Before the

Federal Communications Commission

In the Matter of:

Cybersecurity Labeling for Internet of Things

89 Fed. Reg. 20603, PS Docket No. 23-239

Further Notice of Proposed Rulemaking

Reply Comment of

Electronic Privacy Information Center (EPIC)

May 24, 2024

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

I. Introduction

The **Electronic Privacy Information Center (EPIC)**[1] submits these reply comments to the Federal Communications Commission (FCC or Commission) in response to the Further Notice of Proposed Rulemaking (FNPRM) about additional disclosures proposed in the Commission's rulemaking on Cyber Trust Mark labels for the Internet of Things (IoT), published in the Federal Register on March 25, 2024.[2] Although we tentatively support the Commission's proposals to require disclosures related to high-risk countries in the Trust Mark label, we urge the Commission to also require disclosures about access to consumer data, including indirect methods of obtaining access to data about Americans. Our comments briefly address additional specific questions asked about the Magnuson-Moss Warranty Federal Trade Improvement Act.

We also stress to the Commission that it should clarify that the Bureau and Lead Administrator should determine the *manner* in which privacy disclosures are made, not *whether* or not such disclosures should be made at all, especially as relates to location data and data that could increase risks to the personal safety of consumers such as survivors of domestic violence.

II. We tentatively support the Commission's proposal to require disclosures related to high-risk countries.

The Commission proposes requiring disclosures related to the involvement of high-risk countries in the development and maintenance of internet of things (IoT) products and end user data.[3] The Commission also asks whether additional disclosures are necessary, such as the specific country, the specific hardware or software components, or the specific operations performed in the high-risk country.[4] We support the Commission providing consumers with additional information about privacy and cybersecurity risks to their data, but urge the Commission to also require that the labels include information about data sales or transfers (direct or indirect) to entities within high-risk countries. Such transfers pose significant risks to consumers and to national security, both from direct production, sale, and management of hardware, software, and data, and from indirect data sales and other disclosures of data.

Requiring disclosure of all data transfers to high-risk countries, including indirect transfers, is easily administrable. Manufacturers and developers can put terms into their contracts with their own service providers and other business partners, and commit to enforcing those

[1] EPIC is a public interest research center in Washington, DC seeking to protect privacy, freedom of expression, and democratic values in the information age.

[2] *In Re: Cybersecurity Labeling for Internet of Things*, PS Docket No. 23-239, Further Notice of Proposed Rulemaking, https://www.federalregister.gov/documents/2024/03/25/2024-06249/cybersecurity-labeling-for-internet-of-things [hereinafter "FNPRM"].

[3] *See* FNPRM at ¶ 1, available at https://www.federalregister.gov/documents/2024/03/25/2024-06249/cybersecurity-labeling-for-internet-of-things#p-12.

[4] *See id.* at ¶ 3, https://www.federalregister.gov/documents/2024/03/25/2024-06249/cybersecurity-labeling-for-internet-of-things#p-18.

provisions.[5] Companies should be liable if they do not fulfill these commitments, including failing to audit whether their partners are honoring their contracts.[6] This is vital even for companies that build systems with U.S.-sourced components, that store data in the U.S., and that run firmware updates from U.S. providers, because these companies might still sell or transfer Americans' data or give access to entities in high-risk countries.[7]

Additionally, the Commission asks whether there should be any outright prohibitions on specific components, data storage, or other operations from a high-risk country.[8] We do not take a position on this proposal but note that many experts and policymakers including Senator Ron Wyden have observed that even countries not on the high-risk list could sell or transfer Americans' personal data to entities operating in high-risk countries,[9] and re-iterate that American companies can do the same.

The Commission also asks to what extent the Magnuson-Moss Act might also apply.[10] As we noted in our comments to the Federal Trade Commission, while academics have called for the application of the Magnuson-Moss Warranty Federal Trade Improvement Act (Warranty Act) to deficient cybersecurity practices exhibited by IoT companies, products that are licensed rather than purchased might fall outside the scope of the Warranty Act.[11] That said, to the extent the Warranty Act would apply, we encourage the Commission to structure the requirements of its

---

[5] This is in response to concerns voiced by groups like the National Electrical Manufacturers Association (NEMA). *See* Comments of NEMA at 4 (Apr. 24, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/1042423453771 ("NEMA manufacturers of consumer IoT products typically follow industry best practices and standards to understand what types of data flow through their network, however they may not have the ability to effectively track where the data travels across a network before it reaches its final destination.").

[6] *See, e.g.*, Statement of Commissioner Geoffrey Starks, In Re: AT&T Inc., File No.: EB-TCD-18-00027704, FCC 20-26 at 2 (Feb. 28, 2020), https://docs.fcc.gov/public/attachments/FCC-20-26A5.pdf.

[7] *See, e.g.*, Calli Schroeder and Caitriona Fitzgerald, *TikTok is Not the Only Problem*, EPIC.org (Mar. 23, 2023), https://epic.org/tiktok-is-not-the-only-problem/; Comments of EPIC to the U.S. Department of Justice, *In Re: Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern*, 89 Fed. Reg. 15780 (Apr. 19, 2024), available at https://epic.org/documents/epic-comments-to-doj-regarding-anprm-on-access-to-americans-bulk-sensitive-personal-data-and-government-related-data-by-countries-of-concern/.

[8] *See* FNPRM at ¶ 4, https://www.federalregister.gov/documents/2024/03/25/2024-06249/cybersecurity-labeling-for-internet-of-things#p-19.

[9] *See, e.g.*, Press Release, Wyden Statement on Data Export Executive Order (Feb. 28, 2024), https://www.wyden.senate.gov/news/press-releases/wyden-statement-on-data-export-executive-order; Justin Sherman, *Data Brokerage and Threats to U.S. Privacy and Security*, Written Testimony to U.S. Senate Committee on Finance, Subcommittee on Fiscal Responsibility and Economic Growth, Hearing on "Promoting Competition, Growth, and Privacy Protection in the Technology Sector" (Dec. 7, 2021), https://www.finance.senate.gov/imo/media/doc/Written%20Testimony%20-%20Justin%20Sherman.pdf.

[10] *See* FNPRM at ¶ 5, https://www.federalregister.gov/documents/2024/03/25/2024-06249/cybersecurity-labeling-for-internet-of-things#p-20.

[11] *See* Comments of EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, Federal Trade Commission 191-92 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf (citing to Stacy-Ann Elvy, *Hybrid Transactions and the Internet of Things: Goods, Services, or Software?*, 74 Wash. & Lee L. Rev. 77, 119–24, 154–64 (2017); Dallin Robinson, *Click Here to Sue Everybody: Cutting the Gordian Knot of the Internet of Things with Class Action Litigation*, 26 Rich. J.L. & Tech. 4, 7 (2020)).

Trust Mark so that it constitutes a written warranty under the Warranty Act.[12] We urge the Commission to require that any use of alternative dispute resolution provisions within these warranties do not foreclose subsequent class action litigation;[13] class actions are a vital mechanism for consumers to obtain relief because each harmed consumer on their own often faces strong economic disincentives and other barriers to pursuing litigation.[14]

III. The Commission should enhance its required disclosures about data practices and risks, to better inform consumers and advocates.

In the Trust Mark Report and Order, the Commission acknowledged in its first paragraph that "Internet of Things (IoT) products are susceptible to a wide range of relatively common security vulnerabilities that are increasingly exploited by cybercriminals who are *invading people's privacy* and threatening national security."[15] In her supporting statement, Chairwoman Rosenworcel declared that "the Cyber Trust Mark will help us make informed choices about the security *and privacy* of Internet of Things products we bring into our homes and businesses."[16] In its Order, the Commission directed the Lead Administrator to, within 90 days of their selection being publicly announced,

> submit to the Bureau recommendations on the design of the FCC IoT Label, including but not limited to labeling design and placement (e.g., size and white spaces, product packaging, *whether to include* the product support end date and other security and *privacy information* on the label.)[17]

And to "examine *whether* the label design should include the date the manufacturer will stop supporting the product as well as whether including other security *and privacy information (e.g.*

---

[12] *See* Fed. Trade Comm'n, Businessperson's Guide to Federal Warranty law, https://www.ftc.gov/business-guidance/resources/businesspersons-guide-federal-warranty-law.

[13] *See id.*

[14] *See, e.g.*, Comments of EPIC, National Consumer Law Center, et al., *In Re: Protecting Consumers from SIM-Swap and Port-Out Fraud*, WC Dkt. No. 21-341 at 8-19 (Feb. 12, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10213160552872.

[15] Report and Order and Further Notice of Proposed Rulemaking, *In Re: Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 at ¶ 1 (Rel. Mar. 15, 2024), https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf (emphasis added) [hereinafter "R&O"]. The Commission also quoted the May 2021 IoT Executive Order in its R&O: "persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and *privacy*." *Id.* at ¶ 6 (emphasis added).

[16] Statement of Chairwoman Jessica Rosenworcel, *In Re: Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 at 1 (Mar. 14, 2024), https://docs.fcc.gov/public/attachments/FCC-24-26A2.pdf (emphasis added). *See also* Peter J. Caven, et. al., *Comparing the Use and Usefulness of Four IoT Security Labels* 16 (2024), available at https://www.fcc.gov/ecfs/search/search-filings/filing/10925200278775 ("Even after being required to evaluate products on the basis of security, participants ranked privacy as more important than security in procurement decisions. Thus, effective security label designs could be more salient if these included privacy factors as well as security. Security and privacy concepts are highly intertwined. If privacy is the goal then security is that enabler. It is critical to not only design security in a way that protects consumers, but it is equally important to communicate in a way that reflects consumers' preferences.").

[17] R&O at ¶ 52(d)(v) (emphasis added).

sensor data collection) on the label would be useful to consumers."[18] The Commission also delegated authority to the Bureau to determine:

> *whether* any additional disclosure fields, such as the manufacturer's access control protections (e.g., information about passwords, multi-factor authentication), whether or not the data is encrypted while in motion and at rest (including in the home, app, and cloud), patch policies and security or *privacy information are necessary*.[19]

The Commission should take the opportunity now to emphasize the importance of disclosures related to privacy, in particular location and other sensor information, such as camera and microphone functionality. Model disclosures regarding sensor data developed by experts were submitted into the record and were widely supported by commenters.[20] While it may be prudent to delegate the *manner* of these disclosures, delegating *whether* or not they should be included is misguided and contrary to the record. The Commission should also require disclosures of information that may be vital to forewarning survivors of domestic violence about

[18] R&O at ¶ 110 (internal citations omitted) (emphasis added).

[19] R&O at ¶ 118 (internal citations omitted) (emphasis added) (citing to comments of Consumer Reports and to ex parte of Lorrie Cranor).

[20] *See, e.g.*, Comment of Dr. Lorrie Cranor and Dr. Pardis Emami-Naeini, *In Re: Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 at 2, 9 (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1006679712754; Comment of Consumer Reports at 2, 5, 15-16, 24, 29 (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/100623134834; Reply Comment of Consumer Reports at 5-6 (Nov. 12, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/1111250234240; Reply Comments of EPIC at 20, 24 (Nov. 10, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/111054758013; *see generally* Emami-Naeini, P. et al. Are consumers willing to pay for security and privacy of IoT devices? In *Proceedings of the 32nd USENIX Security Symp*. (2023), available at https://www.fcc.gov/ecfs/document/1213810900539/2 (discussing consumer purchase behaviors, namely that consumers are willing to pay a premium for devices with better security and privacy practices, and that manufacturers fail to disclose the sensing capabilities of their devices,); *see id.* at 13 ("Our qualitative analysis showed that when security and privacy information was not mentioned, participants assumed that the device's practices were not that risky"); Ex Parte, Consumer Reports at 1 (Dec. 13, 2023), https://www.fcc.gov/ecfs/document/1213810900539/6, "CR IoT Security Label Summer Research" at 7-8, https://www.fcc.gov/ecfs/document/1213810900539/5; Letter from Consumer Reports and Carnegie Mellon University at 2 (Mar. 11, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10311301914907. Similarly, some commenters argued for hardwired visual indicators of when sensors such as cameras or microphones are active. *See* Ex Parte, Hacker News Members at 28 (Sept. 14, 2023), https://www.fcc.gov/ecfs/document/109142048721137/3. *Compare with* Comment of ioXt Alliance at 21 (Oct. 6, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/10061850814251.

how their devices or other devices in their home,[21] vehicle,[22] or on their person[23] may be used to attempt to surveil, control, or re-victimize them, as a matter of personal safety, see *infra*.

The IoT Advisory Board (IoTAB) for the National Institute of Standards and Technology (NIST) acknowledges "growing concerns around data privacy, security, and the potential risks associated with the increased connectivity and interdependence of IoT systems" in their most recent report draft, under ER3.1.1.[24] We join commenters in this docket in echoing these concerns about privacy.[25] The IoTAB in its May 2023 meeting emphasized the importance of privacy-specific disclosures, noting that exposure of location data in particular can put certain populations at elevated risk.[26] There are significant risks posed to survivors of domestic violence that also justify broader privacy-related disclosures,[27] as we also explained in our most recent filings in the Safe Connections Act rulemaking.[28] We urge the Commission to require relevant disclosures to help protect the personal safety of survivors, and as such, disagree with

---

[21] *See, e.g.*, Donna Lu, *How Abusers Are Exploiting Smart Home Devices*, Motherboard (Oct. 17, 2019), https://www.vice.com/en/article/d3akpk/smart-home-technology-stalking-harassment; Pieter Arntz, *How to lcok out your ex-partner from your smart home*, Malwarebytes Labs (Jan. 24, 2024), https://www.malwarebytes.com/blog/news/2024/01/how-to-lock-out-your-ex-partner-from-your-smart-home; Starks Letters to Amazon, Sears, Shein, Temu, and Walmart (Mar. 8, 2024), available at https://www.fcc.gov/document/starks-letters-amazon-sears-shein-temu-and-walmart.

[22] *See, e.g.*, *In Re: Supporting Survivors of Domestic and Sexual Violence*, WC Docket No. 22-238, Further Notice of Proposed Rulemaking, FCC 24-38, at ¶ 1 (Apr. 23, 2024), available at https://www.federalregister.gov/d/2024-08642/p-19 [hereinafter "SCA FNPRM"]; Chairwoman on Safe Connected Cars for Domestic Violence Survivors (Jan. 11, 2024), https://www.fcc.gov/document/chairwoman-safe-connected-cars-domestic-violence-survivors.

[23] *See, e.g.*, Michael Levitt, *AirTags are being used to track people and cars. Here's what is being done about it*, All Things Considered (Feb. 18, 2022), https://www.npr.org/2022/02/18/1080944193/apple-airtags-theft-stalking-privacy-tech *but see* Jennifer Pattison Tuchy, *Apple finally adds iPhone alerts for third-party Bluetooth trackers*, The Verge (May 13, 2024), https://www.theverge.com/2024/5/13/24155630/apple-google-airtag-bluetooth-tracker-alert-standard.

[24] Work-in-Progress Draft Report of the Internet of Thing (IoT) Advisory Board (IoTAB) May 13, 2024 In-process Pre-read Draft at 139-40, available at https://www.nist.gov/system/files/documents/2024/05/13/Draft%20IoTAB%20Report%2020240513%20v5.pdf.

[25] *See* Comment of Aspen Digital, *In Re: Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 at 5 (Apr. 24, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10424097853241 ("Customers are concerned about where their personal information is being held, especially when it's countries that have a history of violating civil liberties. Nation-states and criminals can poison data sets, including those used in LLMs, to have connected software engage in harmful behavior.").

[26] *See* IoTAB Committee, *Meeting Minutes, May 16 & 17, 2023*, at 23-24 (May 17, 2023), available at https://www.nist.gov/system/files/documents/2023/07/14/May_2023_IoTAB_Day_1_and_2_Minutes_2023-06-27_v4%20Final.pdf.

[27] *See, e.g.*, Reply Comments of EPIC, Clinic to End Tech Abuse, Madison Tech Clinic, Public Knowledge, and Ranking Digital Rights, *In Re: Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 at 23-26 (Nov. 10, 2023), https://www.fcc.gov/ecfs/search/search-filings/filing/111054758013.

[28] *See* Comments of EPIC and Public Knowledge, *In Re: Supporting Survivors of Domestic and Sexual Violence*, WC Docket No. 22-238 (May 23, 2024), available at https://www.fcc.gov/ecfs/search/search-filings/filing/105242630421222.

commenters who would limit the Commission's concerns in this proceeding strictly to the national security implications of IoT data privacy and data security.[29]

The Commission was established in part "for the purpose of promoting safety of life and property through use of wire and radio communications."[30] As the Commission has already noted in its Safe Connections Act Report and Order: "Domestic violence remains a significant safety and public health issue that results in individual harm and societal costs, affecting not just survivors but also their families, friends, and colleagues."[31] The Commission also cited to Congress's explicit findings in the Safe Connections Act, namely that "perpetrators of violence and abuse . . . increasingly use technological and communications tools to exercise control over, monitor, and abuse their victims," and that "[c]ommunications law can play a public interest role in the promotion of safety, life, and property."[32] Taken together, this suggests that the Commission's directives to promote "safety of life" in regulating our nation's communications infrastructure demand that it use its authority to prevent the misuse of that infrastructure to perpetrate domestic violence[33] and not merely address national security concerns.

IV. Conclusion

We appreciate the opportunity to file reply comments to the Commission's FNPRM on cybersecurity labels for the Internet of Things.

Chris Frascella
Counsel
Electronic Privacy Information Center
1519 New Hampshire Avenue, NW
Washington, DC 20036

[29] *See, e.g.*, Comment of National Association of Manufacturers, *In Re: Cybersecurity Labeling for Internet of Things*, PS Dkt. No. 23-239 at 1 (Apr. 24, 2024), https://www.fcc.gov/ecfs/search/search-filings/filing/10424854410268.

[30] 47 U.S.C. § 151.

[31] Report and Order, *In Re: Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform Modernization, Affordability Connectivity Program*, WC Docket Nos. 22-238, 11-42, 21-450 at ¶ 2 (Rel. Nov. 16, 2023), https://docs.fcc.gov/public/attachments/FCC-23-96A1.pdf; re-iterated in SCA FNPRM at ¶ 3, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-21.

[32] SCA FNPRM at ¶ 4, https://www.federalregister.gov/documents/2024/04/23/2024-08642/supporting-survivors-of-domestic-and-sexual-violence#p-22 (citing to Safe Connections Act of 2022, H.R. 7132, 117th Cong. §§ 3(3), 3(4) (2022), https://www.congress.gov/bill/117th-congress/house-bill/7132/text).

[33] This could include but is not limited to mandatory data collection as part of an investigation or study on promoting safety of life. *See* 47 U.S.C. § 154(n).