Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Facing The IoT's Regulatory, Security And Privacy Risks

By **Rebecca Eisner, Joseph Pennell and Nickolas Card**

Rebecca Eisner

Joseph Pennell

Nickolas Card

Law360, New York (July 19, 2017, 12:05 PM EDT) -- Internet of things (IoT)-compatible devices have been widely implemented over the last five years and growth in the segment is almost certain to continue. Cisco estimates that the number of connected devices will increase from 16 billion (as of 2015) to 26 billion by 2025.[1] This development has been highly visible in the consumer goods sector, with widespread adoption of activity trackers from companies such as Fitbit and smart thermostats from Nest, Honeywell and others. Use of IoT by businesses for business is increasing dramatically as well. With data becoming one of the most valuable corporate assets for any business, smart devices are adding to the treasure trove. These data allow businesses to monitor functions, spot patterns and trends, and more deeply analyze factors relevant to their operations. IoT sensors serve as the eyes and ears of many corporations. Smart devices collect and analyze data in order to manage inventory, monitor equipment for maintenance purposes and optimize utility usage, among other functions. Current legal and regulatory efforts have largely focused on consumer use of IoT, but businesses that use IoT for internal purposes should also pay careful attention to these trends. This article discusses the current legal and regulatory landscape for IoT and data collected through IoT systems, particularly for business (versus consumer) uses and applications, and also addresses cybersecurity, privacy, employee and other risks.

Overview of Existing U.S. Regulatory Landscape for IoT

In spite of IoT's growing popularity, the United States government has largely adopted a "wait and see" approach to specifically regulating this space. At this early stage of adoption, regulators are reluctant to implement IoT-specific rules that could quell innovation, limit potential uses for data or tie companies to outdated technology.

The "wait and see" attitude is exemplified by the Federal Trade Commission (FTC), an organization that many expect to assume primary responsibility for regulating the internet of things, and whose acting head, Maureen Ohlhausen, has cautioned against regulating before actual risk to consumers has materialized.[2] In early 2015, the FTC published a staff report ("Privacy and Security in a Connected

World") focused on (1) protection and use of personal information, (2) security concerns enabling attacks on other systems and (3) risks to personal safety.[3] Still, IoT-specific guidance from the FTC remains intermittent and nonbinding.

Despite the lack of active and specific regulation of IoT, the FTC has pursued enforcement actions against IoT device manufacturers (generally based on alleged unfair or deceptive acts or practices under §5 of the FTC Act). Two recent enforcement actions, brought against ASUS and D-Link, respectively, are representative examples.

The FTC charged ASUS with failing to secure the routers and cloud services that it marketed to consumers. ASUS had marketed security features of its products and claimed they could "protect computers from any unauthorized access, hacking, and virus attacks" and "protect [the] local network against attacks from hackers."[4] Despite these claims, the FTC alleged that the company allowed users to retain the same default login credentials on every router, allowed hackers to use web-based control panels to control consumer products and failed to address security flaws in a timely manner.[5]

The FTC's complaint against D-Link alleged that the company inadequately secured its routers and IP cameras. D-Link promoted the products in question on its own site as "Easy to Secure" with "Advanced Network Security." The FTC cited numerous concerns with D-Link's security practices, including "hard-coded" login credentials, vulnerability to "command injection" attacks and its failure to securely store user login credentials.[6]

Although consumer protection was the main objective of these enforcement actions, businesses that use IoT devices and solutions should monitor FTC enforcement actions to stay abreast of security and other issues that may lead to unfair and deceptive practice claims. Even if a business does not operate in the consumer realm, the FTC classifies companies' employee data as "consumer data" for purposes of its enforcement powers[7], and a company may be held responsible for failing to protect that data, or for such failures by its third-party providers. In 2011, the FTC settled charges against two companies (Ceridian Corporation and Lookout Services Inc.) that failed to take reasonable security measures while storing sensitive data about employees of their business customers.[8] Although these enforcement actions concerned a third-party provider's handling of employee data, companies are required under relevant law, regulations and guidance to select third-party providers carefully (e.g., under Massachusetts data security regulations)[9], so a company could be held responsible for its use of a third-party provider that fails to protect employee data.

Security Concerns

Cybersecurity risks seem to plague some smart devices and their supporting network and cloud platforms in this early stage of maturity in the IoT sector. A common adage in the industry is, "The S in IoT stands for security." The lack of security in IoT solutions is especially problematic for a number of reasons. For example, IoT devices are highly networked, making them attractive potential entry points for hackers looking to access the broader network of a corporation. In addition, IoT devices are highly standardized. If one device in a company's IoT system is affected by a security vulnerability, every similar device in the system is likely to be affected by the same vulnerability.

Some of the more common security weaknesses can be attributed to growing pains in the industry, and these weaknesses may be avoidable. IoT suppliers often come from the hardware industry, and are less likely to have the cybersecurity expertise that is more common in the software industry. For now, these hardware manufacturers may be focusing their development resources on more easily marketable features, such as appearance and battery life, at the expense of security and firmware.

Other risks that accompany IoT devices are structural and potentially unavoidable. IoT devices are typically deployed out in the physical environment, as opposed to being clustered and protected in a secure data center environment. Businesses place IoT devices in remote and unmonitored locations to collect data that would otherwise have been impossible or costly to obtain, but this allows bad actors to more easily obtain access to those devices and compromise a company's network.

Finally, the internet of things can increase risk for companies that have not even implemented the technology. IoT devices are insecure and attackers can coordinate manipulation in large numbers (in what is called a botnet) for malicious purposes. The most prominent example of this type of coordination came on Oct. 21, 2016, when the domain name infrastructure (DNS) company Dyn fell victim to a distributed denial of service (DDOS) attack that caused outages and network congestion across numerous popular websites by using a botnet of compromised digital video recorders and IP cameras.[10] As security expert Bruce Schneier observed, "Your security on the Internet depends on the security of millions of Internet-enabled devices, designed and sold by companies you've never heard of to consumers who don't care about your security."[11]

Data Collection and Usage

The most significant feature of an IoT device is its ability to collect data, which can be used to create greater efficiencies, process improvements and savings, but may create additional legal issues. In particular, companies introducing IoT devices to their business processes need to plan ahead regarding data ownership and personal data collection.

Businesses who purchase IoT solutions, smart devices and related cloud, networking and data storage solutions must carefully consider data ownership and use rights, which generally must be protected through contract terms given challenges in applying intellectual property laws to data.

For example, an original equipment manufacturer (OEM) for an IoT device (or a cloud or analytics provider that is part of an integrated IoT solution) may want rights in business users' data when collected as part of an IoT system. These providers are able to create reports, analyses, information and other products of value from use of that data, and may offer to anonymize and aggregate companies' data before doing so. In practice, however, comparison of overlapping data sets and other analytics techniques may still reveal a company's identity, trade secrets or other competitively sensitive information (despite efforts to anonymize and aggregate data).

Business IoT users will be well-served to consider these issues in advance, and to include appropriate contractual restrictions in their contracts with providers in the IoT supply chain. For example, farmers have started using drones to monitor their farms. There are now suppliers who sell these drones, including related software and training services. Many customers of these drone suppliers will be competitors with one another in the farming industry. The American Farm Bureau Federation recommends farmers understand what they are agreeing to regarding data rights with these types of suppliers.[12] The data gathered by a drone supplier could be analyzed to reveal which farmers are using the best techniques. The drone supplier could even distill or anonymize that analysis and sell it to a farmer's competitors (thereby enabling heightened competition against the farmers who previously had a market advantage).

Companies also need to be aware of the personal data they collect through their IoT implementation. In particular, the collection and use of employee, contractor or user data can trigger privacy concerns in the U.S. under state laws, federal laws and FTC regulation. Even stricter data protection laws apply in the EU with

the forthcoming General Data Protection Regulation (GDPR). Many states have employee privacy laws that may impact the collection and use of IoT business data. Aggregation of machine data in a workplace could potentially create a "Big Brother" effect for employees and users. For instance, idle machinery could be used to infer that an operator is not performing her job, or geolocation data might indicate that an employee is somewhere that he is not supposed to be during working hours. Similarly, businesses might collect employee data through IoT devices for an employee wellness program (e.g., having employees use fitness wearables, such as a Fitbit), which could trigger obligations under HIPAA, EEOC regulations or state laws.

New Liability and Regulatory Risks Created by IoT

Lastly, businesses should assess the potentially increased liability and regulatory concerns that accompany many IoT implementations.

There is the obvious concern of personal safety when IoT devices operate in the physical world. The stories of hacking into connected vehicle systems to overtake and control those vehicles are well known. Employing smart devices outside of a controlled manufacturing setting — like drones, autonomous vehicles and remote-controlled heavy equipment — increases the risk of personal injury and property damage, even when such devices are functioning properly.

While increased data from IoT may yield new insights and benefits, it may also increase regulatory and discovery-related burdens and costs. Litigation holds, discovery requests and record retention policies may apply to smart devices and central databases containing data generated from those devices. Similarly, regulators may request IoT data as part of their regulatory oversight or investigatory powers. Maintaining and searching these increased volumes of data in connection with regulatory oversight and discovery requests will result in added costs to companies using IoT.

Finally, more data and more insights may extend the "foreseeability horizon." As a general legal principle, parties are not normally responsible for damages that they could not have reasonably foreseen. The data collected by a company through its smart devices may make new harms more foreseeable, leading to an increased risk of liability for product defects or other safety problems. For example, if a product manufacturer is able to discern through IoT monitoring that its product is being used in a way that was never intended, and that manufacturer does not redesign its product to improve safety for this unintended use, or do anything to stop that use, should that manufacturer be liable for harm that occurs through that unapproved use? As increased data arguably extends the line of sight, businesses that are using IoT and its data would be well advised to understand and monitor the data, and make necessary adjustments in products, policies and processes to react to it.

Rebecca S. Eisner is the partner-in-charge of Mayer Brown LLP's Chicago office and part of the firm's technology transactions practice. Joseph M. Pennell is a partner and Nickolas S. Card is an associate in the technology transactions practice.

[1] The Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, Fostering the Advancement of the Internet of Things, National Telecommunications & Information Administration (Jan. 12, 2017) available

at https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[2] Sam Thielman, Acting Federal Trade Commission head: internet of things should self-regulate, The Guardian (Mar. 14, 2017), https://www.theguardian.com/technology/2017/mar/14/federal-trade-commission-internet-things-regulation.

[3] FTC Staff Report, Internet of Things: Privacy and Security in a Connected World, Federal Trade Commission (Jan. 27, 2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[4] Lesley Fair, ASUS case suggests 6 things to watch for in the Internet of Things, Federal Trade Commission Business Blog (Feb. 23, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/02/asus-case-suggests-6-things-watch-internet-things.

[5] Ibid.

[6] Federal Trade Commission, FTC Charges D-Link Put Consumers' Privacy at Risk Due to the Inadequate Security of Its Computer Routers and Cameras, Federal Trade Commission Press Releases (Jan. 5, 2017), https://www.ftc.gov/news-events/press-releases/2017/01/ftc-charges-d-link-put-consumers-privacy-risk-due-inadequate.

[7] Federal Trade Commission, FTC Settles Charges Against Two Companies That Allegedly Failed to Protect Sensitive Employee Data, Federal Trade Commission Press Releases (May 3, 2011), https://www.ftc.gov/news-events/press-releases/2011/05/ftc-settles-charges-against-two-companies-allegedly-failed.

[8] Ibid.

[9] 201 Mass. Code Regs. 17.03(2)(f)(1) (June 16, 2017) available at http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

[10] Brian Krebs, Hacked Cameras, DVRs Powered Today's Massive Internet Outage, Krebs on Security (Oct. 21, 2016), https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/.

[11] Bruce Schneier, Regulation of the Internet of Things, Schneier on Security (Nov. 10, 2016), https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html.

[12] Catherine Boudreau, FAA Small Drone Proposal Embraced By Agriculture Industry; Crop Benefits Seen, Bloomberg BNA (Feb. 20, 2015), https://www.bna.com/faa-small-drone-n17179923270/.
