CENTER FOR DEMOCRACY & TECHNOLOGY

15 June 2018

Office of the Secretary
Consumer Product Safety Commission
4330 East-West Highway, Room 820
Bethesda, MD 20814

RE: Docket No. CPSC-2018-0007 -- The Internet of Things and Consumer Product Hazards

The Center for Democracy and Technology (CDT) is a non-profit advocacy organization working to promote democratic values online and in new, existing, and emerging technologies. CDT pursues this mission by supporting laws, policies, and technical tools which empower users, protect privacy, and preserve individual rights online.

CDT respectfully submits these comments in response to Consumer Product Safety Commission's (CPSC, or the Commission) request for written comments on the Internet of Things (IoT) and consumer product hazards.[1] While there is no doubt that the IoT presents enormous value, poorly designed and inadequately secured devices can present risks to consumers' safety and can be exploited for costly cyber-attacks.[2]

As the CPSC explores potential safety issues and hazards in IoT, CDT recommends the Commission:

- Recognize the unique scope and characterization of IoT devices and how this impacts hazardization considerations;
- Identify existing IoT standards to bolster security practices across different consumer product domains;
- Collaborate with relevant stakeholders to provide guidance to consumers and manufacturers on IoT-related informational harms;
- Develop a plan for addressing hazards associated with abandoned and unsupported IoT devices;
- Track IoT products, including component disclosures and IoT designations, for complaint databases.

---

[1] 83 Fed Reg 13123.

[2] CDT has written extensively about security and data governance concerns in the unregulated world of the IoT, including comments in February 2018 on promoting stakeholder action against botnets and other automated threats; in July 2017 on strengthening federal cybersecurity and addressing botnets; and in March 2017 on fostering the advancement of the Internet of Things. Additionally, in April 2018, CDT release a report addressing issues of strict product liability and the Internet of Things which the Commission may find useful in its work. *See* Ctr. for Democracy & Tech., *Comments to the NTIA on Promoting Stakeholder Action Against Botnets and Other Automated Threats* (Feb. 12, 2018), https://cdt.org/insight/comments-to-ntia-promoting-stakeholder-action-against-botnets-and-other-automated-threats/; Ctr. for Democracy & Tech., *Comments to the NTIA on Executive Order 13800* (Jul. 28, 2017), https://cdt.org/insight/request-for-comment-re-strengthening-federal-cybersecurity-and-addressing-botnets/; Ctr. for Democracy & Tech., *Comments to the NTIA on Fostering the Advancement of the Internet of Things* (Mar. 10, 2017), https://cdt.org/insight/cdt-comments-to-the-ntia-on-fostering-theadvancement-of-the-internet-of-things/; Benjamin C. Dean, *Strict Products Liability and the Internet of Things,* Center for Democracy and Technology (Apr. 2018), https://cdt.org/insight/report-strict-product-liability-and-the-internet-of-things/.

I. The Need for Standards and Rules for IoT Devices

There will be an estimated 11.2 billion IoT connected devices by the end of 2018.[3] Of these devices, approximately 7 billion will be consumer products, and that number is expected to approach 13 billion by 2020.[4] IoT holds a great deal of promise for businesses, consumers, and society. IoT can be used to improve upon existing products, introduce new ones entirely, or provide novel safety features, all of which can benefit consumers.

Companies are developing sensors which can detect whether a child is left alone in a car and then ping a parent's smartphone to alert them of this fact;[5] others have created wearables which can alert a caregiver if an elderly individual has fallen, as well as the length of time that they have been on the ground.[6] Yet IoT devices also introduce new risks and potential for new harms. A smart oven could be made to turn on remotely[7], or a smart smoke detector could malfunction due to a software glitch.[8] Each new device that comes online presents another opportunity for hazardization and associated harms that may counter its utility in the marketplace.[9]

Both consumers and businesses agree that security in the IoT should be regulated. A 2017 survey of 1,050 IT and business decision makers, as well as 10,500 consumers, found that, "the vast majority of decision makers (96%) and consumer (90%) respondents state that there should be IoT security regulations."[10] Consumers are concerned not just with hackers or other bad actors, but also data leakage, uncontrolled sharing of information across multiple devices, unauthorized setting adjustments, and inadequate customer support.[11]

These safety and security concerns are compounded by misaligned market incentives related to IoT security. Companies competing in the IoT space are racing to be first to market, as delays in delivering a product can be the difference between market dominance or bankruptcy.[12] Since installing additional

---

[3] Gartner, *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent from 2016* (Feb. 7, 2017), https://www.gartner.com/newsroom/id/3598917.

[4] *Id.* Research firm Gartner Gartner that by 2020, the number of IoT connected devices will approach 20.4 billion, with close to 12.9 billion being consumer products.

[5] Ian Sherr, *Some Truly Useful Tech: A Sensor for Your Child's Car Seat,* CNet (Apr. 6, 2016). https://www.cnet.com/news/some-truly-useful-tech-a-sense-a-life-sensor-for-your-childs-babies-car-seat/.

[6] Anna Cordrea-Rado, *How Smart Home Technology is Empowering Seniors and Combating Social Isolation*, Dell Technologies (Jan. 16, 2018). https://www.delltechnologies.com/en-us/perspectives/how-smart-home-technology-is-empowering-seniors-and-combating-social-isolation/.

[7] John Leyden, *Half-baked Security: Hackers Can Hijack Your Smart Aga Oven 'With a Text Message'*, The Register (Apr. 13, 2017), https://www.theregister.co.uk/2017/04/13/aga_oven_iot_insecurity/.

[8] Lauren Goode, Nest Issues Software Fix for Recalled "Smart" Smoke Alarm, Recode (May 21, 2014), https://www.recode.net/2014/5/21/11627148/nest-recalls-smart-smoke-alarm-issues-software-fix.

[9] Bruce Schneier, *We Need to Save the Internet from the Internet of Things*, Vice Motherboard (October 6, 2016) at https://motherboard.vice.com/en_us/article/ezpq3m/we-need-to-save-the-internet-from-the-internet-of-things.

[10] Gemalto, *The State of IoT Security: Security Takes a Back Seat* 12 (October 31, 2017). https://www.gemalto.com/press/pages/gemalto-survey-confirms-that-consumers-lack-confidence-in-iot-device-security-.aspx.

[11] *Id.* at 13.

[12] Benjamin C. Dean, *Strict Products Liability and the Internet of Things,* at *3.*

security measures and following more rigorous software and hardware development processes can slow down develop time, and thus time to market, companies are disincentivized to follow such processes.[13] Further, while upgradability and patchability are important benefits of the IoT, and should be built into devices and products, this functionality can actually incentivize developers to put out defective software under the auspices of being able to fix bugs down the road.[14] While recognizing the benefits of being able to remotely patch/update a product, such functionality does not eliminate the need for strong security and safety by design. Finally, firms lack a strong incentive to retroactively test products for security and software failures. If a firm discovers a flaw in a product's operational code, disclosing that flaw could lead to costly recalls and bad publicity.[15]

It is also difficult for consumers to evaluate the relative safety and security of IoT devices and, by extension, to make informed purchasing and data sharing decisions.[16] There is currently no widely-embraced security or safety certification program and associated labeling scheme for IoT devices.[17] Most efforts are still in their infancy,[18] and companies need further incentives to develop such programs. Additionally, software source code is protected by a litany of technical barriers and legal rules, and even if a consumer were able to access it, understanding the security and safety implications of code would require the type of expert-level knowledge that the average consumer does not possess.[19] Furthermore, absent a security/safety certification or labeling scheme, manufacturers who use strong security practices are unable to differentiate themselves in the marketplace from others who use weaker standards.[20]

II. Case Studies on IoT Safety

These systemic market failures, as well as a lack of baseline safety and security standards for IoT devices, can lead to defective and hazardous products entering the consumer market. Below, we list a number of IoT consumer products that were shown to have serious safety issues. As the CPSC has emphasized its interest in physical harms associated with IoT devices, we have have chosen to highlight these examples, rather than information harms such as eavesdropping or stealing data, which are addressed later in the comment. Note that while many of these defects were discovered by security researchers, and that many of these vulnerabilities have since been fixed, this list demonstrates the unique nature of the physical safety risks associated with IoT devices.

---

[13] Pfleeger S. L., Libicki M. and Webber M. (2007), "I'll buy that! Cybersecurity in the internet marketplace", *IEEE Security & Privacy*, Issue No. 03, May/June, Vol. 5. at 27.
[14] Benjamin C. Dean, *Strict Products Liability and the Internet of Things,* at *3.*
[15] Arvinder Saini, *The Cost of Fixing Bugs Throughout the SDLC*, Computer Business Review (Mar. 1, 2017), https://www.cbronline.com/enterprise-it/software/cost-fixing-bugs-sdlc/.
[16] Benjamin C. Dean, *Strict Products Liability and the Internet of Things,* at *3.*
[17] Internet Society, *IoT Security for Policymakers* (Apr. 19, 2018), https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/.
[18] *See, e.g.*, *Open Internet of Things Certification Mark*, Principles (last visited June 8, 2018), https://iotmark.wordpress.com/principles/.
[19] Benjamin C. Dean, *Strict Products Liability and the Internet of Things,* at 3.
[20] *Id.* at 4.

- *Smart Thermostats:* Heatmiser is a UK-based company which produces an IoT thermostat which allows a consumer to control the temperature inside their homes. In 2017, Ankit Anubhav of the IoT security firm NewSky showed that by exploiting a vulnerability in Heatmiser's software, he was able to raise the temperature inside a home from 73.4° to 95° Fahrenheit. While Heatmiser patched the bug and offered remediation to its users, this incident demonstrates the potential harms that can come from IoT devices.[21] If such a vulnerability were exploited in the home of an individual physically unable turn off a heating unit, then the potential for physical harm could be high.

- *Smart TVs:* In 2018, Consumer Reports found that smart televisions produced by TCL and Samsung could be hacked to "pump the volume from a whisper to blaring levels." Researchers were able to do so by exploiting a vulnerability in the application programing interface (API) used to control the device.[22] If a small child or an individual with sensitive hearing were sitting close to the television and the volume was suddenly turned up very high, this could damage the individual's hearing.

- *Smart Lights:* In 2016, a team of researchers from the Weizmann Institute of Science showed that smart lights connected to a network could be hacked and made to display lighting patterns that could trigger a seizure in an individual with photosensitive epilepsy.[23]

- *Smart Locks:* In 2017, a number of smart locks made by the company Lockstate were bricked, or made inoperable, by a software update. Although owners possessing keys were still able to unlock their doors, many who did not have keys, including AirBnb renters, were unable to enter residences.[24] If a person was unable to enter a residence to assist another person in the event of an emergency, such a lock could present a substantial product hazard.

- *Smart Speakers*: Researchers at Trend Micro were able to exploit a vulnerability in the API of Sonos and Bose speakers which allowed them to force the speakers to play any file of their choosing. Such a vulnerability could allow a malicious actor to play an inappropriate file or otherwise unwanted sound. Although acknowledging that such a vulnerability would be used more often than not as a prank, the researchers did raise the prospect of using the vulnerability to control device like an Amazon Alexa, which can be linked to critical safety devices like door locks.[25]

---

[21] NewSky Security, *IoT Thermostat Bug Alllows Hackers to Turn Up The Heat* (Jul. 20, 2017), https://blog.newskysecurity.com/iot-thermostat-bug-allows-hackers-to-turn-up-the-heat-948e554e5e8b.
[22] Consumer Reports, *Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds* (Feb. 7, 2018), https://www.consumerreports.org/televisions/samsung-roku-smart-tvs-vulnerable-to-hacking-consumer-reports-finds/.
[23] E. Ronen and A. Shamir, "Extended Functionality Attacks on IoT Devices: The Case of Smart Lights," 2016 IEEE European Symposium on Security and Privacy (EuroS&P), Saarbrucken, 2016, pp. 3-12. https://ieeexplore.ieee.org/document/7467343/
[24] Rhett Jones, *Smart Locks Used by Airbnb Get Bricked by Software Update*, Gizmodo (Aug. 14, 2017), https://gizmodo.com/smart-locks-used-by-airbnb-get-bricked-by-software-upda-1797839523.
[25] Andy Greenberg, *Hackers Can Rickroll Thousands of Sonos and Bose Speakers Over the Internet*, Wired (Dec. 27, 2017), https://www.wired.com/story/hackers-can-rickroll-sonos-bose-speakers-over-internet/?_ga=2.52735914.342770848.1528298440-972631098.1528133750.

As these examples demonstrate, consumer IoT devices have the potential to introduce physical harms that are not present in other products. While the Commission has focused on potential physical harms such as fire, burn, shock, tripping or falling, laceration, contusion, or chemical exposure, there are many other hazards associated with IoT that fall outside this list. Specifically, IoT devices can generate significant physical discomfort, hearing damage, the display of offensive or unwanted content, and the modification of other connected IoT devices. The Commission should consider these, and less obvious IoT related harms, as they work with industry to implement baseline safety and security standards, and engage in compliance, monitoring, and enforcement actions.

III. The Consumer Product Safety Commission's Role in the IoT

The CPSC was established to protect the public against unreasonable risks of injury associated with consumer products.[26] To fulfil this mandate, the CPSC has the power to monitor consumer markets, study and investigate dangers associated with consumer products, and develop safety regulations for the manufacture, sale, and distribution of consumer products.[27] CDT believes the Commission has an important role to play in improving consumer confidence in the IoT, and we would recommend the CPSC engage in the following activities.

A. Recognize the Unique Scope of IoT Products and Devices / Consider Broad Definitions of IoT and Potential Hazardization

A precise definition of the IoT is difficult to craft.[28] Part of the reason for this is that technology continuously evolves and changes in ways that are difficult to anticipate. The Commission has turned its present attention to devices with "a connection to the internet that can transmit or receive data, upload or download operating software of firmware, or communicate with other internet-connected devices."[29] Connectivity provides IoT devices with unique capabilities that are absent in traditional consumer products -- specifically, IoT devices have the ability to (1) transmit diagnostic data about the device (data useful for understanding how devices are performing in the field) and (2) be updated or patched remotely. While this definition is sufficient as a foundation on which to build, CDT urges the commission to consider that internet connectivity can be and often is accompanied by other technological features and capabilities that present important risks and associated harms (e.g. autonomous capabilities). To craft effective policy, the risks and harms from these associated technological capabilities need to be considered alongside those posed by internet connectivity.

However, the risks posed by IoT devices go beyond those created by connectivity. The CPSC refers to the potential harms associated with IoT devices as 'hazardization', or the process by which a product, which

[26] 15 U.S. Code § 2051(b).

[27] U.S. Consumer Product Safety Commission, *2016 Annual Report to the President and Congress* (Jun. 9, 2017), https://www.cpsc.gov/s3fs-public/CPSC_FY16_Annual_Report.pdf?DsHsl4ravzs3IcO8aSlqcVEda06m7d_X.

[28] Dep't of Commerce Green Paper, Fostering the Advancement of the Internet of Things (Jan. 2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf.

[29] 83 Fed Reg 13123.

would otherwise be safe, poses a danger to consumers when connected to the Internet through malicious, incorrect, or careless changes to operational code.[30] CDT would urge the Commision to further consider the interplay between network connectivity, software, hardware, battery, data, and autonomous capabilities in their definition of hazardization. It is not simply the act of being connected to the internet that gives rise to potential harms, but the interplay between network connectivity and the material, and immaterial, component parts of a device that can introduce the potential for harm.[31]

In addition, the ability to automatically transmit and receive data, as well as use the outputs of statistical learning methods both within the device and remotely, allow some IoT devices to autonomously determine their operations without user input ('autonomous capabilities')[32] . These devices are almost always accompanied by at least periodic internet connectivity. Accordingly, in considering the consumer product hazards associated with IoT, and considering the types of devices would need controls or supervisory systems, CDT would urge the commission to include devices which possess autonomous capabilities.

B. Work with Industry Baseline Safety and Security Standards for Certain Classes of IoT Products

There are certain classes of IoT devices that we believe warrant increased attention from the Commission, specifically those whose primary function is safety (e.g., smart smoke detectors) or ones which could cause serious injury or death (e.g., smart toaster). Such products, through careless, malicious, or incorrect changes to operational code, raise substantial product hazards that would not be present in other IoT devices. If such hazards were to arise, and they were determined to constitute a substantial product hazard,[33] the Commission would clearly be within its authority to to require a corrective action plan for products impacted by such problematic code.[34]

There are already many government and industry endorsed security standards of general applicability that the CPSC can embrace, and the Commission could explore with industry whether additional standards are needed for these uniquely dangerous consumer products.[35] Existing standards often

[30] 83 Fed Reg 13123.
[31] Benjamin C. Dean, *Strict Products Liability and the Internet of Things, 1.*
[32] For example, Google's DeepMind AI used information gathered from industrial sensors to automate cooling processes at its data centres and reduce overhead costs. *See* Richard Evans and Jim Gao, *DeepMind AI Reduces Google Data Centre Cooling Bill by 40%.* DeepMind (July 20, 2016), https://deepmind.com/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-40/.
[33] 15 U.S. Code § 2064(a)(2).
[34] 15 U.S. Code § 2064(c).
[35] *See* U.S. Federal Trade Commission, *Internet of Things: Privacy and Security in a Connected World* (Jan. 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; U.S. National Institute of Standards and Technology, *Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things* (Feb. 2018), https://csrc.nist.gov/CSRC/media/Publications/nistir/8200/draft/documents/nistir8200-draft.pdf; *U.S. National Telecommunications and Information Administration, Catalog of Existing IoT Security Standards Version 0.01* (Sept. 2017), https://www.ntia.doc.gov/files/ntia/publications/iotsecuritystandardscatalog_draft_09.12.17.pdf; Broadband Internet Technical Advisory Group, *Internet of Things (IoT) Security and Privacy Recommendations* (Nov. 2016), https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf; U.K. Department for Digital, Culture Media and Sport, *Secure by Design: Improving the Cyber Security of Consumer Internet of Things Report* (Mar. 2018),

include a security by design approach and embrace security controls such as a prohibition on hardcoded passwords, mandatory patching or updating capabilities, fail-safe mechanisms in the event of a loss of connectivity, and a vulnerability disclosure policy, among others.[36] By adopting and monitoring compliance with such standards, the potential for both product defects and substantial product hazards to arise could be lessened. Were such baseline standards to be adopted, the Commission should also consider the unique challenges associated with compliance monitoring and enforcement, as IoT devices often use imported hardware and software and ensuring standards compliance for foreign manufacturers could be challenging.

C. Collaborate with Stakeholders to Address Broader IoT Informational Harms

The Commission has explicitly stated that it does not consider personal data security and privacy issues that may be related to IoT devices to be consumer product hazards that the CPSC would address.[37] CDT would urge the CPSC to reconsider this stance. As other advocates have argued,[38] privacy and security concerns are at the core of what consumers believe to be unsafe about IoT devices. IoT fundamentally shifts how information is managed and it amplifies long-standing challenges, including opacity of data flows and actors, and enables the stockpiling of new sources of intimate data.[39]

This, in turn, gives rise to a number of different privacy-related informational harms. An IoT connected home surveillance camera can be hacked and used to spy on residents.[40] A smart personal assistant can record sensitive personal conversations and leak or distribute that information to third parties.[41] These problems have become pervasive across the IoT, and the advocates and security researchers have had to engage in lengthy efforts to address problematic devices from even the worst repeat offenders.[42]

While consumer privacy enforcement has traditionally fallen to the Federal Trade Commission (FTC) under its authority to protect consumers from unfair or deceptive practices under Section 5 of the FTC Act,[43] the CPSC has also acknowledged a need to collaborate with the FTC, as well as other governmental agencies and bodies. In its 2017 report, *Potential Hazards Associated with Emerging or Future*

---

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.

[36] *Id.*

[37] 83 Fed Reg 13123.

[38] Electronic Privacy Information Center, *Oral Presentation: The Internet of Things and Consumer Product Hazards* (May 16, 2018), https://epic.org/apa/comments/EPIC_CPSC_IoT_May2018.pdf.

[39] UC Berkeley Center for Long-Term Cybersecurity, Privacy and the Internet of Things: Emerging Frameworks for Policy and Design 7 (June 2018), *available at* https://cltc.berkeley.edu/2018/06/07/cltc_report_privacy_iot/.

[40] Danny Palmer, *Researchers Find Security Flaws in Popular Smart Cameras*, *ZD Net* (Mar 13, 2018), https://www.zdnet.com/article/security-vulnerabilities-in-these-popular-smart-cameras-let-hackers-turn-them-into-surveillance/.

[41] Hamza Shaban, *An Amazon Echo Recorded A Family's Conversation, Then Sent it to a Random Person in Their Contacts, Reports Say*, Washington Post (May 24, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/05/24/an-amazon-echo-recorded-a-familys-conversation-then-sent-it-to-a-random-person-in-their-contacts-report-says/.

[42] Afred 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/ (Cybersecurity research firm Cure53 "found that CloudPets' Bluetooth vulnerabilities first demonstrated more than a year ago are still open.").

[43] 15 U.S. Code § 45(a)(1).

Technologies,[44] the CPSC states that when a particular product concern does not fall within its jurisdiction, it will work with federal partners on areas of mutual concern. It would be helpful for the CPSC to outline how they plan to work with the FTC to address informational harms associated with IoT devices. Guidance to consumers and industry is appropriate, particularly as only the CPSC has the authority to require corrective action plans, or recalls.

D. Develop a Plan for Abandoned and Unsupported IoT Devices

Another IoT specific issue that CDT would encourage the Commission to consider are the risks associated with abandoned or no-longer-supported IoT devices.[45] If an unsupported device is found to contain a defect which results in a substantial product hazard, what responsibilities do manufacturers of the product have to fix the vulnerability? Should there be different support timelines IoT products that serve a critical safety function or which could cause serious injury or death, versus those that do not? And how will the CPSC exercise its oversight and recall authority when such hazards are discovered in unsupported or abandoned devices, especially if the manufacturer is no longer in business?

Regarding these questions specifically, the National Telecommunications and Information Administration (NTIA) recently led a multistakeholder process exploring IoT security upgradability and patching.[46] As part of this process, the FTC submitted comments which advocated manufacturers disclosing a guaranteed minimum period of time that they would support a product, in addition to, or instead of, an *anticipated* timeline of support.[47] The FTC further encouraged manufacturers to disclose any changes to functionality (for example loss of app support) that occur when a product is no longer supported.[48] CDT would encourage the CPSC to consider this process and the associated recommendations in exploring new standards and regulations for IoT devices.

E. Track IoT products, including component disclosures and IoT designations for complaint databases

Considering the complexity of the hardware and software ecosystems that support IoT devices and the unique vulnerabilities associated with them, CDT would encourage the Commission to actively monitor the proliferation of these internet-connected devices. Such monitoring could involve collecting information about who is releasing what, to whom, and the number of devices that have been sold.

---

[44] U.S. Consumer Product Safety Commission, *Potential Hazards Associated with Emerging and Future Technologies* (Jan. 18, 2017), https://www.cpsc.gov/s3fs-public/Report%20on%20Emerging%20Consumer%20Products%20and%20Technologies_FINAL.pdf.
[45] Naked Security, *Smart Devices Abandoned on the Road to Nowhere* (Dec. 14, 2016), https://nakedsecurity.sophos.com/2016/12/14/smart-devices-abandoned-on-the-road-to-nowhere/.
[46] U.S. National Telecommunications and Information Administration, *Multistakeholder Process; Internet of Things Security Upgradability and Patching* (Nov. 7, 2017), https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.
[47] U.S. Federal Trade Commission, *Public Comment On Communicating IoT Device Security Update Capability to Improve Transparency for Customers* (Jun. 19, 2017), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-comment-national-telecommunications-information-administration-communicating-iot-device-security/170619ntiaiotcomment.pdf.
[48] *Id.*

Recognizing that such an undertaking could be challenging for all IoT products, CPSC may wish to focus their monitoring and investigative resources on certain classes of IoT products, for example those that provide a critical safety function or could result in serious injury or death, or those devices which experience serious and/or repeated failures.

Along these lines, CDT believes every IoT device should provide disclosures about its components. The NTIA has already announced that its next cybersecurity multistakeholder process will explore software component transparency.[49] The CPSC should engage in this process. More importantly, CDT supports a requirement that all IoT devices contain a 'Bill of Materials'. Such a bill could contain a list of all component materials, parts, and software used in an IoT device.[50] When it is determined that a defect could, or has created a substantial product hazard, such a document could allow enforcement agencies like the CPSC quickly to determine what devices are impacted and better work to remedy the situation. Databases like these are essential to mitigating potential IoT related harms as defective devices and vulnerabilities are not likely to be immediately obvious in the short term. It also will be hard to determine what constitutes a substantial product hazard without some relevant metric such as, for example, the percentage of devices in circulation exhibiting failure, or the absolute number of devices with an unpatchable vulnerability.

CDT would also encourage the Commission to include an IoT designation in its National Electronic Injury Surveillance System (NEISS).[51] NEISS is a searchable database of "deaths, injuries, illnesses, and other harms associated with consumer products."[52] This database is the basis for many CPSC activities, including investigations, research, enforcement, and remedial actions.[53] If the Commission requires a designation which indicates whether a consumer product is internet connected, it may be able to locate clusters of similar hazards which would be hard to locate in isolation. CDT recognizes that determining whether an injury was caused by a software malfunction could be difficult to determine, especially at the point where this data is collected (emergency rooms), yet the knowledge that a device was internet connected could allow researchers to identify clusters or suspicious patterns and investigate further. Finally, CPSC may consider adding an IoT designation on the 'Report an Unsafe Product' form at SaferProducts.gov as doing so may assist the Commission in identifying IoT products that are harming consumers.

IV. Conclusion

With its recall authority and broad mission to protect consumers, the Consumer Product Safety Commission will play an essential role in protecting the public from the most hazardous impacts of the

[49] U.S. National Telecommunications and Information Administration, *NTIA Software Component Transparency* (June 5, 2018), https://www.ntia.doc.gov/SoftwareTransparency.
[50] *Investopedia*, Bill of Materials - BOM, https://www.investopedia.com/terms/b/bill-of-materials.asp.
[51] U.S. Consumer Product Safety Commission, *National Electronic Injury Surveillance System (NEISS),* https://www.cpsc.gov/Research--Statistics/NEISS-Injury-Data.
[52] David H. Carpenter, *The Consumer Product Safety Act: A Legal Analysis, Congressional Research Service* (Apr. 24, 2018), https://fas.org/sgp/crs/misc/R45174.pdf at 7.
[53] *Id.*

Internet of Things. The diversity and range of IoT devices create significant potential for risks to consumers, and absent robust oversight and monitoring from the CPSC, consumer trust in the IoT will be lessened. We thank the Commission for the opportunity to provide comments on on this subject and CDT looks forward to working with the CPSC to advance security standards across the Internet of Things.

Sincerely,

Joseph Lorenzo Hall
Chief Technologist

Joseph Jerome
Policy Counsel, Privacy & Data Project

Michelle Richardson
Deputy Director, Freedom, Security, and Technology Project

Dominic Contreras
Intern, Privacy & Data Project