1350 Eye Street NW, Suite 350, Washington, DC 20005 | 202-768-8950 | fpf.org

Filed online at fcc.gov/ecfs

August 19, 2024

Marlene H. Dortch
Secretary
Federal Communications Commission
Office of the Secretary
45 L Street NE
Washington, DC 20554

Re: Public Safety and Homeland Security Bureau Requests Comment on Implementation of the Cybersecurity Labeling for Internet of Things Program ("IoT Labeling Program")

The Future of Privacy Forum (FPF) welcomes the opportunity to submit comments in response to the Federal Communications Commission's (FCC, or Commission) Further Notice of Proposed Rulemaking (FNPRM) on the IoT Labeling program. In its FNPRM, the FCC seeks additional comment on the design and implementation of its Internet of Things (IoT) Labeling program, which creates a voluntary cybersecurity labeling program for consumer IoT products and was adopted on March 14, 2024 under Section 302 of the FCC Act.[1] FPF supports the inclusion of key information that would ensure individuals understand not only more about cybersecurity risks, but also relevant privacy risks IoT devices may create, and helps people to make informed choices about their devices. FPF is a global non-profit organization dedicated to advancing privacy leadership, scholarship, and principled data practices in support of emerging technologies.

Internet-connected devices, commonly referred to as the "Internet of things" or IoT, have become standard in both consumer and enterprise contexts, with over 15 billion IoT connections worldwide in 2024.[2] The FCC's IoT Labeling program is an important step toward improving transparency around consumer IoT device data practices, and FPF commends the Commission's work in developing this program. Specifically, in its FNPRM, the Commission contemplates the addition of information involving device sensors, data collection, data sharing, and data protection practices to the IoT Label registry.[3] FPF makes the following observations:

---

[1] Federal Communications Commission, *Proposed rule: Public Safety and Homeland Security Bureau Requests Comment on Implementation of the Cybersecurity Labeling for Internet of Things Program* (PS Docket No. 23-239; DA 24-617; FR ID 229959) (Jul. 18, 2024), https://docs.fcc.gov/public/attachments/FCC-24-26A1.pdf.
[2] Statista, *Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033*, https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/.
[3] *Supra* 1, at Sec. 21.

I. The presence of sensors on IoT devices enables sophisticated features, but also poses a number of risks to both cybersecurity and privacy.
II. Information about devices' sensors and data practices can help people make better decisions about the technologies they use, and is thus important information to include in the IoT Label registry.
III. Expanding the IoT Labeling program to cover additional considerations about IoT devices' data practices raises challenges involving program design and implementation that should be addressed.

I. The presence of sensors on IoT devices enables sophisticated features, but also poses a number of risks to both cybersecurity and privacy.

An increasing number of IoT and other consumer devices contain sensors that measure sound, visuals, movement, temperature, pressure, and other information involving users, bystanders, and the surrounding environment. These sensors—which commonly include cameras, microphones, gyroscopes, thermometers, and more—are intended to enable a wide range of features that make IoT devices convenient for both enterprise and home use.[4] For example, "smart" home appliances like thermostats and lighting can monitor and adjust a building's temperature and brightness, respectively, to achieve greater energy efficiency.[5]

As sensors on devices collect more data about users and their environments, those who operate those devices are able to create detailed profiles that may include intimate personal information. The aggregation of personal data may allow those collecting it to learn or infer sensitive information about people,[6] or to track people's behaviors across different spaces.[7] The wealth of personal data may also make devices more appealing targets for hackers, particularly if they're connected with other IoT devices. Sensors can create a vector for malicious actors who have compromised the security of devices to interfere with the privacy and security of the individual using it.

[4] Muhammad Ali Jamshed, Kamran Ali, Qammer H. Abbasi, Muhammad Ali Imran, and Masood Ur-Rehman, *Challenges, Applications and Future of Wireless Sensors in Internet of Things: A Review*, IEEE Sensors Journal. 22(6), pp. 5482-5494 (2022), https://eprints.gla.ac.uk/264052/1/264052.pdf.
[5] *IoT Sensors & Devices: What Are They & What's Their Role in Smart Homes?*, Lanars, https://lanars.com/blog/iot-sensors-and-devices.
[6] Daniel Berrick and Jameson Spivack, *Understanding Extended Reality Technology & Data Flows: Privacy and Data Protection Risks and Mitigation Strategies* (Nov. 17, 2022), https://fpf.org/blog/understanding-extended-reality-technology-data-flows-privacy-and-data-protection-risks-and-mitigation-strategies/.
[7] For more information on the kinds of sensors involved in extended reality (XR) devices, which often include similar sensors as IoT devices, see the attached infographic, "Understanding Extended Reality Technology & Data Flows." Available at https://fpf.org/wp-content/uploads/2022/10/XR-Infographic-Screen-reader-friendly-version.pdf.

II. Information about devices' sensors and data practices can help people make better decisions about the technologies they use, and is thus important information to include in the IoT Label registry.

Information about the presence of sensors in devices, including how they are used and what data they collect, helps people make better decisions about whether and how to use devices. Since different individuals have different security and privacy concerns, specificity about a device's data practices will make for stronger, more personalized threat modeling. For example, a survivor of domestic violence may be more concerned about threats from someone they are physically close to, whereas another person may worry more about attacks from unknown third parties. Transparency helps each person make better product decisions for themselves based on their unique privacy and security concerns.

Greater transparency also provides clarity to individuals regarding whether a device's sensors are actually being used. A device may include a sensor but not actively use it, and may later on choose whether to initiate use of the sensor, depending on user demand, regulatory requirements, or other business considerations.[8] Disclosing what data is collected, and with whom it's shared, will help people better understand when a given sensor listed in the registry is in use, rather than leaving them to assume it is just by virtue of being listed in the registry. Transparency also helps people identify potential security risks, as the inclusion of a sensor—even if not being used—can present an opportunity for exploitation by a malicious actor. When this information is listed in a public, easily accessible place like the registry, rather than in a device's product manual, it allows people to learn it *before* making a purchasing decision.

Transparency is particularly important given the emergence of consumer devices with numerous sensors that collect large volumes of data, some of which may be unfamiliar to the general public. For example, "ambient computing" technologies that sense and react to the presence of humans are likely to grow in popularity, presenting a more convenient, environmentally conscious evolution of IoT.[9] Additionally, extended reality (XR) technologies like augmented reality (AR) contain cameras, microphones, and other sensors that collect vast quantities of data about people's eye and body movements, voices, and surrounding environments.[10] As consumer devices integrate artificial intelligence (AI) tools capable of aggregating and analyzing this data,

---

[8] Such a change in data collection or use should also warrant a disclosure to the user of a change in data practices.
[9] Sabrina Ortiz, *What is ambient computing? Everything you need to know about the rise of invisible tech*, ZDNet (Sep. 13, 2022), https://www.zdnet.com/article/what-is-ambient-computing-everything-you-need-to-know-about-the-rise-of-invisible-tech/.
[10] Daniel Berrick and Jameson Spivack, *Understanding Extended Reality Technology & Data Flows: XR Functions* (Oct. 31, 2022), https://fpf.org/blog/understanding-extended-reality-technology-data-flows-xr-functions/. *See also Supra* 6.

they may be able to infer even more personal information.[11] While transparency alone won't protect people's privacy, it is an important first step.

III. Expanding the IoT Labeling program to cover additional considerations about IoT devices' data practices raises challenges involving program design and implementation that should be addressed.

Should the Commission move forward with its proposal to expand the IoT Label registry to include additional information, such as the presence of sensors and data collection, it should address the logistical issues this decision might raise. First, the Commission should ensure that the experts it recruits to assist with the IoT Labeling program possess the necessary competencies to cover the additional information required. The Report and Order creates a significant amount of infrastructure for running the program, and delegates administrative authority to entities with cybersecurity expertise.[12] Generally speaking, this is appropriate. However, the potential additional information to be included in the registry—such as the presence of sensors, data flows, and data transfers—may be the domain of an organization's privacy or data protection experts. While cybersecurity and privacy are interrelated, the Commission should consider requiring program administrators to possess relevant privacy expertise as well as cybersecurity expertise.[13]

Second, the registry should be designed in a way that is comprehensive and helpful, but that doesn't overwhelm the viewer. The more information added to the registry, the less likely an individual is to read through all of it, so the Commission should be judicious about what is most important to include. Additionally, depending on how the registry is configured, it should contain an accessible mechanism for IoT Label program participants to keep their registry submissions up to date, to ensure the information within remains accurate.

Finally, expanding the registry to include more information may create additional processes for the Commission to undertake, delaying the start of the IoT Label program. The Commission should ensure that any registry or program redesign necessitated by the expansion of the registry does not cause undue delay in rolling out the IoT Label. If it would, the Commission should consider instead commencing the IoT Label program as planned, and engaging in a future process to amend the program to include additional information.[14]

---

[11] Office of the Victorian Privacy Commissioners, *Internet of Things and Privacy – Issues and Challenges*, https://ovic.vic.gov.au/privacy/resources-for-organisations/internet-of-things-and-privacy-issues-and-challenges/.
[12] *Supra* 1.
[13] Anokhy Desai and Cobun Zweifel-Keegan, *Building the next generation of security and privacy professionals*, IAPP (Oct. 2022), https://iapp.org/resources/article/white-paper-building-the-next-generation-of-security-and-privacy-professionals/.
[14] The Commission could undertake this process either under its FCC Act Section 302 authority, or through Sec. 52(d)(iv) of FCC 24-26.

Transparency is a critical component of an effective data protection regime. Educating individuals about their devices' data practices also facilitates a well-educated public that can make more-informed choices about what products they purchase and how they use them. The Commission may also decide at a later date to expand the IoT Labeling program registry to include additional information about how devices collect and use data, in order to further improve transparency.[15]

FPF appreciates the opportunity to comment on these issues, and the FCC's ongoing efforts to improve transparency around consumer IoT devices and data practices. We welcome any further opportunity to provide resources or information to assist in this vital effort. If you have any questions regarding these comments and recommendations, please contact Jameson Spivack at jspivack@fpf.org (cc: info@fpf.org).

Sincerely,

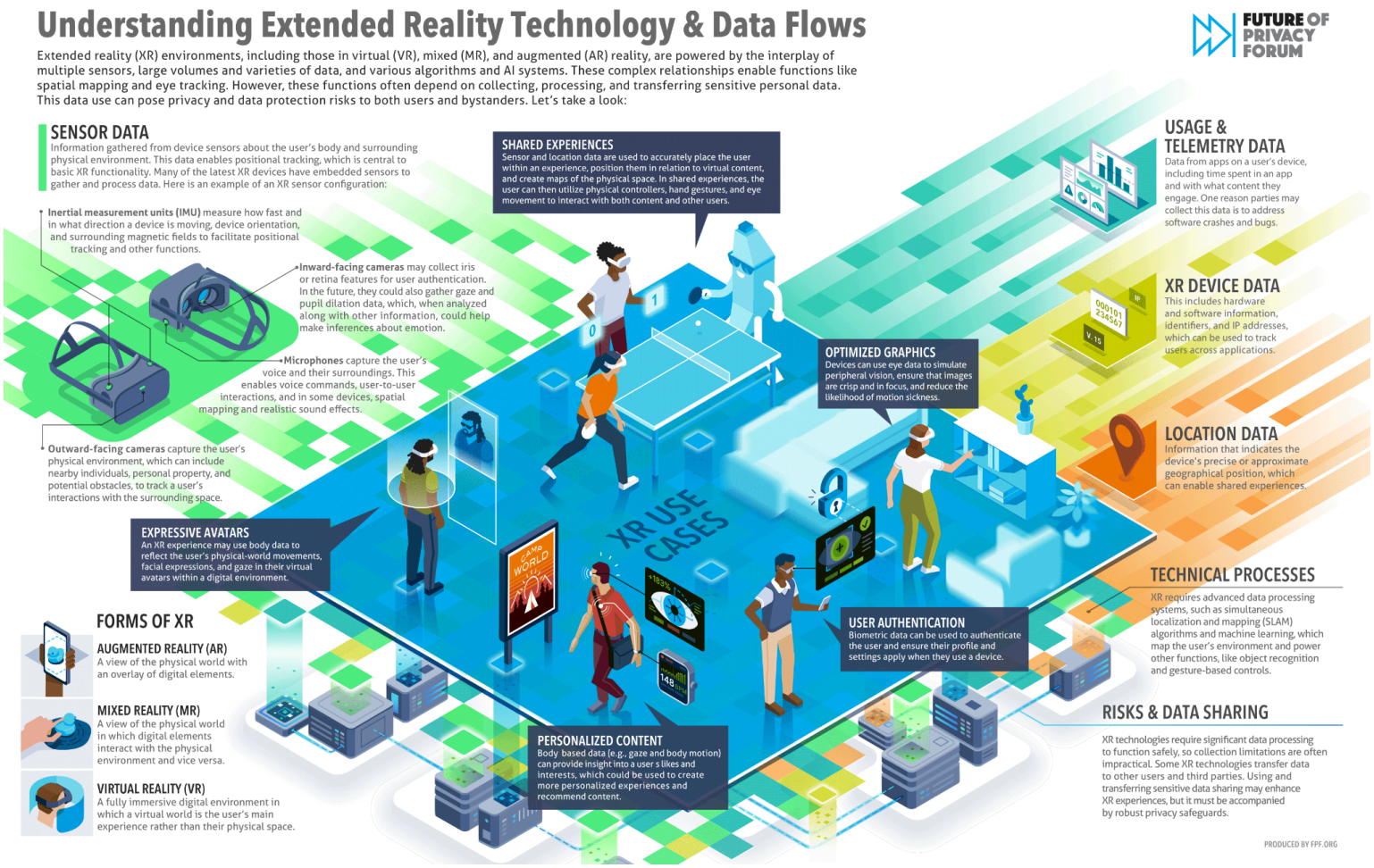
Jameson Spivack, Senior Policy Analyst
Sonia Saini, Policy Intern

The Future of Privacy Forum
https://fpf.org

[15] For example, the FCC could consult the CMU IoT Security and Privacy Label (CISPL), which provides prototypes for consumer IoT labels that contain information relevant for both cybersecurity and privacy. *See* https://www.iotsecurityprivacy.org/labels/.

ATTACHMENT:

"Understanding Extended Reality Technology & Data Flows" - FPF infographic, October 2022, developed by Daniel Berrick and Jameson Spivack[16]



[16] Also available at https://fpf.org/wp-content/uploads/2022/10/XR-Infographic-Screen-reader-friendly-version.pdf.