Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

FTC Report Raises Stakes For 'Internet Of Things' Regulation

By **Allison Grande**

Law360, New York (January 29, 2015, 8:57 PM ET) -- The Federal Trade Commission earlier this week released a long-awaited report detailing its privacy and security expectations for companies that develop devices connected to the "Internet of Things," a move that not only lays the groundwork for stepped-up enforcement by the regulator but also provides fodder for a heated debate over ways to legislate the emerging technology.

In the 71-page report unveiled Tuesday, commission staff laid out a series of concrete steps that businesses that manufacture and sell health monitoring, home security, household appliances and other interconnected devices that are part of the growing Internet of Things should be taking to enhance and protect consumers' privacy and security.

The recommendations included building security into devices at the outset, monitoring the products for security vulnerabilities through their expected life cycle, providing consumers with notice and the ability to choose how their information will be used, and limiting the collection and retention of consumer data.

While the regulator's guidance is not binding, attorneys say that companies that are contemplating or have already made a move into the smart device industry would be wise to heed the commission's recommendations, given that they are likely to form the basis for future enforcement actions in this space.

"FTC staff reports are often the prelude to enforcement actions," Davis & Gilbert LLP partner Gary Kibel said. "While it's not law, the staff report is very helpful for Internet of Things companies to use as a checklist of sorts in order to test their current practices against concerns raised in the report, which can be helpful in avoiding any problems down the road."

As with previous hot-button topics, such as data brokers and mobile cramming, the FTC staff report stems from feedback the agency received on the Internet of Things from industry members, technologists and others during and following a Nov. 19 workshop the agency held on the topic.

"Typically, how it works is that the FTC will hold a workshop on the issue, then a staff report comes out, and that leads to the commission looking at players in the industry to see if they're doing anything improper," Kibel said.

While the commission previously waded into the Internet of Things domain with a September 2013 settlement with Trendnet Inc. over allegedly lax security measures that allowed hackers to tap into Web-connected cameras that the company sold to consumers, attorneys anticipate that, with its expectations now detailed in a formal report, the commission will be much more aggressive in pursuing companies that are perceived to not be living up to their privacy and security obligations.

"Where the FTC views a problem with a company's privacy or security practices, it hasn't been shy about seeking to have those practices changed," said Mayer Brown LLP partner Howard Waltzman, who noted that the regulator recently wrapped up its 50th data security-related consent decree. "The Internet of Things is clearly a concern to the FTC, so to the extent that the commission has a problem with security or perceived privacy abuses, it will seek to bring enforcement actions."

Outside of the commission, federal lawmakers have also been keeping a close eye on the emergence of Internet-connected devices, a focus that is likely to intensify now that the FTC has provided an assessment of the industry and the potential privacy and data security concerns that could emerge.

"The Internet of Things report is a really useful step forward in thinking about new privacy and data security issues that are arising with the growth of new technology," Wiley Rein LLP privacy practice chair Kirk Nahra said. "It focuses attention on how data is being created, analyzed and distributed from a wide range of new sources, [and] it will be thrown into the mix of debate about new legislation or regulations."

While questions have been raised about whether the Internet of Things requires a framework for privacy and security that is different from the one that currently governs more traditional means of data collection, attorneys say it's unlikely that lawmakers will settle on Internet of Things-specific legislation, given the challenges with formulating targeted regulations and the conclusion by the commission staff in its report that such regulation would be premature due to the rapidly evolving nature of the technology.

The staff's conclusion on this front was supported by the Federal Trade Commission's Joshua Wright, the only commissioner to vote against issuing the staff report. While he agreed targeted legislation was unnecessary, he went a step further by criticizing the staff in his dissent for issuing broad-based privacy recommendations without providing the requisite analytical support that the best practices would improve consumer welfare if adopted.

"It's unlikely that Commissioner Wright's recommendations would impact enforcement, but it might impact legislation, since it will certainly be part of the debate with legislation that we can't do this now because we have to analyze this further," Kibel said.

While the odds of enacting focused legislation are slim, the FTC staff did in its report renew the commission's long-running push for Congress to enact strong data security and breach notification legislation and broad-based privacy regulation that is flexible and technology-neutral, proposals that may have a better shot at gaining traction in light of the commission's findings.

The call for data security and breach notification legislation could especially be helped by the Internet of Things report, given the commission's focus on the importance of ensuring that the sensitive data being collected by Web-connected devices is secure, attorneys say. The White House provided a boost to this effort earlier this month when it unveiled a legislative proposal to create a national breach notification

standard.

"When you're going to have a plethora of new devices in this space, it shows why it's so important to have a national policy on data security," Waltzman said. "One of the themes of the FTC report is that companies need to be thinking about security at the beginning stages of the production process, so having a national law would definitely make all companies more focused on data security on the front end while ensuring uniform protections for consumers regardless of what state they live in."

With scrutiny of the Internet of Things marketplace by regulators and lawmakers heating up, attorneys say that companies would be wise to be just as diligent in ensuring that their privacy and security practices are up to muster.

"The main 'lesson learned' for companies — in all industries and for all data — is to understand the implications of the data you are using, and to be smart and fair in thinking about how you collect, analyze and distribute this information," Nahra said.

Although the data security, notice and consent principles are similar to ones that have been expounded by the commission in the past, attorneys and other stakeholders flagged the regulator's increased focus on data minimization as a potential area of tension and concern moving forward.

In its report, the staff recommended that companies consider limiting their collection of consumer data and set reasonable retention periods, a stance that has the potential to clash with companies' growing desire to gather and hold onto consumer data that may be useful for some future business purpose.

"The ticking time bomb in the commission's report is the emphasis on data minimization," said D. Reed Freeman, co-chair of WilmerHale's cybersecurity, privacy and communications practice. "The commission is 'recommending' it now, but it seems to me they are setting up a case for an unfairness action under Section 5 of the FTC Act in the midterm. If it turns out that 'data minimization' is a Section 5 requirement, that would have a profound effect on business, which until now has considered it a best practice."

Companies in the Internet of Things industry should also be sure to keep a close eye on a congressional hearing recently scheduled for Feb. 11, during which the U.S. Senate Committee on Commerce, Science and Transportation will focus on the privacy and security implications of the emerging technology.

"It will be interesting to see the extent to which this hearing aids the congressional debate on data security and privacy, and whether the members conclude that there is a greater need and urgency for legislation before these devices really proliferation," Waltzman said.

--Editing by Katherine Rautenberg and Patricia K. Cole.