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

Regulatory Rules Of The Road For IoT Manufacturers

By **Evan Wolff, Jeffrey Poston, Peter Miller, Kristin Madigan and Stephanie Reiter**


Evan Wolff


Jeffrey Poston


Peter Miller


Kristin Madigan


Stephanie Reiter

(July 28, 2017, 12:08 PM EDT) -- The boundless growth in the development and deployment of interconnected devices (often referred to as the internet of things) for consumer, industrial and other applications has empowered consumers and businesses. The proliferation of "smart" devices for consumers — home security systems, medical devices, fitness monitors, connected cars, and numerous other applications — however, is fraught with privacy and security concerns rising from the collection, storage and transmission of the underlying personal information.

The regulators active in this space have acknowledged that while the technologies and accessibility of these devices are novel, the fundamental legal and regulatory issues are not. As illustrated by recent draft guidance from the U.S. Department of Commerce's National Telecommunications and Information Administration, and responsive comments from Federal Trade Commission staff, the regulatory expectation continues to be that IoT devices will be developed and deployed based on fundamental privacy and data security practices, including the ability to anticipate, manage, and address evolving threats and vulnerabilities. Indeed, in a recent enforcement action, the Federal Trade Commission has issued a closing letter requiring end of life disclosures for an IoT device, and providing new business guidance with clear instructions regarding how internet-connected toy manufacturers must comply with Children's Online Privacy Protection Act. This signals a continuing aggressiveness toward ensuring that IoT devices fall within the privacy and security regimes applicable to more traditional technologies.

Draft NTIA Guidance Regarding Ability to Update IoT Devices

As part of its Digital Economy Agenda, the Department of Commerce has actively encouraged continued innovation in the IoT space. To that end, in April 2016, the NTIA[1] issued a request for comment regarding IoT policy issues, which yielded over 130 responses from IoT manufacturers, solution providers, security experts, and consumer advocates, among other stakeholders. Commenters highlighted the need for a secure lifecycle approach to the development, maintenance, and decommissioning of IoT devices. Based on this feedback, the NTIA convened a multistakeholder process on IoT security, upgradability, and patching with the goal of addressing the following objectives:

- Identify and map relevant issues identified by stakeholders using a transparent, consensus-driven process.

- Mitigate security vulnerabilities in IoT devices through patching and security upgrades to provide users with reasonable assurances that connected devices will be secure, which will help realize the full innovative potential of IoT.

- Create common, standardized definitions regarding security upgradability for consumer IoT as well as strategies for manufacturers to promote transparency and effectively communicate the security features of IoT products to consumers.

In January 2017, the NTIA released a green paper on "Fostering the Advancement of the Internet of Things" summarizing the comments it received and describing the benefits, challenges, and potential roles for the government in promoting development of IoT. Although the commenters appeared to disagree regarding the extent to which current regulations are sufficient to address novel challenges presented by IoT (e.g., notice and consent), the majority of submissions preferred a multistakeholder approach to IoT policymaking.

On April 25, 2017, the NTIA published draft guidance, "Communicating IoT Device Security Update Capability to Improve Transparency for Customers," and requested comments on its proposed "Elements of Updatability": patch and update-related information that manufacturers should disclose to consumers to facilitate transparency and informed decision-making.[2]

The NTIA working group identified three "key elements" that manufacturers should disclose to consumers prior to their purchase of an IoT device: (1) whether the device is capable of receiving security updates; (2) how the device receives security updates (e.g., automatic updates); and (3) the anticipated timeline for providing security update support.

The working group also identified three "additional elements" that manufacturers should consider disclosing to consumers before or after purchase: (1) how the user is notified about security updates; (2) what happens when the device no longer receives security update support; and (3) how the manufacturer verifies the security or functionality of updates.

FTC Response to NTIA's Request for Public Comment

On June 19, 2017, the FTC issued a public comment regarding the NTIA's draft guidance. The FTC recommended that the NTIA incorporate FTC best practices into NTIA's proposed "Elements of Updatability," with the goal of "provid[ing] useful information to consumers, without unduly burdening businesses." The FTC noted the risk of ineffective and confusing consumer disclosures and recommended that, to the extent feasible, manufacturers "minimize the need for disclosures by providing secure products that receive automatic security updates during the device's reasonable lifespan."

After cautioning that "manufacturers should carefully evaluate the effectiveness of their disclosures," the FTC suggested that, in place of NTIA's "anticipated timeline" of support, manufacturers provide a minimum security support period, including the start or end date, to allow consumers to meaningfully evaluate and compare IoT devices. The FTC also recommended adding a fourth element requiring manufacturers to disclose "key use limitations" to consumers prior to purchase for smart devices that

will become highly vulnerable or lose functionality after support ends, particularly when compared with a similar "dumb" device. Such a disclosure may be sufficient to deceive the consumer about the limitation.

The FTC suggested eliminating requiring manufacturers to describe the process by which they secure and install updates on the grounds that it may "impose significant communication costs on industry while providing little, if any, benefit to consumers." The FTC also recommended disclosure of three new "additional elements" to before or after purchase: (1) to the extent that updates cannot be installed automatically, adopt a uniform method for notifying consumers of available updates (e.g., a standard position on device screen) to facilitate increased consumer awareness; (2) to increase registration for security support notifications, allow consumers to affirmatively register only for security support notifications, rather than combining registration with an agreement to receive marketing communications; and (3) provide real-time notifications when security support is about to end, to allow consumers to make more informed decisions about risk mitigation.

Although the FTC's comments "are intended to ensure that the proposed Elements of Updatability reflect its experience with IoT devices and consumers' perceptions of disclosures," and "are not intended to provide a template for FTC law enforcement," the FTC identified additional recommended security practices for IoT manufacturers:

- Apply the elements and the FTC's comments "based on each unique product's function, the types of information it collects, its life span, and the costs of conveying any suggested disclosures."
- Take reasonable measures to design secure IoT devices, and patch vulnerabilities in IoT devices' firmware.
- Balance the benefits of safeguarding against threats with the cost of developing, testing, and deploying software updates to patch devices.
- Implement a process for regularly updating software.
- Provide secure products that receive automatic security updates during the device's reasonable lifespan.

The FTC's public comment to the NTIA closely tracks the FTC's policy positions on privacy and data security, specifically with regard to IoT[3] and more generally with regard to consumer-facing technology.[4] Given the FTC's active and ongoing interest in IoT-related (and other) privacy and data security issues, its independent consumer protection enforcement power, and its jurisdiction over IoT manufacturers, IoT device manufacturers would be well-advised to carefully consider the FTC's recommendations, regardless of whether the NTIA incorporates them.

FTC's IoT-Focused Enforcement and Business Education Activities

The FTC has identified IoT as a current privacy enforcement priority.[5] Many IoT manufacturers fail to appreciate the need to apply the FTC's flexible, well-established privacy and data security principles to

connected devices, resulting in supply chain vulnerabilities, weak links in otherwise compliant systems, and stand-alone products that are collecting data without the necessary protections. As demonstrated by the following enforcement actions and education activities, however, it is clear that the FTC expects businesses to be aware of and comply with the guidance applicable to IoT companies.

Vizio

In February 2016, the FTC brought an IoT enforcement action against Vizio Inc. alleging that Vizio manufactured "smart" televisions that automatically transmitted sensitive consumer viewing data back to its servers. The FTC alleged that Vizio sold the data to third parties without obtaining consumers' informed consent. The accompanying FTC business blog entry encouraged manufacturers to explain their data collections up front, obtain informed consent before collecting and sharing viewing information, make it easy for consumers to exercise options, and reference prior FTC guidance materials about applying consumer protection principles to IoT.

Asustek

In February 2016, the FTC brought an enforcement action against Asustek Computer Inc., a computer hardware manufacturer, for alleged violations of Section 5 of the FTC Act, resulting in unauthorized access to consumers' connected storage devices. Based on Asustek's collective practices, the FTC asserted that it failed to provide reasonable security in the design and maintenance of the software supporting its routers and cloud services, advise consumers of the availability of security updates, and secure its router and related cloud services as advertised. The accompanying FTC business blog entry summarizes security lessons learned from Asustek and other FTC enforcement actions and IoT guidance materials.

D-Link

In January 2017, the FTC filed a complaint against D-Link Corporation, a computer networking equipment manufacturer, and its U.S. subsidiary, alleging that D-Link failed to use reasonable practices to secure its routers and internet protocol cameras, and mischaracterized the level of security protections afforded by its products. The FTC asserts that because hackers could "take simple steps" to exploit the vulnerabilities, D-Link's practices put consumers' privacy at risk. The FTC's press release announcing the D-Link lawsuit highlights the fact that "the FTC has provided guidance to IoT companies on how to preserve privacy and security in their products while still innovating and growing IoT technology."

The FTC also launched an investigation into Google-owned Nest Labs Inc. as a result of its unilateral decision to discontinue security support for a smart product sold by a company that Nest acquired. In a letter to Nest, the FTC noted it "was concerned that reasonable customers would not expect the [product] to become unusable," and "rendering the devices inoperable would cause unjustified, substantial consumer injury." While Nest escaped enforcement due to the limited number of products sold and its decision to alert and provide refunds to customers, the FTC's investigation is instructive. As noted in the accompanying FTC business blog entry, the investigation raised broader issues about what happens when an IoT product becomes inoperable or software support is discontinued. Including representations made to consumers about the lifecycle of IoT products and support.

In June 2017, the FTC updated its six-step compliance plan for companies subject to COPPA. Specifically, the guidance clarifies the FTC's position that internet-connected products marketed towards children may be considered online services subject to COPPA. The guidance is significant in that it puts companies on notice that they may need to comply with COPPA. While it is too soon to say whether this

update will trigger a wave of COPPA investigations and enforcement actions against internet-connected toy manufacturers, companies should be apprised of, and comply with, the FTC's new guidance.

IoT product manufacturers likely will face enhanced scrutiny as connected devices and the ecosystems in which they operate continue expanding. There is no one-size-fits-all solution for mitigating IoT risks. However, adopting reasonable practices that address principles of privacy and security by design, customer choice and notice, and data minimization likely will pass muster under the acting commissioner. This risk-based approach to protecting consumer information likely will foster innovation and consumer confidence.

Evan D. Wolff is a partner in the Washington, D.C., office of Crowell & Moring LLP, co-chairman of the firm's privacy and cybersecurity group and a former adviser to senior leadership at the U.S. Department of Homeland Security.

Jeffrey L. Poston is a partner in the firm's Washington office and co-chairman of the firm's privacy and cybersecurity group.

Peter B. Miller is senior counsel in the firm's Washington office and former chief privacy officer at the Federal Trade Commission.

Kristin Madigan is counsel in the firm's San Francisco office.

Stephanie A. Reiter is an associate in the firm's Washington office.

[1] NTIA, which serves as a member of the Commerce Department's Internet Policy Task Force, is primarily responsible for advising the President on telecommunications and information policy issues, and developing policy relating to online privacy, cybersecurity, online information sharing, and topics related to the Internet economy.

[2] Notably, while the guidance primarily addressed IoT device updates and patches, it cautioned manufacturers and consumers to consider additional security practices and policies to secure their devices.

[3] Careful Connections: Building Security in the Internet of Things and Internet of Things, Privacy and Security in a Connected World

[4] Start with Security