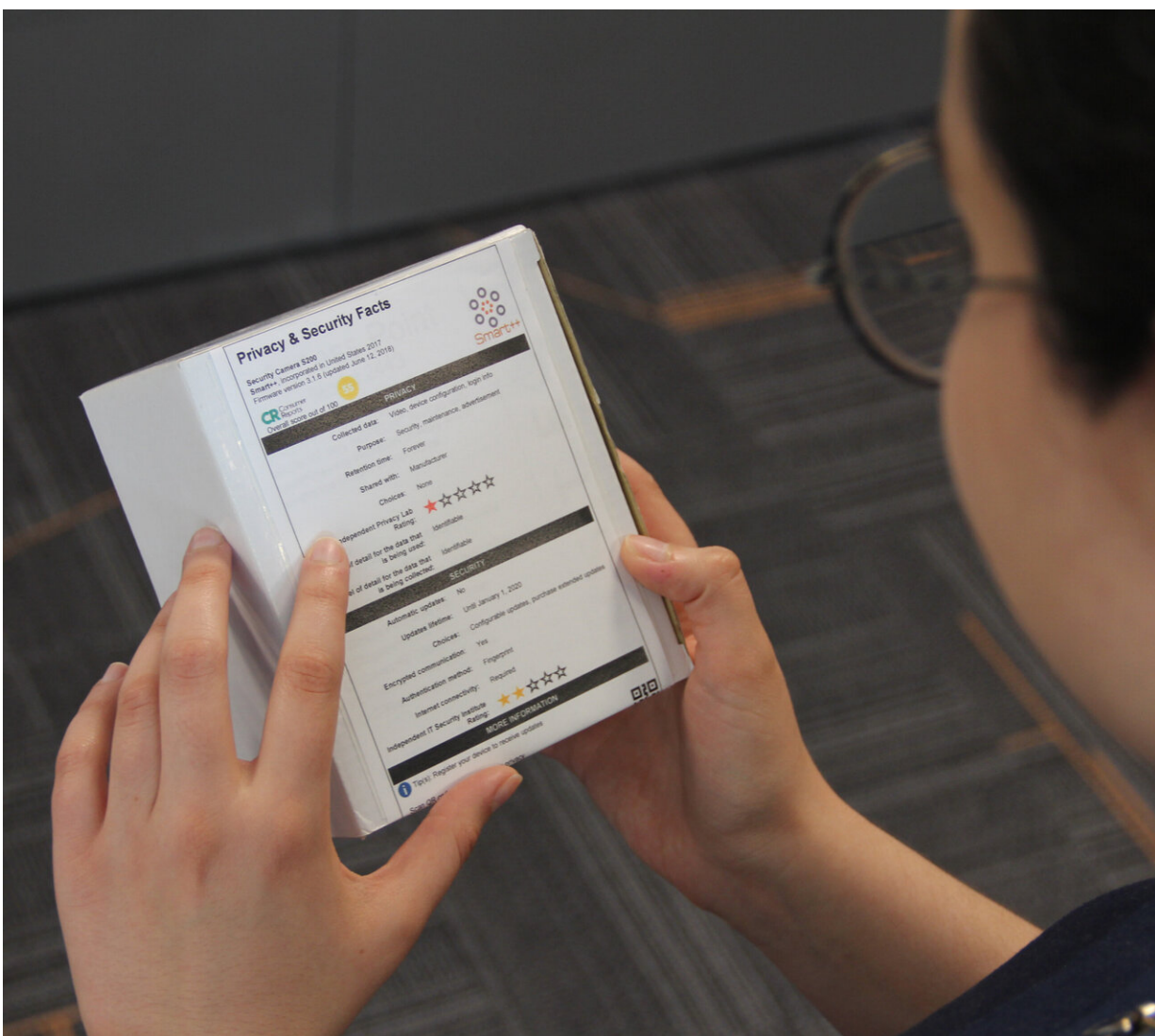# Security and privacy rarely considered before buying IoT devices

June 4 2019, by Daniel Tkacik

CyLab researcher Pardis Emami-Naeini examines a privacy and security label prototype. Credit: Carnegie Mellon University CyLab

In today's often-precarious security and privacy landscape, you'd think consumers would be taking security and privacy risks into serious consideration when purchasing new IoT devices. And you'd be wrong.

In a study presented at the ACM CHI conference in Glasgow last month, researchers from Carnegie Mellon University's CyLab found that security and privacy risks may not be on the list of considerations when consumers purchase new IoT devices.

"Some of the participants said that if they had more information about these risks and what to look for, they would have considered them when purchasing the device," says Pardis Emami-Naeini, a Ph.D. student in the Societal Computing program in Carnegie Mellon's School of Computer Science.

The team interviewed 24 participants – 14 females and 10 males with an average age of 36 years – who all had recently purchased IoT devices ranging from smart home assistants to smart doorbells to activity trackers.

The researchers asked individual participants what considerations went into their purchase. In the beginning stages of the interview, the researchers never mentioned security or privacy to avoid any potential biases in their responses.

"Most of the participants did not consider privacy and security when making their purchase, but had privacy and security related concerns after the purchase," Emami-Naeini says. "These post-purchase concerns were mostly caused by learning about concerns from friends, media reports, or the device functioning in some unexpected way."

Once the participants were prompted with the topics of security and privacy, almost all said they would make security and privacy considerations before purchasing devices in the future. In fact, nearly all said they would be willing to pay a premium of 10 to 30 percent of the base price of the device for security and privacy assurances.
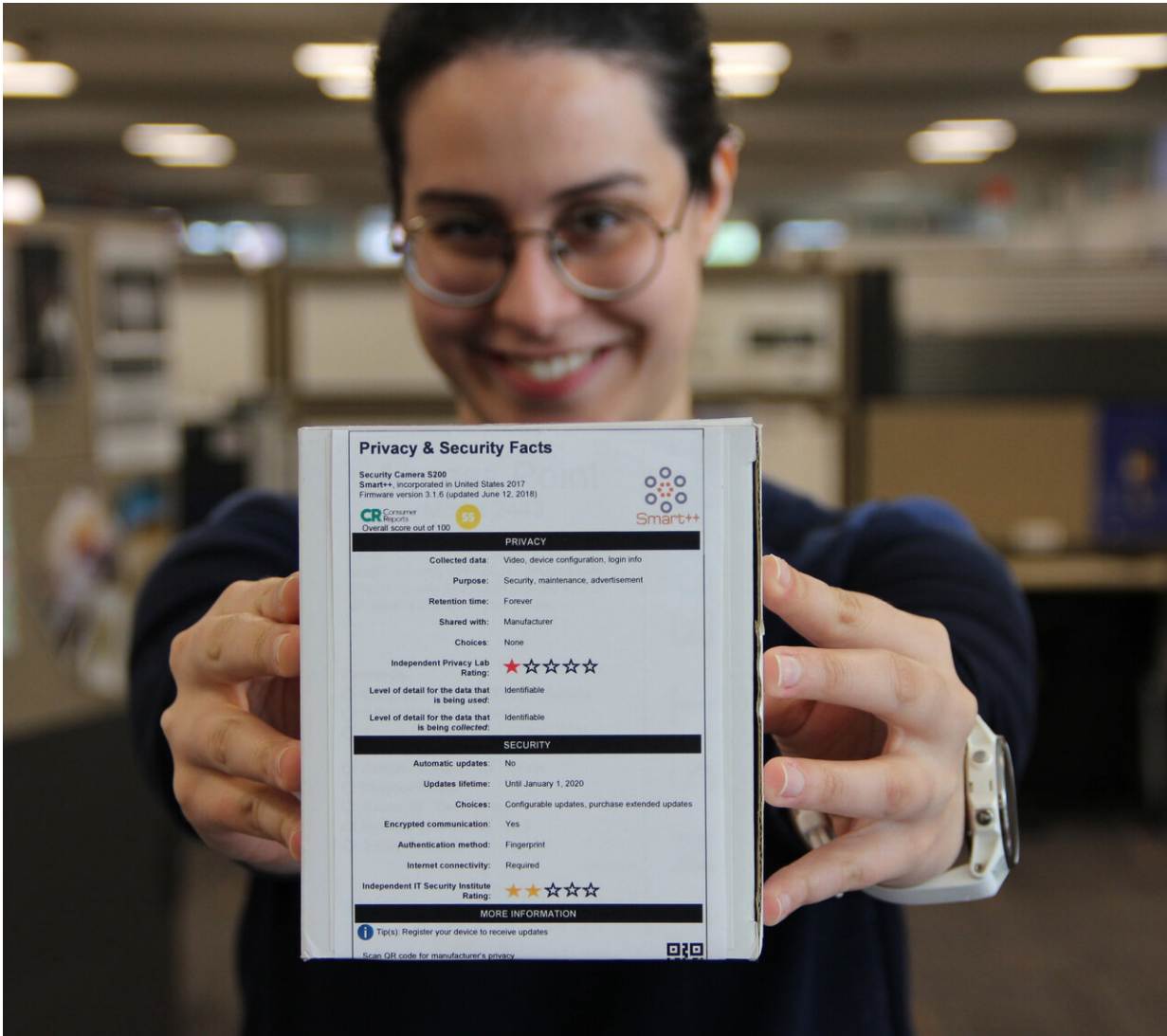
CyLab researcher Pardis Emami-Naeini displays a privacy and security label prototype. Credit: Carnegie Mellon University CyLab

During the final portion of the interview, the researchers presented the interviewees with a prototype privacy and security label, akin to nutrition labels found on food packaging.

"The main purpose of the label is to inform purchase decisions," says Emami-Naeini. "… and in general, the participants found them to be understandable, easy to read, and useful."

One participant went as far as saying that they would "definitely trust" a product that had a security and privacy label over another that did not.

In the study, the researchers acknowledge the challenges associated with adoption and enforcement of the label. Aside from the fact that attempts to encourage these types of standardized privacy disclosures have faltered in the past, the rapid pace of software and firmware updates in IoT devices may make it difficult for manufacturers to keep the labels up to date.

But Emami-Naeini believes a solution of this type is badly needed as it is difficult for consumers to get information about the privacy and security of IoT devices prior to purchase. Participants stated they had been surprised by recent news articles reporting microphones in smart smoke detectors and security systems.

"It's up to the consumers to purchase secure devices or private devices, and we need to empower them to make those decisions themselves," Emami-Naeini says.

Other researchers involved in the study included Human-Computer Interaction Institute researcher Henry Dixon, Institute for Software Research professor Yuvraj Agarwal, and CyLab director Lorrie Cranor.