the Internet of Medical Things Act. Still, some

may question the influence of a voluntary regulatory regime, putting its effectiveness in limbo. However, voluntary consensus standards are used to fill the gap of government regulation in other areas.

Both the Cyber Shield Act and Medical Things Act would bring together government agencies for the purpose of creating a comprehensive and cohesive regulatory plan for IoT device oversight. The Cyber Shield Act requires the Secretary of Commerce to consult with the Secretary of Health and Human Services, the Commissioner of Food and Drugs, the Secretary of Homeland Security and other federal agencies to carry out the program. Similarly, the Medical Things Act calls for collaboration among the Food and Drug Administration, Department of Health and Human Services, the Federal Trade Commission, the Federal Communications Commission, and the Department of Commerce. Personnel from each would serve on the committee that will create medical device standards. This multi-agency involvement would help to create uniformity and consistency in expectations for IoT cybersecurity.

Where the Cyber Shield Act and Medical Things Act fall short is in their failure to offer concrete and well thought out suggestions of specific cybersecurity mechanisms which manufacturers ought to apply. While it is necessary to bring agencies together to collaborate and agree on which standards will apply to devices across industries, experts in the field have a basic understanding of the mechanisms that will be necessary to ensure security. The third bill, the Cybersecurity Improvement Act of 2017 (S.1691, 115 Cong. (2017)), would be extremely helpful in moving the ball forward in this regulatory area, as it is the only one of the three proposed laws that presents actual solutions in the body of the law.

The Cybersecurity Improvement Act would require a vendor of IoT devices meet certain criteria before a U.S. government agency can purchase the device. The legislation requires that the IoT devices are patchable, do not contain known vulnerabilities (if the vendor does identify vulnerability, the government can issue a waiver and purchase the device if the vendor sufficiently explains why the device is secure and presents any controls that can limit the exploitation or impact of the vulnerability), rely on standard protocols, and do not contain hard-coded passwords. Agencies may ask the Office of Management and Budget (OMB), which will monitor the program, for permission to purchase devices that do not meet these standards if they can demonstrate that certain compensating controls have been employed. Agencies can employ their own equivalent, or more rigorous, device security requirements or industry can develop third-party device certification standards that provide equivalent, or more rigorous, device security requirements (as determined by NIST).

The Cybersecurity Improvement Act, though, is limited to only those companies which contract with the government. This is a narrowly cast net and still would leave most of the IoT devices distributed in the United States on a path of insufficient security and excessive vulnerability to hacking.

Another potential pitfall for the regulation of IoT is that mandatory requirements for devices will lead to the forced exodus of small manufacturers from the market as they will not have the resources to meet the required standards. All three acts introduced provide a level of flexibility to protect the interests of businesses with fewer resources than larger manufacturers. The Cyber Shield Act and Medical Things Act provide this flexibility through their voluntary nature. The Cybersecurity Improvement Act works around this dilemma by allowing the OMB to make exceptions for products that may not meet the set standards, if the agency purchasing the device can demonstrate that certain compensating controls have been employed. If the OMB creates a sufficient review process to determine what qualifies as a compensating control, this flexibility will allow for smaller manufacturers to remain suppliers to government, while also encouraging them to strive for a higher standard of cybersecurity. However, if the OMB's review process is too lax, it could be a gaping hole preventing the law from achieving its stated purpose.

The Cyber Shield Act and Cybersecurity Improvement Act prevent against obsolescence of their standards by providing for ongoing review and adjustment of any adopted standards or regulations as the IoT evolves. Under the Cybersecurity Improvement Act, OMB will submit a report to Congress within five years on the effectiveness of guidelines and any recommendations for updates. Meanwhile, under the Cyber Shield Act, every two years the Secretary of Commerce, in consultation with the Cyber Shield advisory committee, will review the cybersecurity and data security benchmarks produced under the proposed Act, and make adjustments as necessary. The proposed laws could improve if they provided an opportunity for review every year as the IoT technological landscape shifts at light speed. While two years seems a reasonable amount of time for review, five years may be too long a wait for this fast-paced arena. Additionally, the Medical Things Act, which does not include a similar review mechanism, would benefit from adding one.

Currently, all three proposed laws are tied up in committee review and show no signs of progressing forward. However, some believe that time is of the essence to ensure that security measures are put in place for the IoT. In a 2014 draft report, the National Security Telecommunications Advisory Committee wrote that the world had "only three years—and certainly no more than five—to influence how IoT is adopted … in a way that maximizes security and minimizes risk. If the country fails to do so, it will be coping with the consequences for generations," see The President's National Security Telecommunications Advisory Committee, NSTAC Report to the President on the Internet of Things 2, (2014). •