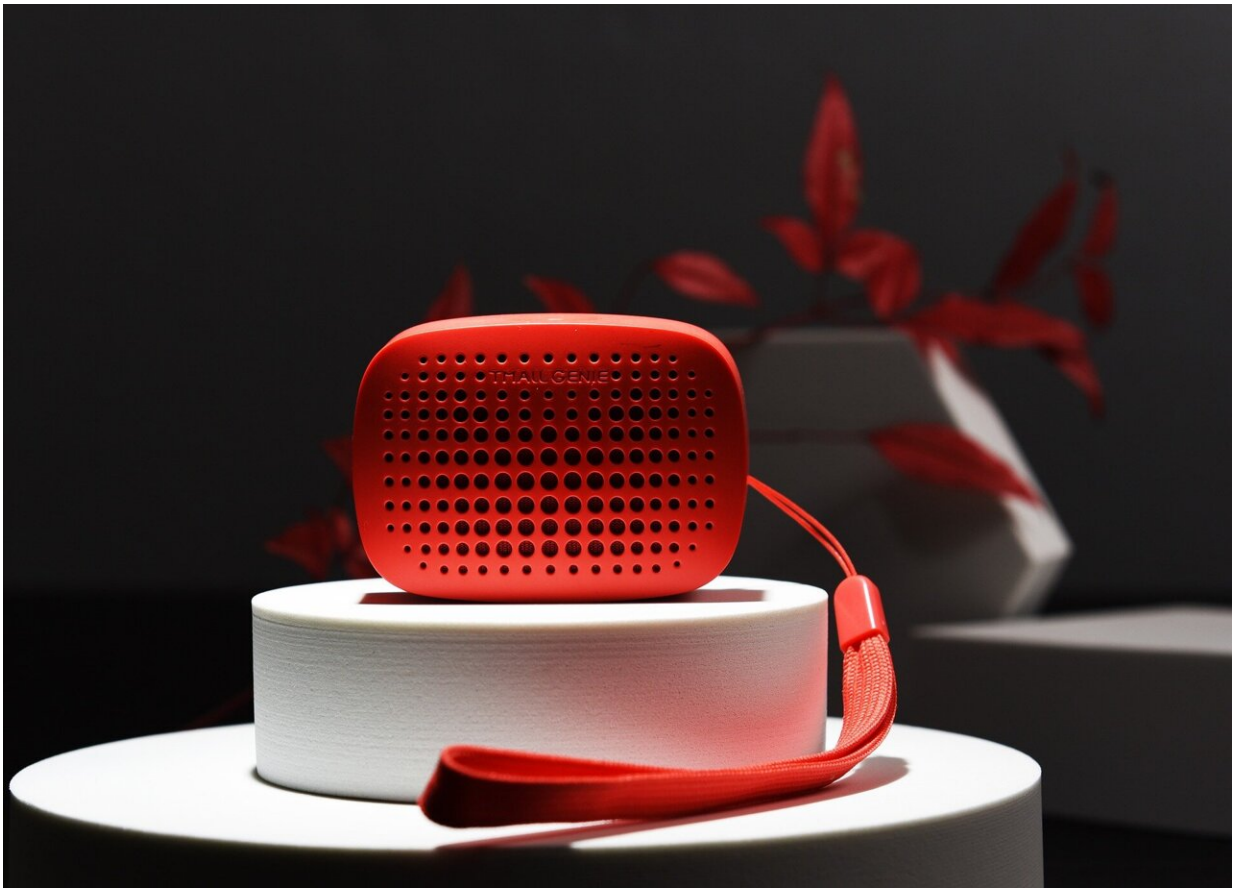
Smart devices: Putting a premium on peace of mind

August 7 2023



Credit: Pixabay/CC0 Public Domain

Two out of five homes worldwide have at least one smart device that is vulnerable to cyber-attacks. Soon, that new smart TV or robot vacuum

you've been considering for your home will come with a label that helps you gauge whether the device is secure and protected from bad actors trying to spy on you or sell your data.

In July, the White House announced plans to roll out voluntary labeling for internet-connected devices like refrigerators, thermostats and baby monitors that meet certain cybersecurity standards, such as requiring data de-identification and automatic security updates.

For tech companies that choose to participate, the good news is that there is a market for such a guarantee. A new survey of U.S. consumers shows that they are willing to pay a significant premium to tell which gadgets respect their privacy and are safe from security attacks before they buy.

But voluntary product labels may not be enough if the program is going to protect consumers in the long run, the authors of the study caution.

"Device manufacturers that do not care about security and privacy might decide not to disclose at all," said Duke University assistant professor of computer science Pardis Emami-Naeini, who conducted the survey with colleagues at Carnegie Mellon University. "That's not what we want."

The average household in the U.S. now has more than 20 devices connected to the internet, all collecting and sharing data. Fitness trackers measure your steps and monitor the quality of your sleep. Smart lights track your phone's location and turn on as soon as you pull in the driveway. Video doorbells let you see who's at the door—even when you're not home.

But for all their convenience, today's smart gadgets still have some glaring privacy and security flaws. You may have read the stories about strangers hacking into baby monitors, companies leaking data about

customers and their passwords, or smart TVs watching you while you are watching them.

One study suggests that the number of attacks on smart devices doubled in the first half of 2021 alone, going from 639 million to 1.5 billion in just six months.

The new program, which resembles the 30-year-old Energy Star labeling program for appliances that meet certain energy efficiency standards, would "raise the bar" for cybersecurity in the home, the White House said in a statement.

Companies that practice transparency would certainly help people make more informed choices about their next smart gadget purchase, said Emami-Naeini, who has been collaborating with government officials and non-governmental stakeholders to inform the design of the cybersecurity label in the U.S. But are such labels a selling point for their products?

In a survey of 180 U.S. consumers, she and colleagues set to find out.

In an experiment conducted online, the researchers asked people to choose between discount offers on two smart devices based on labels showing different levels of protection.

For instance, a coupon worth $15 towards the purchase of a smart speaker that receives automatic security updates, versus $35 off for a smart speaker with no security updates. So a privacy-conscious consumer has to make a trade-off at the time of purchase—is the more secure product worth paying closer to full price?

The findings show that people are willing to shell out up to 50% more for devices labeled with reassuring information about how they deter

attackers or safeguard users' data, as opposed to devices with no label that leave them in the dark. The researchers will present their findings August 9 at the 32nd USENIX Security Symposium in Anaheim, California.

"Consumers are willing to pay significant premiums to have security and privacy labels," Emami-Naeini said. "However, consumers aren't as skeptical as we might hope when information is withheld from them."

When given a choice between a device with a label suggesting that it might not be the safest and no label at all, respondents were willing to pay more for an unlabeled device with no information at all about its security protocols and practices.

"That was a big surprise," Emami-Naeini said.

Without information to the contrary, respondents said they simply assumed that items without warnings were no riskier than other models on the market.

Theoretically, tech companies could take advantage of such charitable assumptions to withhold information they'd rather their customers didn't see, Emami-Naeini said.

That's because currently the label proposed for the U.S. is optional on the part of device makers; manufacturers aren't required to participate.

Consumers may start to see the new cybersecurity labels on U.S. store shelves as early as 2024. Other countries including Singapore, Finland and Australia are deploying similar programs to certify safe smart devices.

But the new research suggests that allowing device makers to either

highlight or hide their security practices could make it all too easy to game the system. Companies who fear that transparency might stigmatize their products or cost them customers could simply opt out, Emami-Naeini said.

"We recommend having a mandatory security and privacy label," Emami-Naeini said.

More information: Pardis Emami-Naeini et al, Are Consumers Willing to Pay for Security and Privacy of IoT Devices?, 32nd USENIX Security Symposium. Aug. 9-11, Anaheim, California.

Provided by Duke University