The Internet of Things

By Howard W. Waltzman[1] and Lei Shen

This article appeared in the July 2015 issue of *Intellectual Property & Technology Law Journal*.

The proliferation of smart phones raised novel privacy and security concerns due to the unprecedented amounts and types of personal information that these devices and their applications could collect, use, store and share. Many aspects of our lives—communications, social interactions, shopping, learning, banking, entertainment, and gaming—were accessible on a single mobile device. Now, with the emergence of Internet-connected wearables, cars, appliances and other devices—or the Internet of Things (IoT)—these concerns are being raised to a new level.

These interconnected devices promise many benefits and make their users' lives more convenient, but also may collect personal and, potentially, intimate, data about a consumer that, in combination with other collected information, forms a detailed and personal profile of consumers. Such information also enables companies to make assumptions about consumers in ways that may be viewed as invasive.

Policymakers are taking note of the proliferation and implications of IoT devices. Policymakers in the United States and around the world are debating how to ensure consumer privacy and security without stifling IoT-related innovation.

FTC Report

The U.S. Federal Trade Commission (FTC) jumped into this debate in 2013, when it brought an enforcement action against TrendNet, Inc., claiming that the company's lax security measures allowed hackers to tap into its Internet-connected cameras. Recently, the FTC took another step in setting expectations for IoT devices when it released a report in January 2015 based on the feedback it received as part of an IoT workshop the agency held in November 2013. The report, titled "Internet of Things—Privacy & Security in a Connected World," highlights the issues involved with the Internet of Things, and details the steps that companies can take to enhance and protect their users' privacy and security.

The FTC's report takes some of the same core privacy principles and recommendations that the FTC had featured in other reports (*e.g.*, security, data minimization, notice and choice) and applies them to IoT devices. Among the recommendations included in the report are:

- **Security.** Companies should incorporate privacy and security by design by building privacy and security into their devices at the outset, rather than as an afterthought in the design process. To do so, a company should consider conducting a privacy and security risk assessment as part of its design process.

In addition, the company should ensure that, when outside vendors are hired, those entities are capable of maintaining reasonable security, and the company should provide reasonable oversight of those vendors. The FTC also released a companion report titled "Careful Connections—Building Security in the Internet of Things" that focuses on its specific security-related recommendations.

- **Data Minimization.** The FTC's report also concludes that companies should practice data minimization by limiting the collection and retention of consumer data. While one of the major benefits of interconnected devices for companies involves the ability to collect large amounts of data that companies can retain for future business purposes and innovation, the FTC cautions that doing so may increase two key privacy-related risks. First, collecting large amounts of consumer data makes a company more enticing to data thieves, and second, it increases the likelihood that the data will be used in ways that consumers do not anticipate. Therefore, the FTC recommends that companies impose reasonable limits on their collection of consumer data, including limiting the collection to non-sensitive data, or data that is necessary to offer the company's product or service. In addition, a company should discard data when it is no longer relevant or needed, or de-identify any data the company chooses to retain.
- **Notice and Choice.** The FTC acknowledged that notice and choice with the IoT is challenging because a lot of the devices do not have a user interface. Therefore, the FTC suggested that a company need not offer a choice to a consumer if the company's expected use is consistent with the context of the interaction (*i.e.*, a use that the consumer would expect given the interaction). However, if the company's anticipated use is inconsistent with the context of the interaction, the company should notify consumers and offer them clear and conspicuous choices regarding how their data will be used or shared, including the opportunity to opt out.

U.S. Senate Hearing

The U.S. Senate Committee on Commerce, Science and Transportation also has been focused on the IoT and held a hearing on February 11, 2015, to discuss this issue. The hearing, titled "The Connected World: Examining the Internet of Things," featured various panelists from the industry. One of the key topics concerned how to strike a balance between innovation and growth with the protection of consumer interests, especially if, as some of the panelists predicted, the IoT ultimately would have more retail and industrial uses than consumer uses. Security was a top concern, with a panelist stressing that security should be built into devices at the outset and throughout a device's life-cycle. Other recommendations included encouraging consumer education and industry transparency.

Despite the concerns, most of the panelists agreed that Congress should not rush to regulate the IoT. Commerce Committee Chairman Sen. John Thune (R-SD) stated, "We should let consumers and entrepreneurs decide where [the Internet of Things] goes, rather than setting it on a Washington, D.C.-directed path." He added, "Let's not stifle the Internet of Things before we and consumers have a chance to understand its real promise and implications."

European Union

The privacy and security issues surrounding the Internet of Things have gained the attention of regulators in the European Union, as well. In October 2014, the EU's Article 29 Data Protection Working Party released an opinion expressing concerns about the IoT that aligned with those expressed in the FTC's report. In particular, the Working Party was concerned with the likelihood that users might not be aware

that data collection and processing is occurring when they use IoT devices. They also were concerned about the amount of data that such devices are collecting. A user's lack of awareness regarding such collection and processing poses a challenge to demonstrating valid consent under EU law. In addition, the large amount of data being retained could violate the European Union's requirement that personal data not be kept longer than necessary for the purpose it was collected. Further, any secondary uses for that data might not be within the scope of the original purpose to which the user consented.

In its guidance, the Working Party, as did the FTC, focused on data minimization and providing consumers with notice and choice. However, the Working Party's guidance in the European Union carries more weight than the FTC's report in the United States: the FTC's report offered best practice recommendations while the Working Party's opinion focused on compliance with EU privacy requirements.

The FTC's report focused on best practices and urged companies involved with the IoT to take concrete steps to protect their users' privacy, but it stopped short of calling for legislation to regulate the area. The FTC reasoned that, given how rapidly the technology is evolving, it would be premature to apply new laws to it. However, the report lays the groundwork for FTC enforcement.

While the FTC's recommendations are not binding, companies should heed the recommendations because they are likely to form the basis for future enforcement actions in this space. Companies also should be mindful of the Working Party's guidance as it reflects how EU regulators are likely to view compliance with EU privacy requirements. The IoT is still in a nascent stage, but policymakers, while mindful of not stifling IoT innovation, clearly want companies to be cognizant of the privacy and security implications of IoT devices.

Endnotes

[1] Howard W. Waltzman is a partner at Mayer Brown LLP, practicing in the areas of communications and Internet law and privacy compliance. Lei Shen is a senior associate in the firm's Privacy & Security and Business & Technology Sourcing practice groups. The authors may be reached at hwaltzman@mayerbrown.com and lshen@mayerbrown.com, respectively.