Bloomberg Law

Privacy Law Watch™

Internet of Things

Despite lax security on most internet of things web-connected devices, the government has failed to put in place a general cybersecurity standard, so companies seeking to get ahead of the curve on IoT security need to pay attention to the Federal Trade Commission's enforcement actions and its guidance, the authors write, adding that companies also need to focus on securing the devices and the data transmitted to the various applications that rely on the device.

Mobile Devices

Internet of Things Security and the FTC—Current And Possible Future Requirements

By Bruce Heiman and Al Sisto

The Promise and Peril of IoT

Introduction

The internet of things (IoT) promises to unleash the information revolution on the broader economy. Electricity did not revolutionize manufacturing until factories were structurally redesigned to use electric motors, decades after electric motors were developed. Similarly, the true productive potential of the internet may only be realized when it works for *all* things, not just computers.

Bruce Heiman is a partner in the global law firm K&L Gates in Washington, where he co-chairs the policy and regulatory practice area.

Al Sisto is the executive chairman of device authority of Device Authority in London, a leading internet of things security company.

The IoT promises to connect everything and propel greater productivity gains on our economy. Estimates are that 50 billion devices will be connected by 2020—just 3 years away. The IoT promises to bring greater efficiencies, increased competitiveness, improved customer service, enhanced consumer convenience, and more effective products and services in the industrial, automotive, transportation, healthcare, utilities, and other sectors.

Unfortunately, the widespread development and use of IoT devices also threatens to unleash wholesale Internet havoc because today those devices are manufactured and enabled without adequate cybersecurity protection. Today, there is no IoT specific cybersecurity statute or regulation. The National Institute for Standards and Technology (NIST) has only begun to extend its framework of best practices to the IoT.

In the meantime, the U.S. Federal Trade Commission (FTC) has issued guidance and used its general authority to prevent unfair or deceptive acts or practices by bringing three enforcement actions against companies offering IoT products with poor cybersecurity. But those cases have all involved deceptive claims about a product's cybersecurity. The question is whether the FTC will follow what it has done with respect to Inter-

net security generally and take action in a case to find that an IoT company's cybersecurity practices are per se inadequate and inherently unfair even if the company makes no claims about the product's security. This would establish baseline security requirements.

Yet even such a ''straight line'' extension of the Commission's cybersecurity thinking to the world of IoT may not be sufficient. A new way of thinking about IoT security appears to be needed, one that does not rely on users and goes beyond username/passwords.

The Problem With IoT: Lack of Security Pervasive and continuous (always on) connections to home and business networks and the internet present significant security challenges. The majority of the devices that have been hooked up to the internet in the past few years are connected with little concern for security. They are generally composed of inexpensive parts and rely on weak password protection, for example. It is now obvious that such weakness can be exploited not only by nation-state actors, but also by criminal groups or even teenagers.

The distributed denial-of-service (DDOS) attack earlier this year highlighted the IoT security problem. The botnet attack on Dyn Inc. was made up of devices like home wi-fi routers (gateways) and Internet Protocol video cameras (sensors) that sent massive numbers of requests to Dyn's Domain Name Service (DNS). The attack was sophisticate and yet simple to achieve. Routers, and hundreds of thousands (maybe millions) of the security cameras connected to them, were infected with a fairly simple program that guessed at their factory-set passwords, often ''admin'' or ''12345'' or even ''password.'' Once infected, they were turned into an army of simple robots. Each one was commanded, at a coordinated times, to bombard Dyn—a small company in Manchester, New Hampshire that provides DNS resolution for a wide range of major websites—with messages that overloaded its circuits. The results of this attack were the unavailability of many e-commerce sites and loss of retail revenue.

These same concerns also exist in the world of IoT for medical devices, industrial controls and autonomous vehicles, among others. Without strong security, they could be compromised and similarly turned into ''bots.'' Importantly, without strong security these IoT devices could be compromised causing loss of life or property and not simply inconvenience.

The FTC Has Set General 'De Facto' Cybersecurity Standards In the absence of a generally applicable federal cybersecurity standard, the FTC has acted under its general statutory authority under Section 5(a) of the FTC Act to address ''unfair or deceptive acts or practices in or affecting commerce.'' Section 5(n) provides that an act or practice may be deemed unfair if it ''causes or is likely to cause substantial injury to consumers'' which is neither reasonably avoidable by consumers nor outweighed by countervailing benefits to consumers.

The FTC currently does not have specific authority to promulgate cybersecurity regulations (even if it might have general authority to issue rules under the FTC Act). Instead, the FTC has de facto established cybersecurity standards by bringing dozens of enforcement actions.

The FTC began addressing cybersecurity in 2000 by taking action against companies that claimed that they took various measures to protect information, but in practice, failed to do so. The FTC alleged in six cases from 2000 to 2005 that the company had engaged in deceptive acts, essentially by misrepresenting to consumers the nature of the company's cybersecurity/privacy protections. Each time, the FTC and the company agreed to settle the action under a consent decree running as long as 20 years. The company agreed not to claim it was doing more than it actually did and to adopt a cybersecurity program that was designed to establish and maintain reasonable and appropriate administrative, technical, and physical safeguards.

However, beginning in 2005 with the BJ's Wholesale Club Inc. case [*See In the Matter of BJ's Wholesale Club Inc.*, FTC No. 042-3160 (Sep. 20, 2005) (complaint)], the FTC began to bring actions against companies whose cybersecurity practices it deemed to be inherently ''unfair'' or unreasonable, independent of whether the company had made any claims about its security practices. In eight cases since the BJ's Wholesale Club case, the FTC has relied exclusively upon its ''unfairness'' authority to establish de facto cybersecurity standards for a broad swath of the U.S. economy (without also asserting a deception claim) [*See In re DSW, Inc.*, FTC No. 052-3096 (Mar. 7, 2006) (complaint); *In re CardSystems Solutions, Inc.*, FTC No. 052-3148 (Sep. 5 2006) (complaint); *In re TJX Companies, Inc.*, FTC No. 072-3055 (Jul. 29 2008) (complaint); *In re Reed Elsevier, Inc.*, FTC No. 0523094 (Jul. 29 2008) (complaint); *In re Dave & Buster's, Inc.*, FTC No. 082-3153 (May 20, 2010) (complaint); *In re EPN, Inc.*, FTC No. 112-3143 (Oct. 3, 2012) (complaint); *In re LabMD, Inc.*, FTC No. 102-3099 (Aug. 28, 2013) (complaint); *In re Accretive Health, Inc.*, FTC No. 122-3077 (Feb. 5, 2014) (complaint)].

These nine cases therefore appear to establish the minimum required by the FTC with respect to ''reasonable'' cybersecurity practices. The agency has required other measures of particular companies when they also claimed to protect particular information and failed to do so (hence, the FTC found them to be ''deceptive'' acts). It remains unclear whether the FTC would find the absence of such measures to be inherently unfair and unreasonable absent the claims.

The FTC Has Moved to Specifically Address IoT Cybersecurity Beginning in 2013 the FTC also has brought enforcement actions against companies offering IoT products. The three cases, however, all involved alleged deceptive claims of security. The remedies—security practices—required by the FTC are consistent and have been amplified by the commission's guidance and comments. But until the FTC moves against a company for inherently unfair practices—as it did in BJ's Wholesale Club—we will not know for sure the minimum baseline IoT security practices required by the FTC.

The FTC's Enforcement Actions **A. 2013/14—TRENDnet.**

The FTC filed a complaint in September 2013 against TRENDnet Inc., a manufacturer of cameras used for home security and baby monitoring, for mispresenting the safety of its devices and thereby engaging in unfair and deceptive security practices. The FTC found that, despite marketing its cameras as ''secure,'' the company actually failed to implement reasonable security measures for its cameras by transmitting and storing user login credentials in plain text and failing to test privacy settings to ensure that video feeds marked as ''pri-

  PRA ISSN 0000-0000

vate'' were actually private [*In re TRENDnet, Inc.*, FTC No. 122-3090 (decision and order)]. As a result, hackers were able to access live feeds from consumers' security cameras and then expose those feeds to public viewing.

In February 2014, TRENDnet agreed to a settlement with the FTC which required the company to establish a comprehensive information security program that addresses security risks that could lead to unauthorized access to or use of the cameras, and to protect the security and confidentiality of information that is stored on the cameras. As part of the security program, TRENDnet must designate an employee to coordinate and be accountable for the program, undergo a comprehensive assessment of risks to the security of the cameras and the information stored on the cameras, implement reasonable safeguards to control those risks identified, and regularly test and monitor the effectiveness of those safeguards. Additionally, TRENDnet must obtain independent third-party audits of its security program every two years.

The FTC specified, among other requirements, that:

■ at a minimum, the risk assessments required. . .should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management; (2) product design, development, and research; (3) secure software design, development, and testing; and (4) review, assessment, and response to third-part security vulnerability reports;

■ the design and implementation of reasonable safeguards to control the risks identified through the risk assessments, including but not limited to reasonable and appropriate software security testing techniques, such as: (1) vulnerability and penetration testing; (2) security architecture reviews; (3) code reviews; and (4) other reasonable and appropriate assessments, audits, reviews, or other tests to identify potential security failures and verify that access to Covered Information is restricted consistent with a user's security settings;

B. 2016—ASUSTek.

The FTC alleged that in July 2016, ASUSTeK Computer, Inc., a Taiwan-based hardware maker, had flaws in the company's routers that put consumers' home networks at risk. ASUSTek marketed its routers as including various security features and advertised that its routers could ''protect from any unauthorized access, hacking, and virus attacks.'' Additionally, the routers featured a ''cloud'' service that ASUSTek advertised as a ''private personal cloud for selective file sharing.'' The FTC charged that ASUSTek failed to take reasonable steps to secure the routers, which ultimately led to the compromise of consumers' connected storage devices and exposed sensitive personal information on the Internet.

Without agreeing to liability, ASUSTek agreed to a settlement with the FTC [*In re ASUSTek Computer, Inc.*, FTC No. 142-3156 (decision and order)]. Under the terms of the settlement, ASUSTek was required to establish and maintain a comprehensive security program subject to independent third-party audits. The terms of ASUSTek's settlement agreement were almost identical to that of TRENDnet. The security program implemented by ASUSTek must also designate an employee accountable for the program, identify risks to the security of the devices and the information stored on or transmitted through the devices, implement safeguards designed to protect against those risks, and regularly monitor the effectiveness of those safeguards. The FTC did, however, also require that the risk assessment include ''prevention, detection, and response to attacks, intrusions, or systems failures'' and also that safeguards applied to access to the device and not just access to the information.

C. 2017—D-Link

In January 2017, the FTC filed a complaint in the Northern District of California against D-Link Corporation, alleging that the company made deceptive claims about the security of its products and engaged in unfair practices that put consumers' privacy at risk [*FTC v. D-Link Corp.*, FTC No. 132-3157 (complaint)]. Specifically, the FTC charged that D-Link failed to take reasonable steps to secure its wireless routers and cameras, despite advertisements that the devices were ''easy to secure'' and contained ''advanced network security.'' Instead, the devices were left vulnerable to hackers, and consumers who used these compromised cameras put themselves at risk of theft or other crimes. For example, the FTC claimed that D-Link failed to protect its routers and cameras against well-known and easily preventable security flaws; they had ''hard-coded'' login credentials, which could allow unauthorized access to the cameras' live feed; and had ''command injection'' flaws, which could allow hackers to take control of consumers' devices and send them unauthorized commands. Additionally, the FTC charged that D-Link failed to maintain the confidentiality of its own private key code, which was used to sign into D-Link software. As a result, the private key code was left publicly available online for six months. Finally, the FTC alleged D-Link failed to secure users' login credentials for its mobile app, despite the availability of free software to ensure such security. Instead, D-Link stored these credentials in clear, readable text on the user's mobile device. D-Link has contested these charges and the case continues to be litigated.

FTC Guidance **A. 2015 Report**

In 2015, the FTC issued a report on the IoT that outlined a series of recommendations for best practices businesses to implement in order to enhance and protect consumers' privacy and security in the digital age. The recommendations seek to identify a threshold for reasonable security implementation and are consistent with the TRENDnet requirements.

Companies should build security into their devices at the outset, rather than as an afterthought in the design process. In doing so, companies should consider conducting a privacy or security risk assessment. As part of this they should use ''smart defaults'' that require consumers and applications to change default passwords (or not use default passwords at all) during the set-up process. Companies also should consider how to minimize the data they collect and retain, and should testing security measures before launching the products.

Importantly, companies also should implement reasonable access control measures to prevent unauthorized access to a device or network. As the FTC explains: ''In the IoT ecosystem, strong authentication could be used to permit or restrict IoT devices from interacting with other devices or systems. The privileges associated with the validated identity determine the permissible interactions between the IoT devices and could prevent unauthorized access and interactions.'' The FTC recommended as well that companies not rely solely on pass-

word protection but also reasonably secure data in transit and in storage through encryption or other means.

The FTC also recommends that companies train employees about the importance of security and best practices for addressing security issues. Additionally, companies must not only ensure that they retain service providers capable of maintaining reasonable security, but also provide oversight to ensure those service providers are exercising reasonable security practices [In re GMR Transcription Services, Inc., FTC No. 122-3095 (complaint) (FTC alleged company outsourced transcription services to independent typists in India without adequately checking to make sure they could implement reasonable security measures. The transcribed notes were stored in clear text on an unsecured server and available through basic Internet searches.)]. Companies also should inform consumers about the length of time they plan to support and release security updates and software patches.

B. 2017 Comments

Most recently, in June 2017, the FTC submitted public comments to the National Telecommunications and Information Administration (NTIA), which is developing guidance for manufacturers to better inform consumers about security updates related to their devices. The NTIA highlighted the ''key elements'' manufacturers should consider communicating to consumers prior to purchasing a device. The FTC recommended modifications to these elements, such as disclosing a minimum amount of time that consumers can expect security support for their device and whether a device will lose core device functions after security support ends. Importantly, the FTC noted that ''one straightforward way to reduce harm'' from poor or over consumer notice'' is to ''minimize the need for disclosures by providing secure products that receive automatic security updates during the device's reasonable lifespan [FTC, Public Comment,''Communicating IoT Device Security Update Capability to Improve Transparency for Consumers.''

For True IoT Security The FTC Will Need to Adopt a Different Approach The vast number of IoT devices means that continued reliance on username/password controls, already a weak link, will no longer suffice. Traditional cybersecurity has focused on network perimeter defense and detection and remediation. That does not work in a world of ubiquitous IoT devices that connect via the Internet and run thousands of applications and that operate on multiple networks simultaneously.

IoT security requires automatically and autonomously controlling from the very start *which devices* can connect, *what* information can be securely sent, and *who* is allowed to access the information and for what purpose. To be practical and effective it all has to be done automatically. It needs to be deployed as part of the normal process of connecting devices to the Internet and be routinely updated over-the-air and behind the scenes as part of normal operation—all without manual intervention.

Such an approach would require establishing:

1. The authenticity of the device when the device is first turned on and ''phones home,'' and each time thereafter. This could be done with a one-time encryption key derived from the unique location, time and components of the device itself (ensuring that only authenticated IoT devices are connected and interacting with an approved IoT application).

2. The security of the information itself from and to the device through encryption – a best practice would be by generating and using *one-time* encryption keys that protect information in transit against alteration or corruption. This data centric encryption solution approach dramatically increases the end to end data security while reducing the risk of key management.

3. The authority of the recipient of the information to actually receive and use that information for approved purposes (again by generating authentication keys). For example, a car sensor may routinely send information to Toyota about auto performance, but a driver may only want their insurance company to have access to speed data to demonstrate safe driving.

4. The provisioning and managing of IoT devices at scale—the technologies, and software supporting devices require the deploying company or agency the ability to remotely attest to the identity and integrity of the device (white-list) and its data continuously to detect unauthorized changes to their defined processes without human intervention, preventing the use of unauthorized devices by and from criminal attackers.

Conclusion

Companies seeking to get ahead of the curve on IoT security need to pay attention to both the FTC's enforcement actions and its expressed guidance. But they also need to think about IoT security differently than the desktop or laptop paradigm and focus on securing the *device* and the *data from the is transmitted to the various applications that rely on the device*.

BY BRUCE HEIMAN AND AL SISTO

To contact the editor responsible for this story: Donald Aplin at daplin@bna.com

  PRA ISSN 0000-0000