epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

Comments of the

ELECTRONIC PRIVACY INFORMATION CENTER

to the

CONSUMER PRODUCT SAFETY COMMISSION

"The Internet of Things and Consumer Product Hazards"

June 15, 2018

The Electronic Privacy Information Center ("EPIC") submits these written comments in response to the Consumer Product Safety Commission's ("CPSC") notice.[1] EPIC testified before the CPSC on this topic[2] and submits these comments to expand upon issues raised at the hearing. We urge the Commission to use its statutory authority to require IoT manufacturers to (1) minimize data collection, (2) enhance transparency and user access to data, (3) conduct privacy impact assessments, and (4) implement privacy and security enhancing techniques.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[3] EPIC is a leading advocate for consumer privacy and an expert on the privacy and security hazards of the Internet of Things.[4] EPIC has testified before Congress on several occasions[5] and has fought for data protection and privacy rights for Internet users at the Federal Trade Commission for more than two decades, filing landmark complaints

---

[1] CPSC, *The Internet of Things and Consumer Product Hazards*, 83 Fed. Reg. 13122 (March 27, 2018), https://www.federalregister.gov/documents/2018/03/27/2018-06067/the-internet-of-things-and-consumer-product-hazards (hereafter "Notice").

[2] Sunny Kang, EPIC International Consumer Counsel, *The Internet of Things and Consumer Product Hazards*, Testimony, CPSC (May 16, 2018), https://www.youtube.com/watch?v=-YSDEkWuxUo&feature=youtu.be.

[3] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.

[4] *See, e.g.*, EPIC, *Internet of Things (IoT)*, https://epic.org/privacy/internet/iot/; EPIC Statement to U.S. House Committee on Energy and Commerce, Subcommittee on Digital Commerce and Consumer Protection, Internet of Things Regulation (May 21, 2018), https://epic.org/testimony/congress/EPIC-HEC-IoTLeg-May2018.pdf; EPIC Comments to the FTC, *On the Privacy and Security Implications on the Internet of Things* (June 1, 2013), https://epic.org/privacy/ftc/EPIC-FTC-IoT-Cmts.pdf.

[5] *See, e.g*, Khaliah Barnes, EPIC Associate Director, Testimony before the U.S. House of Representatives Committee on Oversight and Government Reform, Subcommittee on Information Technology, Transportation, and Public Assets, *The Internet of Cars* (Nov. 18, 2015), https://www.epic.org/privacy/edrs/EPIC-Connected-Cars-Testimony-Nov-18-2015.pdf; Marc Rotenberg, EPIC Executive Director, Testimony before the U.S. Senate Committee on Commerce, Science, and Transportation, *Internet Privacy and Profiling* (June 13, 2000), https://epic.org/privacy/internet/senate-testimony.html; EPIC Statement to Senate Committee on Commerce, Science, and Transportation, *Oversight of the National Telecommunications and Information Administration* (June 12, 2018), https://epic.org/testimony/congress/EPIC-SCOM-NTIA-June2018.pdf.

about privacy violations by Microsoft, Facebook, and Google, among others.[6] And last Fall, EPIC led a coalition of consumer groups that submitted a complaint to the CPSC about the Google Home Mini, urging the Commission to recall the device because a defect caused it to record user conversations without their consent or knowledge.[7]

I. CPSC's Jurisdiction to Regulate IoT Privacy and Security

(1) Statutory Authority

The U.S. Consumer Product Safety Commission ("CPSC" or "the Commission") is empowered by the Consumer Product Safety Act of 1972, 15 U.S.C. §§ 2051−2089 ("CPSA") to protect the public against unreasonable risks of injury associated with consumer products. This enabling statute and subsequent amendments by the Consumer Product Safety Improvement Act of 2008 ("CPSIA") give the CPSC jurisdiction over thousands of consumer products.[8] The Commission's broad authority and technical expertise have been historically critical to ensuring the safety of new technologies entering the marketplace.

Today, the biggest threat to privacy and security in consumer products is posed by the Internet of Things. IoT devices track personal data by seamlessly integrating into the consumers' activities and lifestyles. They blend into everyday objects, and are not readily discernible as an internet-connected device with the capacity to sense, collect, and transmit large-scale personal data. IoT technology is encapsulated in small unobtrusive devices, often without a direct user interface like a screen. Therefore, the ubiquity of IoT sensors and their amassment of granular data pose significant privacy concerns that could threaten the physical safety of consumers.

As an independent regulatory agency with the Congressional mandate to safeguard the public from emerging risks in the "complexities of consumer products," it is incumbent on the CPSC to regulate the privacy and security of IoT devices. CPSC is the best equipped federal agency to address the complexities of IoT—through its interdisciplinary structure of economists, engineers, and lawyers, and the resources to test for security lapses and recall faulty devices before they enter the commerce stream.

---

[6] *See* Complaint and Request for Injunction, Request for Investigation and for Other Relief, *In the Matter of Microsoft Corporation*, (July 26, 2001), https://www.epic.org/privacy/consumer/MS_complaint.pdf; *see also* Complaint, Request for Investigation, Injunction, and Other Relief, *In the Matter of Facebook, Inc*, (Dec. 17, 2009), https://epic.org/privacy/inrefacebook/EPIC-FacebookComplaint.pdf; Complaint, Request for Investigation, Injunction, and Other Relief, *In the Matter of Google, Inc*, (Feb. 16, 2010), https://epic.org/privacy/ftc/googlebuzz/GoogleBuzz_Complaint.pdf; EPIC Comments to FTC, *In the Matter of PayPal, Inc.* (March 29, 2018), https://epic.org/apa/comments/EPIC-FTC-PayPal-ConsentOrder.pdf; EPIC Comments to FTC, *In the Matter of Uber, Inc.* (May 14, 2018), https://epic.org/apa/comments/EPIC-FTC-Revised-Uber-Settlement.pdf.

[7] Coalition Letter to U.S. Consumer Product Safety Comm. On Google Home Mini (Oct. 13, 2017), https://epic.org/privacy/consumer/Letter-to-CPSC-re-Google-Mini-Oct-2017.pdf.

[8] Pub. L. 112-28, August 12, 2011

The Congressional intent in enacting the CPSA was to delegate broad authority to the Safety Commission to address novel consumer hazards. This is evident in the "Findings and Purposes" [Sections 2(a)(1)-(3)] of the CPSA, which state: "(1) an unacceptable number of consumer products which present unreasonable risks of injury are distributed in commerce; (2) complexities of consumer products and the diverse nature and abilities of consumers using them frequently result in an inability of users to anticipate risks and to safeguard themselves adequately; (3) the public should be protected against unreasonable risks of injury associated with consumer products."[9]

Congress was explicit that consumers cannot be left to their own devices to assess the risks of new technology. Hence, CPSC has a statutory mandate to correct the information asymmetry of consumers and manufacturers by addressing the risks that are not obvious to average consumers. The Commission has a duty to keep pace with the technological evolutions of consumer products, and to "(1) conduct research, studies, and investigations on the safety of consumer products and on improving the safety of such products; (2) test consumer products and develop product safety test methods and testing devices" [Section 5(b)(1)-(2)].[10] CPSIA has also enhanced the Commission's enforcement authority to recall and investigate manufacturers on product hazards that pose a risk of harm to consumers.

There is an urgent need for regulatory action on IoT privacy and security. Companies have little incentive to maintain strong standards without regulation on the manufacturing and design of IoT products. And consumers do not have enough information to evaluate the privacy and security implications of these products themselves. This market structure has exacerbated the power imbalance between consumers and the companies with which they conduct business. Consumers are unable to make meaningful choices on devices that significantly impact their security and safety. This has alarming implications for toys that collect children's data, and internet-connected home systems like smoke detectors and security cameras. The Commission's authorization to act on the exigencies of this information asymmetry is clearly set forth by statute.

(2) CPSC's Role in Preventing Consumer Hazards

A core mission statement of the 'U.S. Consumer Product Safety Commission: Strategic Plan 2018-2022' is prevention.[11] The prevention of security and data breaches in IoT devices should be critical to CPSC's regulatory strategy going forward. Conditions that are hazardous to public safety can be intentionally or negligently designed into IoT devices. A major example of such defect, which EPIC has previously brought to the attention of the CPSC,[12] was the "always

[9] 15 U.S.C. § 2051 (1972)
[10] 15 U.S.C. § 2054 (1972)
[11] U.S. Consumer Product Safety Commission, *Strategic Plan 2018-2022*, https://www.cpsc.gov/s3fs-public/CPSC_2018-2022_Strategic_Plan.pdf
[12] Coalition Letter to U.S. Consumer Product Safety Comm. On Google Home Mini (Oct. 13, 2017),

on" Google Home Mini that recorded private conversations without the knowledge or consent of the consumer. EPIC argued, "this is a classic manufacturing defect that places consumers at risk," and "without strong and effective action by the CPSC, the safety risks to consumers and the cost to the national economy will be great."[13]

> The urgency cannot be overstated. As the Internet connects physical devices – refrigerators, thermostats, home locks, and even cars – the risks to consumers are increasing dramatically. Experts in cybersecurity have warned that the United States now confronts the "Internet of Broken Things." And with the Internet of Things, attacks will occur quickly against many objects simultaneously. Poor insulation on the power cord of a toaster may lead to a fire in a particular home. But the exploitation of a vulnerability in a network of thermostats or door locks could be staggering.[14]

We brought the Google Home Mini complaint to the CPSC and not the FTC, precisely because the design defect of the device, intended for the consumer marketplace, created a specific privacy and security risk to consumers. We received a response from the Acting Chairman of the CPSC, stating that "CPSC's authority will not generally extend to situations solely related to consumer privacy or data security, that do not pose a risk of physical injury or illness, or property damage."[15]

This assessment reflects a lack of understanding on IoT and the new threats facing consumers. As renowned security expert Bruce Schneier has said: "The Internet is dangerous—and the IoT gives it not just eyes and ears, but also hands and feet. Security vulnerabilities, exploits, and attacks that once affected only bits and bytes now affect flesh and blood."[16] It is within the Congressional mandate of the CPSC to protect consumers against the dangers posed by IoT.

Manufacturers—not consumers—must bear the responsibility to ensure the security of their products.[17] The products liability theory in tort law is a good fit for hazards caused by insecure devices, and courts have imposed liability when defective software causes physical

https://epic.org/privacy/consumer/Letter-to-CPSC-re-Google-Mini-Oct-2017.pdf.

[13] *Id.*

[14] *Id.*

[15] CPSC Acting Chairman Ann Marie Buerkle, *Response to EPIC and Consumer Privacy Organizations* (Mar. 23, 2018), https://epic.org/CPSC-response-GoogleHomeMini-3.23.18.pdf.

[16] Bruce Schneier, *IoT Cybersecurity: What's Plan B?*, Schneier on Security (Oct. 18, 2017), https://www.schneier.com/blog/archives/2017/10/iot_cybersecuri.html.

[17] *See* Alan Butler, "Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?," 50 U. Mich. J. L. Reform 913 (2017), http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1193&context=mjlr.

injury or death.[18] And "[w]hile DoS [Denial of Service] attacks may not cause the same type of bodily injuries, they are still proximate causes of severe property damage and should be considered reasonably foreseeable given the widespread recognition of the risks they pose."[19]

The Commission must pursue its goal of identifying, assessing, and taking preventative measures against consumer harms. This systematic approach is required for an accountable marketplace where the burden rightfully lies on the manufacturers to meet privacy and security safety standards which can prevent avoidable harms. If manufacturers fail to implement baseline requirements for privacy and security, the Commission should remove their products from the marketplace to prevent a substantial risk of injury to the public.

II. Privacy, Security, and Physical Safety Risks of the IoT

Vulnerabilities in IoT devices can be exploited to threaten consumers' security, privacy, and physical safety. Enforcement action by the CPSC is necessary to address these risks, which are exacerbated by the increasing connectivity and mobile data traffic of IoT as an emerging platform.[20]

The ubiquity of connected devices enables collection of data about sensitive behavior patterns, which could be used in unauthorized ways or by unauthorized individuals. Edith Ramirez, former chairwoman of the FTC, identified three key challenges that the Internet of Things poses to consumer privacy: "(1) ubiquitous data collection; (2) the potential for unexpected uses of consumer data that could have adverse consequences; and (3) heightened security risks."[21]

Companies should adopt privacy and security enhancing techniques in the design process of IoT devices to ensure that they are built to prioritize consumer safety. Regulatory standards will ensure that manufacturers patch security flaws and implement meaningful privacy tools to give users control over their personal data. To be fully compliant, IoT manufacturers should conduct a privacy impact assessment to identify and address risk, test security measures before launch, and avoid default settings that expose the consumer to hackers and data breaches. There

---

[18] *See, e.g.*, Gen. Motors Corp. v. Johnston, 592 So. 2d 1054 (Ala. 1992) (the plaintiff successfully sued General Motors after a defective computer chip caused his truck engine to stall in the middle of an intersection, which led to his car being hit by a tractor trailer, killing his grandson).

[19] *Supra* note 17 at 925.

[20] *See, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper* (March 28, 2017), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.html.

[21] Statement of Former FTC Chairwoman Edith Ramirez, *Privacy and the IoT: Navigating Policy Issues* (Jan 6, 2015), https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf?version=meter+at+0&module=meter-Links&pgtype=article&contentId=&mediaId=&referrer=&priority=true&action=click&contentCollection=meter-links-click.

is a collective need for entities in the IoT supply chain to be transparent about their products to consumers and the CPSC, and to implement technical and commercial measures to promote a high standard of privacy and security as a matter of public safety.

(1) Privacy Risks Cause Consumer Safety Concerns

A. Data Collected from IoT Devices Can Reveal Sensitive Behavior Patterns That Threaten Consumer Safety

One of the primary risks internet users face as IoT expands is that the ubiquitous collection and storage of data about users can reveal sensitive behavior patterns. Datasets collected by IoT monitors like wearables (e.g., Fitbit) and appliance sensors (e.g., Smart Home) reveal unique idiosyncrasies of real life habits and behavior that can easily identify a specific consumer with basic parameters on time, location, and demographic segments.[22] Troves of granular data could be infiltrated by hackers over unsecured networks that connect hundreds of these devices in a community, or one particular device linked to a household. These consequences pose serious risks to the consumers' personal safety, yet manufacturers are not tethered by regulation to design their devices with appropriate safeguards against the unauthorized access and misuse of personal information.

Consumers do not have the tools to protect their data from falling into the hands of malicious actors. IoT devices often do not have an embedded user interface like a screen to directly notify a user when data is collected. This makes it burdensome for consumers to configure privacy settings to restrict data processing. Most likely, consumers are unaware that they may have a choice to opt-out of certain data processing by IoT devices, or that these small, minimalistic items are constantly transmitting their personal information to the web.[23]

Currently, decoupled privacy policies appear in the box packaging of the device, an associated website or mobile app, or nowhere at all.[24] None of these methods are optimal because they each fail to consider how the consumer experience in IoT differs from traditional web browsing or interacting with an app. The lack of a centralized consumer interface in IoT necessitates extra efforts to draw attention to the privacy disclosure of unexpected data practices. However, manufacturers have not taken voluntary steps to convey notice and choice.[25]

---

[22] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 95 (2014), https://ssrn.com/abstract=2409074

[23] J. Bugeja, A. Jacobsson, and P. Davidsson, *On privacy and security challenges in smart connected homes*, European Intelligence and Security Informatics Conference (EISIC) (2016), pages 172–175.

[24] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent,* 93 Tex. L. Rev. 85, 95 (2014), at 141.

[25] Schaub, Florian, *A Design Space for Effective Privacy Notices*, USENIX Association Symposium on Usable Privacy and Security (2015), https://www.usenix.org/conference/soups2015/proceedings/presentation/schaub

B. "Always On" IoT Devices Collect Intrusive Data on Users Without Adequate Privacy and Security Safeguards Against Hackers

Many IoT devices feature "always on" tracking technology that surreptitiously records consumers' private conversations in their homes.[26] These "always on" devices raise numerous privacy concerns, including whether consumers have granted informed consent to this form of tracking. Even if the owner of an "always on" device has consented to constant, surreptitious tracking, a visitor to their home may not. Manufacturers are not required by regulation to incorporate ambient indicators on the device to alert nearby users that the device is recording. This distorts consumer perception of privacy and security in IoT devices. Consumers may simply assume that their personal information is safe from external attacks, even when manufacturers have not implemented safeguards.[27]

Companies say that IoT devices are only recording when triggered by a keyword command. However, they do not explain that in order to detect those words, the devices must always be listening, and the keywords are easily triggered. For example, several Amazon Echo devices treated a radio broadcast about the device as commands.[28] A San Diego television report about a girl using an Echo to order a $170 dollhouse and four pounds of sugar cookies triggered Echo devices across the city to make the same purchase.[29] A recent law enforcement request for Amazon Echo recordings[30] shows that "always on" devices will be much sought-after sources of information by law enforcement, foreign and domestic intelligence agencies, and, inevitably, cybercriminals.

It is particularly alarming that Internet-connected toys have entered the consumer markets without stringent regulations for manufacturers to safeguard the privacy and safety of children. In April 2015, EPIC joined the advocacy group Campaign for a Commercial-Free Childhood to protest Mattel's "Hello Barbie."[31] The toy is a WiFi-connected doll with a built-in microphone. Hello Barbie records and transmits children's conversations to Mattel, where they are analyzed to

[26] EPIC Letter to DOJ Attorney General Loretta Lynch, FTC Chairwoman Edith Ramirez on "Always On" Devices (July 10, 2015), https://epic.org/privacy/internet/ftc/EPIC-Letter-FTCAG-Always-On.pdf.
[27] Serena Zheng, Marshini Chetty, and Nick Feamster, *User Perceptions of Privacy in Smart Homes*, (Feb. 2018): Web. https://arxiv.org/pdf/1802.08182.pdf
[28] Rachel Martin, *Listen Up: Your AI Assistant Goes Crazy For NPR Too*, NPR (Mar. 6, 2016), http://www.npr.org/2016/03/06/469383361/listen-up-your-ai-assistant-goes-crazy-for-npr-too.
[29] Carlos Correa, *News Anchor Sets off Alexa Devices Around San Diego Ordering Unwanted Dollhouses*, CW6 (Jan. 5, 2017), http://www.cw6sandiego.com/news-anchor-sets-off-alexadevices-around-san-diego-ordering-unwanted-dollhouses/.
[30] Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. Times (Dec. 28, 2016), https://www.nytimes.com/2016/12/28/business/amazonecho-murder-case-arkansas.html.
[31] Campaign for a Commercial-Free Childhood, *Stop Mattel's "Hello Barbie" Eavesdropping Doll*, (Feb. 2015) http://www.commercialfreechildhood.org/action/shut-down-hello-barbie.

determine "all the child's likes and dislikes."[32] The doll introduced "always on" voice recording into not only private homes, but specifically into the play of young children.

EPIC joined advocacy groups on filing another complaint to the FTC on two internet-connected toys, My Friend Cayla and i-Que Intelligent Robot, which capture, record, and analyze what children say and respond to them.[33] The complaint alleged that the manufacturer of these products, Genesis Toys, and the technology provider, Nuance Communications, unfairly and deceptively collect, use, and share audio files of children's voices without providing adequate notice or obtaining verified parental consent, and fail to prevent strangers and predators from covertly eavesdropping on children's private conversations, creating a risk of stalking and physical danger.

In sum, both the intentional designs (e.g., Amazon Echo) and unintentional flaws (e.g., Google Home Mini) of IoT devices present risks to consumers.

C. Consumers Face Exposure to Harm from Secondary Uses of Sensitive Data Collected by IoT Devices

The vast quantity of data generated by IoT creates the risk that this data could be used for purposes that are either unnecessary to the provision of a given service or not initially disclosed to the consumer. Smart devices could reveal a wealth of information about consumers' location, media consumption, activity patterns, associations, lifestyle, age, income, gender, race, and health – information with potential commercial value. Companies might attempt to exploit this data by using it to target advertising or selling it directly.[34] Because the Internet of Things generates data from all aspects of consumers' lives, these types of secondary uses could lead to the commercialization of intimate segments of consumers' lives.

D. Recommendation: CPSC Should Require IoT Manufacturers to Minimize Data Collection and Increase Consumer Controls

Despite these risks, manufacturers that collect granular data do not offer equally granular choices on disabling the device sensors. Individuals should always retain control over their personal data, including the right to limit the collection and use of data beyond that necessary to the provision of the service. A "notice and choice" or consent-based approach to privacy protections simply does not work in the Internet of Things. As one commenter explains,

---

[32] Iain Thomson, Hello Barbie: *Hang on, this Wi-Fi doll records your child's voice? What could possibly go wrong?* The Register (Feb. 19, 2015), http://www.theregister.co.uk/2015/02/19/hello_barbie/

[33] In the Matter of Genesis Toys and Nuance Communications, (2016) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf

[34] EPIC Comments to NIST, *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 4,* (Nov. 9, 2009), https://epic.org/privacy/smartgrid/EPIC%20Smart%20Grid%20Comments.pdf.

> Internet of Things devices generally have no screen or keyboard, and thus giving consumers data and privacy information and an opportunity to consent is particularly challenging. Current Internet of Things products often fail to notify consumers about how to find their relevant privacy policy, and once found, such policies are often confusing, incomplete, and misleading.[35]

Notice and choice are insufficient to protect consumer privacy in the traditional online ecosystem,[36] and will be even less effective in the Internet of Things. Moreover, privacy experts have observed that "user choice will frequently be illusory in a ubiquitously sensed environment."[37] Instead, CPSC should require IoT manufacturers to (1) minimize data collection, (2) be transparent about data collection, and (3) implement user controls to access the data collected. This approach would grant consumers affirmative rights and place privacy responsibilities on companies who collect consumer data from connected devices.

Companies should only collect data that is absolutely required for a specific purpose or functionality, and promptly dispose of it afterwards. Data minimization is critical to consumer safety in IoT, because "data that has not been collected or that has already been destroyed cannot fall into the wrong hands."[38] Retaining large amounts of data without a specified purpose and a limited retention period maximizes the potential harm that could result from a hacking incident or data breach. Manufacturers must adopt data minimization as a guiding principle to ensuring operational hygiene and data integrity.

Moreover, companies that collect data from smart devices must be required to provide access to this data for consumers. Many of the consumer benefits[39] of the Internet of Things—reduced costs, time savings, increased convenience—require or would be greatly improved by providing consumers with access to their data. Any data collected by smart devices should be made available to consumers through any laptop, tablet, or smartphone. Furthermore, consumers should also be able to access the basic logic behind any algorithm used by a company or vendor to make a decision about a consumer. For instance, if a Smart Grid central database determines

---

[35] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 Tex. L. Rev. 85, 95 (2014).
[36] *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy*, 2001 STAN. TECH. L. REV. 1 (2001).
[37] Ellen P. Goodman, *The Atomic Age of Data: Policies for the Internet of Things* 24, THE ASPEN INSTITUTE COMMUNICATIONS AND SOCIETY PROGRAM (2015), http://csreports.aspeninstitute.org/documents/Atomic_Age_of_Data.pdf.
[38] Statement of Former FTC Chairwoman Edith Ramirez, *Privacy and the IoT: Navigating Policy Issues* (Jan 6, 2015), https://www.ftc.gov/system/files/documents/public_statements/617191/150106cesspeech.pdf?version=meter+at+0&module=meter-Links&pgtype=article&contentId=&mediaId=&referrer=&priority=true&action=click&contentCollection=meter-links-click.
[39] *See, e.g., 4 ways the internet of things will radically change your life*, WHITEBOARD http://www.whiteboardmag.com/4-ways-the-internet-of-things-will-radically-change-your-life/.

that, based on their energy consumption, certain energy consumers will have their power switched off at certain times of the day, those consumers must be informed that their data classification has changed. Transparency is therefore a vital component of informed user choice. These are necessary safeguards for manufacturers to ensure consumer privacy in the sensitive data collected by IoT devices.

E. Recommendation: CPSC Should Require Manufacturers to Conduct a Privacy Impact Assessment to Identify and Patch Vulnerabilities in IoT Devices

Section 15(b)(2) of the CPSA requires every manufacturer, distributor, and retailer of a consumer product who obtains information which reasonably supports the conclusion that the product contains a defect which could create a substantial product hazard to inform the Commission of such defect or risk:

> SEC. 15. [15 U.S.C. § 2064]. SUBSTANTIAL PRODUCT HAZARDS
>
> (b) Every manufacturer of a consumer product, or other product or substance over which the Commission has jurisdiction under any other Act enforced by the Commission (other than motor vehicle equipment as defined in section 30102(a)(7) of title 49, United States Code), distributed in commerce, and every distributor and retailer of such product, who obtains information which reasonably supports the conclusion that such product—
>
> (1) fails to comply with an applicable consumer product safety rule or with a voluntary consumer product safety standard upon which the Commission has relied under section 9 [15 U.S.C. § 2058];
>
> (2) fails to comply with any other rule, regulation, standard, or ban under this Act or any other Act enforced by the Commission;
>
> (3) contains a defect which could create a substantial product hazard described in subsection (a)(2); or
>
> (4) creates an unreasonable risk of serious injury or death,
>
> shall immediately inform the Commission of such failure to comply, of such defect, or of such risk […]

Title 16 of the Code of Federal Regulations elaborates that manufacturers must determine whether the risk of injury associated with a product is the type of risk which will render the product defective:

> 16 CFR Chapter II, Subchapter B - CONSUMER PRODUCT SAFETY ACT REGULATIONS
>
> §1115.4 Defect.
>
> Thus, whether the information available reasonably suggests a defect is the first determination which a subject firm must make in deciding whether it has obtained information which must be reported to the Commission. In determining whether it has obtained information which reasonably supports the conclusion that its consumer product contains a defect, a subject firm may be guided by the criteria the Commission and staff use in determining whether a defect exists.

Conducting a thorough privacy impact assessment ("PIA") is the first step to identifying potential defects that could compromise the privacy and security of IoT devices.[40] Privacy assessments are a critical part of assessing the level of intrusiveness that new technologies could have on individual rights and safety. Leading privacy scholars Paul de Hert and David Wright have noted the value of publishing the assessments to demonstrate accountability.[41] Moreover, EPIC's "Privacy Impact Assessment" initiative is a key component of the organization's long-running open government project and consumer protection work.[42] Most recently, we advised the UK data protection authority on PIAs[43] and urged that assessments should make clear the risks of automated processing of personal data; increase accountability by embedding PIAs into organizational processes; and encourage privacy-enhancing techniques and data minimization to manage risk.

EPIC recommends that CPSC require PIAs as a procedural safeguard to ensuring transparency and accountability in the commercial processing of personal data by the Internet of Things. Manufacturers of consumer products have a broad obligation under the CPSA to report defects which create a substantial risk of injury to the public.[44] In order for manufacturers to fulfil their reporting duty under Section 15(b)(2), they must first audit their IoT devices to flag up the

[40] David Wright, *Making Privacy Impact Assessment More Effective*, The Information Society, Vol.29:307–315, (2013)
[41] David Wright & Paul de Hert, *Privacy Impact Assessment* (2012), Springer, Law, Governance and Technology Series, Vol. 6. at 27.

[42] EPIC, *EPIC v. FBI - Privacy Assessments*, https://epic.org/foia/fbi/pia/; *See also*, EPIC, *EPIC v. DEA - Privacy Impact Assessments*, https://epic.org/foia/dea/pia/; EPIC, *EPIC v. NSA - Cybersecurity Authority*, https://epic.org/foia/nsa/nspd-54/default.html; EPIC, *EPIC v. Presidential Election Commission*, https://epic.org/privacy/litigation/voter/epic-v-commission/;EPIC, *EPIC Open Government*, https://epic.org/open_gov/; EPIC, *Complaint In re Universal Tennis to the Federal Trade Commission* (May 17, 2017), https://epic.org/algorithmic-transparency/EPIC-FTC-UTR-Complaint.pdf
[43] EPIC Comments to UK Information Commissioner's Office, *Consultation on Data Protection Impact Assessments (DPIAs) Guidance* (Apr. 12, 2018), https://epic.org/algorithmic-transparency/EPIC-ICO-Comment-GDPR-DPIA.pdf
[44] 15 U.S.C. § 2064

potential hazards. Therefore, the Commission should require manufacturers to conduct a thorough PIA on IoT devices as a means to identify, assess, and report privacy and security vulnerabilities.

Requiring PIAs at the manufacturing stage promotes internal oversight of legal and regulatory compliance. PIA processes should be adopted by IoT producers to examine the information flows of personal and potentially sensitive data—detailing how the data is processed and maintained in transit and in storage. IoT manufacturers and technical designers should comprehensively address and explain the complexities of the underlying data processing systems to the Commission. This assessment would help minimize safety risks by requiring manufacturers to understand how their device works, the implications for privacy and security, and to eliminate the potential for unauthorized access or misuse.

Privacy awareness in the device's functionality is key to monitoring and patching vulnerabilities, minimizing data collection, managing data access, and prohibiting secondary uses of data without affirmative consent by the consumer. If, for example, PIA appraisals indicate that de-identification is not feasible at certain volumes of data, then the company should employ differential privacy methods or encryption.

CPSC oversight of PIAs would serve an important function of preventing hazardous conditions from being designed into the products without sufficient consideration. Manufacturers should no longer escape their statutory reporting obligations to the CPSC by remaining ignorant of the harmful risks of their own devices. The Commission has the necessary statutory authority and consumer protection expertise to promote accountability in the supply chain by enforcing privacy and security assessments.

(2) Cybersecurity Risks Can Cause Physical Harms to Consumers

A significant risk to consumers in IoT is security, of both the users' data and their physical person. Many of the same security risks that currently threaten our data will only expand with the growth of IoT. The damage caused by malware, phishing, spam, and viruses will have an increasingly large array of networks in which to spread.[45] Additionally, not all wireless connections for IoT devices are encrypted.[46] Researchers who studied encryption within the Internet of Things found that "many of the devices exchanged personal or private information with servers on the Internet *in the clear*, completely unencrypted."[47]

[45] *See* EUROPEAN COMM'N, A DIGITAL AGENDA FOR EUROPE, 16-18 (2010), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

[46] Federal Motor Vehicle Safety Standards; Event Data Recorders, Docket No. NHTSA-2012-0177 (Comments of Privacy Coalition), 10 https://epic.org/privacy/edrs/EPIC-Coal-NHTSA-EDR-Cmts.pdf.

[47] Nick Feamster, *Who Will Secure the Internet of Things?*, FREEDOM TO TINKER (Jan. 19, 2016) https://freedom-to-tinker.com/blog/feamster/who-will-secure-the-internet-of-things/ (emphasis in original).

A. Unsecured IoT Devices Can Expose Consumers' Personal Information to Malicious Attackers

Unsecured IoT poses risks to physical safety and personal property. Criminals could exploit vulnerabilities in IoT devices and associated services to access, damage and destroy data and hardware or cause physical, or other types of harm. This is particularly true given that the constant flow of data so easily delineates sensitive behavior patterns, and flows over networks that are not always secure, leaving consumers vulnerable to malicious hackers.[48] For instance, a hacker could monitor Smart Grid power usage to determine when a consumer is at work, facilitating burglary, unauthorized entry, or worse.

A recent analysis of Smart Home security reveals additional safety risks posed by the Internet of Things. Researchers were able to remotely unlock front doors and set off fire alarms via Samsung's SmartThings platform.[49] Researchers have also found baby monitors vulnerable to hacking,[50] smart-watch motion sensors that can leak information on what wearers are typing,[51] drug infusion pumps that allow hackers to raise medication dosages to fatal levels,[52] and pacemakers than can send deadly electric shocks through hacked transmitters.[53]

B. Unsecured Connections to IoT Devices Can Cause Botnet Attacks on Individuals and Communities

Where these vulnerabilities can be exploited at scale, impact could be felt by multiple victims across geographic boundaries.[54] Poorly secured IoT devices can be used for botnets that launch network attacks with devastating impacts on the whole community. Hackers could conceivably exploit vulnerabilities on your "smart" refrigerator to carry out a denial of service attack against the network of a city or hospital. In the past few months alone there have been several such attacks. A ransomware attack known as SamSam took down the entire municipality

---

[48] M. Granger Morgan, et. al, *The Many Meanings of "Smart Grid,"* 5 (2009), http://www.epp.cmu.edu/Publications/Policy_Brief_Smart_Grid_July_09.pdf.

[49] Andy Greenberg, *Flaws in Samsung's 'Smart' Home Let Hackers Unlock Doors and Set Off Fire Alarms*, WIRED (May 2, 2016), https://www.wired.com/2016/05/flaws-samsungs-smart-home-let-hackers-unlock-doors-set-off-fire-alarms/.

[50] Dan Goodin, *9 Baby Monitors Wide Open to Hacks That Expose Users' Most Private Moments*, ARS TECHNICA (Sep. 2, 2015), http://arstechnica.com/security/2015/09/9-baby-monitors-wide-open-to-hacks-that-expose-users-most-private-moments/;

[51] Jennifer Abel, *Your Smartwatch Motion Sensors Could Tell Hackers What You're Typing*, CONSUMER AFFAIRS (Sep. 11, 2015), https://www.consumeraffairs.com/news/your-smartwatch-motion-sensors-could-tell-hackers-what-youre-typing-091115.html.

[52] Kim Zetter, *Hacker Can Send Fatal Dose to Hospital Drug Pumps*, WIRED (June 8, 2015), https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/.

[53] Darren Pauli, *Hacked Terminals Capable of Causing Pacemaker Deaths*, ITNEWS (Oct. 17, 2012), http://www.itnews.com.au/news/hacked-terminals-capable-of-causing-pacemaker-mass-murder-319508.

[54] UK Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (Mar. 2018), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf.

of Farmington, New Mexico and two hospitals by exploiting vulnerabilities in IoT devices.[55] The city of Atlanta spent 2.6 million dollars to recover from a ransomware attack that impacted municipal functions including the Police Department and the judicial system.[56]

The IoT has become a "botnet of things"—a massive network of compromised web cameras, digital video recorders, home routers, and other "smart devices" controlled by cybercriminals who use the botnet to launch widespread attacks on vital public services. The threats to physical safety and security caused by IoT devices are real, and it is the CPSC's mandate to make manufacturers accountable for identifying and eliminating these risks before they can reach consumers.

C. Recommendation: CPSC Should Adopt Strong International Standards for IoT Security

The problems discussed above will not be solved by the market. Manufacturers do not bear the negative externalities of compromised IoT devices—consumers do.[57] But consumers are not informed enough to anticipate these risks and act accordingly. Compromised devices often work fine, so most owners of devices that have been pulled into the "botnet of things" will have no idea that their IP cameras, DVRs, and home routers are no longer under their own control. Moreover, consumers rarely have adequate knowledge about the security of an IoT product when they are determining whether to purchase it. This information asymmetry makes it impossible for market forces to regulate the IoT effectively. IoT manufacturers are not incentivized to implement strong privacy and security safeguards through voluntary initiatives.

The UK Government accurately addressed this problem in a recent report entitled "Secure by Design: Improving the Cybersecurity of Internet of Things"[58] and set baseline rules for privacy and security that should be incorporated into the design and manufacturing of IoT.

---

[55] Bill Siwicki, *71% of IoT medical device ransomware infections caused by user practice issues*, Healthcare IT News (March 5, 2018), http://www.healthcareitnews.com/news/71-iot-medical-device-ransomware-infections-caused-user-practice-issues.

[56] Lily Hay Newman, *Atlanta Spent $2.6M to Recover from a $52,000 Ransomware Scare*, Wired (April 23, 2018), https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/.

[57] Bruce Schneier, *Will Giving the Internet Eyes and Ears Mean the End of Privacy?*, THE GUARDIAN (May 16, 2013), http://www.guardian.co.uk/technology/2013/may/16/internet-of-things-privacy-google ("These analytical limitations also mean that companies like Google and Facebook will benefit more from the Internet of Things than individuals – not only because they have access to more data, but also because they have more sophisticated query technology. And as technology continues to improve, the ability to automatically analyse this massive data stream will improve."); Bruce Schneier, *Power and the Internet*, SCHNEIER ON SECURITY (Jan. 31, 2013), https://www.schneier.com/blog/archives/2013/01/power_and_the_i.html ("The Internet empowers everyone. Powerful institutions might be slow to make use of that new power, but since they are powerful, they can use it more effectively."); *See generally*, Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy* 53 STANFORD LAW REVIEW 1393 (2001).

[58] UK Department for Digital, Culture, Media & Sport, *Secure by Design: Improving the cyber security of consumer Internet of Things Report* (March 2018),

> [C]onsumers are struggling to distinguish between good and bad security in devices on sale, primarily due to a lack of information about built-in device security. Additionally at present, consumers are not prioritising good security as a preference over other features included within a product. This further limits the incentives for manufacturers and suppliers to develop products with sufficient security built-in from the start.
>
> The Government can help create the right incentives for industry to improve the security of consumer IoT products and associated services and so facilitate a shift in behaviour across supply chains. In light of the increasing risk of IoT associated attacks, the Government will take the necessary steps to put these incentives in place.[59]

The Commission is empowered by the CPSA to set a mandatory regulation when it determines that compliance with a voluntary standard would not eliminate or adequately reduce a risk of injury, or finds that it is unlikely that there will be substantial compliance with a voluntary standard. [Sec. 9 CPSA, 15 U.S.C. § 2058]

The current regulatory environment is too weak to protect American consumers. Most companies have not adopted voluntary standards on IoT security, which has allowed catastrophic botnet attacks and privacy breaches to occur at the expense of consumer safety. Industry-wide adherence to modern security practices could have prevented many of these attacks.

Therefore, CPSC should establish mandatory privacy and security standards and require certification to these standards before IoT devices are allowed into the market stream. To harmonize the use of cybersecurity standards for international manufacturers, CPSC should coordinate its IoT policy development with strong international guidelines such as the UK Government's "Secure by Design" report.

EPIC agrees with the UK Government's assessment that "there is a need to move away from placing the burden on consumers to securely configure their devices, and instead ensure that strong security is built in by design."[60] The code of practice proposed by the UK government serves as a useful framework for security standards for IoT. In particular, manufacturers should adopt the following:[61]

1. No default passwords

---

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

[59] *Id.* at 1.14 – 1.15.

[60] *Id.*

[61] *Id.*

2. Implement a vulnerability disclosure policy
3. Keep software updated
4. Securely store credentials and security-sensitive data
5. Communicate securely
6. Minimize exposed attack surfaces
7. Ensure software integrity
8. Data protection
9. Make systems resilient to outages
10. Monitor system telemetry data
11. Make it easy for consumers to delete personal data
12. Make installation and maintenance of devices easy
13. Validate input data

This guidance necessitates privacy and security enhancing techniques in the form of a code of practice. This baseline regulation would ease the burden currently placed on consumers to safely install, maintain, and dispose of IoT products with limited information on the privacy and security of each control and default setting. These are smart rules that the CPSC should adopt to establish a rights and responsibilities model in IoT that is clear, functional, and measurable in consumer products. The Commission's initiative in IoT would ensure that consumers can safely and confidently embrace new technologies entering the market with the assurance that manufacturers have a common approach on the safeguards for privacy and security.

Not only would these rules necessitate effective communication across the IoT supply chain to meet safety standards, they would also promote best practices for privacy and security in other sectors associated with internet-connected devices. By implementing this code of practice, CPSC would rightfully shift the responsibility of product safety back to manufacturers where it belongs.

III. Conclusion

The Internet of Things presents important implications for consumer privacy and security. The CPSC must act now to ensure that emerging technologies are implemented in a

way that respects consumer safety. EPIC welcomes the opportunity to work with the Commission on this important issue.

Respectfully Submitted,

Marc Rotenberg,
EPIC President and Executive Director

Sunny Seon Kang,
EPIC International Consumer Counsel

Christine Bannan,
EPIC Administrative Law Fellow