DOI:10.1145/3637630

Lorrie Faith Cranor, Yuvraj Agarwal, and Pardis Emami-Naeini

Privacy

Internet of Things Security and Privacy Labels Should Empower Consumers

Designs should offer useful information and convenience.

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organizations argue there is not sufficient room on product packaging and printed information on a package may become out of date.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

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

QR code on product packaging. We compared this with our full proposed label[7] as well as a middle-ground approach, which includes a few important elements only. We provided a brief educational intervention to half the participants to let them know about the purpose of the U.S. Cyber Trust Mark and accompanying QR code prior to presenting labels for three fictitious smart thermostat products. Study participants strongly favored the two higher-complexity labels over the minimal label that required using a QR code to access any information. Most participants correctly answered questions based on information in these two higher-complexity labels. Few participants scanned the QR codes. Furthermore, while the educational intervention improved their understanding of the QR code's purpose, it notably did only a little to motivate them to scan the QR code.[2]

Our study results suggest it is important to include meaningful information on the package itself rather than rely on consumers to scan QR codes. Consumers in our study found scanning QR codes inconvenient, and some were concerned about potential security issues associated with QR codes. Consumers may make assumptions about the content of labels, and without seeing at least some summary information on the product packaging, may have no reason to scan the QR code or to suspect their assumptions may not be correct. In addition, for consumers who want to compare product labels, it is difficult or impossible to view multiple labels side-by-side on a cellphone screen, but much easier to look at product packages side-by-side. Finally, if the information is available only through a QR code, then consumers will not have access to it when they do not have a cellphone with a camera, QR code reader, and an Internet connection readily available.

Our research sheds some light on the most important information to include on product packaging. Assuming products carrying the trust mark comply with baseline security and privacy standards, it may not be necessary to include information that can be inferred from the fact that a product has the trust mark. However, the presence of the trust mark alone does not offer information about the types of sensors on the device or how data collected through these sensors will be used and shared. Indeed, the proposed Informing Consumers About Smart Devices Act, which has already passed as H.R 538 in the U.S. House of Representatives, would require products to "clearly and conspicuously" disclose they have a camera or microphone if they have one and a consumer could not "reasonably expect" it.[8] We have seen devices such as smart thermostats and smoke alarms sometimes include microphones and other sensors, which can surprise consumers.[1] In fact, we have heard from some manufacturers that they imagine enabling additional functionality on products with a firmware update that turns on previously undisclosed sensors. Thus, we recommend that at minimum, labels on IoT device packaging include a notice about audio and visual sensors and perhaps other sensors consumers find sensitive such as those that can, for example, infer occupancy or behavioral patterns.

Our research also indicates consumers want to know how the data collected by sensors will be used and shared, and that this information is likely to impact their purchase decisions.[6] It would be useful for manufacturers to convey when their devices offer security and privacy protections that exceed baseline standards. For example, the baseline might require the availability of security updates, but without more information, consumers will not be able to distinguish easily between products requiring these updates are applied manually and those that automatically apply them. Or the baseline might require user-changeable passwords, but without more information, consumers will not be able to easily identify products that also include multifactor authentication.

Our research sheds some light on the most important information to include on product packaging.

Consumers Find Privacy Information Most Actionable

Our research indicates consumers are especially interested in data protection and data privacy factors, such as what sensors a device has, who their data is shared with or sold to, and the purposes for which data will be used. In fact, our research shows that while consumers may be satisfied with a simple indicator showing 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.[5] In our studies with consumers, the most important factors affecting risk perception and willingness to purchase a device were related to data privacy. We strongly suggest data privacy factors must be included as a requirement to use the U.S. Trust Mark. In addition, some other countries have already launched their own IoT labeling schemes, and most are basing their requirements on the European Union Standard, ETSI 303 645, which explicitly has data privacy as one of the requirements. The data privacy factors we propose closely match the privacy requirements in the ETSI standard. We believe if the U.S. program does not include data privacy factors, it will lead to compliance challenges for IoT device manufacturers as they try to sell their products globally.

We understand concerns about the size of the label on product packaging, and believe that with a focus on the most critical information that is not implied by whatever baseline standard is adopted, the size of the packaging label may be reduced to something smaller than what we previously proposed (with more complete information provided in the layer 2 label obtained by scanning the QR code). In addition, we suggest the FCC reformat the U.S. Cyber Trust Mark to be more conducive to a compact label. This would include positioning the words to fit compactly under the shield graphic or possibly wrap

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.[3] 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,[4] we conducted an incentive-compatible 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.

Consumers are increasingly aware about connected IoT devices being hacked and having their most sensitive information stolen.

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. C

References

1. Bastone, N. After a big privacy backlash, Google's Nest explains which of its products have microphones and why. *BusinessInsider* (Feb. 24, 2019); https://www.businessinsider.com/google-nest-products-with-microphones-2019-2?op=1
2. Chen, C. et al. Is a Trustmark and QR code enough? The effect of IoT security and privacy label information complexity on consumer comprehension and behavior. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (CHI '24) (May 11–16, 2024); https://doi.org/10.1145/3613904.3642011
3. Emami-Naeini, P. et al. An informative security and privacy "nutrition" label for Internet of Things devices. *IEEE Security and Privacy 20*, 2 (2021); https://www.iotsecurityprivacy.org/research/AnInformativeLabel.
4. 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; https://www.usenix.org/conference/usenixsecurity23/presentation/emami-naeini
5. Emami-Naeini, P. et al. Exploring how privacy and security factor into IoT device purchase behavior. In *Proceedings of the 2019 CHI Conf. on Human Factors in Computing Systems (CHI '19)*; 10.1145/3290605.3300764
6. Emami-Naeini, P. et al. Which privacy and security attributes most impact consumers' risk perception and willingness to purchase IoT devices?. In *2021 IEEE Symposium on Security and Privacy (SP)*. IEEE, 519–536; https://doi.org/10.1109/SP40001.2021.00112
7. Emami-Naeini, P. et al. *Specification for CMU IoT Security and Privacy Label (CISPL 1.0)*. (Jan. 17, 2021); https://www.iotsecurityprivacy.org/downloads/Privacy_and_Security_Specifications.pdf
8. H.R. 538—118th Congress: Informing Consumers about Smart Devices Act. (Oct. 4, 2023); https://www.govtrack.us/congress/bills/118/hr538

Lorrie Faith Cranor (lorrie@cmu.edu) is Director and Bosch Distinguished Professor in Security and Privacy Technologies, CyLab Security and Privacy Institute and FORE Systems Professor, Computer Science and Engineering and Public Policy, Carnegie Mellon University in Pittsburgh, PA, USA.

Yuvraj Agarwal (yuvraj@cs.cmu.edu) is an associate professor of computer science and 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.