JOURNAL REPORTS: TECHNOLOGY

Imagine a Nutrition Label—for Cybersecurity

As the Internet-of-Things proliferates, consumers want to know how their data will be used by the makers of devices—before they buy them

Smart refrigerators are among the connected devices that could be candidates for a data-privacy label, researchers say.
PHOTO: JAE C. HONG/ASSOCIATED PRESS

By Cheryl Winokur Munk
Dec. 8, 2020 9:00 am ET

▶ **Listen to this article**
3 minutes

Your milk and orange juice have nutrition labels. Soon your refrigerator and coffee maker could, too.

For years, consumer privacy advocates have pushed the idea of so-called nutrition labels for devices. Instead of telling consumers how much vitamin B or C a product has, these labels would tell the prospective purchasers how their data will be used and by whom.

Researchers from Carnegie Mellon University's CyLab Security and Privacy Institute are floating a working prototype of how such a label could look. They're providing their label —vetted by researchers and numerous privacy experts—free of charge to Internet-of-Things, or IoT, device makers, standards organizations and others. Discussions for adoption are still in the early stages. But advocates hope device makers will adopt this

type of label, or that organizations such as Underwriters Laboratories, an independent safety-testing and certification company, or Consumer Reports will use at least portions of the label in their review processes, says Lorrie Cranor, the director and Bosch distinguished professor in security and privacy technologies at CyLab.

The label is designed to go on a product's packaging or on the websites where the devices are sold. Products under consideration for carrying the label could include any smart device that is connected to the internet—including security cameras, refrigerators, speakers, home controllers, doorbells, toothbrushes, thermostats, light switches, smart plugs and much more, says Dr. Cranor, who is also a professor of computer science and a professor of engineering and public policy at Carnegie Mellon.

SHARE YOUR THOUGHTS

What data-privacy information would you like to know when you buy a smart appliance? Join the conversation below.

The idea of protecting data privacy becomes more of an issue as more products connect to the internet. On Dec. 8, Apple Inc. began requiring app developers to provide information about their applications' privacy practices before submitting new apps and app updates to the App Store. What's more, consumer organizations are increasingly incorporating data privacy into their ratings, while some states have enacted, or are considering, privacy legislation. The Federal Trade Commission, which also has raised the concept of a nutrition label for privacy, says it continues to support the efforts of industry groups in this area.

Here's a closer look at the Carnegie Mellon label.

A Cyber-Label Guide

Privacy experts are floating a 'nutrition label' for Internet-connected devices. These labels could help consumers understand devices' data-collection and security practices. Below is a proposed cyber label for a fictional device, a smart doorbell. Here's what it tells consumers:

Security & Privacy Overview

① 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 ②

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 ③

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 ④

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

PUBLIC DOMAIN

---

① Overview

Provides basic product information including device name, version number and where it was manufactured.

② Security Mechanisms

Gives consumers information about the device's security, such as whether updates are automatic or manual, and how users can gain access to the device such as through a manufacturer-set password that can be changed by the user. Consumers can also see whether multiple account users are allowed and if there's an option for multi-factor authentication or biometric login.

③ Data Practices

Outlines four mechanisms the devices could use for data collection—video, audio, physiological and location. Highlights what the collected data is being used for, how and where it is stored, and whether the stored data is anonymous or is identifiable. Also illustrates how and with whom customer data is shared or sold, along with other miscellaneous data the device collects. Other data collection is mentioned here and detailed at the link and QR code.

④ More Information

The link and QR code offer a more detailed list of device-specific security and privacy practices, including

hardware safety, software safety, personal safety and encryption and key management.

Source: WSJ reporting

College Rankings

Energy

Funds/ETFs

Health Care

Leadership

Retirement

Small Business

Technology

Wealth Management