Federal Trade Commission Public Comment on
"Communicating IoT Device Security Update Capability to
Improve Transparency for Consumers"
Communicating Upgradability and Improving Transparency Working Group
Multistakeholder Process on Internet of Things Security Upgradability and Patching
National Telecommunications & Information Administration

I. INTRODUCTION

Thank you for the opportunity to comment on the current draft of "Communicating IoT Device Security Update Capability to Improve Transparency for Consumers" ("Elements of Updatability" or "Elements") from the Communicating Upgradability and Improving Transparency Working Group ("Working Group") at the National Telecommunications & Information Administration ("NTIA").[1]

Internet-connected devices—ranging from light bulbs to smart TVs to wearable fitness trackers—are flourishing. The rapid proliferation of such Internet of Things ("IoT") devices in recent years has been truly remarkable, with an estimated 6.4 billion IoT devices in use in 2016—a 30% increase from 2015.[2] And this trend promises to continue: One market analysis firm estimates that consumers and businesses will use more than eight billion IoT devices in 2017.[3]

This burgeoning marketplace offers enormous benefits to consumers.[4] For example, IoT medical devices track health data that informs patients' diagnosis and treatment.[5] Connected cars offer both safety and convenience benefits, such as real-time notifications of dangerous conditions and smartphone starter and sound-system control.[6] And home IoT devices help consumers to monitor energy use, identify maintenance issues, and remotely control devices such as lights, ovens, and wine cellars.[7] IoT promises many other benefits.

---

[1] NTIA Communicating Upgradability and Improving Transparency Working Group, *Communicating IoT Device Security Update Capability to Improve Transparency for Consumers* (Apr. 25, 2017), https://www.ntia.doc.gov/files/ntia/publications/draft-communicating_iot_security_update_0426.pdf.

[2] Press Release, Gartner, Inc., *Gartner Says 6.4 Billion Connected 'Things' Will Be In Use In 2016, Up 30 Percent from 2015* (Nov. 10, 2015), http://www.gartner.com/newsroom/id/3165317.

[3] *See* Press Release, Gartner, Inc., *Gartner Says 8.4 Billion Connected 'Things' Will Be In Use In 2017, Up 31 Percent from 2016* (Feb. 7, 2017), http://www.gartner.com/newsroom/id/3598917.

[4] *See generally* FED. TRADE COMM'N, FTC STAFF REPORT: INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD, 7-10 (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [hereinafter "FTC Staff IoT Report"] (discussing benefits of the IoT).

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

[6] *Id.* at 9.

[7] *Id.* at i, 8-9 (describing "smart meters" that monitor energy use, "water bugs" that detect flooding in basements, and connected lights, ovens and wine cellars with app-based control).

But such benefits may be delayed or foreclosed if consumers do not trust IoT devices. A fundamental component of building that trust is ensuring that the devices are reasonably secure.[8] Poorly-secured IoT devices create opportunities for attackers to steal data or assume device control, harming both device owners and third parties targeted by ransomware or botnets of "zombie" devices.[9] To combat such threats, security researchers and government agencies have emphasized the importance of taking reasonable steps to design secure products and to maintain their security with updates that patch vulnerabilities in the firmware powering IoT devices.[10] In deciding whether and how to patch devices, manufacturers must balance the benefits of safeguarding against various threats with the considerable costs of developing, testing, and deploying software updates.[11]

As IoT manufacturers weigh these costs and benefits, it is important that consumers have the opportunity to do the same. Providing consumers with clear information about whether, how, for how long, and at what cost their IoT devices will receive security support can benefit consumers, foster competition, and promote innovation in security.

As the nation's consumer protection and competition agency, the Federal Trade Commission ("FTC" or "Commission") is committed to protecting consumers' privacy and security interests while promoting competition. In this role, the FTC has addressed the importance of security update practices generally, and has explored the benefits of and challenges to IoT device security in particular. This comment first highlights lessons learned from the FTC's law enforcement, policy initiatives, and consumer and business education. It then recommends that the Working Group consider certain changes in the proposed Elements of Updatability.

We note that we are providing these comments in an effort to ensure that the best practices articulated in the proposed Elements of Updatability are robust and provide useful information to consumers, without unduly burdening businesses. To that end, each business should evaluate the final version of the Elements and these comments, and apply the

---

[8] The Working Group recognizes the importance of secure design and secure updates, observing in the preamble to the Elements that updates "do not offer complete device protection and are not the sole security measures IoT manufacturers or consumers should take." Elements of Updatability at 1.

[9] *See, e.g.*, FTC Notice of IoT Home Inspector Challenge, 82 Fed. Reg. 840-2, 840-41 (Jan. 4, 2017), https://www.ftc.gov/system/files/documents/federal_register_notices/2017/01/iot_frn_pub_010417_-_2016-31731.pdf [hereinafter "IoT Challenge"].

[10] *See, e.g.*, *id.* at 841; FTC STAFF IOT REPORT, *supra* note 4, at 13-14; DEP'T OF HOMELAND SECURITY, STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS, VERSION 1.0 (Nov. 15, 2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf; Bruce Schneier, *The Internet of Things Is Wildly Insecure — And Often Unpatchable*, WIRED (Jan. 6, 2014), https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem/.

[11] The Working Group is exploring this cost-benefit analysis and has developed a presentation outlining the incentives for and barriers to good patching and updating practices. NTIA Communicating Upgradability and Improving Transparency Working Group, *Incentives and Barriers* (Apr. 26, 2017), https://www.ntia.doc.gov/files/ntia/publications/presentation-incentiveswg_0426.pdf.

recommendations based on each unique product's function, the types of information it collects, its life span, and the costs of conveying any suggested disclosures. Unless otherwise noted, these comments are not intended to provide a template for FTC law enforcement.[12] Rather, they are intended to ensure that the Elements of Updatability reflect the FTC's experience with IoT devices and with consumers' perceptions of disclosures.

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 the privacy and security of consumer data, including the FTC Act, which prohibits "unfair" and "deceptive" acts or practices in or affecting commerce.[13] The FTC also enforces statutes that protect certain health, credit, financial, and children's information, and has issued regulations implementing each of these statutes.[14]

Enforcement is one of the FTC's primary tools for protecting consumers' information. The FTC has brought over 500 privacy and security-related cases,[15] including cases against IoT device manufacturers TrendNet (home security cameras and baby monitors), ASUS (routers), and Vizio (smart TVs).[16] The FTC's enforcement actions send an important message to manufacturers about the need to take reasonable steps to safeguard the privacy and security of

[12] As described below, Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45. The FTC brings enforcement actions where a representation, omission, or practice is likely to mislead consumers acting reasonably under the circumstances. *See* FTC Policy Statement on Deception (Oct. 14, 1983), appended to Cliffdale Assoc., 103 F.T.C. 110, 174 (1984). In addition, the Commission challenges as "unfair" any act or practice that "causes or is likely to cause substantial injury to consumers"; where the injury "is not reasonably avoidable by consumers themselves"; and the injury is "not outweighed by countervailing benefits to consumers or competition." 15 U.S.C. § 45(n).

[13] 15 U.S.C. § 45(a). *See generally* FED. TRADE COMM'N, PRIVACY & DATA SECURITY UPDATE: 2016, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2016/privacy_and_data_security_update_2016_web.pdf.

[14] *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 412 (children's online information security and privacy).

[15] *See* Prepared Statement of the Federal Trade Commission On "Examining the Proposed FCC Privacy Rules," Presented by Chairwoman Edith Ramirez and Commissioner Maureen K. Ohlhausen, Subcomm. on Privacy, Tech. & the Law of the Comm. on the Judiciary, U.S. Senate, at 3 (May 11, 2016), https://www.ftc.gov/public-statements/2016/05/prepared-statement-federal-trade-commission-examining-proposed-fcc-privacy.

[16] Vizio, Inc., No. 2:17-cv-00758 (Feb. 6, 2017) (decision and order); ASUSTeK Computer Inc., No. 142 356 (F.T.C. July 18, 2016) (decision and order); TRENDnet, Inc., No. 122 3090 (F.T.C. Jan. 16, 2014) (decision and order).

IoT devices.[17] At the same time, the FTC has recognized that there is no such thing as perfect security. Rather, security is a continuous process of risk management.

Enforcement is not the agency's only tool to protect consumer privacy and data security. The Commission has also undertaken numerous policy initiatives to explore privacy and data security issues related to the IoT. For example, the FTC hosted an IoT workshop and issued a report.[18] That report detailed specific challenges to updating IoT devices, such as hardware limitations, lack of consumer awareness, and economic pressure to focus on manufacturing rather than support.[19] Last year, Commission staff filed a comment with the NTIA that recommended best practices for IoT manufacturers, such as informing consumers of the security support period for their IoT devices.[20] More recently, the FTC hosted workshops exploring the privacy and security implications of specific IoT devices (drones and smart TVs).[21] In January of this year, the Commission announced an "IoT Home Inspector Challenge," a public competition aimed at creating tools (like security update wizards) to protect IoT devices in consumer homes.[22] In a related initiative, later this year, the Commission will be issuing a report on security update practices for mobile devices (arguably the most mature IoT product market), based on information that the Commission has collected from eight mobile device manufacturers.[23]

In addition to these enforcement actions and policy initiatives, the FTC educates consumers and businesses through published guidance and posts on its business and consumer

---

[17] Several of the Commission's consent orders have specifically required companies to issue security updates and/or clearly and conspicuously notify consumers about available updates. *See, e.g.*, HTC America, Inc., No. 122 3049, at 4 (F.T.C. June 25, 2013) (decision and order); ASUSTeK, *supra* note 16, at 6-7; Oracle Corp., No. 132 3115, at 3-4 (F.T.C. Mar. 28, 2016) (decision and order).

[18] *See* Transcript, Fed. Trade Comm'n, Internet of Things: Privacy and Security in a Connected World (Nov. 19, 2013), https://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf; FTC STAFF IOT REPORT, *supra* note 4.

[19] FTC STAFF IOT REPORT, *supra* note 4, at 13-14.

[20] In addition, the staff comment offered observations regarding how interoperability and standardization could impact competition and consumer welfare. *See* Comments of the Staff of the Fed. Trade Comm'n, *In the Matter of The Benefits, Challenges, and Potential Role for the Government in Fostering the Advancement of the Internet of Things*, NTIA Docket No. 160331306-6306-01 (June 2, 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-staff-bureau-consumer-protection-office-policy-planning-national-telecommunications/160603ntiacomment.pdf.

[21] Event Notice, Fed. Trade Comm'n, *Fall Technology Series: Drones* (Oct. 13, 2016), https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones; Event Notice, Fed. Trade Comm'n, *Fall Technology Series: SmartTV* (Dec. 7, 2016), https://www.ftc.gov/news-events/audio-video/video/fall-technology-series-smart-tv-part-1.

[22] *See* IoT Challenge, *supra* note 9.

[23] Press Release, Fed. Trade Comm'n, *FTC To Study Mobile Device Industry's Security Update Practices* (May 9, 2016), https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices. This report will build on the Commission's prior work regarding mobile security updates for mobile devices, including its consent order with mobile device manufacturer HTC America that required the company to patch vulnerable devices and provide consumers with clear and prominent patching notice and instructions. *See supra* note 17.

blogs. For example, the Commission's business education guide, "Start with Security," describes data security fundamentals, such as implementing a process for regularly updating software.[24] The FTC also held four workshops in San Francisco, Austin, Seattle, and Chicago to promote the "Start with Security" principles.[25] The Commission's "Careful Connections" guidance addresses IoT device manufacturers specifically, advising them to consider in advance how they will update devices and notify customers of available updates.[26] And, a recent consumer education blog post described the infamous 2016 Mirai malware attack (in which a botnet of compromised IoT devices attacked popular websites like Netflix, PayPal, and Twitter) and urged consumers to change default settings and passwords and download the latest security updates for their IoT devices.[27]

In some cases the FTC issues specific guidance to companies in lieu of enforcement. Last year, the FTC sent a closing letter to IoT manufacturer Nest regarding its decision to cut off support for the Revolv Smart Home Hub less than eighteen months after it had been sold to consumers.[28] In that case, the FTC declined enforcement because of (1) the limited number of devices sold; (2) the company's decision to offer full refunds to all purchasers; and (3) the company's prominent promotion of its refund policy.[29]

III. RECOMMENDATIONS

As a preliminary matter, the Commission commends the inclusive voluntary multistakeholder process in which industry, government, and consumer representatives have developed the Elements of Updatability.[30] Stakeholders have worked together collaboratively to identify flexible best practices that can provide important guidance for companies that have

---

[24] FED. TRADE COMM'N, START WITH SECURITY: A GUIDE FOR BUSINESS (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business ("Outdated software undermines security. The solution is to update it regularly . . . . [H]aving a reasonable process in place to update and patch third party software is an important step to reducing the risk of a compromise.").

[25] *See, e.g.*, Event Notice, Fed. Trade Comm'n, *Start with Security – Chicago* (June 15, 2016), https://www.ftc.gov/news-events/events-calendar/2016/06/start-security-chicago.

[26] FED. TRADE COMM'N, CAREFUL CONNECTIONS: BUILDING SECURITY IN THE INTERNET OF THINGS (Jan. 2015), https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-building-security-internet-things (advising IoT manufacturers to consider the following questions: "How will you provide updates for products that are already out there? Will you offer them for free? Will updates happen automatically?").

[27] Ari Lazarus, *What You Need to Know to Secure your IoT Devices*, Fed. Trade Comm'n Consumer Blog (Dec. 7, 2016), https://www.consumer.ftc.gov/blog/what-you-need-know-secure-your-iot-devices.

[28] Letter from Mary Engle to Richard J. Lutton, Jr. re: Nest Labs, Inc., FTC File No. 162-3119 (Jul. 7, 2016), https://www.ftc.gov/system/files/documents/closing_letters/nid/160707nestrevolvletter.pdf [hereinafter "Nest Closing Letter"].

[29] *See id.*; *see also* Jessica Rich, *What happens when the sun sets on a smart product?*, Fed. Trade Comm'n, Business Blog (Jul. 13, 2016), https://www.ftc.gov/news-events/blogs/business-blog/2016/07/what-happens-when-sun-sets-smart-product.

[30] *See* Background, Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching, NTIA, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security (describing voluntary multistakeholder process used to develop guidelines).

questions about how to implement security updates and how best to inform consumers about them. Voluntary, consensus-based guidelines developed through such processes can have a strong advantage over government regulation in that they can be adapted to specific circumstances and can be updated relatively easily over time.

The Elements of Updatability divides its guidance into two categories: (1) "key elements" that IoT device manufacturers should convey to consumers, before sale, to facilitate informed purchasing decisions; and (2) "additional elements" manufacturers should communicate to consumers either pre- or post-purchase.

The Commission agrees that providing consumers with certain security-related information can empower their purchasing and use decisions, and the Commission commends the Working Group for identifying such elements. At the same time, we note that effective notification is difficult to get right. Poor disclosures, including overly extensive disclosures, can actually impede consumers' ability to make informed choices.[31] One straightforward way to reduce harm from this problem is to minimize the need for disclosures by providing secure products that receive automatic security updates during the device's reasonable lifespan.[32] If manufacturers do offer choices about security updates, they should carefully evaluate the effectiveness of their disclosures.[33]

In this Section, the Commission recommends supplementing the proposed Elements of Updatability, in several ways. First, this Section agrees that consumers would benefit from pre-sale communication of clear, actionable information about support period and the effect of support curtailment, but recommends certain adjustments to the "key elements." Second, it suggests modifying the "additional elements" that can be disclosed before or after sale. Finally, it recommends omitting guidance about informing consumers of update process security, in order to reduce the communication burden on industry and minimize the likelihood of overwhelming consumers with information not central to their role in preserving the device's security.

---

[31] *See, e.g.*, Jim Bettman, et al., *Consumer Decision Making*, Handbook of Consumer Behavior 50–84 (Thomas S. Robertson, *et al*., eds.) (1991) (providing overview of consumer decision making, including overload); Naresh K. Malhotra, *Information Load and Consumer Decision Making*, Journal of Consumer Research 8, Mar. 1982, at 419–430 (same); Debra L. Scammon, *Information Load and Consumers*, Journal of Consumer Research 4 (3), 1977, at 148–155 (same); Brian Stanton, *et al*., *Security Fatigue*, IT Professional 18, Sept.-Oct. 2016, at 26-32 (reporting that "decision fatigue" made respondents more likely to use poor security practices).

[32] If automatic security updates require any users action (*e.g.*, affirmative user acceptance of an update), the manufacturer should, per Element A.2, inform consumers of what action is required.

[33] FTC research has shown that effective disclosure is possible, but can take significant work to do well. *See, e.g.*, Jim Lacko & Jan Pappalardo, *Improving Consumer Mortgage Disclosures*, FTC Bureau of Economic Staff Report (2007), https://www.ftc.gov/sites/default/files/documents/reports/improving-consumer-mortgage-disclosures-empirical-assessment-current-and-prototype-disclosure-forms/p025505mortgagedisclosurereport.pdf (discussing effective disclosures in the context of consumer mortgages).

A. Recommendations for Supplementing the Key Elements that Manufacturers Should Consider Communicating to Consumers Prior to Purchase

The Elements of Updatability suggest that companies disclose three key elements before sale: (1) whether the device can receive security updates; (2) how the device receives security updates; and (3) the anticipated timeline for the end of security support. The Commission agrees that providing such information before sale would help consumers to meaningfully evaluate and compare IoT devices' security. But the Commission recommends adjusting the third element (support timeline) and adding a fourth element (key use limitations).

First, when describing support period, manufacturers should consider whether they can disclose a *minimum* security support period in addition to, or instead of, an "anticipated timeline" for support. In the Commission's experience, aspirational claims can mislead consumers under certain circumstances. It is possible, for example, that consumers would perceive a statement that a company "anticipates" supporting a device for, say, 30 months as a *guarantee* of the full 30 months of support (or otherwise misconstrue an "anticipates" disclosure). In that case, curtailing support prior to the anticipated time could injure any consumer who relied on that anticipated timeline at the time of purchase. By contrast, disclosing a guaranteed minimum support period would give consumers clear, concrete information with which to compare devices.[34] And providing a minimum support period with an anticipated timeline would clarify the timeline's conditional nature.

The Commission agrees with the Working Group that when providing a support period, consumers would benefit most from knowing the specific date on which support will stop (*e.g.*, Jan. 1, 2025).[35] The Commission recommends, however, that manufacturers who opt to describe a general time period (*e.g.*, two years of support) inform consumers *when* that support clock starts (or started). Without a start time, a consumer may buy a device expecting the full support period, even if the clock started much earlier. For example, a consumer expecting two years of security support from the date of purchase may only receive one year of support if the clock started at the time of the product's initial market release, a year earlier. For this reason, any company describing a general time period should also state the support start date or, preferably, the support end date.

---

[34] Manufacturers should also disclose any stand-alone costs associated with the minimum support period before purchase. If manufacturers know the cost of extended support at the point of sale, they should communicate that information as well, so that consumers understand the total cost of their purchase. *Cf.* Comments of the Fed. Trade Comm'n, *In re: Consumer Information and Disclosure*, CG Docket No. 09-158, at 2-8, Fed. Comm. Comm'n, https://www.ftc.gov/sites/default/files/documents/advocacy_documents/ftc-comment-federal-communications-commission-concerning-consumer-information-and-disclosure/v100000consumerinfocomments.pdf (recommending that price advertisements reflect the total price the consumer actually pays, to avoid confusing customers about a material fact).

[35] Participants in the April 26th multistakeholder meeting on the draft Elements raised this point. *See* Agenda, NTIA Multistakeholder Process, Internet of Things (IoT) Security Upgradability and Patching (April 26, 2017), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

Finally, the Commission recommends that if a "smart" device will stop functioning or become highly vulnerable when security support ends, and if consumers would expect a similar "dumb" device to have a longer, safer lifespan, then manufacturers should disclose those key use limitations to consumers prior to purchase.[36] In some cases, such disclosures may be necessary to prevent consumer injury. FTC staff has stated that "unilaterally rendering [] devices inoperable" contrary to consumers' reasonable expectations "would cause unjustified, substantial consumer injury that consumers themselves could not reasonably avoid."[37] With respect to the IoT, consumers may not expect a largely mechanical device, like a refrigerator or a toaster, to suddenly lose basic functionality because of lapsed support, when that support is significantly shorter than the expected life of a similar "dumb" product. To the contrary, in some cases, a consumer may reasonably expect an unsupported "smart" device to fail in such a way that it continues to perform its basic mechanical function (*i.e.*, "fail dumb"). For example, consumers may reasonably expect that if a smart toaster loses connectivity or the ability to be activated through an app once security support ceases, it would still function as a conventional toaster. A pre-purchase disclosure that the toaster will stop working when support ends on *x* date would avoid deceiving consumers about this key use limitation.

B. Recommendations for Additional Elements that Manufacturers Should Consider Communicating to Consumers Before or After Purchase

The Elements of Updatability identify "additional elements" that manufacturers should consider communicating to consumers before or after purchase. The Commission recommends certain additional considerations.

First, manufacturers should consider adopting a uniform notification method (*e.g.*, a standard position on the device's screen or in the notification center of the device-related app). Security researchers have identified a formidable obstacle to updating IoT devices: consumers often remain unaware of the updates, particularly when the only way to find an update is for the user to actively search the manufacturer's website.[38] As noted above, providing automatic updates may be the best way to avoid this problem. Absent automatic updates, adoption of an

---

[36] The guidance currently recommends that manufacturers disclose this fact, along with other information about what happens when a device no longer receives support, either before or after purchase (per Element B.2). While a manufacturer may want to describe certain information, such as extended support plans, after purchase, manufacturers should describe key use limitations prior to purchase, for the reasons described below.

[37] *See* Nest Closing Letter, *supra* note 28, at 2. *See also* Letter from Mary Engle to Randal M. Shaheen re: MLB Advanced Media, L.P., FTC File No. 082-3043 (Oct. 9, 2008), https://www.ftc.gov/sites/default/files/documents/closing_letters/mlb-advanced-media-l.p./081009mlbamclosingletter.pdf (observing that companies must provide consumers with sufficient information to convey the "inherent limitations on the use of the products they buy") (quoting FED. TRADE COMM'N, PROTECTING CONSUMERS IN THE NEXT TECH-ADE: A REPORT BY THE STAFF OF THE FEDERAL TRADE COMMISSION, at 16 (Spring 2008), https://www.ftc.gov/sites/default/files/documents/reports/protecting-consumers-next-tech-ade-report-staff-federal-trade-commission/p064101tech.pdf).

[38] *See, e.g.*, FTC STAFF IOT REPORT, *supra* note 4, at 13 n. 56 (citing Kashmir Hill, *'Baby Monitor Hack' Could Happen To 40,000 Other Foscam Users*, FORBES (Aug. 27, 2013), www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/; IoT Challenge, *supra* note 9, at 840-41.

easy-to-find, standardized notification method would facilitate consumer awareness initiatives and help purchasers efficiently locate updates.

Second, manufacturers should consider enabling consumers to sign up, either at the point-of-sale or after, for affirmative notifications about security support (separate from marketing communications, which might deter consumers from agreeing to receive such information). Manufacturers could use this contact information not only to notify device owners of updates during the support period, but also to notify owners of devices that no longer receive security support of particularly critical security threats. Such notifications could apprise consumers of security risks and steps to reduce risks (*e.g.*, change passwords and default settings when first enabled or remove them from network access when security support ends).

Finally, to build on a point made in the previous paragraph, manufacturers should consider providing consumers with real-time notifications *when* support is about to end (which could be communicated through the uniform notification method, a push notification on a device-related app, or by the opt-in described above). Prompt notification that security support will end soon would enable consumers to make better informed choices about how to mitigate risk stemming from the end of security support. Some consumers may choose to find alternative support, or simply to forgo support; but for some consumers, an end-of-life notification would prompt device replacement.[39]

C. Recommendation to Omit the Description of How the Manufacturer Secures Updates and the Update Process

We recommend that the Working Group omit the final "additional element," a description of how the manufacturer secures updates and the update process. When providing updates, manufacturers must, of course, ensure that the process is reasonably secure.[40] Explaining those safeguards to consumers, however, imposes significant communication costs on industry while providing little, if any, benefit to consumers. Specifically, manufacturers following this guidance would be obliged to undertake the difficult task of "balancing clarity and ease of understanding with completeness" on what many consumers may view as an arcane topic.[41] Moreover, communicating this information may actually undermine the efficacy of other update-related communications. As noted *supra* at 6, the more extraneous information consumers receive, the more likely they are to feel overburdened by choice and ignore critical

[39] As noted *supra* at 8, such notifications should *not* be marketing communications, which may deter consumers from agreeing to receive security notifications. In addition, manufacturers that do not provide automatic security updates should consider disclosing their security update schedule, so that consumers know when to look for security updates. Indeed, in some contexts, such as the smartphone market, disclosure of update frequency has become an important point of comparison for security-focused purchasers. *See, e.g.*, Overview, Blackberry Mobile, http://www.blackberrymobile.com/us/ (last visited May 15, 2017) ("Best-in-class monthly Android security updates"); Security Blog, Samsung Mobile, http://security.samsungmobile.com/introsm.html (last visited May 15, 2015) (identifying devices that receive monthly and quarterly updates).

[40] *See supra* at 2 (describing the importance of reasonable security measures).

[41] *See* Elements of Updatability, at 4.

information.[42] For these reasons, we recommend that the Working Group exclude this element from its guidance.

IV. CONCLUSION

Thank you again to NTIA and all of the stakeholders that contributed to this process. The FTC continues to devote substantial resources in this area and looks forward to working with NTIA to foster competition and innovation in the IoT marketplace while protecting consumers.

[42] *See supra* note 31 (describing consumer "decision fatigue" when presented with too much information).