CENTER FOR DATA INNOVATION

June 15, 2018

Alberta Mills, Office of the Secretary
Patricia Adair, Office of Hazard Identification and Reduction
Consumer Product Safety Commission
4330 East-West Highway
Bethesda, MD 20814

Dear Ms. Mills and Ms. Adair,

On behalf of the Center for Data Innovation (datainnovation.org), we are pleased to submit comments in response to the Consumer Product Safety Commission's (CPSC's) request for comments on the Internet of Things and consumer product hazards.[1]

The Center for Data Innovation is the leading think tank studying the intersection of data, technology, and public policy. With staff in Washington, D.C., and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The Center is a non-profit, non-partisan research institute affiliated with the Information Technology and Innovation Foundation.

The Internet of Things (IoT) is a term used to describe the set of physical objects embedded with sensors or actuators and connected to a network, which can include everything from intelligent home devices to smart factories to connected cars. Many consumer devices make up the Internet of Things, including health and fitness wearables, smart appliances for the home, and even gadgets for pets. Some of these devices present safety risks to consumers—as any electronic device might. However, these products may also include cybersecurity risks which can expose consumers to new safety concerns. For example, a hacked smart lock could provide criminals access to a home or property, a malware on a smart home appliance could overheat to the point of causing a fire, and a security vulnerability in a medical device may be exploited to cause bodily harm to an individual. While many IoT devices do not present safety risks, some do, and regulators should pay attention to those potential risks. In particular CPSC should pay attention to certain cybersecurity threats, a risk that it has not traditionally considered, but resist creating any prescriptive rules for IoT devices.

[1] "The Internet of Things and Consumer Product Hazards," Federal Register, March 27, 2018, https://www.federalregister.gov/documents/2018/03/27/2018-06067/the-internet-of-things-and-consumer-product-hazards.

There are four types of scenarios in which an IoT device may cause consumer harm.

Scenario	Description
Type 1	Traditional hazards not unique to IoT devices, such as faulty wiring.
Type 2	An IoT device has a security vulnerability that can be exploited to create a hazardous condition, such as overheating. These vulnerabilities may or may not be patchable.
Type 3	An IoT device has a security vulnerability that can be exploited to create opportunities for hazardous conditions, such as remotely disabling a smart fire alarm so that it does not sound during an emergency, or disabling a smart lock so that someone can break into a house. These vulnerabilities may or may not be patchable.
Type 4	Hazards related to privacy, which do not pose a risk of physical injury or death.

As CPSC has noted, it is not concerned with data privacy issues, and thus should only be concerned with type 1, 2, and 3 scenarios. However, the rise of cyber-physical systems, i.e. the Internet of Things, creates the need for CPSC to consider cybersecurity threats that create opportunities for physical harm.

For Type 1 scenarios, CPSC already has processes in place to handle potential consumer safety risks. CPSC does not need to handle the risk of a consumer being shocked from a smart toaster any differently than the risk presented by an ordinary toaster.

For Type 2 and 3 scenarios, CPSC should make a distinction between IoT devices that can be remotely patched and those that cannot. Devices with vulnerabilities that can be remotely patched in a secure manner present significantly less risk than those that cannot. While IoT device makers should make information about updates publicly available, if they can remotely patch the devices, CPSC should not require these companies notify their customers individually. Given the frequency with which automatic software updates may be issued, issuing notifications for these patches would needlessly inundate consumers with information they may not want. Product safety recall notices are still somewhat limited, which makes them more likely to get attention from consumers when they receive them. CPSC should ensure that companies do not use recall notices every time they patch security bugs. CPSC should also seek guidance on this issue from the National Telecommunications and Information Administration (NTIA), which runs a working group devoted to researching IoT security, patching, and upgradability.[2]

Companies that need to either manually update or repair a device, or recall entirely an IoT device, should go through CPSC's standard process of creating a corrective action plan, just as they would for non-IoT products.[3]

CSPC should not introduce additional product safety guidelines for IoT devices. First, the Internet of Things is still a relatively nascent set of technologies. The declining costs of sensor technology, connectivity, and data storage has led to the rapid growth of the Internet of Things in recent years, but this technology is still new. For example, Amazon's Echo smart home speaker was only introduced in November 2014.[4] Introducing prescriptive safety standards prematurely would limit innovation. Second, many devices have multiple types of uses, and different uses have different security requirements. Consumers should have flexibility to make their own choices about how to use IoT devices based on their personal security preferences and risk tolerances. Third, the Internet of Things is comprised of a wide variety of different kinds of devices, and it is unlikely that uniform safety standards would make sense to apply to all of these devices. For example, an unsafe fitness tracker likely poses substantially less risk of consumer harm than an unsafe smart oven. And fourth, it is important to recognize that there are few IoT devices that are entirely new kinds of devices, as device manufacturers can easily integrate sensors and connectivity to any manner of products, and many of these devices already comply with safety standards.

Moreover, market forces address many of the security concerns of IoT devices. For example, major retailers like Amazon have delisted products that poorly implement cyber security controls.[5] Over the long term, the goal of lawmakers and regulators should be to reduce information asymmetry in the market for secure IoT devices, such as by encouraging companies to go beyond the letter of the law to share more information with consumers about their security practices, much like companies publish privacy policies. Right now, most companies only offer vague claims of "taking cybersecurity seriously," but offer little information that consumers can use to easily differentiate the quality of

[2] "The NTIA IoT Security Upgradability and Patching," National Telecommunications and Information Administration, accessed June 14, 2018, https://www.ntia.doc.gov/files/ntia/publications/iot_wg1_standards_jan31.pdf.
[3] "Recall Handbook," Consumer Product Safety Commission, March 2012, https://www.cpsc.gov/s3fs-public/8002.pdf.
[4] Darrell Etherington, "Amazon Echo Is a $199 Connected Speaker Packing an Always-On Siri-Style Assistant," *TechCrunch,* November 6, 2014, https://techcrunch.com/2014/11/06/amazon-echo/.
[5] Alfred Ng, "Amazon Will Stop Selling Connected Toy Filled with Security Issues," *Cnet*, June 5, 2018, https://www.cnet.com/news/amazon-will-stop-selling-connected-toy-cloud-pets-filled-with-security-issues/.

security in different IoT products. If companies were obligated to publish more detailed security policies, it would put pressure on their competitors to improve their security practices. Consumer Reports, for example, may be more likely to recommend certain smart devices if their security measures exceed those of their competitors.

One benefit of publishing security policies is that it would give individual companies the freedom to manage risk as they see fit, rather than the oft-floated idea of having the government mandate a specific set of security measures.[6] If consumers had more information about the security of products, they could make more informed decisions. And if companies fail to uphold their stated practices, and these failures are either intentional or result in actual harm, then regulators like the FTC could take swift enforcement action.

In summary, CPSC should pay more attention to some of the unique cybersecurity risks that exist with IoT devices, but it should not pursue any prescriptive regulations for device security.

Sincerely,

Daniel Castro
Director
Center for Data Innovation
dcastro@datainnovation.org

Joshua New
Policy Analyst
Center for Data Innovation
jnew@datainnovation.org

[6] Daniel Castro, "How Congress Can Fix 'Internet of Things' Security," *The Hill*, October 28, 2016, http://thehill.com/blogs/pundits-blog/technology/303302-how-congress-can-fix-internet-of-things-security.