LILY HAY NEWMAN SECURITY 06.09.2020 07:00 AM

IoT Security Is a Mess. Privacy 'Nutrition' Labels Could Help

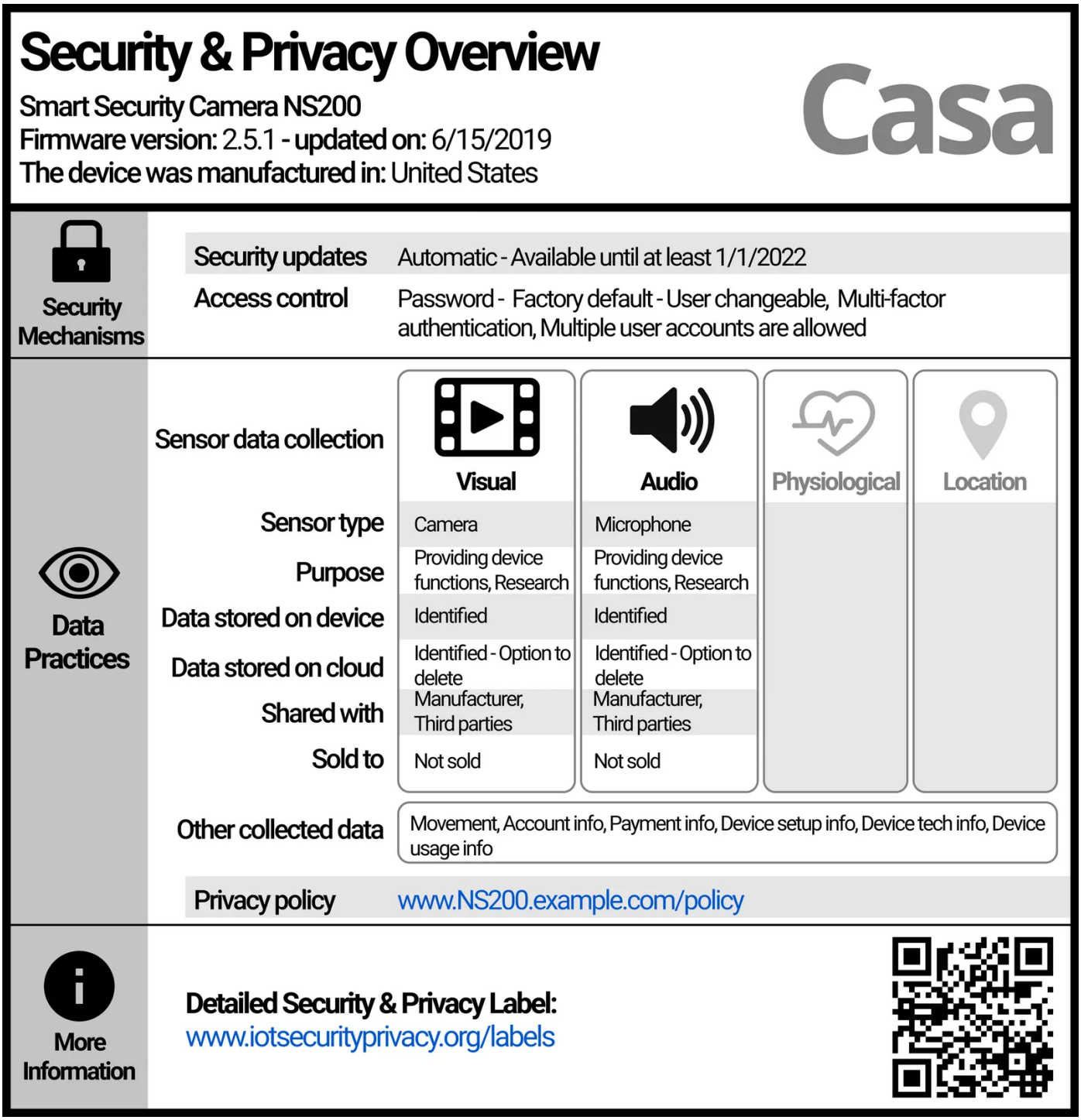
Just like with foods that display health information the package, researchers are exploring a tool that details how connected devices manage data.

An easy-to-read label might help people better understand potential risks ILLUSTRATION: ELENA LACEY; GETTY IMAGES

THE INTERNET-OF-THINGS SECURITY crisis has been building for more than a decade, with unprotected, unpatchable gadgets fueling botnets, getting attacked for nation state surveillance, and just generally being a weak link for networks. Given that IoT security seems unlikely to magically improve anytime soon, researchers and regulators are rallying behind a new approach to managing IoT risk. Think of it as nutrition labels for embedded devices.

At the IEEE Symposium on Security & Privacy last month, researchers from Carnegie Mellon University presented a prototype security and privacy label they created based on interviews and surveys of people who own IoT devices, as well as privacy and security experts. They also published a tool for generating their labels. The idea is to shed light on a device's security posture but also explain how it manages user data and what privacy controls it has. For example, the labels highlight whether a device can get security updates and how long a company has pledged to support it, as well as the types of sensors present, the data they collect, and whether the company shares that data with third parties.

“In an IoT setting, the amount of sensors and information you have about users is potentially invasive and ubiquitous," says Yuvraj Agarwal, a networking and embedded systems researcher who worked on the project. "It’s like trying to fix a leaky bucket. So transparency is the most important part. This work shows and enumerates all the choices and factors for consumers."



COURTESY OF IOT CARNEGIE MELLON UNIVERSITY

Nutrition labels on packaged foods have a certain amount of standardization around the world, but they're still more opaque than they could be. And security and privacy issues are even less intuitive to most people than soluble and insoluble fiber. So the CMU researchers focused a lot of their efforts on making their IoT label as transparent and accessible as possible. To that end, they included both a primary and secondary layer to the label. The primary label is what would be printed on device boxes. To access the secondary label, you could follow a URL or scan a QR code to see more granular information about a device.

"We wanted to understand whether this information can convey risk and whether participants really understood what this information means," says Pardis Emami-Naeini, a privacy researcher who led the work. "Based on the study, we found that some of the factors are really important. For example, if the data is being shared or sold to third parties, people are really concerned about this. And that hugely changed their risk perception, as does whether the device has multifactor authentication."

Another key aspect of the security and privacy label project is that the information is also encoded to be machine readable. This way, even if different countries or industries develop their own assessment tools, there's still a way to compare and process all the data. The researchers point out that data from the labels could make it easier to search for products by their privacy and security features, creating the potential for these to be mainstream product considerations rather than niche points that are difficult for consumers to research. Ecommerce websites could even offer filters for privacy and security features like they already do for things like price, weight, or screen size. In this way, consumers could make intentional choices about the products they buy, with digital safety as one of the factors.

The researchers say that they've had a lot of private-sector and congressional interest in their label. But so far they've only been able to make example labels based on imaginary products or mock up labels for real products based on public data. The researchers are looking for a manufacturer to pilot the labels in a more serious way, with honest information about the products.

There is real momentum toward doing these types of tests. Finland, Singapore, and the United Kingdom are all working on national IoT label programs focused on security. And while some IoT security bills have floated around the US Congress, the National Telecommunications and

Information Administration within the Department of Commerce is actively working on a similar type of project for software. The idea is to develop a software "bill of materials" that would help the industry keep track of all the different open source and third-party components that go into one single software program or platform.

"Standardization I think will help, just like the ingredients label on food educates people about how much sugar or sodium they're consuming," says Chris Wysopal, chief technology officer of the software auditing firm Veracode. "Standardizing a software bill of materials would make it more clear to a consumer what they're getting."

The researchers are realistic that for their work to have a long-term impact there would either need to be widespread voluntary adoption of the label by manufacturers or a government mandate to do so. But they say that's why they've designed the label with room for manufacturers to explain their choices to consumers.

"There may be a really good reason that your thermostat has a microphone, but if the company doesn't tell you, then you're shocked," says Lorrie Cranor, director of Carnegie Mellon's usable privacy and security lab. "If they tell you about the microphone up front and explain why that is, then you might say 'Oh, OK, that makes sense.'"

Conventional wisdom says that consumers won't typically pay a premium for privacy and security features. The researchers had preliminary findings, though, that an easy-to-read label might help people better understand potential risks and make them more willing to pay more for strong guarantees. It will take more investigation to expand on that finding, and the easiest way to do extensive testing would be for companies to start adopting security and privacy labels on their IoT products. You likely won't be seeing IoT privacy labels on store shelves anytime soon. But the stakes are high enough that something certainly needs to change.

More Great WIRED Stories

- Covid-19 will accelerate the AI health care revolution
- What is Clubhouse, and why does Silicon Valley care?
- How to sleep when the world is falling apart

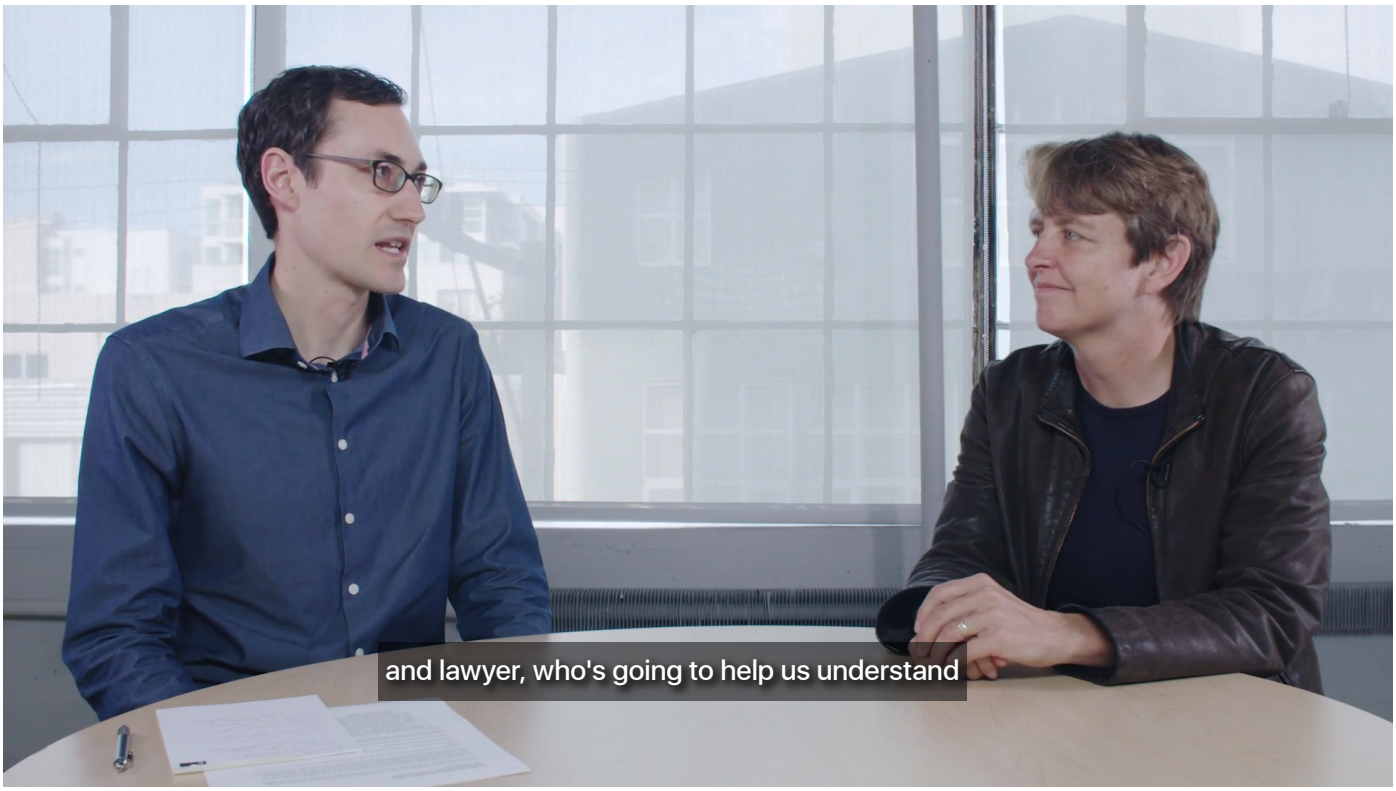
- Video-chat juries and the future of criminal justice
- 26 *Animal Crossing* tips to up your island game
- 👁️ Is the brain a useful model for AI? Plus: Get the latest AI news
- 💻 Upgrade your work game with our Gear team's favorite laptops, keyboards, typing alternatives, and noise-canceling headphones

---

Lily Hay Newman is a senior writer at WIRED focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate magazine and was the staff writer for Future Tense, a publication and project of Slate, the New America Foundation, and Arizona State University. Additionally... Read more

SENIOR WRITER

Featured Video



Why Some Cities Are Banning Facial Recognition Technology

A handful of US cities have banned government use of facial recognition technology due to concerns over its accuracy and privacy. WIRED's Tom Simonite talks with computer vision scientist and lawyer Gretchen Greene about the controversy surrounding the use of this technology.

TOPICS IOT PRIVACY