Cooley

January 29, 2015

On January 27, 2015, the Federal Trade Commission (FTC) released a staff report titled *Internet of Things—Privacy and Security in a Connected World*. The report summarizes the topics discussed and input provided by participants at a workshop of the same name that the FTC held on November 19, 2013. The report also provides the first staff-level recommendations on the Internet of Things (IoT).

Definition of the IoT

The report defines the IoT to include "consumer-facing devices, as well as products and services that are not consumer-facing, such as devices designed for businesses to enable automated communications between machines." Specifically, the report points to "'things' such as devices or sensors—other than computers, smartphones, or tablets—that connect, communicate or transmit information with or between each other through the Internet." Despite this broad definition, the report explicitly states that it does not address devices that are sold in a business-to-business context (e.g., sensors in hotel networks) or are machine-to-machine connections used generally for business efficiency (e.g., tracking inventory), even though those types of devices might have a significant effect on consumer privacy.

Benefits and risks

The report examines the "benefits and risks" of the IoT. According to participants at the workshop, some benefits of the IoT include managing healthcare at home, providing "richer data" in order to improve diagnosis and treatment, analyzing home energy use, and conducting real-time vehicle diagnostics.

The report separates risks into two categories: security risks and privacy risks. The staff report identifies IoT security risks as threats to consumers from the: (1) enabling of unauthorized access to and misuse of personal information; (2) facilitation of attacks on other systems; and (3) creation of safety risks. The first two risk factors are the more traditional types: identity theft and potential denial-of-service attacks. The third risk factor is focused on a newer, physical threat such as hacking in to a medical device (e.g., an insulin pump) or remotely tampering with a vehicle's braking systems. The report does note that all of these risks may be present in traditional computing environment—it's just that they are "heightened" in the context of the IoT. The report states that the exacerbating factors are that (1) companies entering into the IoT market may be inexperienced with security issues and (2) many of the devices are inexpensive and "essentially disposable," making software updates difficult or impossible.

With respect to privacy, the report identifies risks to include "direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information—risks already presented by traditional Internet and mobile commerce." The report suggests data usage without consumer consent or safeguards against inaccuracies offsets any potential benefits. For example, the report cites an example where an insurer could use data from a fitness tracker to price health insurance. Another example involves electronic "eavesdropping" whereby unencrypted data from camera devices could lead to spying into previously private parts of a home.

Application of Fair Information Practice Principles

The report states that Workshop participants debated applying the Fair Information Practice Principles (FIPPs)—notice, choice, access, accuracy, data minimization, security, and accountability—to the IoT. Data security, data minimization, notice, and choice became the focus of the debate. According to the report there was some agreement among participants that data security should be incorporated into IoT devices. As to data minimization—the limiting of data collected and retained by a company—there was more division of opinion. The report includes more concerns than support for data minimization. For example, the report cites a participant's concern that "[r]estricting data collection with rules like data minimization could severely limit the potential opportunities of the Internet of Things" if beneficial uses emerged subsequent to the time the data was first collected. Finally, the report notes that workshop participants offered several options for notice and choice, many

of which empowered the consumer to opt-in and manage data collection.

FTC staff recommendations

The report contains several staff recommendations around data security, data minimization, and notice and choice. These recommendations are drawn from the workshop discussions described above.

Data security

The staff recommends that IoT companies:

1. Implement "security by design" by building security into their devices at the outset, rather than as an afterthought. This concept includes privacy or security risk assessments, consciously considering the risks presented by the collection and retention of consumer information, consideration of how to minimize the data they collect and retain, and testing their security measures before launching their products.
2. Ensure that their personnel practices promote good security.
3. Work to ensure that they retain service providers that are capable of maintaining reasonable security, and provide reasonable oversight to ensure that those service providers do so. Failure to do so could result in an FTC enforcement action.
4. Implement a defense-in-depth approach for systems with significant risk, in which security measures are considered at several levels.
5. Consider implementing reasonable access control measures to limit the ability of an unauthorized person to access a consumer's device, data, or even the consumer's network. For example, strong authentication techniques should be used "to permit or restrict IoT devices from interacting with other devices or systems" while at the same time not impeding the device's usability.
6. Continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities.

Data minimization

The staff agreed with participants that data minimization is "relevant and important" to the IoT and recommends:

1. Companies should examine their data practices and business needs and develop policies and practices that impose reasonable limits on the collection and retention of consumer data.
2. To the extent that there is a need to collect and maintain data to satisfy a business purpose, companies should also consider whether they can do so while maintaining data in deidentified form.

Notice and choice

According to the report, the staff believes that providing notice and choice is important, even if traditional methods of providing notice and choice may need to be modified as the IoT evolves. Notice and choice is "particularly important when sensitive data is collected." The staff acknowledges the practical difficulty of providing notice when there is no consumer interface and recommends a wide variety of options including:

1. Choices at point of sale
2. Tutorials
3. Codes on the device
4. Choices during set-up
5. Management portals or dashboards
6. Icons that convey "important settings and attributes"
7. Out-of-band communications as requested by a consumer
8. General privacy menus
9. A "user experience" approach

The report states that whatever form the privacy choice offered, it must be clear and prominent.

Legislation

Currently, the FTC staff does not call for new IoT legislation, saying that it's premature given the speed of

evolution in the space. The FTC will continue to use existing tools to ensure that IoT companies continue to consider security and privacy issues as they develop new devices. These tools include:

1. Law enforcement through the FTC Act, the Fair Credit Reporting Act (FCRA), the health breach notification provisions of the HI-TECH Act, the Children's Online Privacy Protection Act (COPPA), and other laws that might apply to the IoT.
2. Consumer and business education tailored to the IoT.
3. Participation in multi-stakeholder working groups that are developing IoT guidelines.
4. Advocacy with other federal and state agencies, state legislatures, and courts to promote consumer protections.

While it may not have current plans to push for new IoT-specific legislation, Commission staff did advocate for broader general powers. Stating that its current authorities mean the FTC "cannot mandate certain basic privacy protections … absent a specific showing of deception or unfairness," the Commission staff recommends flexible broad-based legislation that will address privacy concerns beyond those just in the IoT. To emphasize its belief in the need for further legislation, the staff repeated this point as the very last sentence of the Conclusion to the report.

The future of IoT policy

The next step for the FTC is unclear. The Commission voted 4-1 to issue the report with Commissioner Joshua Wright dissenting. Commissioner Maureen Ohlhausen wrote a separate supporting statement. In his dissent, Commissioner Wright expressed disappointment that the report was a series of policy recommendations and best practices that, in his judgment, lacked analytical support showing that they would improve consumers' well-being. Notwithstanding this lack of unanimity and despite various negative initial reactions, ensuring consumer protections for the IoT remains a high priority for FTC Chairwoman Edith Ramirez.

Congress has also shown interest in the IoT. Representatives Darrell Issa (R-CA) and Suzan DelBene (D-WA) have created the Congressional Internet of Things Caucus, and the Senate Committee on Commerce, Science, and Transportation has announced a Feb 11, 2015 hearing on the subject. Look for similar action from the House Energy and Commerce Committee.

Practice tips

Companies in the IoT space can take steps now to reduce risk. These include:

1. Reviewing security policies and procedures for current and future products.
2. Reviewing the amount of data that is collected and ensure that there is a specific business purpose.
3. Reviewing privacy notices to ensure they are clear and conspicuous.
4. Creating (or reviewing) options that allow users to manage how their data is used.

Our Government Analytics practice group works closely with our Privacy & Data Protection practice group to track these and other regulatory issues involving privacy and cybersecurity. We can provide you with additional information or insights, tailored to your or your organization's needs.

Key Contacts

Matthew D. Brown **San Francisco**	**brownmd@cooley.com** **+1 415 693 2188**
Adam Ruttenberg Washington, DC	aruttenberg@cooley.com +1 202 842 7804
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090
Vince Sampson Washington, DC	vsampson@cooley.com +1 202 728 7140