The White House launched a new U.S. Cyber Trust Mark in July 2023, unveiling the design and announcing the U.S. Federal Communications Commission (FCC) would be soliciting comments on a wide range of details, including the requirements for using the mark on product packaging. Our group from Carnegie Mellon University (CMU) created a video shown at the launch event, showcasing our vision for the consumer experience purchasing Internet of Things (IoT) products with the benefit of a security and privacy label that would accompany the U.S. Cyber Trust Mark (see the accompanying figure). We had previously spent several years conducting consumer research to inform the design of our IoT label.

We submitted comments to the FCC and have been participating in industry-convened groups aiming to build a consensus on details surrounding IoT labeling. We have received substantial pushback from industry players on the idea of including anything more than a QR code next to the mark on a package label; some organizations argue there is not sufficient room on product packaging and printed information on a package may become out of date. We have also observed resistance to including any privacy-related information; some organizations prefer to include only information about device security. However, our research with consumers suggests purchasers of IoT products would appreciate and benefit from some of the most relevant information about both security and privacy included alongside QR codes on product packaging.

Consumers Want Information on Packaging
We conducted a 518-participant online research study in summer 2023 to gain empirical evidence as to how consumers would react to seeing only a minimal label with a trust mark and security. However, our research with consumers suggests purchasers of IoT products would appreciate and benefit from some of the most relevant information about both security and privacy included alongside QR codes on product packaging.

Privacy
Internet of Things Security and Privacy Labels Should Empower Consumers
Designs should offer useful information and convenience.

Frames from the Carnegie Mellon IoT label video shown at the U.S. Cyber Trust Mark launch event. Top left: Two smart thermostat boxes are shown on a store shelf with a closeup of their package labels, which include the U.S. Cyber Trust Mark. Top right: A consumer scans the QR code on one of the labels using a cellphone. Bottom: After scanning the QR code, the consumer views a more-detailed label on their phone. The video is available online at: https://youtu.be/odaklOk1G8I?t=3554
Our research sheds some light on the most important information to include on product packaging.
around the shield. In addition, it might be feasible to adjust the shield so a QR code could be placed in the center of the shield. We also suggest a flexible approach that would encourage more information to be placed on packaging for larger products where there is sufficient space, but allow a more compact representation for smaller packages or even inclusion on the products themselves since the packing is discarded by most consumers after installation.

How to Get Useful Information to Consumers

In addition to the IoT label on a package and available via QR code, it is important all label information be readily available on a centralized and trusted registry in a machine-readable format, for example, JSON or XML. This allows the information to be searched and indexed on search engines, automatically included in a standardized form on retailer product pages, or used as a comparison shopping factor by retailers that offer consumers the ability to compare products on their websites. It also allows the development of tools that can verify whether the declared practices in a label actually match the device behavior, such as whether its network traffic is really encrypted, how often it is updated after a known vulnerability disclosure, and so forth. In addition, third parties may develop apps or Web-based product comparison tools that can automatically recommend products to consumers based on their preferences. For example, at CMU, we piloted IoTSparrow, a tool enabling shoppers to select the security and privacy features most important to them and view side-by-side comparisons of products. Consumer groups or IoT device retailers might offer Web-based comparison tools.

While the U.S. Cyber Trust Program is currently meant to be voluntary, we are concerned an entirely voluntary program is likely to benefit bad actors (that is, device manufacturers who do not qualify for the U.S. Cyber Trust Mark), perhaps more so than good actors. In our recent research, we conducted an incentive-competitive study to determine the premium consumers are willing to pay for devices with IoT Security and Privacy labels. We compared similar devices: one with a label showing good security and privacy attributes, another with a label showing bad security and privacy attributes, and finally, one with no security or privacy label information, the status quo today. Our results indicated consumers are willing to pay significant premiums for devices with good security and privacy as compared to devices with bad security and privacy or even those with no information provided. This is promising since it shows that manufacturers with good security and privacy practices can benefit from displaying this information on a label. However, when participants compared devices with bad security and privacy to a device with no information, they preferred the one without any information since they did not believe it would be as bad as the one with clearly stated bad practices. In other words, bad actors are incentivized to not disclose their security and privacy information at all since consumers do not assume the worst. In order to avoid this problem and ensure the labeling program benefits consumers and improves the overall security of IoT devices, we recommend moving toward mandatory labeling requirements.

Research demonstrates consumers really do want security and privacy information about IoT products readily available and prominently displayed at the time of purchase. Consumers are increasingly wary about connected IoT devices being hacked and having their most sensitive information stolen. While the “early adopters” of IoT products were willing to use these products despite these risks, the next wave of mass-market IoT consumers will naturally be more risk averse and will need assurances these products can indeed be trusted. Our research indicates consumers strongly prefer products with clearly disclosed security and privacy attributes and will pay a premium for devices with better practices. For the U.S. Cyber Trust Mark to best support consumers, it must provide both security and privacy information in a convenient and readily accessible form that lends itself to easy comparison shopping. If IoT “nutrition labels” are to empower consumers, they must be designed with consumers in mind.

References

8. H.R. 538—118th Congress: Informing Consumers about Smart Devices Act. (Oct. 4, 2023); https://www.govtrack.us/congress/bills/118/hr538

Conrad Cliner (conrad@cmu.edu) is a research staff at Bosch Distinguished Professor in Security and Privacy Technologies, Cybersecurity, and Public Policy, Carnegie Mellon University in Pittsburgh, PA, USA.

Yuvraj Agarwal (yuvraj@cs.cmu.edu) is an associate professor of computer science and the director of the Systems Networking and Energy Efficiency (SYNERGY) Lab at Carnegie Mellon University in Pittsburgh, PA, USA.

Pardis Emami-Naeini (pardis@cs.duke.edu) is an assistant professor of computer science, electrical and computer engineering, and public policy and the director of the Duke Interdisciplinary Security, Privacy, and Interaction Research (InSPIre) Lab at Duke University in Durham, NC, USA.

© 2024 Copyright held by the owner/author(s).

MARCH 2024 | VOL. 67 | NO. 3 | COMMUNICATIONS OF THE ACM 31