Before the
CONSUMER PRODUCT SAFETY COMMISSION
Washington, DC

In the Matter of The Internet of Things and Consumer Product Hazards	Docket No. CPSC-2018-007

To: Consumer Product Safety Commission
Date: June 15, 2018

Comments of the Staff of the Federal Trade Commission's Bureau of Consumer Protection

I. Introduction

The staff of the Federal Trade Commission's ("FTC") Bureau of Consumer Protection ("BCP") (hereafter "BCP staff') appreciate this opportunity to comment[1] on the Consumer Product Safety Commission's ("CPSC") Notice of Public Hearing and Request for Written Comments ("RFC") on *The Internet of Things and Consumer Product Hazards.*[2] Among other things, the RFC seeks comment on existing Internet of Things ("IoT") safety standards, how to prevent hazards related to IoT devices, and the role of government in the effort to promote IoT safety.

The market for Internet-connected devices—ranging from light bulbs to smart TVs to wearable fitness trackers—is flourishing. The rapid proliferation of such devices in recent years has been truly remarkable, with an estimated 8.4 billion IoT devices in use in 2017—a 31% increase from 2016.[3] And this trend promises to continue: it is estimated that 55 billion IoT devices will be installed around the world by 2025.[4]

This burgeoning marketplace offers enormous benefits to consumers—including many products that offer safety benefits.[5] For example, IoT medical devices track health data that

[1] These comments represent the views of the staff of the Bureau of Consumer Protection. The Commission has voted to authorize BCP staff to submit these comments.
[2] 83 Fed. Reg. 13122 (Mar. 27, 2018).
[3] *Gartner Says 8.4. Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016*, GARTNER (Feb. 7, 2017), https://www.gartner.com/newsroom/id/3598917.
[4] Peter Newman, *The Internet of Things 2018 Report: How the IoT is Evolving to Reach the Mainstream with Businesses and Consumers*, BUS. INSIDER INTELLIGENCE (Feb. 26, 2018), http://www.businessinsider.com/the-internet-of-things-2017-report-2018-2-26-1.
[5] *See generally* FED. TRADE COMM'N, FTC STAFF REPORT: INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, 7-10 (Jan. 2015) [hereinafter FTC IOT REPORT], https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-

informs patients' diagnosis and treatment.[6] Connected cars offer both safety and convenience benefits, such as real-time notifications of dangerous conditions and smartphone starter and sound-system control.[7] And home IoT devices called "water bugs" detect flooding in basements, while other devices monitor energy use, identify maintenance issues, and remotely control devices such as lights, ovens, and wine cellars.[8] Consumers also may purchase devices such as Internet-connected locks, burglar alarms, cameras, and garage doors for their physical safety.

But such benefits may be foreclosed if IoT devices themselves are a hazard. Like any other consumer product, IoT products might present hazards such as fires and burns, shock, and chemical exposure. IoT devices might also create additional technology-related hazards associated with the loss of a critical safety function, loss of connectivity, or degradation of data integrity.[9] For example, a car's braking systems might fail when infected with malware,[10] carbon monoxide detectors or fire alarms might stop working with the loss of connectivity,[11] and corrupted or inaccurate data on a medical device might pose health risks to a user of the device.[12] Consumers' physical safety could also be at risk if an intruder had access to a connected lock, garage door, or burglar alarm.

Requiring IoT devices to have perfect security would deter the development of devices that provide consumers with the safety and other benefits discussed above.[13] Conversely, insecure devices can erode consumer trust if consumers cannot rely on the safety and security of

---

workshop-entitled-internet-things-privacy/150127iotrpt.pdf (discussing benefits of the IoT) (Commissioner Wright dissenting and Commissioner Ohlhausen issuing a concurring statement).

[6] *Id.* at 7-8.

[7] *Id.* at 9.

[8] *Id.* at i and 8-9.

[9] CONSUMER PROD. SAFETY COMM'N, POTENTIAL HAZARDS ASSOCIATED WITH EMERGING AND FUTURE TECHNOLOGIES, 16 (Jan. 18, 2017) [hereinafter CPSC EMERGING TECHNOLOGIES REPORT], https://www.cpsc.gov/content/potential-hazards-associated-with-emerging-and-future-technologies (citing potentially new consumer product hazards related to IoT, including loss of safety function, loss of connectivity, and issues related to data integrity).

[10] *See, e.g.*, Jeff Plungis, *Your Car Could Be The Next Ransomware Target*, CONSUMER REPORTS (June 01, 2017), https://www.consumerreports.org/hacking/your-car-could-be-the-next-ransomware-target/. *See also* Catalin Cimpanu, *Volkswagen and Audi Cars Vulnerable to Remote Hacking*, BLEEPINGCOMPUTER (April 30, 2018), https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/ and Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4 M Vehicles For Bug Fix*, WIRED (July 24, 2015), https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[11] *Cf.* Richard Speed, *Three-Hour Outage Renders Nest-Equipped Smart Homes Very Dumb*, THE REGISTER (May 17, 2018), https://www.theregister.co.uk/2018/05/17/nest_outage/ (reporting that an outage in the Nest system left consumers "unable to arm/disarm or lock/unlock" their homes remotely, leaving frustrated consumers to set their alarms and lock their doors manually).

[12] Shaun Sutner, *FDA and UL weigh in on security of medical devices, IoT*, IOT AGENDA, https://internetofthingsagenda.techtarget.com/feature/FDA-and-UL-weigh-in-on-security-of-medical-devices-IoT.

[13] The FTC does not expect perfect security. *See e.g.* Prepared Statement of the Fed. Trade Comm'n, *Protecting Consumer Information: Can Data Breaches be Prevented? Before the Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade, U.S. House of Representatives*, 4 (Feb. 5, 2014), https://energycommerce.house.gov/hearings/protecting-consumer-information-can-data-breaches-be-prevented/ ("[T]he Commission has made clear that it does not require perfect security; that reasonable and appropriate security is a continuous process of assessing and addressing risks; that there is no one-size-fits-all data security program; and that the mere fact that a breach occurred does not mean that a company has violated the law.")

their device.[14] Companies that manufacture and sell IoT devices must take *reasonable* steps to secure them from unauthorized access. Poorly-secured IoT devices create opportunities for attackers to assume device control, opening up risks that may include safety hazards.[15] For example, hackers used the Mirai botnet—composed of IoT devices, such as IP cameras and routers, infected with malicious software—to engage in a distributed denial of service ("DDoS") attack of unprotected residential building management systems in Finland. By blocking Internet access, hackers sent these connected management systems into an endless cycle of rebooting, leaving apartment residents with no central heating in the middle of winter.[16] Also, earlier this year, researchers discovered vulnerabilities in Internet-connected gas station pumps that, when remotely accessed, would allow hackers not only to steal credit card information but also change the temperature and pressure in gas tanks, potentially causing explosions.[17]

Although the request for comment specifically notes that the CPSC "will not address personal data security or privacy implications of IoT devices," security risks associated with IoT devices may implicate broader safety concerns, not just privacy. For example, a criminal who hacks into a connected-home network could not only collect information about consumers who live in the house, but also could activate or deactivate home security devices, potentially causing threats to personal safety.[18] A company setting up a program to address security risks on its IoT device should take measures to secure that device from hackers, for both privacy *and* safety issues. Through this comment, BCP staff shares some of its expertise in promoting IoT device security, and makes certain recommendations to the CPSC. The recommendations focus on three issues: (1) best practices for predicting and mitigating against security hazards; (2) the process for encouraging consumers to register for safety alerts and recall information; and (3) the role of government in IoT security.

II. Background on the FTC

The FTC is an independent administrative agency responsible for protecting consumers and promoting competition. As part of its consumer protection mandate, the FTC enforces a wide range of laws to protect consumers' privacy and security. The primary law enforced by the FTC, the FTC Act, prohibits unfair and deceptive acts or practices in or affecting commerce,

---

[14] *See e.g.* FED. TRADE COMM'N, MOBILE SECURITY UPDATES: UNDERSTANDING THE ISSUES, 1 (Feb. 2018) [hereinafter "MOBILE SECURITY REPORT"], https://www.ftc.gov/reports/mobile-security-updates-understanding-issues; FTC IOT REPORT at 20-21; and Comments of the Staff of the Fed. Trade Comm'n, *In the Matter of Communicating IoT Device Security Update Capability to Improve Transparency for Consumers*, Nat. Telecomm. Info. Admin. (June 19, 2017), https://www.ftc.gov/policy/advocacy/advocacy-filings/2017/06/ftc-comment-national-telecommunications-information.

[15] *Id. See also* Chris Morris, *465,000 Pacemakers Recalled on Hacking Fears*, FORTUNE (Aug. 31, 2017), http://fortune.com/2017/08/31/pacemaker-recall-fda/; and Lisa Vaas, *350,000 Cardiac Devices Need a Security Patch*, NAKED SECURITY (May 4, 2018), https://nakedsecurity.sophos.com/2018/05/04/half-a-million-pacemakers-need-a-security-patch/.

[16] Richard Chirgwin, *Finns Chilling as DDoS Knocks Out Building Control System*, THE REGISTER (Nov. 9, 2016), https://www.theregister.co.uk/2016/11/09/finns_chilling_as_ddos_knocks_out_building_control_system/.

[17] Alfred Ng, *Hackers Should Be Pumped About Gas Station Security Flaws*, CNET (Mar. 12, 2018), https://www.cnet.com/news/gas-stations-online-are-easy-access-for-managers-and-hackers/.

[18] *See e.g.* John Leyden, *Half Baked Security: Hackers Can Hijack Your Smart Aga Oven 'With a Text Message,'* THE REGISTER (April 13, 2017), https://www.theregister.co.uk/2017/04/13/aga_oven_iot_insecurity/.

including unfair and deceptive privacy and security practices.[19] In the context of IoT security, this means that companies should maintain a reasonable security program and keep the promises they make to consumers concerning the security of their devices. The FTC also enforces sector-specific statutes that protect certain health, credit, financial, and children's information, and has issued regulations implementing each of these statutes.[20]

The FTC has used its authority under these laws to protect consumers from insecure IoT devices.[21] For example, in the *TRENDnet* case, the FTC alleged that the company engaged in unfair and deceptive security practices related to its Internet-connected cameras.[22] The complaint alleged that the company's failure to reasonably test and review the camera's software for security problems; failure to encrypt data in storage and transit; and failure to monitor third-party security vulnerability reports led to a breach of private video feeds.[23] Likewise, in the *ASUS* case, the FTC alleged that the company's failure to reasonably secure its routers led to the unauthorized access of consumers' home networks.[24] The FTC's enforcement actions send an important message to companies about the need to secure and protect Internet-connected devices.

The FTC also has pursued numerous policy initiatives designed to enhance device security in an Internet-connected world. For example, the FTC has hosted workshops on the Internet of Things generally,[25] mobile security,[26] drones,[27] connected TVs,[28] ransomware,[29] and

---

[19] 15 U.S.C. § 45. (For an unfair act or practice to violate Section 5 of the FTC Act it must "cause[] or [be] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." Additionally, deception requires a material representation, omission, or practice that is likely to mislead consumers, who are acting reasonably under the circumstances. *See* Fed. Trade Comm'n, *Policy Statement on Deception* (Oct. 14, 1983), https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.)

[20] *See, e.g.*, Health Breach Notification Rule, 16 C.F.R. Part 318 *et seq.* (health information breach notification); Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*. and 16 C.F.R. Part 600 (consumer reporting information security and privacy); Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. Part 314 *et seq*. (financial information security); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501 *et seq*. and 16 C.F.R. Part 312 (children's online information security and privacy).

[21] *See e.g.*, VTech Electronics Ltd., FTC No. 1623032 (Jan 8, 2018) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/162-3032/vtech-electronics-limited; TRENDnet, Inc., No. C-4426 (Feb. 7, 2014) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter; ASUSTeK Computer, Inc., FTC No. 1423156 (Feb. 26, 2016) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter; and VIZIO, Inc., No. 2:17-cv-00758 (Feb. 6, 2017) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc.

[22] TRENDnet, Inc., *supra n. 22.*

[23] *Id*.

[24] ASUSTeK Computer, Inc., *supra n.* 22.

[25] *See generally*, FTC IOT REPORT; *see also* FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY AND SECURITY IN A CONNECTED WORLD (Nov. 19, 2013) (workshop), https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world.

[26] MOBILE SECURITY REPORT at 18.

[27] FED. TRADE COMM'N, FALL TECHNOLOGY SERIES: DRONES (Oct. 13, 2016) (workshop), https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones.

[28] FED. TRADE COMM'N, FALL TECHNOLOGY SERIES: SMART TV (Dec. 7, 2016) (workshop), https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv.

[29] FED. TRADE COMM'N, FALL TECHNOLOGY SERIES: RANSOMWARE (Sept. 7, 2016) (workshop), https://www.ftc.gov/news-events/events-calendar/2016/09/fall-technology-series-ransomware.

connected cars.[30] In its staff report from 2015 on the Internet of Things, the FTC made several recommendations for security best practices, including recommendations that companies conduct risk assessments, test their security measures before launching their products, train employees on security, and monitor products throughout their life cycle.[31] In a more recent report on mobile device updates, the FTC discussed the complex and often time-consuming process that companies face when updating mobile devices.[32] While noting that industry participants have taken steps to streamline the process, the report recommends that manufacturers consider taking additional steps to deliver security updates to user devices faster. It also recommends that manufacturers consider telling users how long a device will receive security updates and when update support is ending.[33]

To encourage consumers to implement security updates, last year the FTC held its *IoT Home Inspector Challenge*, a public competition aimed at spurring the development of security update-related IoT tools.[34] The winning contestant developed a tool to enable users with limited technical expertise to scan their home Wi-Fi and Bluetooth networks to identify and inventory connected devices. The tool would also flag devices with out-of-date software and other common vulnerabilities, and provide instructions to consumers on how to update each of their devices and fix other vulnerabilities.[35]

Finally, the FTC engages in consumer and business education regarding IoT device security. On the business education front, the Commission launched its *Start with Security* initiative,[36] *Stick with Security* blog series,[37] and "*Careful Connections*" IoT guidance,[38] which apply to businesses considering security issues in the IoT space. For example, the Commission's *Careful Connections* guide emphasizes a risk-based approach to device security, encouraging device manufacturers to evaluate the risks to their devices and prioritize the allocation of security

---

[30] FED. TRADE COMM'N, CONNECTED CARS: PRIVACY, SECURITY ISSUES RELATED TO CONNECTED, AUTOMATED VEHICLES (Jun. 28, 2017) (workshop), https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.

[31] *See generally*, FTC IOT REPORT.

[32] *See generally*, MOBILE SECURITY REPORT.

[33] *Id.* at 71-72.

[34] *See* FTC Notice of IoT Home Inspector Challenge, 82 Fed. Reg. 840-2, 840-41 (Jan. 4, 2017), https://www.ftc.gov/system/files/documents/feeral_register_noticies/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

[35] *FTC Announces Winner of its Internet of Things Home Device Security Contest*, Fed. Trade Comm'n (July 26, 2017), https://www.ftc.gov/news-events/press-releases/2017/07/ftc-announces-winner-its-internet-things-home-device-security.

[36] FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015) [hereinafter START WITH SECURITY], https://www.bulkorder.ftc.gov/system/files/publications/pdf0205-startwithsecurity.pdf.

[37] Thomas B. Pahl, *Stick With Security*, FTC BUSINESS BLOG (Sept. 22, 2017), https://www.ftc.gov/news-events/blogs/business-blog/2017/09/stick-security-put-procedures-place-keep-your-security.

[38] FED. TRADE COMM'N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (Jan. 2015) [hereinafter CAREFUL CONNECTIONS], https://www.ftc.gov/system/files/documents/plain-language/pdf0199-carefulconnections-buildingsecurityinternetofthings.pdf.

resources where they are most needed.[39] On the consumer education front, a consumer education blog post describes the 2016 Mirai malware attack, in which the Mirai botnet, as described above, attacked a service used by a number of popular websites like Netflix, PayPal, and Twitter, knocking them offline. The education piece urged consumers to change default settings and passwords and download the latest security updates for their IoT devices.[40]

III. Discussion

The CPSC requests comment on numerous issues. This comment focuses in particular on three: (1) What are some best practices for predicting and mitigating against safety hazards? (2) How can the CPSC encourage consumers to register for safety alerts and recall information? (3) What is the appropriate role of government in IoT security?

A. What are best practices for predicting and mitigating against safety hazards?

The FTC has provided IoT manufacturers with a host of guidance on how to predict and mitigate against privacy, security, and safety hazards. The discussion in this section is premised on the notion that there is no "one size fits all" approach to securing IoT devices. The level of reasonable security will depend on many factors, including the magnitude of potential risks, the likelihood of such risks, and the availability of low-cost tools to address the risks. This comment focuses on guidance in three areas in particular: risk assessment; reasonable vendor oversight for devices and other interdependent products; and software updates, product "expiration" dates, and default settings.

1. Risk Assessment

As the CPSC is well aware, a risk assessment is a starting point for a company to evaluate its security program. A risk assessment can help identify reasonably foreseeable threats and hazards, and solutions for mitigating against such threats and hazards. While the IoT industry is relatively new, companies have been conducting assessments to identity and mitigate against threats and hazards for several years. Companies can build on 20 years of lessons learned by security experts, who have already identified low-cost solutions to some common concerns raised by the Internet of Things.[41]

One example of a reasonably foreseeable risk is that hackers can compromise user credentials to take over an IoT device.[42] The FTC has recommended that companies test

---

[39] CAREFUL CONNECTIONS at 1-2.
[40] Ari Lazarus, *What You Need to Know to Secure Your IoT Devices*, FTC CONSUMER BLOG (Dec. 7, 2016), https://www.consumer.ftc.gov/blog/2016/12/what-you-need-know-secure-your-iot-devices.
[41] *See* CAREFUL CONNECTIONS at 2 (*E.g.* apply standard encryption techniques, apply "salt" to hashed data, and consider rate limiting).
[42] *See* FTC cases concerning the security of credentials, such as Twitter, Inc., FTC No. 0923093 (Mar. 11, 2011) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation; Reed Elsevier, Inc., FTC No. 052094 (Aug. 1, 2008), https://www.ftc.gov/enforcement/cases-proceedings/052-3094/reed-elsevier-inc-seisint-inc-matter; Guidance Software, Inc., FTC No. 0623057 (April 3, 2007), https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation; and Twitter, Inc., FTC No.

authentication techniques and consider whether techniques, such as multi-factor authentication (such as a password and a code sent to a phone) or biometric authentication, are appropriate.[43] The FTC has also recommended that companies consider risks at the point where a service communicates with an IoT device, such as the interface between the device and the cloud.[44] Security experts have long warned against attack vectors such as cross-site scripting attacks, where malicious scripts are injected into otherwise trusted websites, and cross-site request forgery attacks, where unauthorized commands are sent from a user the website trusts.[45]

Finally, the FTC has recommended that companies test a product's security measures before launch. There are readily available, free or cost-effective tools for most basic security testing tasks—network scanning for open ports, reverse engineering of programming code, checking password strength, and vulnerability scans.[46]

2. Service Provider Oversight

While security protections are generally the responsibility of the manufacturer, IoT devices often are a product of components and software from a variety of service providers.[47] Prior to selling their products to consumers, IoT manufacturers should take reasonable measures to evaluate the overall security of those products, including any risks that their service providers might introduce.[48] Companies should provide oversight by exercising due diligence in their selection of service providers, incorporating security standards into their contracts, and taking reasonable steps to verify compliance with those security standards on an ongoing basis.[49]

In circumstances where companies have failed reasonably to oversee the security practices of their service providers, the FTC has taken action.[50] For example, in its case against *BLU Products*, the FTC alleged that a mobile device manufacturer had violated Section 5 of the FTC Act by failing to maintain reasonable security when, among other things, it failed to exercise oversight of its service provider.[51] In part, the FTC alleged that the company did not even put in place basic contractual provisions requiring its service providers to maintain

---

0923093 (Mar. 11, 2011) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/092-3093/twitter-inc-corporation.

[43] CAREFUL CONNECTIONS at 3.

[44] *Id.* at 4.

[45] *Id.* Fuzzing – a testing method that sends a device or system unexpected input data to detect possible defects – is one example of an approach recommended by security experts to addressing these issues as well as discovering other implementation bugs. *See also*, *Fuzzing*, Open Web Application Security Project, https://www.owasp.org/index.php/Fuzzing.

[46] *Id.* at 5.

[47] *Se,e e.g.*, CPSC EMERGING TECHNOLOGIES REPORT at 6.

[48] CAREFUL CONNECTIONS at 1 ("There's no one-size-fits all checklist to guarantee the security of connected devices. What's reasonable will depend on a number of variables, including the kind and amount of information that's collected, the type of functionality involved, and the potential security risks.").

[49] START WITH SECURITY at 11.

[50] BLU Products, FTC No. 1723025 (April 30, 2018) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/172-3025/blu-products-samuel-ohev-zion-matter; Lenovo, Inc., FTC No. 1523134 (Sept. 13, 2017), https://www.ftc.gov/enforcement/cases-proceedings/152-3134/lenovo-inc; and Upromise, Inc., FTC No. 1023116 (April 3, 2012), https://www.ftc.gov/enforcement/cases-proceedings/102-3116/upromise-inc.

[51] BLU Products, *supra* n. 50.

reasonable security. As a result of the company's alleged failures, consumer data was put at an unreasonable risk of unauthorized access. In this case consumers' text message contents, call and text logs, and real-time location were shared with a Chinese service provider that did not have a business need for the information, in violation of the company's privacy policy.[52]

As another example, in the FTC's recent case against *Lenovo*, the Commission alleged that Lenovo preinstalled third-party ad-injecting software on its laptops that created serious security vulnerabilities.[53] The complaint noted that, even after its service provider informed Lenovo of security problems during the development of the software, Lenovo did not seek further information and approved the software's use on Lenovo laptops.[54] This was one factor, among others, cited in the complaint alleging that Lenovo violated Section 5 by failing to implement reasonable security in overseeing its vendors.[55]

3. Ongoing Oversight, Updating, and Patching

The FTC has recommended that companies have an ongoing process to keep up with security practices as threats, safety hazards, technologies, and business models evolve. This involves at least two components.

First, companies should take steps to stay abreast of threats identified in the marketplace by, for example, signing up for email updates from trusted sources; checking free databases of vulnerabilities identified by security researchers; and maintaining a channel through which security researchers can reach out about risks.[56] Indeed, in many cases, the FTC has alleged, among other things, that the failure to maintain an adequate process for receiving and addressing security vulnerability reports from security researchers and academics is an unreasonable practice, in violation of Section 5 of the FTC Act.[57]

Second, companies should take reasonable steps to address threats to privacy, security and safety after launching products, including by issuing updates and patches. In our recently conducted study of mobile security updates, we found that the security update process varies significantly among mobile device manufacturers, and although they have made improvements, bottlenecks remain.[58] We encouraged all actors in the ecosystem to ensure that devices receive security updates for a period of time that is consistent with consumers' reasonable expectations. Such support should be a shared priority, reflected in policies, practices, and contracts among all parties involved in the creation of a device.[59] We also recommended that industry streamline the

---

[52] *Id.*
[53] Lenovo, Inc., *supra* n. 50.
[54] *Id.*
[55] While the BLU and Lenovo cases involve privacy and security, the same types of oversight of service providers would help prevent them from introducing safety hazards into IoT devices.
[56] CAREFUL CONNECTIONS at 7.
[57] *See e.g.* HTC America, FTC No. 1223049 (July 2, 2013) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/122-3049/htc-america-inc-matter; and TRENDnet, Inc. FTC No. 1223090 (Feb. 7, 2014) (complaint), https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.
[58] MOBILE SECURITY REPORT at 65.
[59] *Id.* at 69.

security update process. In particular, we noted that companies should patch vulnerabilities in security-only updates when the benefits of more immediate action outweigh the convenience of a bundling a security update with a functionality update.[60] Finally, we recommended that device manufacturers consider giving consumers more and better information about security update support.[61] Specifically, we recommended that manufacturers interested in providing security update information consider adopting and disclosing minimum guaranteed security support periods (and update frequency) for their devices.[62] We further recommended that they consider giving device owners prompt notice when security support is about to end (and when it has ended), so that consumers can make informed decisions about device replacement or post-support use.[63]

B. How can the CPSC encourage consumers to sign up for safety alert and recall information?

Although manufacturers can update some devices automatically, many devices require consumers to take affirmative steps to install the update. In particular, consumers must know how – and where – to check for security updates and how to install them. As the number of devices within the home multiply, the task of updating devices could become increasingly daunting. As noted above, in 2017, the FTC sponsored a prize competition under the America Competes Act to assist consumers and drive innovation in this area.[64] Encouraging the development of tools that allow consumers to monitor and maintain the security of their personal IoT devices will likely bring more general awareness to the issue, in addition to direct benefits to consumers that adopt those tools.

BCP staff recommends that the CPSC consider how companies might provide consumers with the opportunity to sign up for communications regarding safety notifications and recalls for IoT devices. Such a process could borrow from CPSC's existing process of allowing consumers to sign up for safety notifications regarding infant and toddler products.[65] That process in part requires manufacturers and retailers of durable infant and toddler products to provide consumers with a safety registration card for mail-in registration. The registration card must also include an URL for online registration.[66] Given that consumers purchasing IoT devices necessarily have an Internet connection, however, it is likely that online registration would be a more effective option in the IoT space.[67]

---

[60] *Id.* at 71.
[61] *Id.*
[62] *Id.*
[63] *Id.* at 71-72.
[64] *See* 82 Fed. Reg. 840 (2017).
[65] 74 Fed. Reg. 68677. *See also, Consumer Registration Cards for Durable Infant or Toddler Products*, CONSUMER PROD. SAFETY COMM'N, https://www.cpsc.gov/Business--Manufacturing/Business-Education/Durable-Infant-or-Toddler-Products/Durable-Infant-or-Toddler-Product-Consumer-Registration-Cards/.
[66] *Id.*
[67] For example, some panelists at the CPSC IOT HEARING raised the opportunities for application interfaces, pop-up notifications, and on-device alerts. CONSUMER PROD. SAFETY COMM'N, PUBLIC HEARING ON THE "INTERNET OF THINGS AND CONSUMER PRODUCT HAZARDS," (May 16, 2018) [hereinafter CPSC IOT HEARING], https://www.youtube.com/watch?v=7RdbpJ_eD98. Additionally, many online retailers have a direct

Some consumers may be dissuaded from registering on the expectation that they will receive unwanted marketing communications. Indeed, a recent survey showed that, while many consumers like receiving marketing communications, 12 percent of consumers do not register products because they do not want to share their personal information.[68] BCP staff recommends that, to address potential concerns of these consumers, the CPSC should consider how companies might offer consumers a choice, during the product registration process, about whether they want to receive marketing communications.[69]

C. What is the appropriate role of government in promoting IoT safety?

At the CPSC's IoT hearing, many panelists discussed the value of regulation and IoT-specific standards.[70] Although BCP staff does not take a position on whether or not the CPSC should implement regulations relating to IoT device hazards, to the extent the CPSC considers such regulation, we suggest that any such approach be technology-neutral and sufficiently flexible so that it does not become obsolete as technology changes.

In addition, to the extent that the CPSC considers certification requirements for IoT devices,[71] the CPSC should consider requiring manufacturers to publicly set forth the standards to which they adhere. Such disclosures would improve transparency and provide consumers with information to better evaluate the safety and security of their IoT products. The FTC could use its authority under the FTC Act to take action against companies that misrepresent their security practices in their certifications. This additional tool would provide an enforcement backstop to help ensure that companies comply with their certifications. Examples of enforceable statements to consumers could include statements on websites, on a retail packaging, on the device itself, or in the user interface of the device.

---

relationship with customers and, in some instances, might be in a better position to effectuate notice of safety recalls to purchasers.

[68] *See, e.g., New Study: Millennials and Affluent Consumers Want to Connect with Brands Immediately Post-Purchase via Mobile*, REGISTRIA (April 26, 2017) [hereinafter Registria survey], http://www.marketwired.com/press-release/new-study-millennials-affluent-consumers-want-connect-with-brands-immediately-post-purchase-2212124.htm (Registria also finds that 25 percent of survey respondents cite safety and recall notifications as the most important reason to register their product). *See also, "Should you register that new product? Product-registration cards—and the info you put on them—aren't always needed for warranty coverage,"* CONSUMER REPORTS (Dec. 2013), *available at* https://www.consumerreports.org/cro/2013/12/do-you-need-to-register-new-products-you-buy/index.htm ("When you buy a toaster or TV, or receive one as a gift, is it the manufacturer's business to ask about your income, education, hobbies, and car? Frankly, no. Nevertheless, many products include registration cards harvesting personal information that companies then sell to marketers. The companies get money; you get peppered with spam and sales pitches.").

[69] 15 U.S.C. § 2056 (Consumer Product Safety Standards). *See also, Contact/FAQ*, Consumer Prod. Safety Comm'n, https://www.cpsc.gov/About-CPSC/Contact-Information (discussing the CPSC's authority to develop voluntary standards, issue mandatory standards, and research potential hazards), and *Voluntary Standards*, Consumer Prod. Safety Comm'n, https://www.cpsc.gov/Regulations-Laws--Standards/Voluntary-Standards/ (discussing the development of voluntary standards in collaboration with stakeholders, such as industry groups, government agencies, and consumer groups).

[70] CPSC IOT HEARING, https://www.youtube.com/watch?v=7RdbpJ_eD98.

[71] 83 Fed. Reg. 13122 (Mar. 27, 2018) ("Should certification to appropriate standards be required before IoT devices are allowed in the marketplace?").

IV. Conclusion

BCP staff hopes that this information has been of assistance in furthering CPSC's inquiry into protecting consumers from the hazards associated with Internet-connected devices. The FTC continues to devote substantial resources in this area and looks forward to working with CPSC and other stakeholders to foster competition and innovation in the IoT marketplace while protecting the safety of consumers.