wiley

NEWSLETTER

FTC Report on Internet of Things Confirms Growing Interest in Privacy and Security for Innovators

February 2015

On January 27th, following a 4-1 vote, the Federal Trade Commission (FTC) issued an anticipated Staff Report on the *Internet of Things: Privacy and Security in a Connected World (IoT)*. Growing out of a 2013 workshop and discussions with industry, academics, and consumer groups, the Report contains observations and recommendations for consumer-facing devices.

It also includes lists of security and privacy considerations and recommendations for industry as they develop and launch products and services.

The Report is not without controversy. Its "lengthy discussion of industry best practices and recommendations for broad-based privacy legislation" were criticized by Commissioner Wright, who dissented from the decision to publish. He argued that the recommendations were "without analytical support to establish the likelihood that those practices and recommendations, if adopted, would improve consumer welfare."

Commissioner Olhausen concurred in the decision to issue the Report, but explained that she disagreed with, among other things, "the recommendation for baseline privacy legislation because I do not see the current need for such legislation." She also has concerns about recommended data minimization principles that rely on the "precautionary principle." She noted that the Report "misses the opportunity to explore fully the emerging tension between information technology (including IoT) and the FIPPs approach to protecting consumer privacy."

Authors

Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Practice Areas

Internet of Things

This Report signals to innovators, manufacturers, retailers, and consumers that law and policy will continue to pose a challenge, particularly in the face of shifting consumer expectations. Industry should closely study this report and be mindful of the FTC's assertive role in the IoT.

Innovation in IoT Poses Opportunities and Challenges

The Report observes that "The IoT explosion is already around us, in the form of wearable computers, smart health trackers, connected smoke detectors and light bulbs, and essentially any other Internet-connected device that isn't a mobile phone, tablet, or traditional computer."

The Report highlights benefits and risks—both security and privacy related—from IoT.

- With respect to security risks, the Report states that consumers could be harmed by unauthorized access and misuse of personal information, the facilitation of attacks on other systems, and the creation of safety risks.
- With respect to privacy, the Report notes that risks involve "the direct collection of sensitive personal information, such as precise geolocation, financial account numbers, or health information" which can be collected over time and in a volume not previously possible.

The Report notes several policy challenges that arise in this context. Examples include the application of traditional privacy principles to the IoT, acknowledging debate over whether the Fair Information Practice Principles (FIPPs) and "the principles of data minimization, notice, and choice" continue to apply to the IoT. The FTC did not resolve these issues but noted that they remain challenging and continue to be addressed on a domestic and global scale.

The FTC Identifies Concrete Issues for Companies to Consider

The FTC did offer its views and some advice to industry on security and privacy measures to consider. For example, with respect to security measures, the FTC identifies several steps that companies should consider, many of which are key at product development time.

- "Companies should implement 'security by design' by building security into their devices at the outset, rather than as an afterthought." Also companies should "do a privacy or security risk assessment, consciously considering the risks presented by the collection and retention of consumer information." Companies should minimize the data they collect and test their security before launch.
- "Companies must ensure that their personnel practices promote good security," including to "ensure that product security is addressed at the appropriate level of responsibility within the organization." Training and oversight are important to the FTC.
- "Companies must 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 law enforcement action."

- "For systems with significant risk, companies should implement a defense-in-depth approach, where security measures are considered at several levels." This may include encryption, and taking steps to "reasonably secure data in transit and in storage."
- The FTC notes that some participants in the workshop argued that "companies should 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."
- "Companies should continue to monitor products throughout the life cycle and, to the extent feasible, patch known vulnerabilities."

The Report elaborates on all of these issues, and addresses important issues around data minimization, notice, and choice, including suggestions about consumer interfaces and best practices for the use of information collected. Taken with the White House's report on Big Data and other developments, this Report provides a baseline for regulatory expectations.

Innovators, manufacturers, collectors, and users of consumer data should consider each of the steps and practices identified in the Report.

The FTC Will Be Watching

The private sector should expect increasing vigilance by the FTC: "As physical objects in our everyday lives increasingly detect and share observations about us, consumers will likely continue to want privacy. The Commission staff will continue to enforce laws, educate consumers and businesses, and engage with consumer advocates, industry, academics, and other stakeholders involved in the IoT to promote appropriate security and privacy protections. At the same time, we urge further self-regulatory efforts on IoT, along with enactment of data security and broad-based privacy legislation."

Innovators and consumers alike can anticipate continued federal and state interest in privacy and security of consumer devices capable of connecting to the Internet.