Ask the experts: What Should Be on an IoT Privacy and Security Label?

Pardis Emami-Naeini  Yuvraj Agarwal  Lorrie Faith Cranor  Hanan Hibshi
You may have one of these
Or even these
People are concerned about losing their privacy

People say they care about privacy but they continue to buy devices that can spy on them

Experts explain why people are giving mixed signals about smart tech.

By Rani Molla | @ranimolla | May 13, 2019, 5:40pm EDT

Consumers concerned about connected home privacy, still few implement safety practices

Smart devices spark privacy concerns among consumers: study

Sibbie Marcellus
Reporter
Yahoo Finance December 14, 2018

CyLab Carnegie Mellon University Security and Privacy Institute
Smart devices are getting hacked
Smart devices are getting hacked

Access Control
IoT companies are sometimes forgetful

SECURITY CAMERAS

Google calls Nest's hidden microphone an 'error'

The tech giant didn't inform customers that the home security hub had a microphone.

BY ALFRED NG, MEGAN WOLLERTON | FEBRUARY 20, 2019 10:46 AM PST
IoT companies are sometimes forgetful

Google calls Nest's hidden microphone an 'error'

The tech giant didn't inform customers that the home security hub had a microphone.

BY ALFRED NG, MEGAN WOLLERTON | FEBRUARY 20, 2019 10:46 AM PST
There is still a lot that we don’t know
There is still a lot that we don’t know
How to effectively provide this information?
Positive attitude toward labels

- **Almost all** wanted to know about privacy and security before the purchase
- **Almost all** were willing to pay a premium for such info (10% - 30%)
  - Assurance on being protected
  - Peace of mind

Source: Emami-Naeini et al., CHI 2019
Policy makers are also excited about IoT labels

'Cyber Shield Act' Aims To Establish Cybersecurity Standards for IoT Devices
The bill, introduced by Democratic legislators on Tuesday, would direct a committee to create security labels for products that meet those standards.
By Haley Samsel Oct 24, 2019

Regulatory proposal on mandatory IoT security label
Retailers will only be able to sell items with an Internet of Things (IoT) security label which would tell consumers how.

Singapore to introduce security label for smart home devices
The proposed Cybersecurity Labelling Scheme aims to enhance consumer awareness around secured products.

Finland launches cybersecurity label for IoT devices
Catherine Chapman 27 November 2019 at 12:39 UTC
Updated 28 November 2019 at 12:12 UTC
Policy makers are also excited about IoT labels

What should be on IoT privacy and security labels?
Three-round Delphi method with 22 experts

• Converging opinions without direct confrontation (Dalkey & Helmer, 1963)
• Conducted over multiple rounds of interviews and surveys
• Controlled feedback loop for convergence
Expert recruitment criteria

• Computer science or engineering professor in the field of privacy and security
• 10+ years of research or practice in privacy, security, or policy
• Author of notable books in the field of privacy and security
• Active involvement in cybersecurity standardization
• Leading a corporate IoT product team
One interview and two survey rounds

We conducted a 6-step thematic analysis (Braun & Clarke, 2006)
Labels to inform consumers’ purchase behavior

What's good about a label is that it empowers the consumer to make a more active decision about cybersecurity rather than just being completely 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.
Other perceived values of the label

- Increasing accountability and transparency
- Incentivizing manufacturers to compete on privacy and security

"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."
We designed a layered label

Primary layer (Jul’19)

Secondary layer (Jul’19)
Factors to include on the primary layer

- Security update lifetime
- Type of collected data
- Availability of automatic security updates
- Availability of default passwords
Factors to include on the secondary layer

• Retention time
• Data inference
• Data storage
• Special data handling practices for children’s data
Semi-structured interviews with IoT consumers

- Recruited 15 IoT consumers from the United States
- Conducted 1-hour semi-structured interviews
- Iteratively improved the design of the label
Non-comparative and comparative purchase
Attitudes toward the design of the label

• A few participants preferred single-layer label
  • Inconvenience of using the phone or scanning the QR code
  • Feeling of not being shown the whole picture

• Most participants expressed positive attitudes toward layered design
  • More useful information could fit on the layered label
  • Easily get insight into
    • Information presented on the primary layer
    • Manufacturer’s privacy and security practices
Label should work for both consumers and experts

"Labels are both for customers and experts such as tech journalists and consumer advocacy groups. If they see something that is questionable, they will raise it in the public press or will raise it with regulatory authorities. The label is not just for the consumer, but there’s another feedback process that works through experts."
Changes we applied to the label

• Almost all requested to move data sharing, and data selling to the primary layer
• Removed icons used for the automatic security update and default password
Security & Privacy

Smart Security Camera, NS200
Firmware version 2.5.3: updated on 9/15/2019

Security certification level: gold

Security Updates will be available until: 1/1/2022

Automatic security updates 😊
No factory-set default password 😊

Privacy certification level: silver

Device is equipped with:
- That collects
  - For the purpose of
    - Will be stored at:
      - Will be processed at:
        - Level of detail:

Other sensors to detect:
- Temperature, carbon monoxide

Privacy Statement: www.NS200privacypolicy.com

---

Security & Privacy Overview

Smart Security Camera, NS200
Firmware version 2.5.1: updated on: 9/15/2019
The device was manufactured in: United States

Security updates: Automatic (available until 1/1/2022)
Access control: Password, Factory default, User-changeable, Multiple user accounts are allowed

Data Practices

Sensor data collection
- Purpose
  - Providing device functions, research
  - Identified
  - Identified, Option to delete

- Data stored on device
  - Manufacturer

- Data stored on cloud
  - Manufacturer

- Shared with
  - Not sold

- Sold to
  - Not sold

Other collected data:
- Presence, Temperature, Carbon monoxide, Usage information, User-entered Information

Privacy policy: www.NS200.example.com/privacypolicy

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

---

CyLab Carnegie Mellon University
Security and Privacy Institute
## Security & Privacy Overview

**Smart Security Camera, NS200**  
**Firmware version 2.5.1; updated on: 6/15/2019**  
The device was manufactured in: United States

| Security & Privacy Details | Smart Security Camera, NS200  
Firmware version 2.5.1; updated on: 6/15/2019  
The device was manufactured in: United States |
|----------------------------|--------------------------------------------------|
| **Security updates** | Automatic (available until 1/1/2022)  
Access control | Password, Factory default, User-changeable, Multiple user accounts are allowed |
| **Security mechanisms** | Security oversight: Audits performed by internal security auditors  
Ports and protocols: www[NS200.example.com]/port  
Hardware safety: www[NS200.example.com]/hesafety  
Software safety: www[NS200.example.com]/ssafety  
Personal safety: www[NS200.example.com]/psafety  
Vulnerability disclosure and management: www[NS200.example.com]/vulndisc  
Software and hardware composition list: www[NS200.example.com]/bom  
Encryption and key management: www[NS200.example.com]/key |
| **Data practices** | Collection frequency: Value depends on device's usage pattern  
Data stored on device | Identified  
Data stored on cloud | Identified  
Shared with | Not sold  
Sold to | Not sold  
Other collected data | Presence, Temperature, Carbon monoxide, Usage information, User-entered information  
Privacy policy | www[NS200.example.com]/privacy-policy |
How to further improve the label?

• Exploring the design elements of the label
• Testing the effectiveness of the label in realistic settings
Specification document details

- 70+ IoT privacy and security references
- Taxonomy, consumer explanation, additional information, best practices

Prior work is mainly focused on security of IoT devices
We designed a tool to generate the label

- An interactive form
- Download options:
  - JSON
  - XML
  - HTML
IoT labels to provide transparency

• Designed the label with input from experts
• Evaluated the usability of the label
• Prepared a specification document for the label
• Developed a tool to generate the label

Most recent version of the labels, tool, and the specification are available at

www.iotsecurityprivacy.org

Special thanks to Shreyas Nagare for the tool and website development.