Consumer Federation of America

May 2, 2018

Testimony of Rachel Weintraub,

Legislative Director and General Counsel, Consumer

Federation of America and

Susan Grant,

Director of Privacy and Consumer Protection, Consumer

Federation of America

Before the

U.S. Consumer Product Safety Commission

Hearing

The Internet of Things and Consumer Product Hazards

Consumer Federation of America (CFA), an association of nearly 300 nonprofit consumer organizations across the United States, welcomes the request by the Consumer Product Safety Commission (CPSC) for public input about the potential safety issues and hazards associated with internet-connected consumer products and how they should be addressed.[1] The research firm Gartner estimated that by the end of 2017 there would be 8.4 billion "connected things" in use worldwide, of which more than 5 billion would be consumer applications, and that by the year 2020 these numbers will have more than doubled.[2]

In an article,[3] Bruce Schneirer, a cyber security expert, wrote, "With the advent of the Internet of Things and cyberphysical systems in general, we've given the internet hands and feet: the ability to directly affect the physical world. What used to be attacks against data and information have become attacks against flesh, steel and concrete." We are concerned that these attacks against flesh, steel and concrete can lead to product safety injuries and deaths and property damage.

---

[1] U.S. Consumer Product Safety Commission, The Internet of Things and Product Safety Hazards, Notice of public hearing and request for written comments, Vol. 83 No. 59 Fed. Reg. 13122 (March 27, 2018), *available at* https://www.gpo.gov/fdsys/pkg/FR-2018-03-27/pdf/2018-06067.pdf

[2] Press release February 7, 2017, *available at* https://www.gartner.com/newsroom/id/3598917.

[3] Bruce Schneirer, Motherboard, "The Internet of Things Will Turn Large-Scale Hacks into Real World Disasters," July 25, 2016, *available at* https://motherboard.vice.com/en_us/article/qkjzwp/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster

While the Internet of Things (IoT) offers many potential benefits for consumers, there are many concerns as well, including concerns about safety and security. To give consumers confidence in using connected products, ensure their well-being, and reduce risks posed by connected products, it is crucial for policymakers to put adequate protections in place.

Internet of Things Safety Concerns

The January 2017 CPSC staff report, *Potential Hazards Associated with Emerging and Future Technologies*, noted the advantages for consumers of home-based smart appliances, alarm systems, thermostats, medication monitors and other connected devices, but also pointed out that these products may have little internal security or could have defects that pose hazards:

> Each smart device represents an opening to hackers or software failures that can interfere with the device's basic operation. One potential hazard is that a homeowner may believe that an alarm is seemingly functional, yet through software bugs or intentional interference, the safety device is not responsive to conditions like rising CO levels, and does not alert the household.[4]

Of course, it is not only a device such as an alarm or a monitor ceasing to function that could create a safety hazard; if a connected device starts operating when it should not due to a software defect or intentional interference – for instance, an oven, toaster, or coffee machine turning on and overheating – it could cause a fire or other serious damage.

The risk of injury due to software defects is not a new problem. For instance, the Food and Drug Administration (FDA) issued recalls for MedTronic devices in 2004, 2012, and 2016 because of software issues that led to patient overdoses, resulting in harm and even deaths.[5] The potential for hacking with Internet of Things (IoT) devices, however, presents another set of risks entirely. The decision to disconnect the wireless functionality of Vice President Cheney's pacemaker because of fear that terrorists might hack it vividly illustrates this problem.[6] Last year's massive "WannaCry" hacking attack that, among other things, disabled hospital computer systems in the UK, forcing them to turn patients away, is a good example of how software vulnerabilities can be exploited, whether for financial gain, as it was in that case, or for other motives.[7] In another example, the Mirai malware has been used to turn connected home devices such as "smart TVs" into "botnets" for a variety of malicious purposes.[8] Just as consumers' devices can be taken over to launch denial of service attacks against websites, send spam or extort ransoms, so could they

---

[4] https://www.cpsc.gov/s3fs-public/Report%20on%20Emerging%20Consumer%20Products%20and%20Technologies_FINAL.pdf at 5.
[5] *See* recall notices at https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRES/res.cfm?id=34649, https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRes/res.cfm?id=107986 and https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfRes/res.cfm?id=150480
[6] *See* Washington Post, "Yes, terrorists could have hacked Dick Cheney's heart" October 21, 2013, https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/?utm_term=.b9d6abbc8fa2.
[7] *See* Bloomberg, "Extortionists Mount Global Hacking Attack Seeking Ransom" May 12, 2017, https://www.bloomberg.com/news/articles/2017-05-12/patients-turned-away-as-british-hospitals-hit-by-cyber-attack
[8] *See* Hacker News, "Three Hackers Plead Guilty to Creating IoT-based Mirai DDOS Botnet," December 13, 2017, https://thehackernews.com/2017/12/hacker-ddos-mirai-botnet.html.

be employed in ways that could result in physical injury, such as causing connected medical equipment to stop functioning.

Wearable devices such as activity trackers and smartwatches constitute another serious area of concern, especially given their popularity and wide use. The CPSC staff report noted the potential for burns, skin irritations, hearing damage and other physical harms that may be caused by wearables.[9]

The CPSC staff report also cited concerns that electronic disturbances could prevent connected products from operating properly as designed.[10] A paper[11] about product safety and the IoT recently released by the Organization for Economic Cooperation and Development (OECD) cited this and other points made in the CPSC staff report and outlined many other potential safety risks. For instance, lack of implementing software updates could affect the operation or security of connected products; "planned obsolescence" may affect how the products function or cause them to stop operating entirely; data used by the connected products could be incorrect or become corrupted, affecting their operation; and augmented reality applications may miss-identify an object in the real world, causing a human to act contrary to his or her safety. In addition, the paper notes that connected devices could distract consumers, causing injury, and that consumers could rely on information provided by a device in error and injure themselves or others as result.

To that point, the incident involving the Uber self-driving car that struck and killed a pedestrian in Arizona is instructive.[12] We do not know yet exactly what caused the car not to respond appropriately to the person who was walking across the road in front of it, but clearly the "safety operator" placed too much reliance on the autonomous driving system to prevent the deadly incident. As a result of the crash, Uber has temporarily ceased its self-driving car program and questions[13] are being raised in many quarters about what should be done to ensure that self-driving technology is safe.

In our view, the collection and use of personal data from connected devices also raises safety concerns. We note that the CSPC's Federal Register notice[14] about this IoT proceeding says "We do not consider personal data security and privacy issues that may be related to IoT devices to be consumer product hazards that CPSC would address." Yet, the CPSC's staff report cites as one of the risks of wearable devices the fact that they may collect sensitive personal data, from

---

[9] *Supra* at 7.
[10] *Supra* at 5.
[11] OECD (2018), "Consumer product safety in the Internet of Things," *OECD Digital Economy Papers*, No. 267, OECD Publishing, Paris, http://dx.doi.org/10.1787/7c45fa66-en.
[12] *See* Jim McPherson, "How Uber's Self-Driving Technology Could have Failed in the Fatal Tempe Crash," Forbes March 20, 2018, https://www.forbes.com/sites/jimmcpherson/2018/03/20/uber-autonomous-crash-death/#6bf9c10a7fbe
[13] *See* Dan Lohrmann, "After Crash: Tough Questions to Consider on Autonomous Vehicles," Government Technology March 25, 2018, http://www.govtech.com/blogs/lohrmann-on-cybersecurity/after-crash-tough-questions-to-consider-on-autonomous-vehicles.html.
[14] https://www.federalregister.gov/documents/2018/03/27/2018-06067/the-internet-of-things-and-consumer-product-hazards.

health-related information to the GPS location of children.[15] We believe that this is a valid safety concern for the CPSC to consider.

Last year CFA and other consumer organizations asked the Federal Trade Commission (FTC) to investigate after research commissioned by the Norwegian Consumer Council revealed that certain smartwatches that are promoted to help parents monitor their children and keep them safe can actually expose them to privacy and security harms, including enabling strangers to communicate with them and track their locations.[16] Among other risks, this could obviously result in physical harm to children. As connected devices proliferate, these types of privacy and security problems in the digital world will increasingly impact consumers' safety in the physical world.

Earlier this month the FTC warned two of the companies that market the smartwatches that they may be violating the Children's Online Privacy Protection Act which, among other things, requires parental consent for websites and online services to collect, use or share personal data about children and to keep that data secure. It is worth noting, however, that the FTC would need to seek an injunction to stop the sale of these devices until these issues are resolved, a step that it has not taken. Furthermore, the agency cannot issue product recalls or adopt mandatory security standards.

Policy Solutions

There are resources from the public and private sector to encourage good practices concerning designing and deploying connected devices. For instance, the Online Trust Alliance, originally formed as an industry working group and now an initiative of the Internet Society, has published an IoT "Trust Framework" and other materials which cover, among other things, security considerations for connected devices.[17] On the government side, the Interagency International Cybersecurity Standardization Working Group recently issued the *Draft NISTIR 8200 Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)*.[18] Its purpose is to "inform and enable policymakers, managers, and standards participants as they seek timely development of and use of cybersecurity standards in IoT components, systems, and services."

While best practices and voluntary standards are helpful, they may not be adequate to protect consumers from the potential safety risks of using connected devices. As noted in the OECD paper, the IoT raises questions about whether current product safety and product liability laws need to be rethought.[19] In particular, the report cites three policy challenges: the impact of the IoT on distinctions between hardware and software, products and services; the question of liability, and communicating safety to consumers.

---

[15] *Supra* at 6 and 7.
[16] *See* press release at https://consumerfed.org/press_release/smartwatches-parents-safeguard-children-put-risk/
[17] *See* https://otalliance.org/initiatives/internet-things.
[18] *See* https://csrc.nist.gov/publications/detail/nistir/8200/draft.
[19] *Supra* starting at 21.

On the issue of liability, the Center for Democracy & Technology (CDT) recently published a paper, *Strict Product Liability and the Internet of Things*,[20] which posits that while strict product liability has not tended to be applied to designers, manufacturers or retailers of digital products because their failure is usually limited to economic harm, the failure of IoT products is more likely to result in property damage or physical harm. The paper explores the reasons why market forces have not incentivized the security of digital technologies and the public policy options to address the issue.

Last year, Consumers International (CI), an association of nonprofit consumer organizations around the world, issued principles and recommendations for fostering consumer trust in the IoT.[21] Among other things, CI called for the concept of "safety" in general and sector-specific product safety legislation to be broadened to reflect new cybersecurity, data protection and product safety concerns, as well as the development of international standards and the adoption of best practices. On liability, CI recommended a new approach that would include a clear and robust product liability framework that protects consumers if they suffer damage caused by connected products or service, clear information about who is responsible, and rules that ensure that consumers are fully compensated if they are harmed.

In addition, CI made a number of recommendations to address the issue of connected devices being obsolete, including that they should be easily upgradable and, as far as possible, making devices, adaptors and other connection points compatible with each other to reduce the potential for new interfaces to render them unusable.

In December of 2016, the Office of Oversight and Investigations, Minority Staff, issued a report: *Children's Connected Toys: Data Security and Privacy Concerns*.[22] The report found that "connected toys" offer many promising applications to children but also "raises serious privacy and data security concerns."[23] While the concerns raised are focused on risks to children's privacy, including risks that could lead to physical threats, the report documents the unequivocal responsibility that the manufacturers of connected toys have to address these concerns and a failure to secure consumer data. Relevant to CPSC's request for written comments, we urge the manufacturers of connected products to address these and other product safety threats at the initial stages of the design process.

---

[20] Benjamin C. Dean, CDT, April 2018, *available at* https://cdt.org/files/2018/04/2018-04-16-IoT-Strict-Products-Liability-FNL.pdf.

[21] Consumers International, *Securing Consumer Trust in the Internet of Things*, 2017, *available at* https://www.consumersinternational.org/media/154809/iot-principles_v2.pdf.

[22] Office of Oversight and Investigations, Minority Staff Report: Children's Connected Toys: Data Security and Privacy Concerns, available online at https://www.commerce.senate.gov/public/_cache/files/c9edea45-05a2-42ab-a9e4-22e5db7bc0ed/8B6F6A6FDCD06F07DE4352BE4505824D.12.14.16-ranking-member-nelson-report-on-connected-toys.pdf

[23] *Ibid* at 1.

Recommendations

Voluntary and Mandatory Standards

Product safety risks posed by connected products should be addressed as early as possible in the design of the products. Manufacturers of connected products must show the same commitment to addressing product risks regardless of whether the cause is due to a software, hardware, or other design defect. While mandatory standards are often preferable because they are enforceable, existing voluntary or mandatory standards can be updated to include the unique product safety risks posed by connected products. For example, ASTM F-963, which has been codified by the CPSC as a mandatory standard could be strengthened to include hazards posed by connected toys.

Interagency Working Group

In addition to updating existing voluntary and mandatory standards, strengthening product liability laws, and having meaningful and effective manufacturer codes of conduct, we urge the CPSC to create an Interagency Working Group with the Federal Trade Commission and any other agency that shares jurisdiction over connected products. The Interagency Working Group should have clear goals, clear deadlines, and a commitment to effectively address the risks posed by connected products. As an initial goal, within six months of its creation the Interagency Working Group should prepare a document that it will submit to Congress and make publicly available, which would:

- Describe the harms posed by connected products;
- Outline each agency's jurisdiction and authority to address these issues;
- Provide information about the actions taken thus far by each agency to address the risks posed by these products;
- Report on whether existing voluntary efforts are keeping pace with the growth of connected products and the risks they pose to consumers; and
- Make recommendations for any additional authority and resources that are needed to better address these hazards.

The public would benefit from the sharing of agency expertise and knowledge and from a joint commitment to addressing the risks posed by connected products.

Conclusion

We appreciate that the CPSC is holding this hearing on the Internet of Things and Consumer Product Hazards. We urge the agency to use its existing authority to address product safety risks posed by connected products, to engage with voluntary standards organizations to address these issues through updating existing standards to address the specific risks posed by connected products, and to work closely and concretely with other agencies that share jurisdiction over connected products, such as the FTC and the FDA, to address product safety risks posed by connected products.