Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of:	)	
	)	
Cybersecurity Labeling for Internet of Things	)	PS Docket No. 23-239
	)	

Reply Comment of Electronic Privacy Information Center (EPIC)

Communications and Technology Law
Clinic at Georgetown Law
Counsel for the Electronic Privacy
Information Center

Michele Gilman, Acting Director
michele.gilman@georgetown.edu

Lauren Harriman, Clinical Teaching Fellow
L.Harriman@georgetown.edu

Kristen Abram and Lindsay Sergi,
Student Attorneys

Via electronic filing
November 10, 2023

Electronic Privacy Information Center (EPIC)
John Davisson, Senior Counsel and Director of Litigation • davisson@epic.org
Christopher Frascella, Counsel • frascella@epic.org
Washington, D.C.
www.epic.org

The following organizations sign on to this comment:

Clinic to End Tech Abuse (CETA)
Lana Ramjit, Director of Operations • lana.ramjit@cornell.edu
New York, New York
https://www.ceta.tech.cornell.edu

Madison Tech Clinic
Rahul Chatterjee, Assistant Professor, University of Wisconsin-Madison
chatterjee@cs.wisc.edu
Madison, Wisconsin
https://techclinic.cs.wisc.edu

Public Knowledge
Sara Collins, Director of Government Affairs • sara@publicknowledge.org
Washington, D.C.
https://publicknowledge.org

Ranking Digital Rights (RDR)
info@rankingdigitalrights.org
Washington, D.C.
https://rankingdigitalrights.org

Table of Contents

I. Summary of Proceeding.

The undersigned organizations appreciate the opportunity to comment on the Commission's Notice of Proposed Rulemaking (NPRM) on the voluntary cybersecurity labeling of IoT devices program. The label's primary goal of ensuring consumer trust and confidence in the cybersecurity of their IoT devices will best be achieved through clear guidelines for label design and criteria. With this in mind, we believe that the Commission's guidelines for label criteria and design must set minimum cybersecurity standards, emphasize consumer accessibility, and establish mechanisms for enforcement that apply to the full IoT product, which includes the IoT device itself and its auxiliary components. Below, we discuss these criteria and recommendations responsive to questions proposed by this NPRM.

II. Introduction.

The Electronic Privacy Information Center (EPIC), the Clinic to End Tech Abuse (CETA), the Madison Tech Clinic, Public Knowledge, and Ranking Digital Rights (RDR) submit these comments in response to the Federal Communications Commission (FCC)'s August 2023 invitation for public comment concerning the agency's proposed creation of a voluntary cybersecurity labeling program for Internet of Things (IoT) devices.[1]

The Electronic Privacy Information Center is a public interest research center established in 1994 to protect privacy, freedom of expression, and democratic values in the information age through advocacy, research, and litigation.[2] EPIC has previously commented on other matters

[1] Cybersecurity Labeling for Internet of Things, Notice of Proposed Rulemaking, 88 Fed. Reg. 65937 (rel. Aug. 10, 2023) (hereinafter NPRM). Section numbers refer to the NPRM as the Commission released it, not as it appeared in the Federal Register.

[2] Electronic Privacy Information Center, *About Us,* https://epic.org/about (last visited Oct. 9, 2023).

related to privacy and transparency before the FCC,[3] and regularly comments before other agencies on related matters.[4]

We firmly support the FCC's creation of a voluntary cybersecurity labeling program and urge that the program be robust in its requirements, administration, and enforcement. Specifically, this comment will touch on the overall landscape of IoT cybersecurity and the needs of particularly vulnerable populations. It will also address how label qualification criteria should be designed with consumer priorities, such as data minimization, in mind. The label on the product itself should be easily readable, accessible, and point consumers to a second, digital version with additional, detailed information for those who would like it. In order to properly enforce the guarantees of the label, the FCC should require periodic recertification, with random post-certification audits to confirm compliance. Finally, there should be no safe harbor in civil litigation for usage of the label, as it would decrease both consumer trust and industry compliance with the label criteria.

---

[3] *See* Comments of EPIC, Center for Democracy and Technology (CDT), Privacy Rights Clearinghouse, and Public Knowledge, *In re* Data Breach Reporting Requirements, WC Dkt. No. 22-21 (Mar. 24, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1032465071814; *see also* Comments of EPIC, CDT, and Ranking Digital Rights, *In re* Empowering Broadband Consumers Through Transparency, CG Dkt. No. 22-2 (Feb. 16, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/102161424008021.

[4] *See, e.g.,* Electronic Privacy Information Center (EPIC) & Consumer Reports, Comment Letter on Requests for Information (Oct. 31, 2023), https://www.regulations.gov/comment/ONCD-2023-0001-0028; Electronic Privacy Information Center, *EPIC, Consumer Reports Urge National Cyber Director to Consider Consumer Privacy and Promote Prevalent Cybersecurity* Practices (Nov. 1, 2023), https://epic.org/epic-consumer-reports-urge-national-cyber-director-to-consider-consumer-privacy-and-promote-prevalent-cybersecurity-practices; Electronic Privacy Information Center (EPIC), Comment Letter on Proposed Trade Regulation Rule on Commercial Surveillance & Data Security (Nov. 2022), https://www.regulations.gov/comment/FTC-2022-0053-1195; Electronic Privacy Information Center, *FTC Rulemaking on Commercial Surveillance & Data* Security, https://epic.org/ftc-rulemaking-on-commercial-surveillance-data-security (last visited Nov. 6, 2023).

III. The Commission Should Provide Guidance on Label Criteria and Design.

As the popularity and development of IoT devices grows globally, examples of privacy and security breaches continue to proliferate. A number of high-profile instances involving the hacking of video and audio enabled devices have rightly raised concerns among consumers regarding the safety of IoT devices.[5] Beyond these widely publicized instances of IoT device cybersecurity breaches, malicious actors also use unpatched vulnerabilities to take control of large numbers of mobile phones, turn their radios into signal jammers, and take down mobile networks, making consumer privacy and cybersecurity on IoT devices a major issue for consumers.[6]

While consumers continue to show interest in smart devices, information regarding the security and privacy of IoT devices is often buried within in-box instruction manuals consumers cannot access until after purchase. Once consumers do have access to this information, it's largely too long and technical for the average buyer to use and make an informed decision.[7] Furthermore, manufacturers often prematurely halt device support and inadequately

---

[5] Pardis Emami-Naeini, Yuvraj Agarwal, Lorrie Faith Cranor, & Hanan Hibshi, *Ask the Experts: What Should Be on an IoT Privacy and Security Label?*, IEEE Symposium on Security and Privacy, 447 (May 2020), https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9152770.

[6] Federal Communications Commission (FCC), *Statement of Commissioner Nathan Simington Re: Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Notice of Proposed Rulemaking (2023), https://docs.fcc.gov/public/attachments/FCC-23-65A4.pdf (citing Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, Patrick McDaniel, & Thomas La Porta, On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core, 16th ACM Conf. on Comput. and Communications Sec. 223 (Nov. 2009), https://www.cise.ufl.edu/~traynor/papers/ccs09a.pdf).

[7] *See generally* Kristen L. Walker, *Surrendering Information Through the Looking Glass: Transparency, Trust, and Protection*, 35 J. of Pub. Pol'y and Mktg. 144 (2016).

communicate the length and scope of security support, leaving even informed consumers in the dark about the safety of their IoT devices.[8]

The proposed cybersecurity labeling program represents an opportunity to meet the goals of the White House's recent National Cybersecurity Strategy.[9] A key component of this strategy aims to expand IoT security labels, empowering consumers to make informed comparisons and ultimately "[create] a market incentive for greater security across the entire IoT ecosystem."[10]

While there are a number of vulnerable populations with special needs for IoT device privacy and cybersecurity, our label recommendations will specifically underscore the unique concerns of survivors of intimate partner violence (IPV). The discussion of distinct considerations for survivors of IPV will appear in sections outlining the importance of consumer education regarding data collected by IoT devices and design recommendations for the secondary cybersecurity label.

As the public continues to entrust IoT devices with greater responsibility, it is important that consumers have confidence in their devices' security.[11] To ensure that the label both protects and educates consumers, the FCC should provide clear guidance on (A) what the label should represent and contain, and (B) label design.

---

[8] *See Statement of Commissioner Nathan Simington, supra* note 6.

[9] *See* The White House, *National Cybersecurity Strategy*, 20 (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[10] *See id.*

[11] Pillar Three of the National Cybersecurity Strategy emphasizes "mak[ing] our digital economy more trustworthy" by "promoting privacy and security of personal data." The White House, *FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy* (Mar. 2, 2023), https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy.

A. What the Label Represents.

The label should represent a reliable marker of IoT device cybersecurity and privacy for consumers at the point of sale, whether online or in-store. The primary goal of this voluntary labeling program is to ensure consumer confidence in the cybersecurity of devices, a goal that can only be achieved through clear labeling criteria that prioritize consumer accessibility and strong minimum cybersecurity and privacy standards.

To ensure that content of IoT device cybersecurity labels effectively convey potential device privacy and security risk to consumers, label criteria should (i) apply to the full IoT product, (ii) align with reasonable consumer expectations, (iii) impose data minimization requirements, and (iv) outline parameters for device support.

i. Labeling criteria should apply to the full IoT product, including auxiliary components. (Responsive to Section 13.)

Labeling criteria should apply to the full IoT product in order to adequately protect consumers against potential cybersecurity risks associated with the product. The National Institute of Standards and Technology (NIST) defines an IoT product as "[a]n IoT device or IoT devices and any additional product components (e.g., backend, mobile app) that are necessary to use the IoT device beyond basic operational features."[12] This differentiation is crucial because IoT products are often purchased as a single IoT device, but still require other components—like

[12] *See* Michael Fagan, Katerina Megas, Paul Watrobski, Jeffery Marron, & Barbara Cuthill, *Profile of the IoT Core Baseline for Consumer Products*, National Institute of Standards and Technology, Department of Commerce, 2 (Sept. 2022), https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8425.pdf (hereinafter NIST IR 8425).

companion user applications—to operate.[13] While the IoT device itself plays a central role in the IoT product, many additional product components are vital to operation.[14]

Furthermore, "these additional product components have access to the IoT device and the data it creates and uses—making them potential attack vectors that could impact the IoT device, customer, and others . . . . Since these additional components can introduce new or unique risks to the IoT product, the entire IoT product, including auxiliary components, must be securable."[15] Realistically, consumers often have minimal control over these additional components because they are frequently necessary for the primary device to operate. Therefore, labeling criteria should apply to the full IoT product in order to adequately protect against potential cybersecurity risks associated with the product.[16]

ii. Labeling criteria should consider the reasonable expectations of an IoT consumer. (Responsive to Section 14.)

Labeling criteria should consider the reasonable expectation of an IoT consumer as suggested by the Department of Commerce's National Institute of Standards and Technology (NIST)'s Profile of the IoT Core Baseline for Consumer IoT Products.[17] This core baseline should serve as a starting point for manufacturers to identify the cybersecurity capabilities their

---

[13] *See id.* (explaining that in many cases, the IoT product may be purchased as one piece of equipment but still require other components to operate such as a companion user application or smartphone).

[14] *See id.* (explaining that while other components may be vital to the operation of the IoT product, the IoT device itself plays a central role to the product and is generally the focus of the operation of the product).

[15] *See id.* at 3.

[16] This definition is also supported by industry commenters like USTelecom. USTelecom, Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things, 6 (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1005095460108.

[17] *See* NIST IR 8425, *supra* note 12, at 2-16.

customers may expect from the IoT devices they sell.[18] As noted by numerous industry commenters, the best practice for building out cybersecurity labeling criteria is to prioritize the use of existing expertise.[19]

NIST's core baseline for the IoT device consumer profile was developed through external engagement with stakeholders regarding the needs of consumers, the assessment of vulnerabilities available in the public domain, and a year of outreach that generated hundreds of comments related to cybersecurity labeling for consumer IoT devices.[20] As one of the country's oldest physical science laboratories, with an industry vision of "creating critical measurement solutions and promoting equitable standards," NIST's core baseline provides a strong framework for IoT device consumer expectations.[21] We discuss consumer-friendly design further below.

iii. Labeling criteria should require the practice of data minimization for certification. (Responsive to Section 27.)

Data minimization should be a required practice for applying the U.S. Trust Mark label. Data minimization is a core feature of modern privacy and data protection policy.[22] This principle asserts that "data should only be collected, used, or disclosed as reasonably necessary

---

[18] *Id.*

[19] *See* Telecommunications Industry Association (TIA), Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10062191628584; USTelecom Comment Letter, *supra* note 16.

[20] *See* NIST IR 8425, *supra* note 12, at 17.

[21] National Institute of Standards and Technology (NIST), *About NIST*, U.S. Department of Commerce, https://www.nist.gov/about-nist (last updated Jan. 11, 2022).

[22] *See* Federal Privacy Council (FPC), *Fair Information Practice principles (FIPPs)*, https://www.fpc.gov/resources/fipps (last visited Nov. 6, 2023); *see also* Cobun Zweifel-Keegan, *Maximize your minimization and other takeaways form the FTC's Drizly case*, Int'l Ass'n of Priv. Professionals, (Oct. 26, 2022), https://iapp.org/news/a/maximize-your-minimization-and-other-takeaways-from-the-ftcs-drizly-case.

to provide the service requested by a consumer."[23] Criteria related to data minimization should "limit data collection as well as secondary uses and disclosure of the data that is amassed and stored."[24] As noted by other commenters, consumers see a link between cybersecurity and privacy, and data minimization is a practical way to ensure both forms of protection of consumers' data.[25] Consumer data breaches tend to involve personal data acquisition by malicious actors, and minimizing this possibility should be part of the labels' goals. Ultimately, "this framework is designed to enable processing and sharing of personal data that reflects the *volition of the consumer*, instead of permissions obtained under the fiction of informed consent."[26]

The most ambitious and consumer privacy-centric application of this goal would be the prohibition of all secondary uses with limited exceptions. Prohibiting most secondary use and third-party disclosure[27] while explicitly carving out certain exceptions for IoT devices and their auxiliary components would help mitigate consumer risk. Consumer Reports' Model State Privacy Act provides a baseline for carving out certain secondary and third-party disclosure exceptions like limiting the collection or sharing of a consumer's personal information if every

---

[23] Electronic Privacy Information Center, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, 3 (2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.

[24] *Id.* at 4.

[25] Consumer Reports, Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/100623134834.

[26] How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking, *supra* note 23, at 7.

[27] *See id.* at 16.

aspect of that commercial conduct takes place wholly outside of specified commercial purposes.[28]

The Commission should build data minimization into the label qualification criteria by requiring companies to only collect data reasonably necessary for the operation of the device. A company does not need to protect data that it does not collect. Ultimately, the consumer is safer if companies do not collect more data than they actually need to make the device work for its stated purposes.

iv. Labeling criteria should outline specific parameters for device support. (Responsive to Section 40.)

We recommend that the Commission not set explicit date ranges for device support warranty, but rather set parameters defining specific aspects of "support" and the frequency at which they should be provided to consumers. This proposition has received broad support in the comment docket from consumer-focused groups, industry groups, and individual consumers.[29] FCC Commissioner Simington, the White House's National Cybersecurity Strategy white paper,

[28] *See* Consumer Reports Digit. Lab, *Model State Privacy Act*, 18 (2021), https://advocacy.consumerreports.org/wp-content/uploads/2021/02/CR_Model-State-Privacy-Act_022321_vf.pdf (referencing model language in "Section 4. Exceptions").

[29] *E.g.,* Telecommunications Industry Association, Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things, 2-3 (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10062191628584; Consumer Reports Comment Letter, *supra* note 25.

and many consumers on this comment docket have all expressed concern about the warranty of cybersecurity of IoT devices.[30]

Relevant frameworks for IoT product vulnerability management include the Cybersecurity & Infrastructure Security Agency's (CISA) OASIS Common Security Advisory Framework (CSAF) Version 2.0 standard, the NIST's Profile of the IoT Core Baseline for Consumer IoT Products, and the European Telecommunications Standard Institute's (ETSI) Cyber Security for Consumer Internet of Things Baseline Requirement.[31]

As noted in Consumer Reports' comment, the NIST IoT criteria are based on product focused cybersecurity outcomes rather than specific requirements. The logic behind this is that an outcome-based approach allows for the flexibility required by a diverse marketplace of IoT products. Ultimately, it is the responsibility of FCC as the "scheme owner" (entity that manages the labeling program) to ensure that supporting evidence demonstrates that the product meets the expected outcomes.[32]

---

[30] *E.g.,* Owen Daniel Thompson, Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things (Sept. 5, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1090657138759; Theodore Rambert, Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things (Sept. 5, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1090630234624; Benjamin Carlsson, Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things (Sept. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/109061379827446. *See also* National Cybersecurity Strategy, *supra* note 9, at 20; Statement of Commissioner Nathan Simington, Fed. Communications Commission, https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-devices/simington-statement.

[31] OASIS Open, *Common Security Advisory Framework Version 2.0* (Nov. 18, 2022), https://docs.oasis-open.org/csaf/csaf/v2.0/os/csaf-v2.0-os.html; *See also* ETSI, *CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements*, (June 19, 2020), https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf.

[32] *See* Consumer Reports Comment, *supra* note 25.

Finally, while the CSAF framework is a guide for non-commercial IoT devices like Industrial Control Systems (ICS), Operational Technology (OT), and Medical Devices, its language promoting the creation, update, and interoperable exchange of security advisories presents a comprehensive and applicable guide to managing reports of vulnerabilities for consumer IoT devices.[33]

B. Label Design.

We propose that the FCC include a cybersecurity seal on the device itself in addition to a dual-level FCC cybersecurity label on the product packaging. To facilitate ease of readability and understanding, IoT device cybersecurity label design should (i) be similar in format and location to traditional nutrition labels, (ii) be accessible and machine readable, and (iii) employ a dual layer design system.

i. The label should be prominently placed, clear, and provide critical privacy and security information akin to a "nutrition label." (Responsive to Sections 29, 35.)

The privacy and security label should figure prominently on the accompanying device and provide critical privacy and cybersecurity information.[34]

The Commission's notice of proposed rulemaking for internet service provider labels states that "[p]roviders must be required to prominently display the label . . . [t]his means it has to be more than just a hyperlink to a separate page or pop-up window."[35] Ultimately, all

---

[33] Lindsey Cerkovnik, Daniel Larson, Justin Murphy, & Brandon Tarr, *Transforming Vulnerability Management: CISA Adds OASIS CSAF 2.0 Standard to ICS Advisories* (Sept. 29, 2023), https://www.cisa.gov/news-events/news/transforming-vulnerability-management-cisa-adds-oasis-csaf-20-standard-ics-advisories.

[34] Emami-Naeini, *supra* note 5.

[35] Empowering Broadband Consumers Through Transparency, Notice of Proposed Rulemaking, 87 Fed. Reg. 76959 (eff. Jan. 17, 2023), at 30.

information a consumer needs to make an informed purchase, including the IoT product's advertising and cybersecurity label, should exist on the product box for in-person sales, or on a single webpage in close proximity to the original ad at the point of sale online.

In the context of privacy, researchers have found that "privacy nutrition labels" can effectively convey information to website visitors and mobile app users.[36] Some experts emphasize the positive role of privacy and security labels in raising IoT companies' account-ability; for example, "There is value in forcing the company to write a list down even if the consumer doesn't understand it. If you said, 'list your open ports,' there would be an incentive to make them few."[37] Creating clear, easy-to-understand IoT device cybersecurity labels helps empower consumers to make informed choices and incentivizes competition and innovation in the marketplace.[38] Finally, we recommend adopting requirements for consistent label format and display location to facilitate ease of IoT product comparison for consumers.

ii. Beyond the scope of privacy and cybersecurity, the label should also be accessible and machine readable. (Responsive to Section 56.)

The label design should be accessible to people with disabilities so that all consumers have access to information about IoT device cybersecurity risk and should be machine readable so that consumers can use third party comparative tools to make a well-informed purchase.[39] It is important that people with disabilities have full access to the labels with or without the use of assistive technology. To best ensure accessibility to people with disabilities, we recommend that

---

[36] Emami-Naeini, *supra* note 5, at 447.
[37] *Id.*
[38] *Id.*
[39] Empowering Broadband Consumers Through Transparency, *supra* note 35 (referencing point of sale definition).

the Commission rely on the well-established legal requirements outlined by the Americans with Disabilities Act (ADA) alongside the Web Accessibility Initiative's robust guidance.[40]

Requiring machine readability for the proposed cybersecurity labels would help ensure that third party websites that compare, review, and recommend IoT products can efficiently access accurate, current information to relay to consumers. Machine readability refers to "data in a format that can be easily processed by a computer without human intervention while ensuring no semantic meaning is lost."[41] The FCC should require machine readability for both the primary and secondary labels.

iii. The label should employ a dual layer design system. (Responsive to Sections 35, 37.)

A two-tiered design should include (a) an easily glanceable primary layer and (b) a secondary layer that displays additional cybersecurity and privacy information.[42] The primary layer should be either a physical label located on the product box or displayed online at point of sale—regardless, this label should include only information which is important to most consumers and which most consumers readily understand. The secondary layer should be more detailed and exist online, accessible via a QR code or URL located near the bottom of the primary label layer.[43] Some commenters have advocated for simpler labels, as they are concerned that consumers will not be able to understand more complex labels. However, recent preliminary research shows that consumers do understand higher-complexity labels and are able

---

[40] Americans With Disabilities Act, 42 U.S.C. § 12101 (1990); *see also* WC3*, Web Content Accessibility Guidelines (WCAG) 2.2, Level AA* (Oct. 5, 2023), https://www.w3.org/TR/WCAG22.

[41] Empowering Broadband Consumers Through Transparency, *supra* note 35.

[42] Emami-Naeini, *supra* note 5, at 32-33.

[43] *Id.* at 32.

to answer questions based on information in these higher-complexity labels.[44] Furthermore, consumers preferred the higher-complexity labels, making them the most effective method.[45]

a) The primary layer should include information that is most likely to convey potential cybersecurity risk to consumers. (Responsive to Section 39.)

When determining what information to require for the primary layer located on the product box or displayed at point of sale online, the Commission should evaluate both the information's relevance to privacy and security and its likelihood of conveying risk to consumers.[46] In a recent study from Carnegie Mellon University, researchers found that consumers preferred a mock primary cybersecurity label that grouped information into three categories: (1) security mechanisms, (2) data practices, and (3) more information. Consumers find this categorization useful because, although the concepts of "privacy" and "security" are nearly inextricable, "consumers may have preferences for one aspect more than the other and stating them separately better enables consumer choice and education."[47] The recommendations immediately following the figure below build upon CMU's overall label design.

---

[44] Lorrie Cranor, Yuvraj Agarwal, & Pardis Emami-Naeini, Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things, 1-2 (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1006679712754.

[45] *Id.*

[46] *See* Emami-Naeini, *supra* note 5, at 448.

[47] *Id.* at 454.

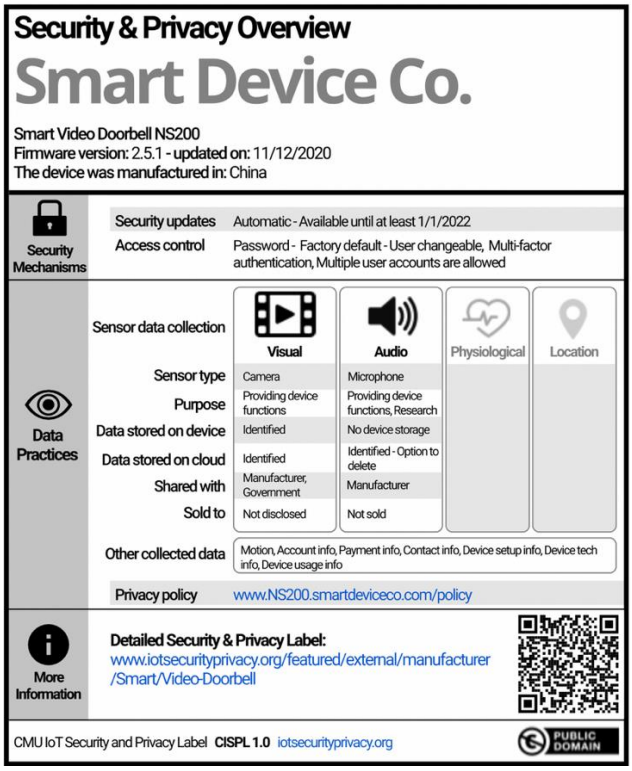


Fig. 1: Primary layer of the mock label in the CMU study. This layer should be printed on IoT product packaging and appear online alongside the product on retailer websites.

(1) Security Mechanisms.

The "Security Mechanisms" section of the primary label should include information on access controls, firmware version number and date, and information about continuing updates. The primary label should list access controls for the device and related apps (e.g., none, single-user account, multi-user account).[48] Additionally, we recommend that the firmware version number and date appear on both the primary and secondary label; the secondary label section below discusses this further. For clarification about updates, an asterisk should be included next

[48] *Id.* at 454.

to the final update date, directing consumers to review more continuously updated information regarding security updates available in the secondary layer of the label.

(2) Data Practices.

The "Data Practices" section should include information on the type, purpose, and location of data being collected so that consumers can accurately assess the privacy risks associated with a particular IoT device.[49] When applicable, the *type* of data being collected should indicate what kind of sensor is being used to collect this particular type of data (e.g., video, audio, physiological, geolocation).

Research shows that the purpose of data collection is one of the most important factors consumers weigh when making privacy choices regarding IoT devices.[50] Despite the importance of this factor to consumers, 67% of Americans say they don't understand what companies are doing with their data.[51] With this in mind, the W3C's Platform for Privacy Preferences (P3P) framework of twelve identified "purpose categories" is a useful framework for drafting primary label purpose categories.[52] Additionally, research indicates that many consumers are aware of the

---

[49] *Id.*

[50] *See* Bram Bonné, Saj Teja Peddinti, Igor Bilogrevic, & Nina Taft, *Exploring decision making with Android's runtime permission dialogs using in-context surveys*, 2017 Symposium on Usable Privacy and Security (SOUPS) 195, 195-210 (July 12, 2017); Hosub Lee & Alfred Kobsa, *Understanding user privacy in Internet of Things environments*, IEEE 3rd World Forum on Internet of Things 407, 407-12 (Dec. 12, 2016); Pedro Giovanni Leon, Blase Ur, Yang Wang, Manya Sleeper, Rebecca Balebako, Richard Shay, Lujo Bauer, Mihai Christodorescu, & Lorrie Faith Cranor, *What matters to users?: factors that affect users' willingness to share information with online advertisers*, 2013 Symposium on Usable Privacy and Security (SOUPS) 1, 7 (July 24, 2013).

[51] *See* Colleen McClain, Michelle Faverio, Monica Anderson, & Eugenie Park, *How Americans View Data Privacy*, Pew Rsch. Ctr., (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy.

[52] *See* W3C, *Web Content Accessibility Guidelines (WCAG) 2.2,* Background on WCAG 2, WCAG 2 Layers of Guidance (Oct. 5, 2023), https://www.w3.org/TR/WCAG22.

different privacy and cybersecurity implications associated with local data storage versus cloud storage.[53] With this in mind, displaying location of data storage on the primary label empowers consumers to make an informed assessment of the trade-offs between security and convenience.[54]

(3) More Information.

The "More Information" section should include URLs and QR codes that direct consumers to more detailed information about the IoT product's privacy and cybersecurity specifications in the expanded secondary label (see III.B.iii.b.3), as well as resources for vulnerable consumers that may be at risk for IoT device enabled domestic and intimate partner violence. More detailed specifications would be helpful to tech-savvy consumers, as well as to consumer advocates, to ensure that the labels are faithfully representing the capabilities of the device and the practices of the manufacturer.

Specifically, the "More Information" section on the primary label should also include a brief directive informing consumers impacted by tech-enabled abuse of pertinent resources, similar to best practice language displayed by broadcast networks prior to airing content related to suicide.[55] The pertinent resources linked from this directive should allow consumers to learn more about common bad-actor use case scenarios of IoT devices with surveillance capabilities

---

[53] *Id.*

[54] Emami-Naeini, *supra* note 5, at 255.

[55] *See* National Action Alliance for Suicide Prevention, *National Recommendations for Depicting Suicide*, 1 https://theactionalliance.org/sites/default/files/real_stories_natl_recommendations_for_depicting_suicide.pdf (last visited Oct. 26, 2023).

and how a consumer can access device override features to protect themselves.[56] In sum, the "More Information" section of the primary label presents an opportunity to direct consumers to more detailed information related to their specific needs and interests.

b) The secondary layer should be reserved for information that requires more explanation to convey consumer risk and information that is less crucial to a consumer's evaluation of the device's level of cybersecurity. (Responsive to Section 43.)

When determining what information should appear on the secondary, rather than primary layer, the Commission should evaluate whether the information in question requires substantial detail to adequately convey consumer risk and whether the information is less crucial to a consumer's evaluation of the device's level of cybersecurity.[57] Where information is important and able to be simply conveyed, it should be prioritized on the primary layer of the label; however, details that may only be of interest to more tech-savvy consumers or consumer advocates are appropriate to push out to the secondary layer. For continuity, the secondary layer should be broken down into the same categories as the first: (1) security mechanisms, (2) data practices, and (3) more information regarding physical actuations, a device's independent connectivity, and resources for consumers vulnerable to IoT enabled IPV.

---

[56] *See* Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, & Rahul Chatterjee, *Abuse Vectors: A Framework for Conceptualizing IoT-Enabled Interpersonal Abuse*, 32 USENIX Security Symposium 69, 74-77 (Aug. 2023), https://www.usenix.org/system/files/usenixsecurity23-stephenson-vectors.pdf (discussing common IoT surveillance features used by abusers).

[57] *See id.* at 70.

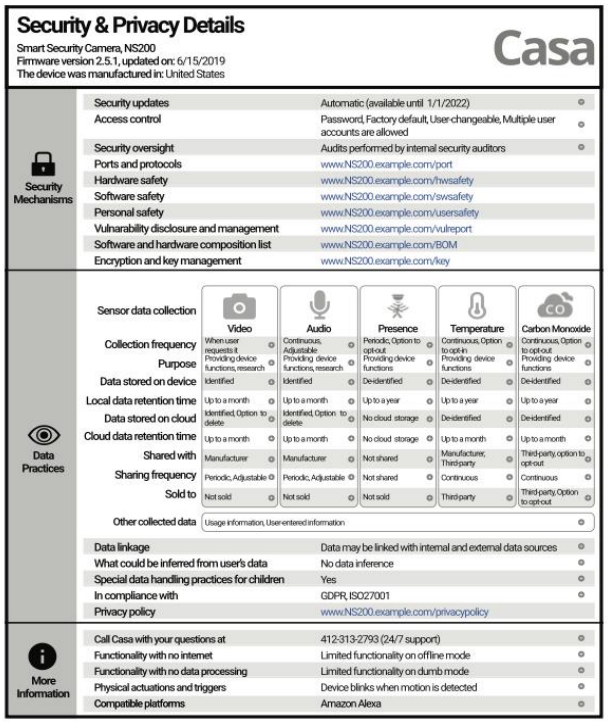


Fig. 2: Secondary layer of the label accessible via URL or QR code displayed within the "More Information" section of the primary layer.[58]

While our secondary label content recommendations slightly deviate from those of CMU, we do recommend the adoption of their overall label design.

(1) Security Mechanisms.

The "Security Mechanisms" section on the secondary label should include information on access control for device and apps (e.g., none, single-user account, multi-user account), ports and protocols, vulnerability and disclosure management, whether or not the device is getting cryptographically signed and critical automatic security software updates, and a continuously

[58] Emami-Naeini, *supra* note 5, at 458.

updated date reflecting when software updates will be provided along with software version number and date information.

Note that we recommend that the software version and number and date information appear on both the primary and secondary label. Given the frequency at which firmware updates occur and the importance of consumers having access to this information upon purchase, it is important that software version information appear on both layers of the label. The printed primary label should reflect the IoT device's software version at factory reset and the digital secondary layer should automatically update as part of the device's software update process to reflect the device's current software version.

(2) Data Practices.

The "Data Practices" section of the secondary label should include information on type of sensor(s) on the device; frequency of data sharing (e.g., continuous, on demand) and collection (e.g., once a month, on install); granularity of the data being collected, used, and shared (e.g., identifiable, aggregate); retention time; and relevant security and privacy laws and standards to which the device complies (e.g., ISO 27001, GDPR).

Although all of this information is indeed important for consumers to have access to, research shows that most consumers do not "understand the privacy and security implications of the frequency of data sharing."[59] Putting this information on the secondary layer aligns with the notion that information that has a higher likelihood of conveying risk to consumers should be prioritized to appear on the first layer.

[59] Emami-Naeini, *supra* note 5, at 454.

(3) More Information.

The "More Information" section of the secondary label should include information on a device's tracking and surveillance capabilities, its potential for harm to victims of IPV, and whether the IoT device can function without an internet connection.[60]

Having access to this information is particularly crucial for consumers experiencing, or at risk of, IPV. With the rise of IoT devices, abusers are finding new ways to perpetuate abuse digitally. Examples of this IoT enabled abuse include covert attachment of GPS trackers to vehicles to stalk victims, and the resetting of entry codes on smart locks to prevent victims from entering their own homes.[61] Many times, abusers perpetuate this abuse without hacking into the device; instead they use their victim's or shared log-in information to access devices.[62] Many times, the victims of IPV do not realize that their abusers are using their own IoT devices against them.[63] This lack of knowledge makes proving abuse in court difficult due to a lack of IoT device access logs reflective of abusive conduct. Even if they know about the abuse, they

---

[60] While abuse can and is perpetrated through devices that the survivor is aware of, it can also be perpetrated through covert devices. While this is likely outside of the scope of this proceeding, the harm caused by covert surveillance devices should be kept in mind when regulating the IoT industry. *See* Stephenson, *supra* note 56, at 76-77 (discussing several methods of covert surveillance using IoT devices).

[61] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, & Rahul Chatterjee, *"It's the Equivalent of Feeling Like You're in Jail": Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse*, 32 USENIX Security Symposium 105, 110 (Aug. 2023), https://www.usenix.org/conference/usenixsecurity23/presentation/stephenson-lessons.

[62] "Hacking" as it is used in this comment refers to accessing digital devices by overcoming security features, as opposed to mere unauthorized access where users access digital devices by exploiting security vulnerabilities.

[63] *See* Lessons from IoT-Enabled Intimate Partner Abuse, *supra* note 61*,* at 111-12. The paper specifically notes that many devices do not have access logs, which prevents survivors from seeing that their devices are being accessed.

frequently are unable to change their device settings to cut off their abuser's access.[64] For example, one survivor related a scenario involving a Ring doorbell that was registered to the abuser's name.[65] Even though the abuser did not live in the house, Amazon refused to disable the abuser's access because they were the named owner of the device.[66]

This lack of accessible education around IoT devices themselves, the data they collect, and how to prevent bad actors from accessing them is a serious problem, and the Commission's labeling program can bridge some of this education gap. The label should tell consumers what kinds of data the device collects, such as audio or geolocation. This would help survivors recognize that their devices can be used to perpetuate abuse.

As the discussion of the primary layer's "More Information" section notes, a URL and/or QR code should direct consumers to learn more about common bad-actor use case scenarios of IoT devices with surveillance capabilities as part of the pertinent resources included in that section. Additionally, devices designed to surveil or control a home should be designed to allow individuals physically residing in the home to override a remote order that may be intended to abuse them. A simple and effective way to communicate these potentially harmful use cases to consumers within the expanded format of the secondary layer is to use a chart similar to the one created by the USENIX Association, which breaks down an IoT product's surveillance

---

[64] *"It's the Equivalent of Feeling Like You're in Jail": Lessons from Firsthand and Secondhand Accounts of IoT-Enabled Intimate Partner Abuse* gave the example of the Ring doorbell that was registered to the abuser's name. Even though the abuser did not live in the house, Amazon refused to disable the abuser's access. Lessons from IoT-Enabled Intimate Partner Abuse*, supra* note 61, at 115.

[65] *Id.*

[66] *Id.*

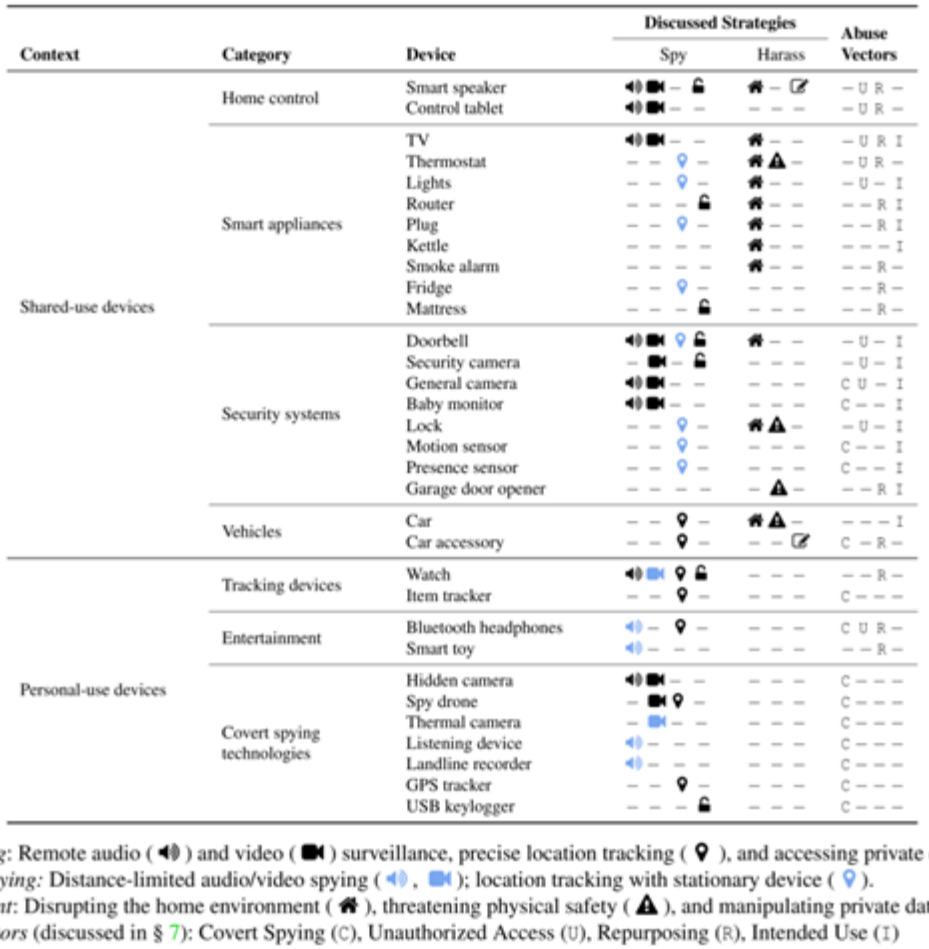
capabilities into category, context, and abuse strategies of spying and harassment.[67] Note that the example below represents multiple types of IoT devices and that any single device would likely only require a single row to convey context, category, and possible strategies of surveillance and harassment.

The label criteria should be designed not only to help mitigate some of this abuse, but also to facilitate consumer education around the vulnerability of their own devices.[68] Ultimately, using the same standardized, easily identifiable symbols (e.g., traditional symbols for audio and video) that appear on the primary label can explain more complex cybersecurity concerns related to physical actuations and the unique concerns of consumers experiencing IPV.

---

[67] Stephenson, *supra* note 56, at 75. Other commenters also support the label providing transparency around device surveillance capabilities. *See* Consumer Reports, Comment Letter on Proposed Rule for Cybersecurity Labeling for Internet of Things (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/100623134834.

[68] Part of the solution may include features to make hidden devices visible. Apple and Google have announced that they are developing features to address this after widespread reports of abusers using GPS devices to stalk victims. *See, e.g.,* Sarah Perez, *Apple and Google team up on industry spec to make Bluetooth tracking devices, like AirTag, safer*, TechCrunch (May 2, 2023), https://techcrunch.com/2023/05/02/apple-and-google-team-up-on-industry-spec-to-make-bluetooth-tracking-devices-like-airtag-safer.



Context	Category	Device	Discussed Strategies: Spy	Discussed Strategies: Harass	Abuse Vectors
Shared-use devices	Home control	Smart speaker	🔊 📹 – 🔓	🏠 – ✎	– U R –
		Control tablet	🔊 📹 – –	– – –	– U R –
	Smart appliances	TV	🔊 📹 – –	🏠 – –	– U R I
		Thermostat	– – 📍 –	🏠 ⚠ –	– U R –
		Lights	– – 📍 –	🏠 – –	– U – I
		Router	– – – 🔓	🏠 – –	– – R I
		Plug	– – 📍 –	🏠 – –	– – R I
		Kettle	– – – –	🏠 – –	– – – I
		Smoke alarm	– – – –	🏠 – –	– – R –
		Fridge	– – 📍 –	– – –	– – R –
		Mattress	– – – 🔓	– – –	– – R –
	Security systems	Doorbell	🔊 📹 📍 🔓	🏠 – –	– U – I
		Security camera	– 📹 – 🔓	– – –	– U – I
		General camera	🔊 📹 – –	– – –	C U – I
		Baby monitor	🔊 📹 – –	– – –	C – – I
		Lock	– – 📍 –	🏠 ⚠ –	– U – I
		Motion sensor	– – 📍 –	– – –	C – – I
		Presence sensor	– – 📍 –	– – –	C – – I
		Garage door opener	– – – –	– ⚠ –	– – R I
	Vehicles	Car	– – 📍 –	🏠 ⚠ –	– – – I
		Car accessory	– – 📍 –	– – ✎	C – R –
Personal-use devices	Tracking devices	Watch	🔊 📹 📍 🔓	– – –	– – R –
		Item tracker	– – 📍 –	– – –	C – – –
	Entertainment	Bluetooth headphones	🔊 – 📍 –	– – –	C U R –
		Smart toy	🔊 – – –	– – –	– – R –
	Covert spying technologies	Hidden camera	🔊 📹 – –	– – –	C – – –
		Spy drone	– 📹 📍 –	– – –	C – – –
		Thermal camera	– 📹 – –	– – –	C – – –
		Listening device	🔊 – – –	– – –	C – – –
		Landline recorder	🔊 – – –	– – –	C – – –
		GPS tracker	– – 📍 –	– – –	C – – –
		USB keylogger	– – – 🔓	– – –	C – – –

Full spying: Remote audio (🔊) and video (📹) surveillance, precise location tracking (📍), and accessing private data (🔓).
Limited spying: Distance-limited audio/video spying (🔊 , 📹); location tracking with stationary device (📍).
Harassment: Disrupting the home environment (🏠), threatening physical safety (⚠), and manipulating private data (✎).
Abuse vectors (discussed in § 7): Covert Spying (C), Unauthorized Access (U), Repurposing (R), Intended Use (I)

Fig. 3: This chart categorizes multiple smart devices by potential abuse strategies and abuse vectors.[69]

IV. Enforcement.

Labeling programs are only as good as their enforcement. To gain consumer confidence and ensure adequate incentives for improved cybersecurity, the cybersecurity label must be backed by a robust enforcement program. Additionally, the cybersecurity label should not operate as a safe harbor for tort liability stemming from a cybersecurity breach.

[69] *Id.* at 75.

A. To be successful in gaining consumer confidence, the cybersecurity label must be backed by a robust enforcement program.

Without an effective enforcement mechanism, consumers will have no reason to believe that the label aligns with the product's real-world cybersecurity. Furthermore, an ineffective enforcement mechanism would allow bad actors to take advantage of the goodwill created by the cybersecurity program, leaving consumers with products that they mistakenly believed would be secure. This would be particularly problematic for a government-backed label. If the government is going to take the time to validate a product's cybersecurity measures through this label, the labeling regime needs to have teeth. To enforce adherence to the label, the FCC should utilize (i) independent, post-certification audits, (ii) consequences for non-compliant products modeled on the ENERGY STAR® disqualification procedures, and (iii) a cure period to allow companies opportunity to patch cybersecurity vulnerabilities before being deemed noncompliant.

i. The FCC should implement thorough, independent post-certification audits of labeled products to ensure continued compliance. (Responsive to Sections 24-26, 32-33, 51.)

After a stringent, independent initial certification, the FCC should implement post-certification audits to identify noncompliant products. An effective model of a government-labeling program is the ENERGY STAR® program, in which the Environmental Protection Agency certifies environmental efficiency.[70] However, unlike ENERGY STAR®, the IoT Cybersecurity label is not meant to capture a product's compliance at a single point in time. Instead, it must represent a product's continued compliance. In order to ensure the success of this program, the Commission should rely on random audits in addition to periodic recertification.

---

[70] Environmental Protection Agency, *About ENERGY STAR®*, https://www.energystar.gov/about (last visited Oct. 15, 2023).

The audit must be more than a checklist noting what procedures are in place. The audit must test whether these procedures are effective. For example, asking whether a device uses strong password requirements is not enough to determine whether the device's password requirements are in fact adequate.[71] Instead, an auditor must test whether they can create a weak password despite the requirements in place.[72] Anything less risks overlooking the failure of policies that only appear to work on paper, which defeats the purpose of the audit in the first place.[73]

---

[71] Complex passwords are one of the most effective ways to protect devices. However, the most common passwords for IoT devices are weak, leaving devices more susceptible to hackers. Danny Palmer, *Is 'admin' password leaving your IoT device vulnerable to cyberattacks?*, ZDNET (Apr. 26, 2017), https://www.zdnet.com/article/is-admin-password-leaving-your-iot-device-vulnerable-to-cyberattacks.

[72] *See* Comments Of The Electronic Privacy Information Center, Center For Digital Democracy, and Consumer Federation Of America, to the California Privacy Protection Agency, Electronic Privacy Information Center, PR 02-2023 (Mar. 27, 2023), https://epic.org/documents/comments-of-the-electronic-privacy-information-center-center-for-digital-democracy-and-consumer-federation-of-america-to-the-california-privacy-protection-agency (hereinafter "EPIC CPPA Comment") (citing Kevin G. Coleman, Security Assessment or Security Audit?, infoTECH Spotlight (Sept. 21, 2009), https://it.tmcnet.com/topics/it/articles/64874-security-assessment-security-audit.htm).

[73] For example, the audits of Twitter following a 2011 consent decree failed to detect Twitter's noncompliance with the decree. Whistleblower Peter Zatko noted that part of this failure came from the audit's lack of investigation into whether the policies on paper played out as intended in practice. EPIC CPPA Comment, *supra* note 72 (citing Data Security at Risk: Testimony from a Twitter Whistleblower: Hearing Before the S. Comm. on the Judiciary, 117th Cong. (2022) (testimony of Peter Zatko), https://www.judiciary.senate.gov/meetings/data-security-at-risk-testimony-from-a-twitter-whistleblower).

A successful audit also requires auditor independence. Most sectors utilizing auditing recognize independent auditors as the gold standard.[74] Non-independence can severely hinder an audit's effectiveness, preventing successful identification or resolution of problems.[75] Other governmental entities recognize independence as an important factor in audits.[76] ENERGY STAR® utilizes independent certification bodies for its verification testing.[77] The California Privacy Protection Agency recently released draft regulations that would require businesses

---

[74] *See, e.g.*, Paul Munter, *The Importance of High Quality Independent Audits and Effective Audit Committee Oversight to High Quality Financial Reporting to Investors*, Securities and Exchange Commission (Oct. 26, 2021), https://www.sec.gov/news/statement/munter-audit-2021-10-26 (stating that auditor independence is foundational to credibility of financial statements); *Commission Adopts Rules Strengthening Auditor Independence*, Securities and Exchange Commission (Jan. 22, 2003), https://www.sec.gov/news/press/2003-9.htm (discussing the SEC's implementation of Sarbanes-Oxley's strengthened auditor independence requirements following the Enron financial scandal, which was partially perpetuated by functionally non-independent financial auditors).

[75] One of the most high-profile examples comes from the financial sector. The collapse of Enron highlighted an increased need for auditor independence, as this was one of the largest contributing factors in Enron's collapse. *See* Michael Peregrine & Charles Elson, *Twenty Years Later: The Lasting Lessons of Enron*, Harvard Law School Forum on Corporate Governance (Apr. 5, 2021), https://corpgov.law.harvard.edu/2021/04/05/twenty-years-later-the-lasting-lessons-of-enron (discussing how Enron's lack of independent audit and oversight significantly contributed to its collapse).

[76] Independent audits most often come up in the context of financial audits, and the SEC requires that financial auditors be independent. 17 CFR § 210.2-01 (1972) (discussing the SEC's requirement that qualified accountants be truly independent from their audit clients). However, other types of audits also typically require auditor independence. For instance, ENERGY STAR®'s verification testing also requires the testing to be done by independent parties. *See Verification Testing of Products*, ENERGY STAR®, https://www.energystar.gov/partner_resources/products_partner_resources/brand_owner_resources/verification_testing_products (last visited Oct. 14, 2023).

[77] *Disqualification Procedures ENERGY STAR® Products*, ENERGY STAR (Feb. 28, 2018), https://www.energystar.gov/sites/default/files/asset/document/Disqualification_Procedures_0.pdf .

which process personal information to periodically audit their cybersecurity practices.[78] The CPPA notes that while the auditor could be internal to the business, the auditor must:

> be free to make decisions and assessments without influence by the business being audited, including the business's owners, managers, or employees; and shall not participate in activities that may compromise, or appear to compromise, the auditor's independence. For example, the auditor shall not develop, implement, or maintain the business's cybersecurity program, nor prepare the business's documents or participate in the business activities that the auditor may review in the current or subsequent cybersecurity audits.[79]

This standard reflects the understanding that for an audit to be effective, the auditor must be free of internal pressures or biases. As such, any third-party administrator should be independent of the industry groups they are seeking to regulate. Independent, thorough audits are the best method to ensure continued compliance with the Cybersecurity Label.

ii. Enforcement mechanisms must be robust in order to maintain consumer confidence. (Responsive to Section 51.)

The Commission seeks comment on how to enforce the labeling program requirements. We propose that the Commission expand upon the mechanisms of the ENERGY STAR® label, given the increased risk IoT devices pose to the consumer.

Currently, the EPA relies on independent verification testing to uncover whether a product does not meet ENERGY STAR® standards.[80] If a product is disqualified, the company manufacturing the noncompliance product must:

- Cease shipment of units displaying the ENERGY STAR® label;

---

[78] *Draft Cybersecurity Audit Regulations For California Privacy Protection Agency*, California Privacy Protection Agency (Sept. 8, 2023), https://cppa.ca.gov/meetings/materials/20230908item8.pdf.

[79] *Id.* at 7.

[80] *Disqualification Procedures ENERGY STAR® Products, supra* note 77.

- Cease labeling associated units as ENERGY STAR®;
- Remove ENERGY STAR® references from related marketing materials; and
- Cover or remove labels on units within brand owner control.[81]

The EPA then subsequently updates the disqualified products list on the ENERGY STAR® Program Integrity webpage with the disqualified product information.[82] To ensure that companies actually do remove the ENERGY STAR® label from disqualified products and their marketing materials, the EPA also maintains a Retail Store-Level Assessment to identify any products that are improperly labeled as ENERGY STAR®.[83] The FCC's cybersecurity enforcement mechanism should include all of these actions, to protect both consumer expectations and good industry actors.

To help remedy consumer harms, the FCC should consider implementing a "cure period" for non-compliant companies to fix discovered vulnerabilities. A cure period gives good actors the opportunity to fix any issues without incurring penalties and ultimately ensures more protection of consumer data.[84] A short and enforced cure period is necessary because of the differences in potential harms between a false ENERGY STAR® certification and a false IoT

---

[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] The longer a vulnerability remains unpatched, the more likely that a bad actor will be able to exploit it. Allowing a short cure period will incentivize companies to fix vulnerabilities quickly, giving less opportunities for exploitation. As noted by Consumer Reports, other Federal agencies follow this rationale in requiring prompt cybersecurity incident disclosures. Consumer Reports Comment Letter, *supra* note 25, at 31 (*citing* U.S. Securities and Exchange Commission, *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (last accessed Oct. 6, 2023), https://www.sec.gov/news/press-release/2023-139).

Cybersecurity certification.[85] False ENERGY STAR® certifications lead to consumers paying more money than expected, either through increased energy costs or through a premium for a seemingly environmentally efficient product.[86] An IoT device breach can compromise security cameras, enabling thieves to effectively break into locations, enable blackmailers to harass individuals with material from the individual's personal security cameras, and cause other irrevocable privacy-related harms.[87] Furthermore, this type of breach could also negatively impact national security, like when location data from a popular fitness app exposed the location of secret U.S. military bases.[88] As the White House National Cybersecurity Strategy notes, insufficient IoT device security can cause incredible harm, and enforcement mechanisms should reflect this severity.[89] Additionally, while the ENERGY STAR® model is effective as a marketplace cure, it will not be able to fully remedy consumer harms in the event of cybersecurity noncompliance. In order to address this additional element of harm, enforcement

---

[85] Other commenters also support using a short cure period in the event of a breach. *See* Consumer Reports Comment Letter, *supra* note 25.

[86] *See* Office of Public Affairs, *DOE Reaches Agreement with LG Electronics, USA, On Refrigerator Energy Matter*, Department of Energy (Nov. 14, 2008), https://www.energystar.gov/ia/partners/manuf_res/PressRelease_DOE_LG_SettlementAgreement.pdf (discussing consumer benefits from ENERGY STAR® branded products).

[87] Mike Elgan, *IoT Security: Thieves Are Targeting Smart Cameras – Here's How To Stop Them*, SecurityIntelligence (June 3, 2021), https://securityintelligence.com/articles/iot-security-smart-camera-thieves.

[88] Alex Hern, *Fitness tracking app Strava gives away location of secret US army bases*, The Guardian (Jan. 28, 2018), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases.

[89] *See* National Cybersecurity Strategy, *supra* note 9, at 2-4. *See also* Statement of Commissioner Nathan Simington, Federal Communications Commission, https://www.fcc.gov/document/fcc-proposes-cybersecurity-labeling-program-smart-devices/simington-statement. Harms can be economic, from identity theft to industrial sabotage, or can even be physical, as in the case of hacks of medical devices.

mechanisms should be expanded to include the short cure period requirement in order to ensure effective consumer protections are in place.

If a company chooses not to fix the vulnerability, the FCC should consider utilizing administrative remedies to address the harm to the consumer. Such administrative remedies could include requiring the company to notify impacted consumers, corrective advertising, and financial penalties. ENERGY STAR® remedies include financial penalties and given the severity of potential damages in a cybersecurity incident, financial penalties should also be available to address deliberately noncompliant IoT actors.[90]

The FCC should also consider civil enforcement actions for a company that falsely puts the IoT certification mark or label on their products. No company should be allowed to trade on the label's goodwill without putting in the work required to build that goodwill, and any penalties should make the Commission's commitment to consumer trust clear. In this scenario, we encourage the FCC to take enforcement action or refer the matter to the Federal Trade Commission (FTC) to prosecute under its authority to combat deceptive acts or practices. The FTC already engages in civil litigation to combat false "Made in USA" claims, and that litigation has been promising.[91]

---

[90] One settlement agreement required LG Electronics to pay consumers the estimated difference in energy costs over a fourteen-year period in addition to repairing devices to the extent possible to make them compliant. Office of Public Affairs, *DOE Reaches Agreement with LG Electronics, USA, On Refrigerator Energy Matter*, Department of Energy (Nov. 14, 2008), https://www.energystar.gov/ia/partners/manuf_res/PressRelease_DOE_LG_SettlementAgreement.pdf.

[91] *FTC Issues Rule to Deter Rampant Made in USA Fraud*, Federal Trade Commission (July 1, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/07/ftc-issues-rule-deter-rampant-made-usa-fraud.

If a cybersecurity incident, such as a security breach, reveals noncompliance with label criteria, the FCC should consider more stringent penalties than a pure labeling violation with no consequential harm. Without more stringent penalties, consumers may conclude that the FCC's remedies are inadequate, and consumers will subsequently lose confidence in the label. Furthermore, penalties are necessary to create a deterrent against companies' non-compliance. In a situation where consumers experience harm as the result of a company's negligence, any penalty sought should reflect the harm caused.

iii. The Cybersecurity Label should not factor into the reasonableness standard for tort liability stemming from a cybersecurity breach. (Responsive to Section 52.)

The Cybersecurity Label should not factor into the reasonableness standard for tort liability stemming from a cybersecurity breach. In the event of litigation over a cybersecurity breach, companies should not be able to use the label as a defense. One of the top priorities of the National Cybersecurity Strategy is to hold makers of insecure products accountable for not taking reasonable precautions to secure their products.[92] As the White House notes, when organizations "fail to act as responsible stewards for this data, they externalize the costs onto everyday Americans."[93] Consumers are least able to bear the costs of a company's lack of care, with the greatest harm falling on vulnerable populations.[94] To prevent this, organizations with insecure products should bear the costs of their failure to implement reasonable cybersecurity.

A safe harbor provision would directly contradict the National Cybersecurity Strategy as well as consumer expectations, and allowing self-certification would further contradict both.

---

[92] National Cybersecurity Strategy, *supra* note 9, at 20-21.
[93] *Id.* at 19.
[94] *Id.*

Ultimately, the goal of the proposed label is to help increase consumer confidence in the cybersecurity capabilities of their IoT devices. Many industry commenters urge the FCC to establish a 'safe harbor' that would essentially allow companies to skirt compliance with other data security laws, fundamentally undermining the label's goal of bolstering consumer confidence. A safe harbor provision would not only place undue weight on a voluntary labeling program, but also veer beyond the authority of the FCC to preempt the legal proceedings of other jurisdictions. Accordingly, the FCC should clarify in the rule that the certification should not and cannot be used to avoid liability from a cybersecurity breach. Not only would a breach involving a product carrying the label shake consumer trust in the label; the availability of a "safe harbor" would fail to incentivize companies to keep their products safe and secure. The safe harbor would also disincentivize timely reporting of breaches, as companies are required to timely report breaches regardless of culpability.[95] Data breach reporting is typically strict liability—regardless of fault, if a breach occurs, a company is required to report that to both regulators and affected consumers.[96] Allowing a safe harbor use of the label in this context could enable companies to flout their breach reporting obligations, which in turn makes devices less safe.

Allowing self-certification to qualify for the label would further undermine consumer confidence. Indeed, the Department of Justice has created an entire initiative dedicated to prosecuting government contractors who falsely self-certify that their cybersecurity is sufficient,

---

[95] Consumer Reports Comment Letter, *supra* note 25, at 38-39.
[96] *Id.*

which is unfortunately common.[97] As a result, self-certification may be relevant when a company is recertifying that it is using the same procedures as when it submitted its initial application, but self-certification is not appropriate beyond this usage.

Furthermore, as noted by other commenters, a formal safe harbor program may not actually be a useful defense in litigation. While approval to use the cybersecurity label would be relevant in determining whether a company's cybersecurity practices were reasonable, the company would still need to prove that they were in compliance with the program in order to take advantage of such a defense.[98] It is possible that a company approved to use the label but would not in fact be in compliance with its obligations; that company should not be able to avoid liability through its mere participation in the labeling program.

Noncompliance with label obligations may come to light during a cybersecurity incident. In these cases, consumers are likely to view insulation from liability with skepticism and distrust. They are not likely to see previous years of compliance as a sufficient basis to excuse current negligence, and any safe harbor provision may contribute to this perception in the public eye. If that comes to pass, the label will fail at one of its most basic goals: ensuring consumer confidence in the cybersecurity of their devices.

V. Conclusion.

The FCC should consider the needs and expectations of consumers when designing the cybersecurity label. Consumers would reasonably expect that a device's cybersecurity

---

[97] Office of Public Affairs, *Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative*, Department of Justice (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[98] Consumer Reports Comment Letter, *supra* note 25.

certification would apply to all of the pieces of the device that they use, which is why labeling criteria should apply to auxiliary components in addition to the device itself. Consumers want their data to remain secure, which is why earning the right to place the label should require companies to only collect the data their product actually needs, and to describe what that data is. Consumers deserve to know how long they can safely use their devices, which is why Commissioner Simington and many individual commenters ask that the label include this type of information as well as a concrete definition of device support.[99] A prominently placed, easily readable label helps ensure that consumers can get the information they need at a glance, while interested consumers could use the secondary tier of the label to get more detailed information if they choose. Implementing a cure period for noncompliant products would incentivize industry to patch cybersecurity issues, thereby leading to more secure devices for consumers. Periodic recertification and audits ensure that consumers can trust that the label is up-to-date, and not allowing a safe harbor use for the label ensures that companies that fail to follow best practices are held accountable. Ultimately, these features are necessary to protect consumers, incentivize companies to create and maintain safe and secure products, and achieve the program's goals.

We thank the Agency for the opportunity to comment on its proposal for the cybersecurity label and are eager to continue working with the FCC to ensure the success of the label for all consumers.

---

[99] Statement of Commissioner Nathan Simington, *supra* note 6.

Respectfully submitted,

Electronic Privacy Information Center
Clinic to End Tech Abuse
Madison Tech Clinic
Public Knowledge
Ranking Digital Rights

By:

/s/ _____
Michele Gilman, Esq.
Michele.Gilman@Georgetown.edu
Lauren Harriman, Esq.
Kristen Abram, *Student Attorney*
Lindsay Sergi, *Student Attorney*
Communications & Technology Law Clinic
Georgetown Law
500 First St. NW
Suite 720
Washington, DC 20001

Counsel for the Electronic Privacy Information Center

Filed: November 10, 2023