An Informative Security and Privacy "Nutrition" Label for Internet of Things Devices

Pardis Emami-Naeini | University of Washington
Janarth Dheenadhayalan | Amazon Web Services
Yuvraj Agarwal and Lorrie Faith Cranor | Carnegie Mellon University

Consumers are concerned about the security and privacy of their Internet of Things (IoT) devices. However, they cannot easily learn about their devices' security protections and data practices before purchasing them. We designed a usable and informative IoT security and privacy label.

In recent years, Internet of Things (IoT) devices have soared in popularity among consumers around the world. A growing number of homes are now equipped with IoT devices to bring about benefits, ranging from improving energy efficiency to helping automate routine tasks. However, IoT devices within our homes also potentially expose users to a wide range of cybersecurity threats, including devices getting hacked or users' private information being sold to third parties. For users to better protect themselves against the potential risks of IoT devices, they need to know about the security capabilities of these devices as well as what data devices collect and how data are used and stored. For example, during the Mirai botnet attack, hundreds of thousands of IoT devices around the world got targeted and infected, partially due to devices having insecure default passwords.[1] These attacks could have been mitigated if consumers were more informed about the use of default passwords on their devices and the potential risks associated with it, and whether there was a way for them to change those passwords. Currently, this information is generally not readily available to consumers when they are making purchase decisions.

One way to communicate information about the privacy and security practices of devices is through labels. Product labels are not a new concept; they have been around for decades to effectively inform consumers about food nutrients, over-the-counter drug dosage, and energy efficiency of appliances. Food nutrition labels in particular were developed to decrease obesity by helping consumers purchase healthier food products. Other objectives of food nutrition labels include encouraging food companies to compete to produce healthier products and allowing governments to support consumers' health-related behaviors without mandating specific nutritional requirements.

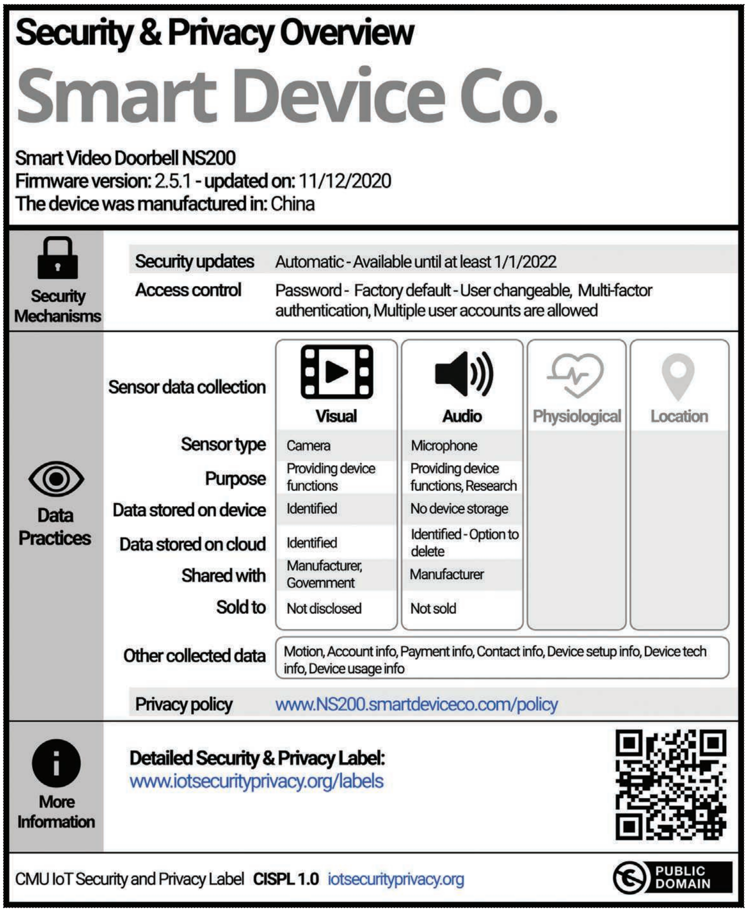
Digital Object Identifier 10.1109/MSEC.2021.3132398
Date of current version: 29 December 2021

In the context of privacy, researchers have found that "privacy nutrition labels" can be effective in conveying information to users visiting websites[2] and using mobile apps.[3] Indeed, Apple has recently started including app privacy labels in the iOS App store, generated from information submitted by app developers. Building on prior label design research, we designed a usable and informative privacy and security label for IoT devices.

In this article, we first describe our IoT label design process and discuss proposals for privacy and security ratings. We then introduce our label specification and generator and discuss ways our label's machine-readable format can enable new uses of label information. Finally, we discuss label adoption and enforcement.

The Label Design Journey

We began by conducting a series of in-depth one-on-one interviews with 24 consumers of IoT devices. We found that although IoT consumers are concerned about privacy and security, they are unable to find information about the privacy and security features of the IoT devices they are considering for purchase.[4] Almost all interviewees acknowledged the importance of knowing privacy and security information related to IoT devices before making purchase decisions and were interested in having such information in a label format. One participant reported, "As opposed to those long policy documents that you usually need to read, I think this is a very efficient way and I cannot think of a better way than this."



Security & Privacy Overview

Smart Device Co.

Smart Video Doorbell NS200
Firmware version: 2.5.1 - updated on: 11/12/2020
The device was manufactured in: China

Security Mechanisms

Security updates	Automatic - Available until at least 1/1/2022
Access control	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed

Data Practices

Sensor data collection	Visual	Audio	Physiological	Location
Sensor type	Camera	Microphone		
Purpose	Providing device functions	Providing device functions, Research		
Data stored on device	Identified	No device storage		
Data stored on cloud	Identified	Identified - Option to delete		
Shared with	Manufacturer, Government	Manufacturer		
Sold to	Not disclosed	Not sold		

Other collected data: Motion, Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info

Privacy policy: www.NS200.smartdeviceco.com/policy

More Information

Detailed Security & Privacy Label:
www.iotsecurityprivacy.org/labels

CMU IoT Security and Privacy Label **CISPL 1.0** iotsecurityprivacy.org

PUBLIC DOMAIN

Figure 1. The primary layer of the label.

Some participants said they would even pay a small premium for having usable privacy and security labels at the time of purchase, especially when purchasing a device that they perceive to collect more sensitive information (e.g., a smart camera capturing images). This strong interest among our consumer study participants motivated us to work toward designing a usable and informative IoT privacy and security label.

The next step was to identify the information that should be included on the label. Given consumers' scarce attention, presenting them with the most relevant security and privacy information in the most digestible form is crucial. To determine the most important information to include on IoT privacy and security labels, we conducted interviews and solicited the opinions of 22 privacy and security experts from industry, academia, government, and nongovernmental organizations.[5] We found that differences in opinions were driven less by fundamental differences in beliefs, but rather by differences in work experience and priorities. For example, some experts were more knowledgeable about specific security mechanisms, standards, or regulations, and prioritized factors related to their area of expertise or their organization's mission. Experts acknowledged the current lack of adequate and understandable privacy and security information for IoT devices and emphasized the importance of having usable and informative IoT labels. One expert said, "What's good about a label is that it empowers the consumer to make a more active decision about cybersecurity rather than just being helpless as to what the security of her device might be. . . . the average consumer doesn't have a privacy, security, or a legal department to review this stuff before they buy it. Enterprises do, but consumers do not, so someone's gotta be looking out for consumers and giving the consumers this information."

Some experts emphasized the positive role of privacy and security labels in raising IoT companies' accountability; for example, "There is value in forcing the company to write a list down even if the consumer doesn't understand it. If you said, 'list your open ports,' there would be an incentive to make them few."

Our experts identified 47 pieces of information they considered important to include on the label, including information related to data practices, security mechanisms, and the device manufacturer. To avoid overwhelming consumers, we designed a two-layer label.

The primary layer (see Figure 1) is the concise format of the label that can be printed and attached to a product package. The secondary layer (see Figure 2) is an online format of the label and can be accessed through the primary layer, by scanning a QR code or typing in the uniform resource locator (URL) that is placed at the bottom of the primary layer.

To examine the efficacy of our IoT label in conveying information that is understandable, we interviewed consumers of IoT devices and asked them to explain each attribute of the label. While there were a few points of confusion, overall, our participants were able to accurately explain the content of both layers of the label. One participant observed that the label could inform both consumers and experts: "Labels are both for customers and for experts, such as tech journalists, consumer advocacy groups, who are capable of understanding it and who will click on the things, and if they see something that is questionable will raise it in the public press, will raise it with regulatory authorities, and otherwise. The label is not just for the consumer, but also there's another feedback process that works through experts to the extent that the information is available at all."

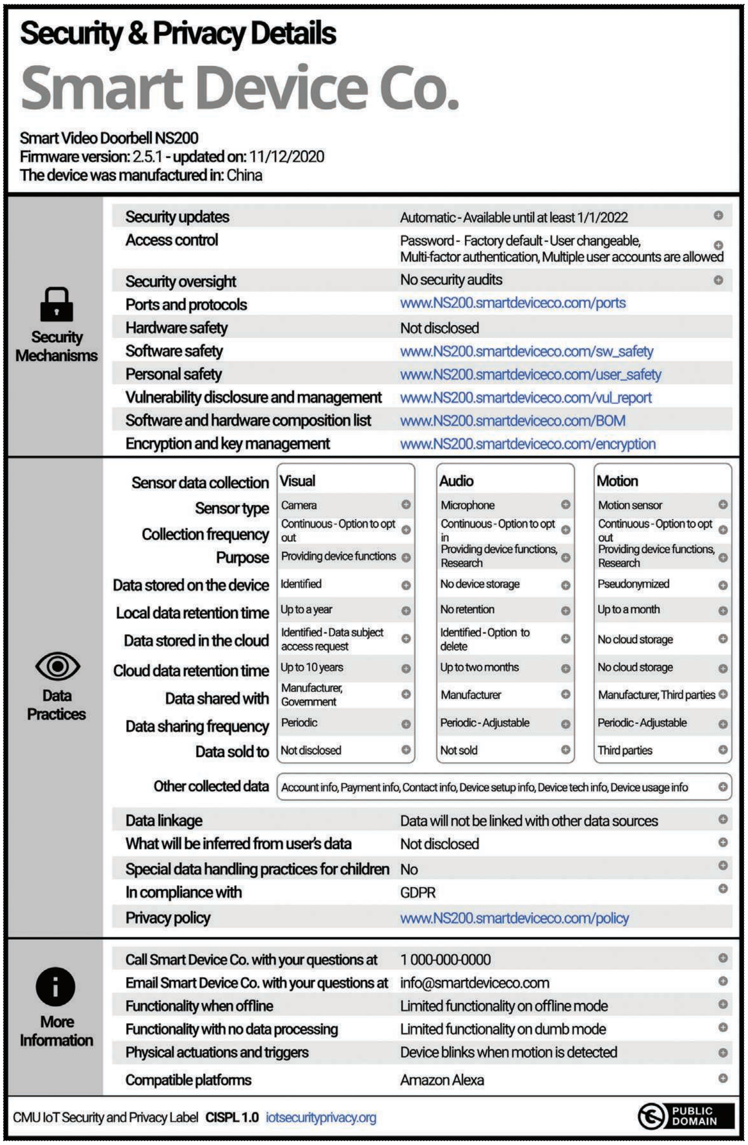
To further evaluate the effectiveness of our label, we conducted a large-scale online study with hundreds of crowdsourced participants.[6] Our findings indicated that almost all of the label content effectively conveys risks to participants and impacts their reported desire to purchase IoT devices.

Among the label information, we found that knowing that data are being sold to third parties has the most impact on increasing participants' perception that a device is risky. A concerned participant mentioned, "Once data are sold, you do not know where or what it is being used for, or if it will be sold again. This will enable tracking by companies you are unaware of." Conversely, our analysis showed that knowing that the collected data will not be retained on the cloud strongly decreases participants' perception that an IoT device is risky.

The impact of almost all privacy and security attributes on risk perception was aligned with their effectiveness in changing participants' reported willingness to purchase the IoT device. However, there were some exceptions. For example, although participants reported that having multifactor authentication (MFA) would decrease the risks they associate with an IoT device, they mentioned that they would not be willing to purchase such a device, mainly due to its usability challenges, i.e., the inconvenience of using MFA on their devices. One of our participants who was concerned about having MFA for their shared in-home smart speaker said, "Accessing the device via authentication would then become a hassle and/or annoying. For instance, what if my wife or a guest wanted to use the speaker?"

Another commonly mentioned reason to justify unwillingness to purchase devices with risk-reducing security features was the desire to have agency over the privacy and security practices of their devices. One participant explained they prefer to purchase IoT devices with manual security updates rather than automatic updates, "I want to have full control over updating my devices to decrease the risk of installing an update that has a security flaw."

Although the label content was mostly effective in conveying risks to participants, we did find a few misconceptions. A few participants thought that if the label indicates that the device does not receive updates, that signals a more secure device compared to the one that



Security & Privacy Details

Smart Device Co.

Smart Video Doorbell NS200
Firmware version: 2.5.1 - updated on: 11/12/2020
The device was manufactured in: China

Security Mechanisms

Security updates	Automatic - Available until at least 1/1/2022 ⊕
Access control	Password - Factory default - User changeable, Multi-factor authentication, Multiple user accounts are allowed ⊕
Security oversight	No security audits ⊕
Ports and protocols	www.NS200.smartdeviceco.com/ports
Hardware safety	Not disclosed
Software safety	www.NS200.smartdeviceco.com/sw_safety
Personal safety	www.NS200.smartdeviceco.com/user_safety
Vulnerability disclosure and management	www.NS200.smartdeviceco.com/vul_report
Software and hardware composition list	www.NS200.smartdeviceco.com/BOM
Encryption and key management	www.NS200.smartdeviceco.com/encryption

Data Practices

Sensor data collection	Visual	Audio	Motion
Sensor type	Camera ⊕	Microphone ⊕	Motion sensor ⊕
Collection frequency	Continuous - Option to opt out ⊕	Continuous - Option to opt in ⊕	Continuous - Option to opt out ⊕
Purpose	Providing device functions ⊕	Providing device functions, Research ⊕	Providing device functions, Research ⊕
Data stored on the device	Identified ⊕	No device storage ⊕	Pseudonymized ⊕
Local data retention time	Up to a year ⊕	No retention ⊕	Up to a month ⊕
Data stored in the cloud	Identified - Data subject access request ⊕	Identified - Option to delete ⊕	No cloud storage ⊕
Cloud data retention time	Up to 10 years ⊕	Up to two months ⊕	No cloud storage ⊕
Data shared with	Manufacturer, Government ⊕	Manufacturer ⊕	Manufacturer, Third parties ⊕
Data sharing frequency	Periodic ⊕	Periodic - Adjustable ⊕	Periodic - Adjustable ⊕
Data sold to	Not disclosed ⊕	Not sold ⊕	Third parties ⊕

Other collected data: Account info, Payment info, Contact info, Device setup info, Device tech info, Device usage info ⊕

Data linkage	Data will not be linked with other data sources ⊕
What will be inferred from user's data	Not disclosed ⊕
Special data handling practices for children	No ⊕
In compliance with	GDPR ⊕
Privacy policy	www.NS200.smartdeviceco.com/policy

More Information

Call Smart Device Co. with your questions at	1 000-000-0000 ⊕
Email Smart Device Co. with your questions at	info@smartdeviceco.com ⊕
Functionality when offline	Limited functionality on offline mode ⊕
Functionality with no data processing	Limited functionality on dumb mode ⊕
Physical actuations and triggers	Device blinks when motion is detected ⊕
Compatible platforms	Amazon Alexa ⊕

CMU IoT Security and Privacy Label **CISPL 1.0** iotsecurityprivacy.org PUBLIC DOMAIN

Figure 2. The secondary layer of the label.

receives updates, "If there are no updates, then the system must be providing maximum security already."

Privacy and Security Ratings

Some of our consumer interview participants wanted to see security and privacy ratings on the labels to more conveniently compare security and privacy practices of IoT devices without having to wade through lots of details. In addition, a rating from a known organization may be more trustworthy than self-reported information from a manufacturer.

Similar to the Energy Star rating system managed by the U.S. Environmental Protection Agency and the U.S. Department of Energy, the idea of star ratings has been proposed for IoT devices to help consumers make informed purchase decisions. In a hearing of the U.S. Senate Committee on Commerce, Science, and Transportation's Subcommittee on Security, Senator Ed Markey suggested a five-star security rating system for IoT products.[7] In our study, while privacy and security experts were supportive of ratings on the label, they also mentioned two potential challenges of including them.

> **For users to better protect themselves against the potential risks of IoT devices, they need to know about the security capabilities of these devices as well as what data devices collect and how data are used and stored.**

The first challenge relates to the rating scale. Experts suggested that consumers might have trouble distinguishing a large number of ratings, yet a more granular scale could help manufacturers better differentiate their privacy and security practices. One of our expert participants, who works in industry, discussed this issue: "I'm sure industry people, manufacturers, will want more in there. What would happen if you had something like this is it might start to grow based on features they want reflected in that rating. Then I can see it becoming a bigger and bigger scale."

Experts mentioned that ratings might pose an unhealthy incentive for IoT companies to achieve full-star ratings only to be able to compete in the market. Companies may be able to game the ratings to get all of the stars and, eventually, all products will have all stars, whether they deserve them or not. One of our expert interviewees, who was an academic, explained, "The problem I have with ratings like this is that everybody's gonna get a five star, because everybody's gonna figure out how to get the five star."

To address these challenges, some experts discussed the idea of having multiple certification levels (e.g., silver, gold, and platinum) with a secure baseline or minimum standard instead of star ratings. This is similar to what the Leadership in Energy and Environmental Design standards use for rating energy efficiency and sustainability of buildings. One of our experts reported, "I think consumers should know it passes the minimum security level. If I'm buying a space heater, I know they're not allowed to sell me one that will set on fire. I don't have to say, oh, it has a 70% score that it will set the house on fire."

Since the lowest certification level indicates a safe device, there is a risk that manufacturers will aim to achieve the lowest level and not bother pursuing higher levels. Market competition may encourage manufacturers to pursue higher certification levels, especially for devices where the consequences of security breaches are most severe, such as smart door locks. A number of efforts are currently focused on developing and delivering security and privacy ratings and certifications. We review two of these efforts here.

Digital Standard

In 2017, *Consumer Reports* launched the Digital Standard for evaluating consumer IoT products. This standard, which focuses on four categories—security, privacy, ownership, and governance and compliance—remains under development. The security category of the Digital Standard includes build quality, data security, and user safety.

Build quality refers to product stability and whether "software was built and developed according to the industry's best practices for security." The Cyber Independent Testing Lab, a Digital Standard partner, is actively evaluating and scoring software of IoT devices according to a number of factors. Our label design includes a software safety features element, where manufacturers can provide a URL with information related to software security. Data security includes authentication, encryption, ability to update, security audits, and vulnerability disclosure program. All of these factors are also included on our label.

The user safety category has not yet been defined in the Digital Standard, although developer notes indicate it will be related to avoiding abuse and harassment. Media reports suggest there are many incidents involving consumer IoT devices being used for domestic abuse.[8]

However, device manufacturers appear to be doing little to address the risks associated with abuse involving their devices. We have included a factor called personal safety, which provides a place where device manufacturers can indicate available safeguards against abusive behavior once such safeguards have been implemented. Further discussions with experts are needed to determine how to address significant safety issues effectively on the label. As one of the experts we interviewed explained, "Safety means if your car gets hacked, you die. The room that has a laser attached and if it gets hacked, it kills you. A drone can be reprogrammed to dive-bomb your child. I'm not sure how to capture that on the label."

The privacy section in the Digital Standard includes user controls, data use and sharing, data retention, and overreach. The assessment procedure for almost all of the privacy factors in the standard involves verifying the company's claimed data practices with actual data practices.

All of the privacy factors mentioned in the Digital Standard are covered in our proposed label, except overreach. Overreach, or "collecting too much data," focuses on determining whether data collection is beneficial to the user, fully disclosed, the minimum necessary for functionality, and private by default. This seems like an area where a third-party assessment rather than a self-report is likely warranted.

> **Market competition may encourage manufacturers to pursue higher certification levels, especially for devices where the consequences of security breaches are most severe, such as smart door locks.**

As some of the experts we interviewed mentioned, consumers may weigh privacy and functionality tradeoffs differently. Thus, it may be difficult to capture a single privacy rating that makes sense for all consumers. In addition to providing detailed information about data practices, a future privacy rating system could be customized based on a consumer's stated privacy preferences, which could change over time.

Underwriters Laboratories

The five-level Underwriters Laboratories (UL) certification process includes 44 requirements over seven categories: software updates, data and cryptography, logical security, system management, customer-identifiable data, protocol security, and process and documentation.

While our proposed label includes factors from all seven categories, a third-party evaluation is needed to assess compliance with requirements. Our label can inform consumers about security and privacy and goes into more detail about privacy issues than UL's customer identifiable data category. By adding the UL certification to our label, we could offer users a single concise assessment of device security that complements the more detailed information provided on the label.

Label Specification and Generator

We prepared an extensive specification document for our label.[9] For each attribute in the label, we specify the values and subattributes the attribute can take, other references that mention the attribute, additional information that manufacturers can potentially provide, and best practices related to the attribute.

To prepare the specification document, we studied more than 70 IoT privacy and security references from industry, nonprofit organizations, government agencies, and academia. All of our label attributes have been mentioned at least once in these references. Security attributes are mentioned on average 20 times, whereas the average number of references for each privacy attribute is only five. This huge discrepancy shows how little current standards and guidelines discuss privacy practices of IoT devices compared to their security mechanisms.

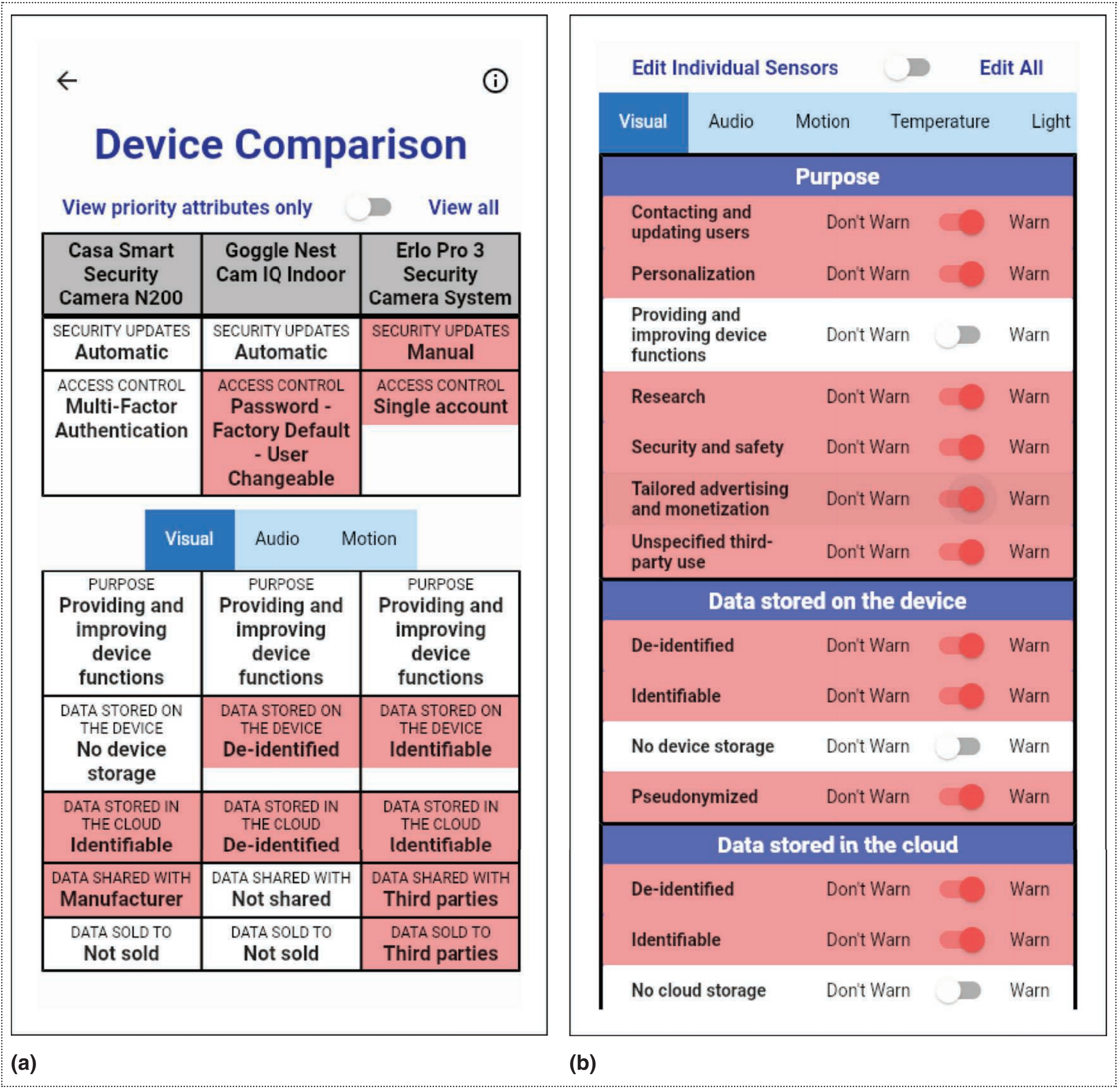
To enable manufacturers to generate labels and help standardizing our label design, we created a web-based label generator. Our tool allows users to generate their own labels by filling out a form and selecting the appropriate values for each privacy, security, and general attribute. As users are filling out the form, they can see the label being updated in real time. At any point, users can download a machine-readable JavaScript Object Notation (JSON) format of the label and edit it themselves. The JSON file can be uploaded back to our web-based label generation tool to modify or add to the label. In addition to JSON, the tool lets users download the XML and HTML formats of the label as well. The most up-to-date version of our tool can be found at www.iotsecurityprivacy.org.

Machine-Readable Label

Our label's machine-readable format facilitates other use cases, including developing comparison shopping search engines and apps. We developed a mobile application to aid consumers' understanding about the security and privacy practices of devices when they are considering purchasing them and to facilitate comparison shopping. By scanning the QR code or the barcode on the product package, users can access and easily compare the privacy and security label information of the IoT devices they are considering. Specifically, the Compare feature of our app enables users to compare security and privacy attributes of the scanned IoT devices side-by-side and get an overall picture of how well devices match their personal preferences [see Figure 3(a)]. The Preferences feature allows users to specify which privacy and security attributes they want to be warned about if they appear on an IoT device label [see Figure 3(b)].

By providing transparency at the network level, IoT labels could also help maintain the security of the network. With the advent of advanced wireless communication standards, more and more devices are connecting to the network and communicating with each other. Similar to Manufacturer Usage Descriptions, IoT devices can broadcast their privacy and security attributes to all of the other network-connected devices via a machine-readable (JSON) version of our label.

Although transparency at the network level could enable users and network administrators to more effectively detect anomalies in the network, it is imperative to carefully study the privacy implications being introduced by such transparency. Based on the objective of data collection and data sharing, the network administrator must determine which attributes of the IoT label should be publicly available and which attributes need special authorization to be accessed. For example, it might not be safe for everyone to know about the ports and protocols of a



Device Comparison

View priority attributes only ○ View all

Casa Smart Security Camera N200	Goggle Nest Cam IQ Indoor	Erlo Pro 3 Security Camera System
SECURITY UPDATES Automatic	SECURITY UPDATES Automatic	SECURITY UPDATES Manual
ACCESS CONTROL Multi-Factor Authentication	ACCESS CONTROL Password - Factory Default - User Changeable	ACCESS CONTROL Single account

Visual | Audio | Motion

PURPOSE Providing and improving device functions	PURPOSE Providing and improving device functions	PURPOSE Providing and improving device functions
DATA STORED ON THE DEVICE No device storage	DATA STORED ON THE DEVICE De-identified	DATA STORED ON THE DEVICE Identifiable
DATA STORED IN THE CLOUD Identifiable	DATA STORED IN THE CLOUD De-identified	DATA STORED IN THE CLOUD Identifiable
DATA SHARED WITH Manufacturer	DATA SHARED WITH Not shared	DATA SHARED WITH Third parties
DATA SOLD TO Not sold	DATA SOLD TO Not sold	DATA SOLD TO Third parties

(a)

Edit Individual Sensors ○ Edit All

Visual | Audio | Motion | Temperature | Light

Purpose			
Contacting and updating users	Don't Warn	●	Warn
Personalization	Don't Warn	●	Warn
Providing and improving device functions	Don't Warn	○	Warn
Research	Don't Warn	●	Warn
Security and safety	Don't Warn	●	Warn
Tailored advertising and monetization	Don't Warn	●	Warn
Unspecified third-party use	Don't Warn	●	Warn
Data stored on the device			
De-identified	Don't Warn	●	Warn
Identifiable	Don't Warn	●	Warn
No device storage	Don't Warn	○	Warn
Pseudonymized	Don't Warn	●	Warn
Data stored in the cloud			
De-identified	Don't Warn	●	Warn
Identifiable	Don't Warn	●	Warn
No cloud storage	Don't Warn	○	Warn

(b)

Figure 3. Screenshots of our developed phone application (designed and implemented by Michelle Ling), which show (a) the side-by-side comparison of IoT devices according to their privacy and security practices, and (b) how users can specify their personal preferences related to privacy and security attributes.

device, as they can use this information to attack the device and thereby the network.

Label Adoption and Enforcement

In order for labels to be practically useful, they need to be widely used and to convey accurate information. Use of labels may be mandated by regulations or strongly encouraged through "safe harbor" provisions. Even in the absence of regulatory mandates, retailers may require labels on products they sell or may promote products that have labels. Some manufacturers may adopt labels voluntarily to gain consumer trust. As a study consumer participant mentioned, "I would definitely trust something that had this above something that didn't."

Prior work has shown the impact of company size and reputation on consumer trust and purchase behavior. As a result, smaller and lesser-known companies will likely take longer to develop consumer trust. However, a label may help level the playing field by allowing companies to be transparent about the privacy and security of their devices and work toward providing protective privacy and security practices to assure their consumers.

Past efforts to encourage standardized privacy disclosures have faltered in the absence of regulatory mandates. We believe enforcement mechanisms are needed to ensure that there are consequences for companies that convey inaccurate information on their labels. In the United States, the Federal Trade Commission or state attorneys general would likely prosecute companies who are found to make false claims on their labels, similar to what happens when companies are found to make false claims in their privacy policies.

In late March 2021, U.S. Senator Edward J. Markey and U.S. Congressman Ted W. Lieu (re)introduced the Cyber Shield Act. This legislation creates a voluntary cybersecurity certification program for consumer IoT devices. As part of this policy, there will be an advisory board comprising diverse experts from industry, academia, government, and consumer groups to specify a cybersecurity benchmark for IoT devices. Manufacturers can then attach a "Cyber Shield" label to their products, voluntarily certifying that their devices meet the benchmark.

In May 2021, a White House Executive Order was signed to improve the nation's cybersecurity and protect the federal governments' networks.[10] As part of the executive order, the National Institute of Standards and Technology has been commissioned to work with appropriate federal agencies to set up a pilot program for creating labels for IoT devices disclosing their cybersecurity practices. The order highlighted the "ease of use for consumers" as one of the primary goals of the labeling scheme.

Other countries around the world are developing privacy and security labels for IoT devices, including the United Kingdom, Finland, and Singapore.

The United Kingdom

In 2018, the U.K. government published the Code of Practice for Consumer IoT Security, which includes 13 guidelines of good security practices for IoT manufacturers to follow. Later in 2019, the European Telecommunications Standards Institute (ETSI) published the Technical Specification 103 645, the first globally-applicable industry standard for consumer IoT security based on the Code of Practice guidelines.

Three of the Code of Practice guidelines were leveraged by the U.K. government in the design of their IoT label, which requires use of unique passwords, implementing a vulnerability disclosure policy, and specifying the date after which the device will no longer receive security updates. Our label includes password practices and update lifetime on the primary layer and a link to the vulnerability disclosure and management policy on the secondary layer.

Based on a public consultation process, the U.K. government decided not to proceed with a voluntary labeling scheme for now due to the potential challenges for retailers to validate the manufacturers' claims on the label. We believe having a third-party assessment body could address this concern. However, the U.K. government argues that having a self-assessment procedure would reduce manufacturers' cost by empowering them to conduct relevant assessments that are appropriate for their devices.

In April 2021, the U.K. government proposed a new cybersecurity law for IoT devices. Following the new law, IoT manufacturers have to disclose and inform consumers for how long their devices will be receiving security updates. The legislation will ban IoT manufacturers from having universal default passwords for their products. In addition, IoT manufacturers need to provide a vulnerability reporting program with a point of contact for the public to easily report a new vulnerability.

Finland

Finland is the first European country to certify IoT devices with a "Security Mark" to increase consumers' awareness of devices' security practices at the time of purchase. To receive this certification, the IoT manufacturer must submit a security compliance form to the Finnish Transport and Communications Agency Traficom. There are currently eight IoT companies that have products in Traficom's pilot program and that have received the security badge, including Polar, Cozify, and Philips Hue.

IoT companies can voluntarily apply for a security mark by completing a compliance form. The Cyber Security Center then assesses the claims in the form and, if appropriate, issues the security mark. The requirements mentioned in the compliance form are based on the ETSI standard. The attributes in the compliance form are: the availability of timely and signed security updates, the lifetime of software updates, list of certifications and regulations the device has complied with, access control, having a vulnerability disclosure program, the average time to patch the vulnerability, what personal data are being collected, how data are being collected, the purpose of data collection, who has access to the data, where the data are being stored, information on encryption and key management, and information on ports, protocols, and services and how they are secured. Our label covers all of the attributes listed in the compliance form.

Singapore

In October 2020, the Cyber Security Agency (CSA) of Singapore launched their Cybersecurity Labeling Scheme (CLS) for IoT devices. Under this scheme, the IoT devices will be rated based on their level of security. To allow IoT manufacturers and the market to adjust, the labeling is rolled out as a voluntary program. To incentivize manufacturers' adoption of the scheme, CSA has waived the label application fee until early October 2021. CSA's main goals to label IoT products are to help consumers make informed purchase decisions and at the same time incentivize IoT manufacturers to develop and provide products with enhanced security practices.

CLS was first introduced to cover Wi-Fi routers and smart home hubs as they are often the gateways into home networks. Since January 2021, the plan has been extended to cover all categories of consumer IoT devices, including security cameras, smart lights, and smart door locks.

The CLS rating could be any of four levels, ranging from satisfying basic security requirements to device undergoing structured third-party penetration tests. As of July 2021, 24 IoT devices have been granted the CLS label. The first two levels need manufacturers' declaration of conformance to security baseline requirements within ETSI EN 303 645, including having no default password, providing information on encryption and key management protocols, and offering public vulnerability disclosure policy. Our label provides information on all of the required metrics for the four rating levels specified by the CSA.

Other International Activities

To further improve the security of IoT devices at the international level, in July 2019, the Homeland Security and Public Safety Ministers of Australia, Canada, New Zealand, the United Kingdom, and the United States agreed to work toward enhancing the security by design for consumer IoT devices and engage other nations to do the same. In addition, the partner countries (France, Uruguay, the United Kingdom, Canada, Senegal, Japan, the United States, and New Zealand) in the IoT Security Platform suggested nine common principles to consider while developing international frameworks. Some of these principles are to ensure having security updates for the device with a specified minimum length of support, requiring unique credentials, encrypting the data in transit and at rest, enabling easy data deletion for users, protecting personal information, and implementing a vulnerability disclosure policy.

IoT devices could expose consumers to privacy and security risks. Despite their concerns, IoT consumers currently have no easy way to find privacy and security information for IoT devices before making their purchase decisions. To inform consumers' purchase decision-making process, we proposed a privacy and security label for IoT devices, similar to nutrition labels for food items. We incorporated and combined the inputs of privacy and security experts as well as consumers throughout our label design process. The final label is machine readable and has a layered design that covers security mechanisms, data practices, and general information about the IoT device. To facilitate the label generation process, we prepared a specification document and designed a tool to enable manufacturers to conveniently generate labels for their devices. We also developed a mobile app that allows consumers to easily compare IoT devices based on their privacy and security practices. There are still some open questions on IoT labeling that are worth exploring to effectively transition our label from a proof of concept to practice.

Do labels impact real-world purchase behavior? To design and evaluate our IoT label, we conducted interviews and surveys with hundreds of consumers of IoT devices. Although the self-reported responses indicate the strong desire to have security and privacy labels at the time of purchase, the effectiveness of the label in actual purchase behavior needs to be investigated in the future.

Do manufacturers have enough incentive to adopt the labels? It is important to investigate whether device manufacturers have enough motivation to adopt the labels and how they can be further incentivizied to do so. If consumers value IoT security and privacy labels enough to pay more for devices that have these labels, companies may be incentivized to adopt them. Regulatory safe harbors or mandates may offer an alternative path to adoption.

What design elements should we consider to increase the information communication of the label? The research on food and drug labels have shown that the design elements of the label, such as its fonts or the text color, significantly influence the effectiveness of the label in informing consumers' decision making. In our studies, we did not look into the impact of design elements.

Future work should explore what design changes should be applied to further improve the information communication of IoT security and privacy labels. ■

Acknowledgments

We thank the editor and the reviewers for their feedback, which helped improve this article. The research described in this article could have not been completed without the invaluable feedback and efforts of several amazing collaborators over the years. We are especially thankful to Harold Dixon, Hanan Hibshi, Shreyas Nagare, Supawat Vitoorapakorn, and Michelle Ling. This work was supported in part by DARPA and the Air Force Research Laboratory FA8750-15-2-0277, NSF awards TWC-1564009 and SaTC-1801472, and the Carnegie Mellon CyLab Security and Privacy Institute.

This work involved human subjects or animals in its research. Approval of all ethical and experimental procedures and protocols was granted by Carnegie Mellon University's Institutional Review Board.

References

1. G. Graff, "How a dorm room minecraft scam brought down the Internet," Wired, Dec. 2017. https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/ (accessed Aug. 1, 2021).
2. P. G. Kelley, J. Bresee, L. F. Cranor, and R. W. Reeder, "A nutrition label for privacy," in *Proc. 5th Symp. Usable Privacy Security*, 2009, p. 4.
3. P. G. Kelley, L. F. Cranor, and N. Sadeh, "Privacy as part of the app decision-making process," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2013, pp. 3393–3402.
4. P. Emami-Naeini, H. Dixon, Y. Agarwal, and L. F. Cranor, "Exploring how privacy and security factor into IoT device purchase behavior," in *Proc. CHI Conf. Hum. Factors Comput. Syst.*, 2019, p. 534.
5. P. Emami-Naeini, Y. Agarwal, L. Cranor, and H. Hibshi, "Ask the experts: What should be on an IoT privacy and security label?" *IEEE Security Privacy*, vol. 1, pp. 771–788, May 2020, doi: 10.1109/SP40000.2020.00043.
6. P. Emami-Naeini, J. Dheenadhayalan, Y. Agarwal, and L. F. Cranor, "Which privacy and security attributes most impact consumers' risk perception and willingness to purchase IoT devices?" in *Proc. IEEE Symp. Security Privacy (SP)*, 2021, pp. 1937–1954. doi: 10.1109/SP40001.2021.00112.
7. "Strengthening the cybersecurity of the Internet of Things," U.S. Senate Committee on Commerce, Science, & Transportation, Apr. 2019. https://www.commerce.senate.gov/public/index.cfm/hearings?ID=A6113AB7-E89B-48C7-B555-E3CBB1466040 (accessed Nov. 19, 2021).
8. N. Bowles, "Thermostats, locks and lights: Digital tools of domestic abuse," New York Times, Jun. 23, 2018. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html (accessed Jun. 3, 2020).
9. P. Emami-Naeini, Y. Agarwal, and L. F. Cranor, "Specification for CMU IoT security and privacy label," Carnegie Mellon Univ., Pittsburgh, PA, USA. [Online]. Available: https://iotsecurityprivacy.org/downloads/Privacy_and_Security_Specifications.pdf
10. "Executive order on improving the nation's cybersecurity," The White House, May 12, 2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/ (accessed Aug. 1, 2021).

Pardis Emami-Naeini is a postdoctoral scholar at the University of Washington, Seattle, Washington, 98195, USA. Her research interests lie at the intersection of security and privacy, usability, and human–computer interaction. Pardis received a Ph.D. in computer science from Carnegie Mellon University (CMU). She was selected as a Rising Star in electrical engineering and computer science in October 2019 and was awarded the 2019–2020 CMU CyLab Presidential Fellowship. Contact her at pardis@cs.washington.edu.

Janarth Dheenadhayalan is a software engineer at Amazon Web Services. His research interests are in the fields of hardware accelerators and machine learning to enhance computer security and privacy across multiple facets of application domains. Dheenadhayalan received a M.Sc. in electrical and computer engineering from Carnegie Mellon University. His contribution to this article was completed when he was with Carnegie Mellon University. Contact him at janarth.dhayalan@gmail.com.

Yuvraj Agarwal is an associate professor and director of SynergyLabs at Carnegie Mellon University, Pittsburgh, Pennsylvania, 15213, USA. His lab focuses on research at the intersection of hardware and software systems, and in the recent past, his group has focused on energy efficiency, security, and privacy as a central research theme. Agarwal received a Ph.D. from the University of California, San Diego. He is a Member of IEEE, the Association for Computing Machinery, and USENIX. Contact him at yuvraj@cs.cmu.edu.

Lorrie Faith Cranor is the director and Bosch Distinguished Professor of the CyLab Security and Privacy Institute and FORE Systems Professor of Computer Science and Engineering and Public Policy at Carnegie Mellon University, Pittsburgh, Pennsylvania, 15213, USA. She is a leading researcher in both online privacy and usable privacy and security. She is a Fellow of IEEE, the Association for Computing Machinery (ACM), and the American Association for the Advancement of Science, and a member of the ACM CHI Academy. Contact her at lorrie@cmu.edu.