Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

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

COMMENTS OF CONSUMER REPORTS, CARNEGIE MELLON UNIVERSITY, PUBLIC KNOWLEDGE, ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), NEW YORK UNIVERSITY

We appreciate the opportunity for further comment on the Public Notice associated with the plan for the U.S. Cyber Trust Mark. The FCC has the potential to build a program that boosts both national security and overall consumer trust in connected devices. With that goal in mind we would like to share our thinking around some of the questions the agency has asked in the Public Notice.

Our goal is to boost consumer confidence in the U.S. Cyber Trust Mark, thus increasing the likelihood that they will look for the mark and purchase products that will advance the agency's goals of protecting U.S. networks and sites from various cyber attacks, including botnet attacks that can take down critical infrastructure.

With that in mind we have focused on five aspects of the Public Notice.

In Paragraph 16 the agency asks about how to handle a variety of complaints associated with the IoT Labeling Program. We believe that there should be a clear and public process by which the agency handles complaints. When a researcher or other entity finds an inconsistency with the labeling information on an IoT product, they should report that to the manufacturer, the CLA that tested the product, the Lead Administrator, and the FCC. Having a record of complaints publicly available at the FCC will assure transparency and induce both trust and good behavior on the part of manufacturers. The manufacturers and the CLA should have an opportunity to rectify the complaint, provided they can do so within the 20 days. If the complaint is still not rectified, the Lead Administrator should escalate the complaint to the FCC, which should take action to remove the mark and ensure the manufacturers update the data within the registry. The FCC should have the ability to remove the mark if the mark has been applied without going through the testing process or if the information displayed on the label does not reflect the current status of the product.

If the issue is that a company has not applied for a mark, but is displaying it anyway, then that complaint should be brought to the FCC and the Lead Administrator. If a company is fraudulently displaying the mark, the FCC should adopt disqualification procedures similar to ENERGY STAR's, including ceasing shipments of units displaying the label, ceasing the labeling of associated units, removing references to the label from marketing materials, covering or removing labels on noncompliant units within the brand owner's control, and conducting retail store level assessments to identify mislabeled products. Displaying a trustmark without meeting the qualification and receiving permission from the FCC is likely to constitute a deceptive or unfair trade practice under FTC and state consumer protection law, so the FCC should refer violations to those agencies for potential enforcement where it lacks the capacity to bring its own enforcement actions.

In Paragraph 17 the Bureau asks about confidentiality for applicants. commenters believe that the current requirements of the program are such that confidentiality is not necessary, as these elements will eventually make their way onto a public-facing label. Additionally, if a manufacturer wishes to shield aspects of their application to protect a product ahead of its launch, they can apply for confidentiality for specific aspects of their applications, much as they do already with equipment authorization applications. To keep the entire process confidential by default is overreach.

We feel similarly for the applications filed by the CLAs, although it is possible that a CLA could make a case for keeping the details of their sensitive business information confidential. However, when it comes to their testing methodologies, there is value in being able to understand them, and assess them against the current industry best practices and existing standards.

In Paragraph 21 the Bureau asks about the elements that should be included in the label. As CR and CMU wrote in the response[1] to the draft of the Report and Order, we believe that companies should disclose more than the original 10 elements required by the Report and Order. These include the following:

[1] Lorrie Cranor, Yuvraj Agarwal, Omer Akgul, Justin Brookman, Stacey Higginbotham to the Federal Communications Commission. March 12, 2024. Docket No. 23-239. https://www.fcc.gov/ecfs/search/search-filings/filing/10312223315399

- Types of sensors on the devices including cameras, microphones, thermometers, presence sensors, etc.
- List the data and the inferences those sensors collect especially if they can be used to detect location or sensitive information about a person such as their presence, behavioral patterns or health attributes.
- List the entities that the sensor data is shared with following the schema listed in the Specification for CMU IoT Security and Privacy Label created by CMU. Examples include manufacturers, third parties, service providers, the public, etc.[2]
- Does the manufacturer have a publicly accessible vulnerability disclosure program?
- Does the manufacturer have a dedicated point of contact for security researchers?
- Data encryption information such as
  - Is the data encrypted on the device (at rest)?
  - Is the data encrypted while stored in the cloud?
  - Is the data encrypted end-to-end while in transit?
- Access control mechanisms
  - Does the manufacturer use MFA?
  - Does the manufacturer prevent a reset to a default password? (devices that do allow a default password should not be allowed to receive the mark)
  - Does the manufacturer enable a user to change the default password?
  - When users are added to the account or access mechanisms change, is the user alerted?
- Deprovisioning
  - Can the consumer delete all of their data from the device?
  - Can the consumer delete all of their data from the cloud?
- If the minimum guaranteed support time frame for a particular product is zero or unanswered this product should not be able to receive the mark

Most importantly, the lack of required mention of privacy information, especially sensor data collection and its purpose, in the information linked to the label is a serious oversight that must be corrected in order to meet the needs of American consumers and establish their trust in the program.

As mentioned in its original comment with the FCC,[3] CMU research shows that consumers want to see a lot of security and privacy information on product packaging, and especially want to see

[2] Specification for CMU IoT Security and Privacy Label section 3.9 page 37.

[3] Carnegie Mellon comments at 3 citing Pardis Emami-Naeini, Henry Dixon, Yuvraj Agarwal, and Lorrie Faith Cranor. 2019. Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems (CHI '19). Association for Computing Machinery, New York, NY, USA, Paper 534, 1–12. https://www.fcc.gov/ecfs/search/search-filings/filing/1006679712754

data protection and data privacy factors, such as what sensors a device has, what inferences are made, who their data is shared with or sold to, and the purposes for which data will be used. In fact, CMU research shows that while consumers may be satisfied with a simple indicator that their device is secure, they would like more information about data privacy factors and expect this knowledge will give them agency, for example to cover a camera lens or position a device where it is less likely to pick up sensitive audio.

In CMU studies with consumers, the most important factors that affected risk perception and willingness to purchase a device were related to data privacy. We strongly suggest that data privacy factors need to be included as a requirement to get the U.S. Trust Mark. In addition, many other countries have already launched their own IoT Labeling scheme, and most are basing their requirements on the European Union Standard, ETSI 303 645[4], which explicitly has data privacy as one of the requirements. The data privacy factors on Carnegie Mellon's CISPL label closely match with the privacy requirements in the ETSI standard. We believe that if the U.S. program does not consider data privacy factors it risks causing significant divergence in terms of international harmonization, which will lead to challenges for IoT device manufacturers and consumers.

The additional security elements we call for are listed as part of NIST 8425 Consumer IoT Profile and will make consumer IoT devices more secure. Their presence on the label will also help familiarize consumers with best practices required for good cyber hygiene, which will help raise the overall security awareness of the U.S. population. Additionally, most reputable consumer IoT device companies are already building the additional security elements we call for into their IoT products. Many of those, especially those associated with the security of the IoT device itself, are called for in the newly created Connectivity Standards Alliance IoT device Security Specification, released in March.[5] As it currently stands, the 10 elements currently required in the FCC Report and Order are not enough to assure consumers that their connected IoT devices have been designed with security in mind, and do not address consumers' main concerns when they are thinking about the security of their IoT devices. By adding these elements the devices will both become objectively more secure and also assure consumers that their data is protected. This will benefit the program overall because it will lead to consumers searching out the mark and purchasing products that are more secure and transparent about their data privacy practices.

As a final note on the additional security requirements, many of these, such as the list of sensors, the mechanisms for deprovisioning a device and changing access to the device, also have the

[4] ETSI. "Cyber Security for Consumer Internet of Things: Baseline Requirements." June 2020. https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[5] Connectivity Standards Alliance. "IoT Device Security Specification Version 1.0." March 18, 2024. https://csa-iot.org/wp-content/uploads/2024/03/23-80986-013-PSWG-1.0-Specification-18-March-2024.pdf

benefit of helping survivors of domestic violence gain control of any product used in their home as a means of surveillance or control, or helping guests of hotels or short-term rental properties discover covert recording devices such as cameras. At a minimum being able to discover/identify (e.g., via broadcasting protocols such as mDNS and UPnP) and then look up information on a product found within the home can help individuals discover how a spouse or partner or hotel/rental host may be able to surveil them.

In Paragraph 22 the Bureau seeks comment on the registry design. As CR mentioned in its original comments on the original Notice of Proposed Rulemaking, Consumer Reports and CMU believe strongly that the registry should be accessible and provide information in a standardized data format. Programmatic access to a registry will enable new use cases for researchers, retailers, and even smart home companies that will enable consumers to streamline the act of managing and keeping their devices secure.

As noted in CR's original comments,[6] "Companies providing data as a condition for receiving permission to use the mark should be required to enter their data in a uniform manner — using the same data format — into a database that consumers, entrepreneurs, and device manufacturers can access programmatically using an Application Programming Interface (API). This enables several security-friendly and consumer-friendly applications. For example, a smart home controller or hub could use the information in the registry to sequester devices that are beyond their support date automatically into their own VLAN. Or an employer could build an application for an employee to use to check the types of IoT devices in their home for potential violations of the business' security policies. As smart home devices become more common, to ensure their security, we will need some way to automatically manage them."

It's one thing to envision a future of beneficial services built on the registry. But the agency rightly asks how such a registry should be designed. Given that the FCC has decided on a decentralized approach, we propose that any registry adopted should follow these design principles to ensure the security and integrity of the registry, thus inspiring consumer confidence in the label.

- Manufacturers need to publish label data according to a universal versioned schema (JSON) that includes standard machine-readable representations of all required attributes and the associated values? FCC needs a registry of where all the label data exists (URLs).
- FCC needs the ability to validate / check the health of the data at those URLs (e.g. ping to see if it still exists? Is the schema up-to-date?)
- The QR code should pull data either directly from the CLA (which will receive updates and the information from the manufacturers) or hit a redirect where the original QR request can be validated before pulling data from the manufacturer's site.

[6] Consumer Reports comments at page 28.

- Manufacturers will have the ability to push updates to the CLA server.
- Researchers, retailers, and third-party software providers should have the ability to access label data from the CLA servers using an API that is consistent across all CLAs (perhaps by being proposed by the lead CLA and implemented by the individual CLAs).
- The FCC and Lead Administrator should have the ability to write to the CLAs' databases to correct errors or remove products.
- The ability to make pull requests to the CLA server should be available to everyone, with provisions to allow trusted entities to exceed rate limits.
- Manufacturers should digitally sign their updates into the CLA servers to ensure that changes are authenticated and logged.
- The CLAs should digitally sign their label approvals and any changes they make to the registry to ensure that their approvals and changes are authenticated and logged.

In paragraph 23 the Bureau asks about display options for the registry. As third-party researchers and consumer-focused organizations, we believe that having programmatic access to the registry information in a standardized data format using machine-readable JSON allows for a wide variety of use cases including the ones the FCC has mentioned in the Public Notice. When it comes to providing consumers with information about the security of their IoT devices, providing an open platform for accessing the information makes the most sense and also encourages innovative uses of the program to build new services that could boost overall security. As all of the data provided in the registry is designed to be publicly shared at a consumer's request, artificially limiting its presentation serves no purpose except to stymie research and efforts to innovate around this security information.

With the U.S. Trust Mark, the FCC is embarking on an ambitious program that should boost individual and national security and help protect consumer privacy. We appreciate the chance to comment on the more technical aspects of the program and believe our collective organizations' many years of research in cybersecurity, abusive practices, and consumer desires around privacy and security provide nuanced understanding of how to build a program that will inspire trust and truly improve overall cybersecurity.

If you have any questions please feel free to reach out to Stacey Higginbotham or Lorrie Cranor.

Respectfully,

Lorrie Cranor
CyLab Director and Bosch Distinguished Professor in Security and Privacy Technologies, FORE Systems University Professor of Computer Science and Engineering & Public Policy
Carnegie Mellon University

lorrie@cmu.edu

Yuvraj Agarwal
Associate Professor, Software and Societal Systems Department
Carnegie Mellon University
yuvraj@cs.cmu.edu

Omer Akgul
Postdoctoral Researcher, Software and Societal Systems Department
Carnegie Mellon University
oakgul@cmu.edu

Justin Brookman
Director of Technology Policy
Consumer Reports

Stacey Higginbotham
Policy Fellow
Consumer Reports
stacey.higginbotham.consultant@consumer.org

John Bergmayer
Legal Director
Public Knowledge
john@publicknowledge.org

Danny Yuxing Huang
Assistant Professor, Center for Cyber Security
New York University
dhuang@nyu.edu

Chris Frascella
Counsel
Electronic Privacy Information Center (EPIC)
frascella@epic.org