NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Tradeoffs, Transparency, and Shared Responsibility:

Exploring Users' Perceptions of Smart Home Security and Privacy in the U.S.

Julie Haney, PhD

Susanne Furman, PhD

National Institute of Standards and Technology

Yasemin Acar, Dr. rer. nat.

University of Paderborn

Disclaimer

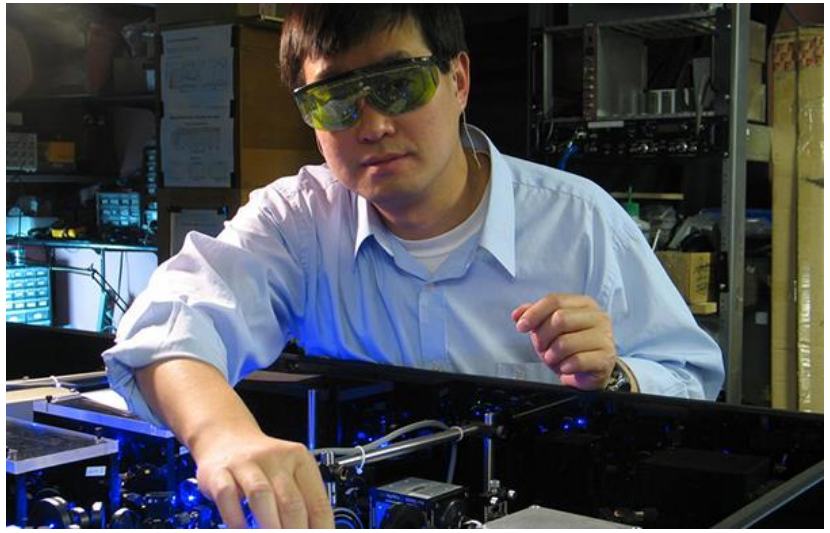
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the products mentioned are necessarily the best available for the purpose.

NIST Mission

- **NIST:** To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life

- **Information Technology Lab:** To cultivate trust in IT and metrology.

©Robert Rathe



©Nicholas McIntosh Photography

Visualization & Usability Group

Championing the Human in Information Technology

- **Public Safety**
- **Biometrics Usability**
- **AI Perceptions**
- **Usability Standards**
- **Human-Centered Cybersecurity**

Human-Centered Cybersecurity

Championing the Human in Cybersecurity

- Conduct research and other human-centered projects at the intersection of cybersecurity and human factors
- Provide actionable guidance so that the human element can be considered in cybersecurity decisions, processes, and products

Projects

Past Efforts

- Authentication
- Security & privacy perceptions
- Cryptographic development
- Cybersecurity advocacy

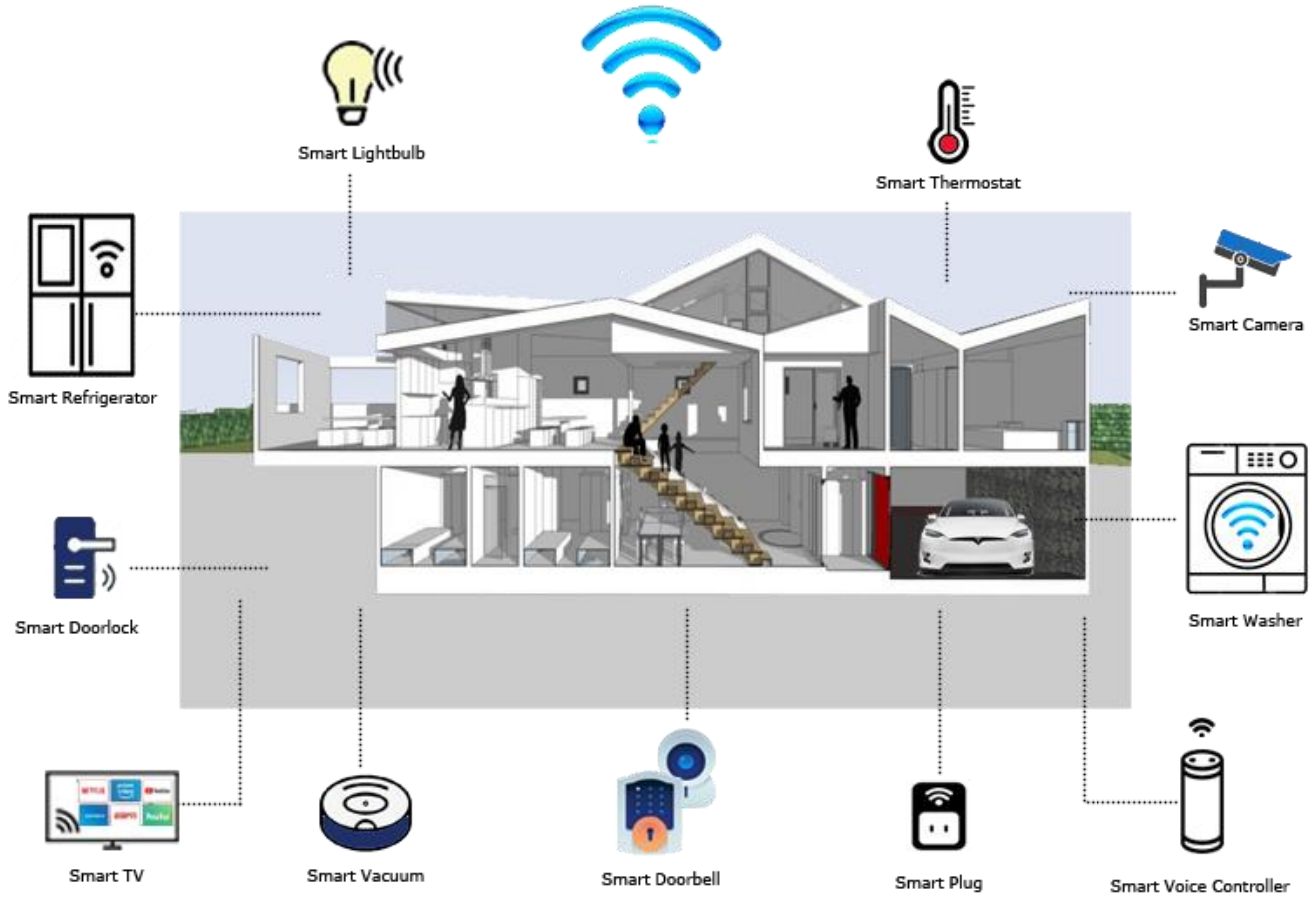
Recent Efforts

- Youth security & privacy
- Phishing
- Security awareness & training
- Research-practice gap
- Smart home security & privacy

Smart Home Security & Privacy

7

Smart Home Devices



Security & Privacy Challenges

Make changes in the physical world

Cannot be accessed or managed in the same ways as conventional IT devices

May have lifecycle support issues

What's really at risk?

- Device security
- Data security
- Privacy
- Safety

Smart Homes & Users

Increasing adoption

Users may have limited understanding of the technology and security/privacy implications

Few protection mechanisms

Users have few options to improve security/privacy of devices that may fall short to begin with

Research Efforts

Our Research

Purpose: To develop a deeper understanding of users' smart home security and privacy perceptions, actions, and challenges.

Ultimate goal: To inform efforts to better meet the security and privacy needs of smart home users while improving overall security and privacy outcomes.

Research Studies

Interviews	Smart home updates survey	General S & P perceptions survey
In-depth, semi-structured interviews of 40 active users of at least two categories of smart home devices	Within-subjects survey of 412 active users of smart home devices in at least two categories of interest	Between-subjects survey of 401 active users of a smart home device in at least one category of interest
Security and privacy concerns, actions, responsibility, & wishlist	Update perceptions, experiences, preferences, challenges & differences per device category	Concerns, actions, responsibility & differences per device category

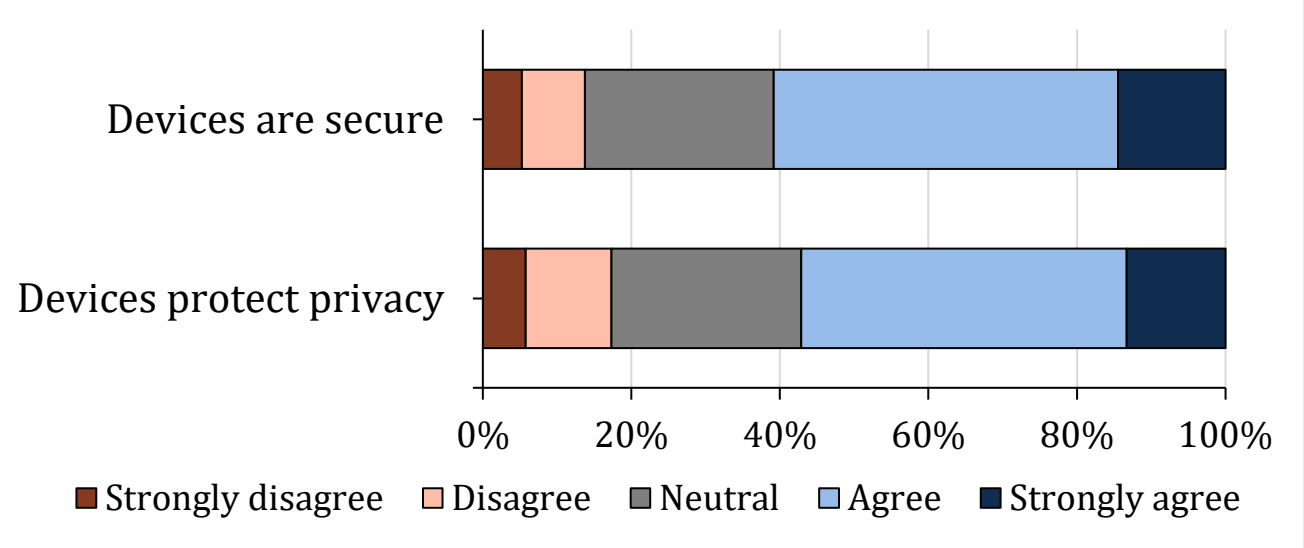
Device Categories

- Voice assistants
- Thermostats
- Security devices
- Sensors
- Lighting devices

Security & Privacy Concerns

Device Security

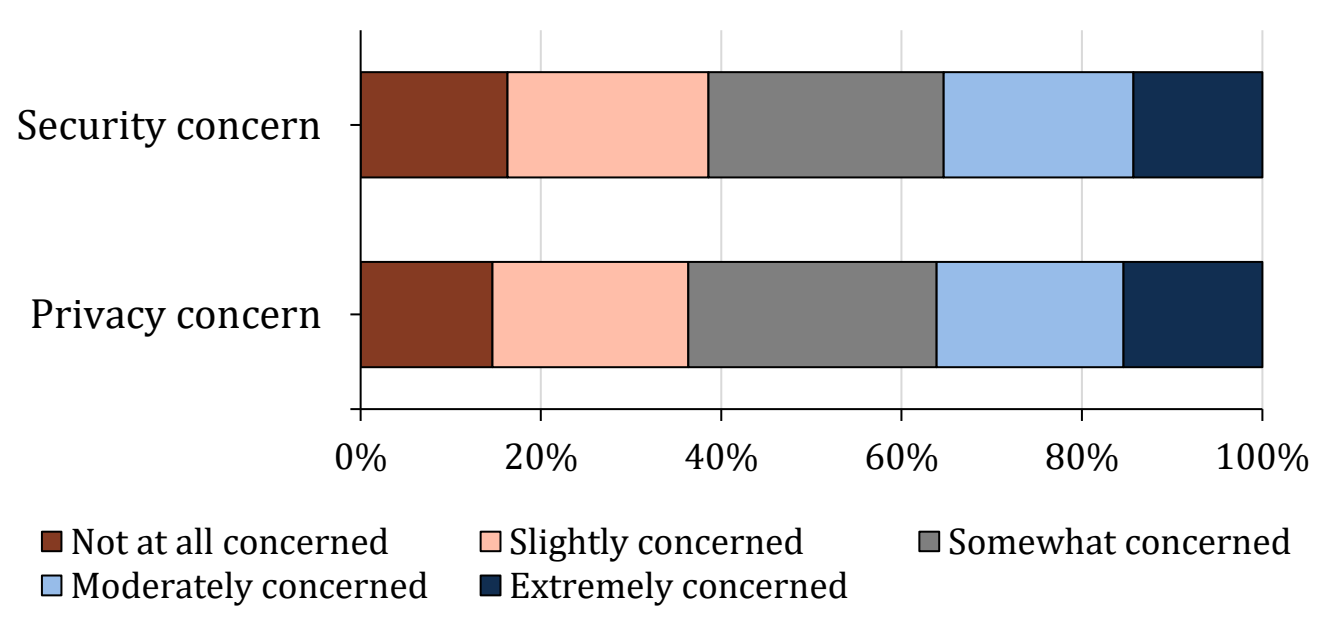
"I think that most of these <category> smart home devices are secure."
"I think that most of these <category> smart home devices protect my privacy."



- Agreement ratings highest for security devices (80% sec, 70% priv) and sensors (70% sec, 61% priv)
- Agreement ratings for voice assistants (35% sec, 39% priv) significantly lower than other device categories

Results from general S & P survey

Level of Concern



- Level of security concern lowest for thermostats (28%) and highest for sensors (42%)
- Level of privacy concern lowest for thermostats and security devices (31%) and highest for sensors and voice assistants (42%)
- No statistically significant differences across categories

Results from general S & P survey

Security & Privacy Concerns

Audio/video access
(privacy & security)

Data breach
(privacy & security)

Government surveillance
(privacy & security)

Data collection
(privacy)

Household profiling
(privacy)

Physical safety
(security)

Results from interview study

Reasons for Lack of Concern

Benefits outweigh the risks.

"I know there's the potential of a security leak, but yet, I like having the convenience" (P01)

My data/devices aren't that interesting.

"I go on faith that they [hackers] don't find me interesting enough." (P23)

The chances of being hacked are low.

"Somebody would have to pluck us at random to really be at risk." (P25)

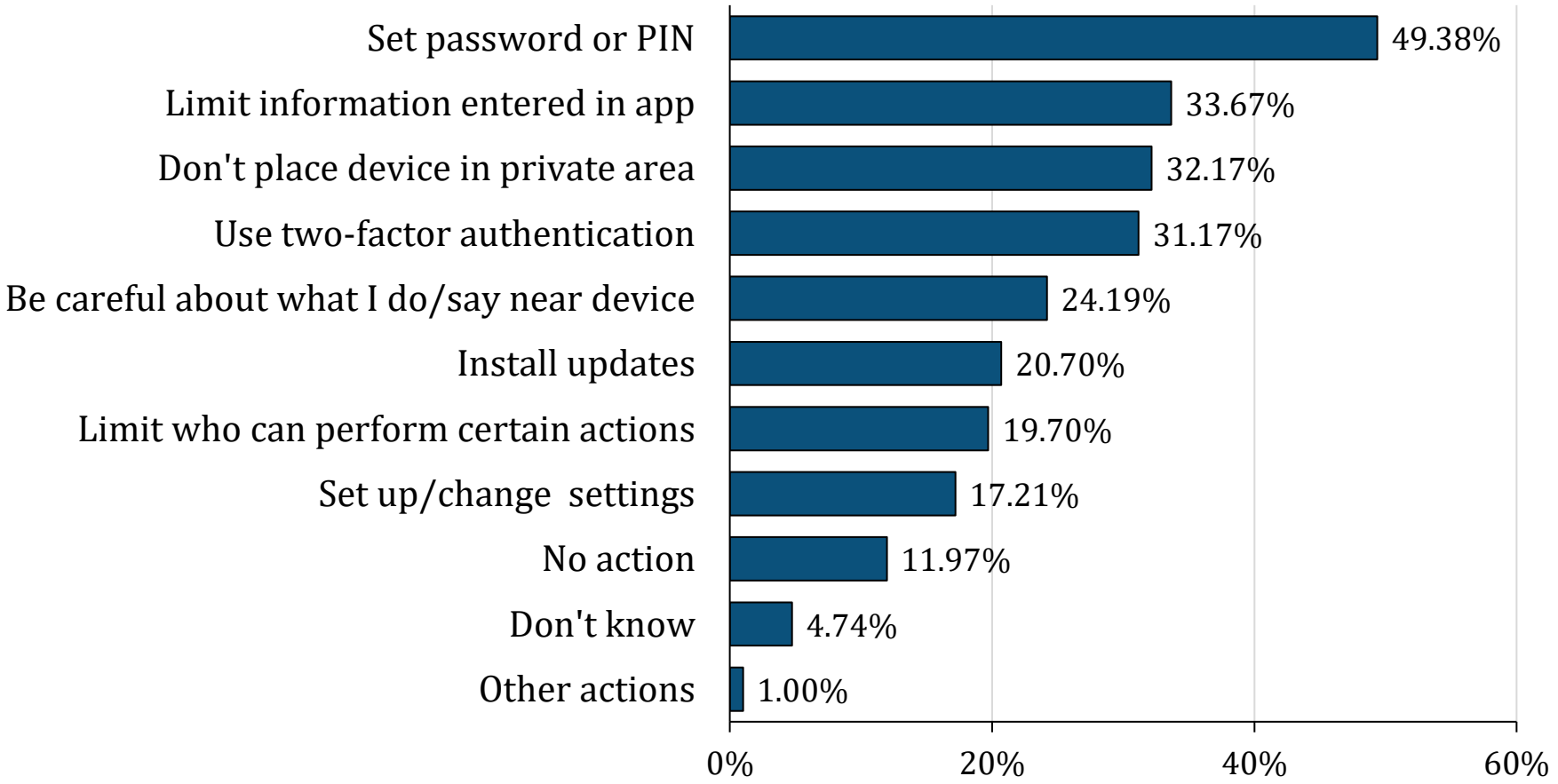
I trust the manufacturer.

"These are pretty big companies…Maybe that's why I'm feeling a little more secure than not." (P06)

Results from general S & P survey and interview study

Security & Privacy Mitigations

Device Mitigations



- Participants with security devices significantly more likely to set a password
- Participants with voice assistants significantly less likely to set up/change security/privacy settings

Results from general S & P survey

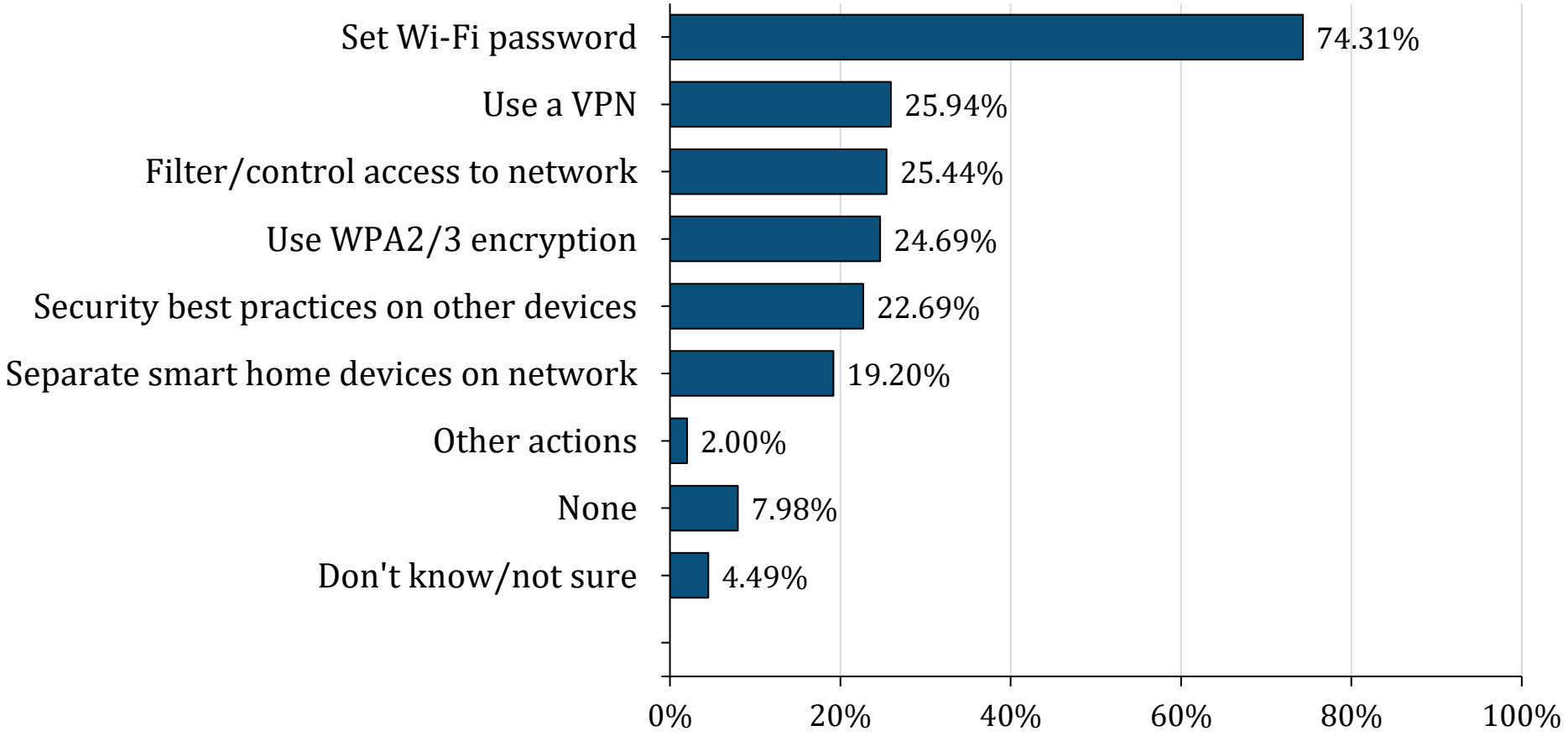
Smart Home Updates

- Majority thought updates were important and urgent; voice assistants and lighting significantly less
- Top problems included disruption, unclear notifications, unclear purpose, update failure/undesirable changes
- Update modes inconsistent
- Automatic updates preferred for voice assistants and thermostats
- Manual updates preferred for security devices and sensors

> Some devices will send me a text message. . . saying that we're going to be updating a device at this time, and it will apply the updates automatically. Other devices, I need to go into their own specialty apps and…check for an update. Some devices, I actually have to go to a website and download something.
> (P11, interviews)

Results from smart home updates survey

Home Network Mitigations



Results from general S & P survey

Reasons for Lack of Action

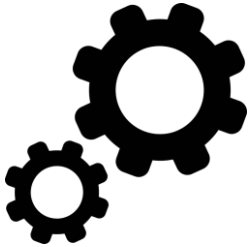
I'm satisfied with what I've done.

"I have my own unique passwords that aren't dictionary words, so that's how I mitigate." (P10)

I don't understand security/privacy enough.

"I'm not going to educate myself on network security... This stuff is not my forte." (P08)

Manufacturers don't give me options.



"I've been given very little methods to alleviate my concerns." (P13)

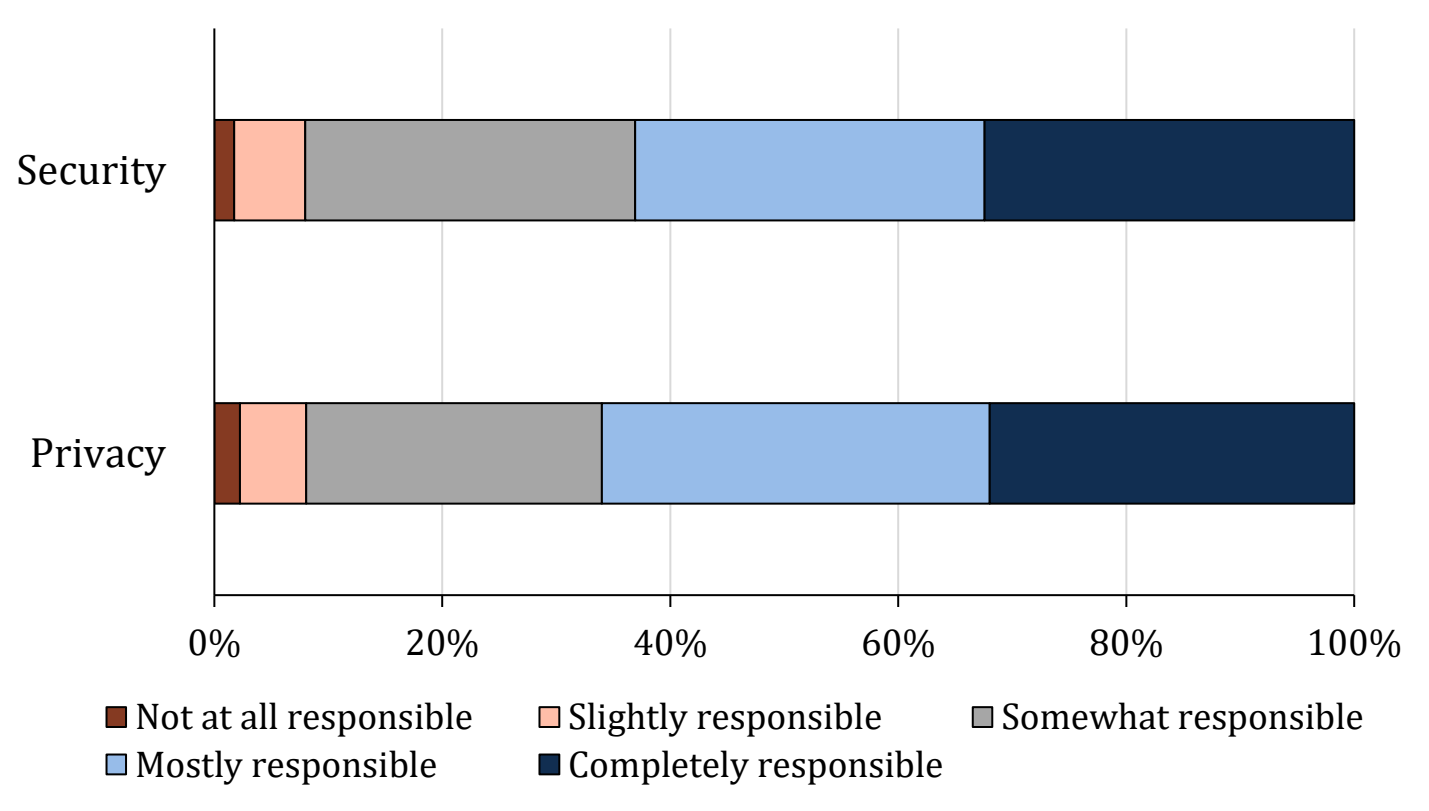
I don't understand the device enough.

"You really don't know what the devices are broadcasting…Is it doing more than you think?" (P11)

Results from general S & P survey and interview study

Security & Privacy Responsibility

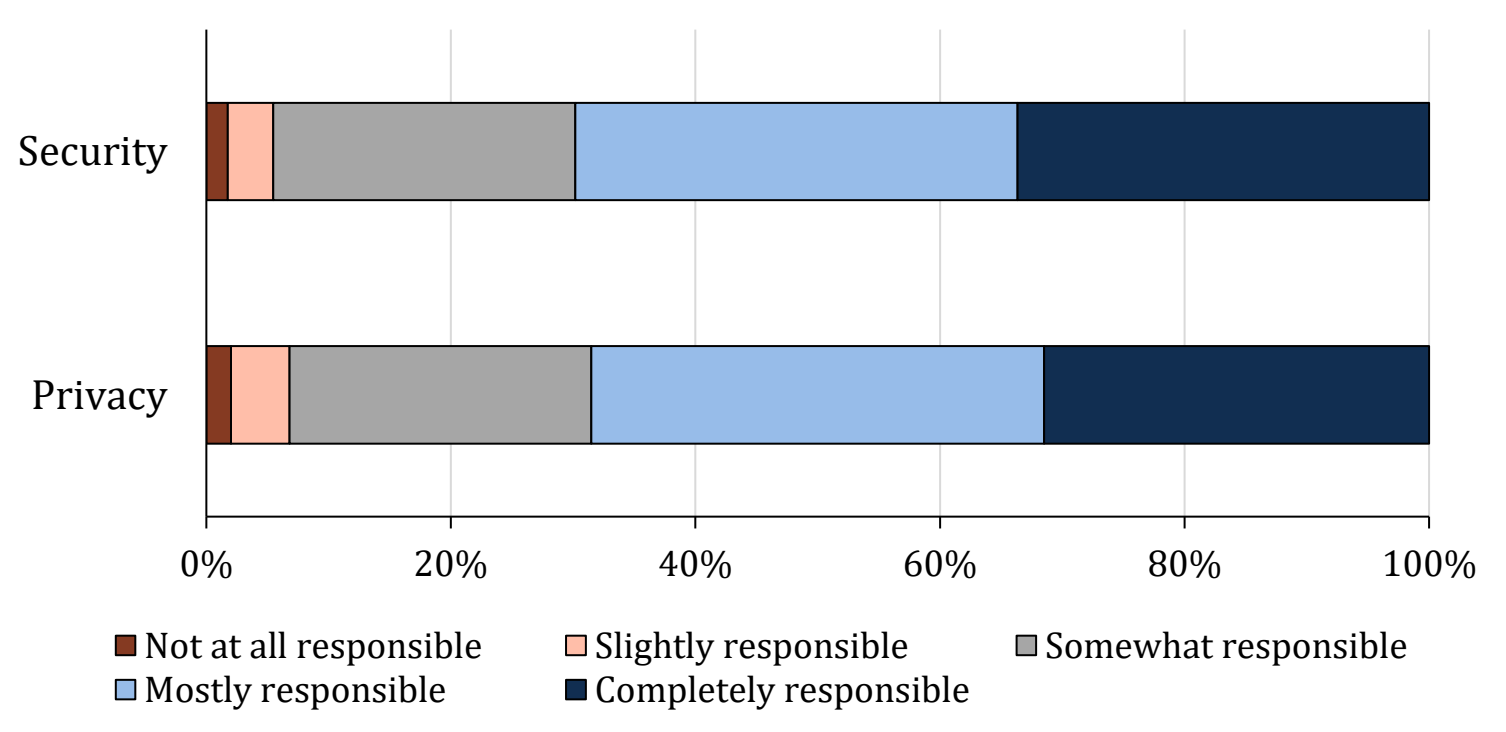
Personal Responsibility



> I feel like the default is always full access, so you have to really look for and pursue stricter settings. (P18)

Results from general S & P survey and interview study

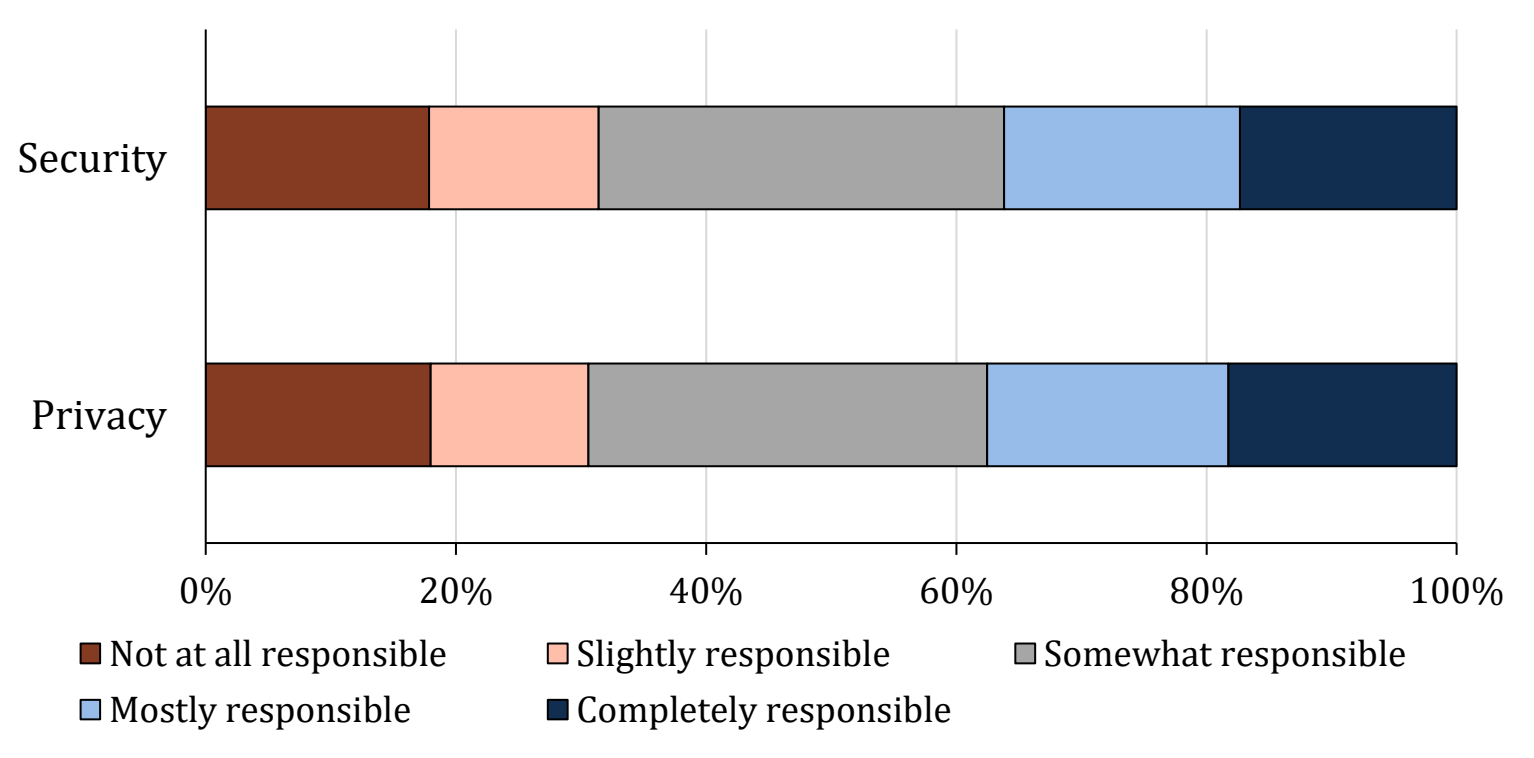
Manufacturer Responsibility



> They need to do everything [since they are] taking so much money for all that. (P09)

Results from general S & P survey and interview study

Government Responsibility



> Responsibility goes on the government to protect your citizens.
> (P29)

Results from general S & P survey and interview study

Shared Responsibility

> I think the company is responsible for it…In terms of government oversight, the government is in some way…Ultimately – and we're talking about accountability – you are responsible for your information because everyone else doesn't really care about you any more than you care about you.
>
> (P08)

Implications

Users

Inconsistent relationships between being concerned, accepting personal responsibility, and taking actions

Belief that some categories of devices are less secure/privacy respecting (voice assistants) or more important to protect (security devices and sensors)

Informed personal responsibility requires better awareness, opportunities for taking action, and more tips about what to do

Manufacturers

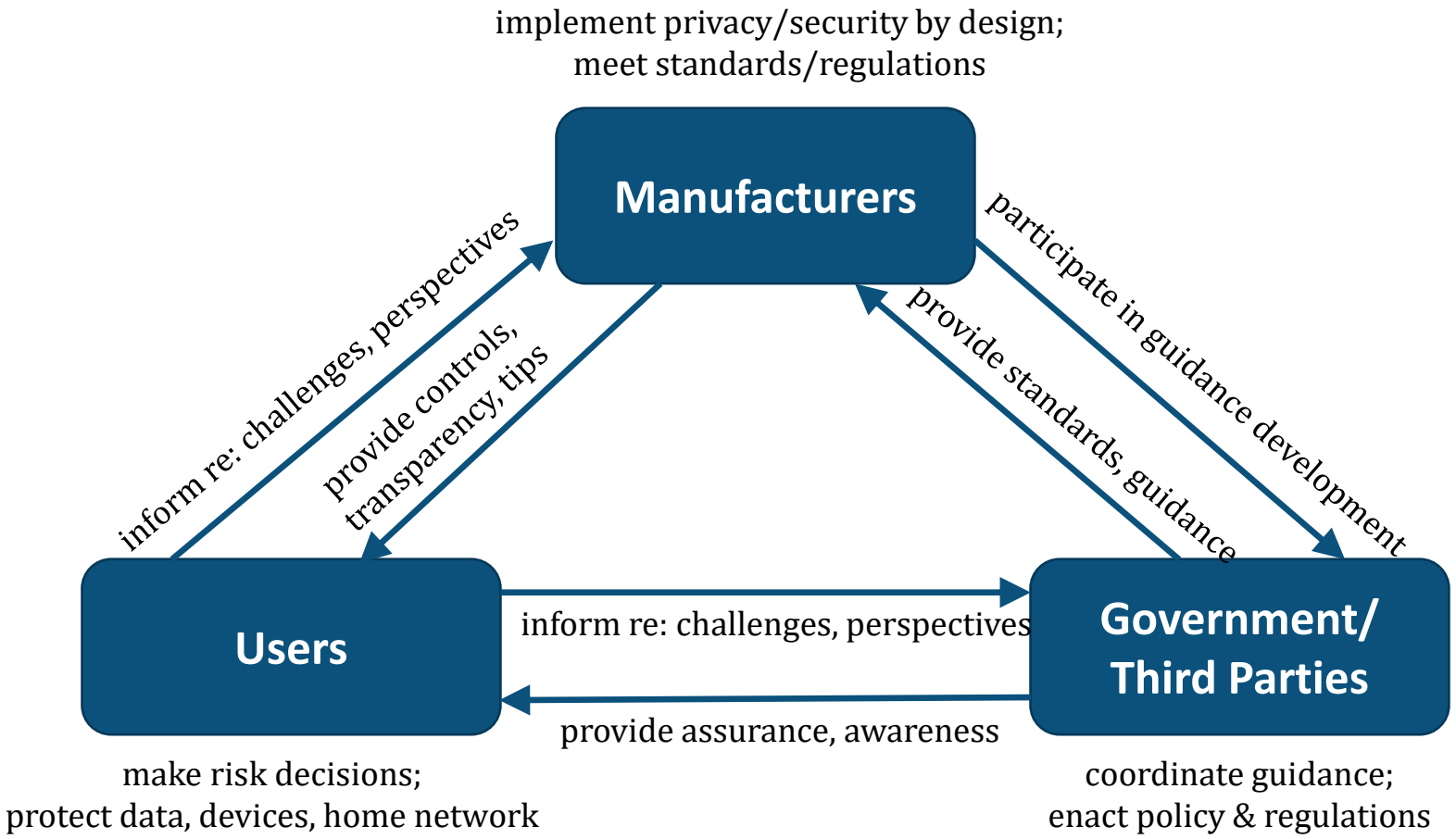
Participants differ on their trust of manufacturers to produce secure, privacy-respecting devices

Expectation that manufacturers should build secure and privacy-protecting devices out-of-the-box while also offering users some control

Government/3rd parties

Desire for security and privacy regulation to uphold and support manufacturer responsibility

Interdependent Relationship



Supporting Users

Transparency

"We've got to do something to protect people's information, or at least make them aware of what exactly is being utilized and sold." (P31)

Secure & Private by Design

"I'd like to see the vendors take more responsibility and take more action to secure their own devices." (P15)

More Control & Choices

"There would be some of these products that I have been avoiding purchasing that I might purchase if they provided more granular control." (P15)

Tips & Instructions

"I think I need to be advised on good practices that I could take…and then I would probably implement them." (P35)

Research Papers

Interview study:

- "It's the Company, the Government, You and I": User Perceptions of Responsibility for Smart Home Privacy and Security. *USENIX Security Symposium*. 2021
- Smart Home Security and Privacy Mitigations: Consumer Perceptions, Practices, and Challenges. *International Conference on Human-Computer Interaction*. 2020
- Towards Usable Updates for Smart Home Devices. *Socio-Technical Aspects in Security Workshop.* 2020
- NISTIR 8330 – Research Report: User Perceptions of Smart Home Security and Privacy. 2020.

Updates survey:

- User Perceptions and Experiences with Smart Home Updates. *IEEE Symposium on Security & Privacy*. 2023
- Smart Home Device Loss of Support: Consumer Perspectives and Preferences. *International Conference on Human-Computer Interaction.* 2023

Thank you!

human-cybersec@nist.gov

https://csrc.nist.gov/projects/human-centered-cybersecurity