Consumer Perceptions of Smart Home Privacy and Security

Julie Haney[1], Susanne Furman[1], & Yasemin Acar[2]

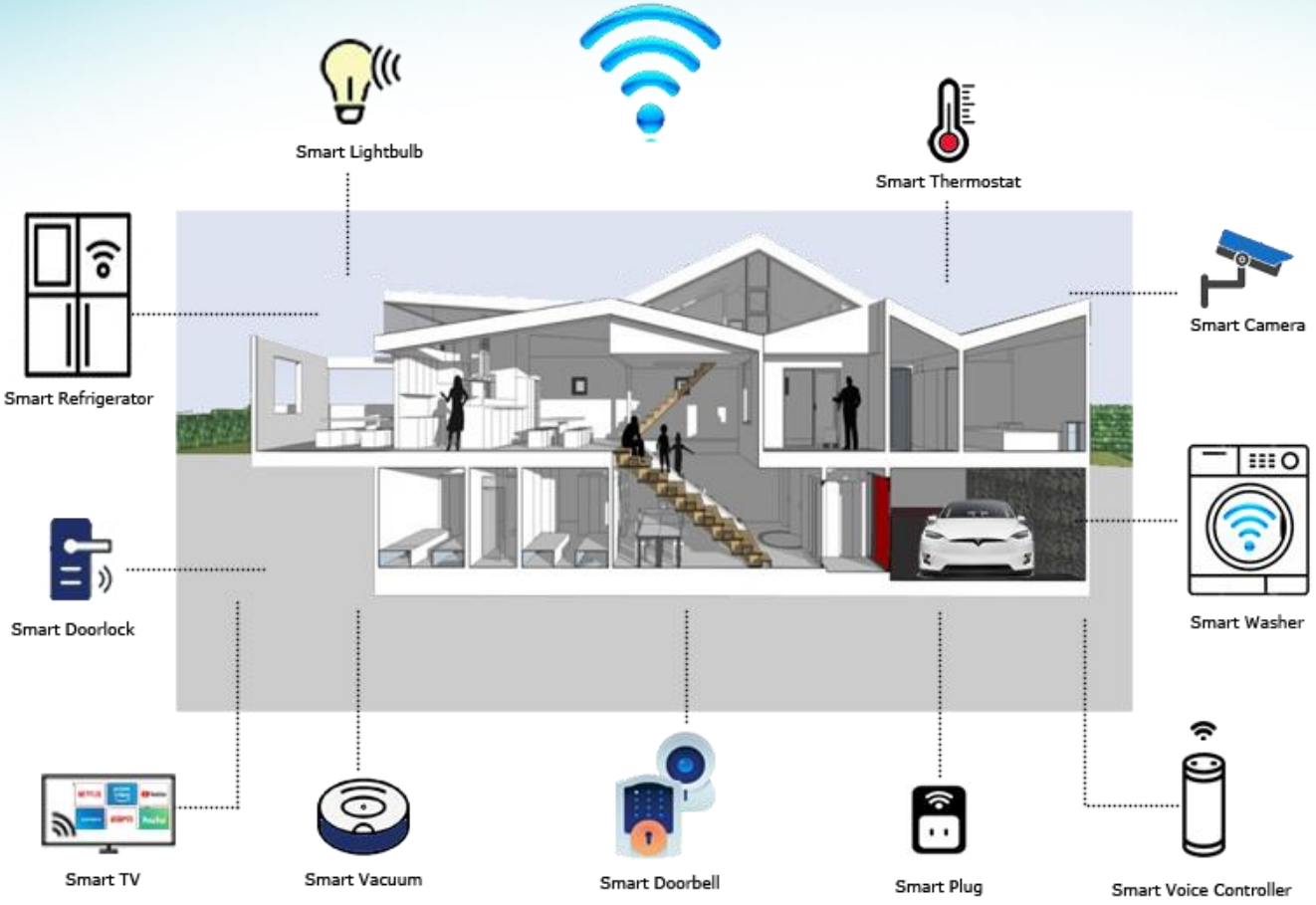
[1]National Institute of Standards and Technology
[2]Leibniz University Hannover

September 24, 2019

Disclaimer

Throughout the presentation, certain commercial companies or products may be identified to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the companies or products identified are necessarily the best available for the purpose.

Smart Home Technologies

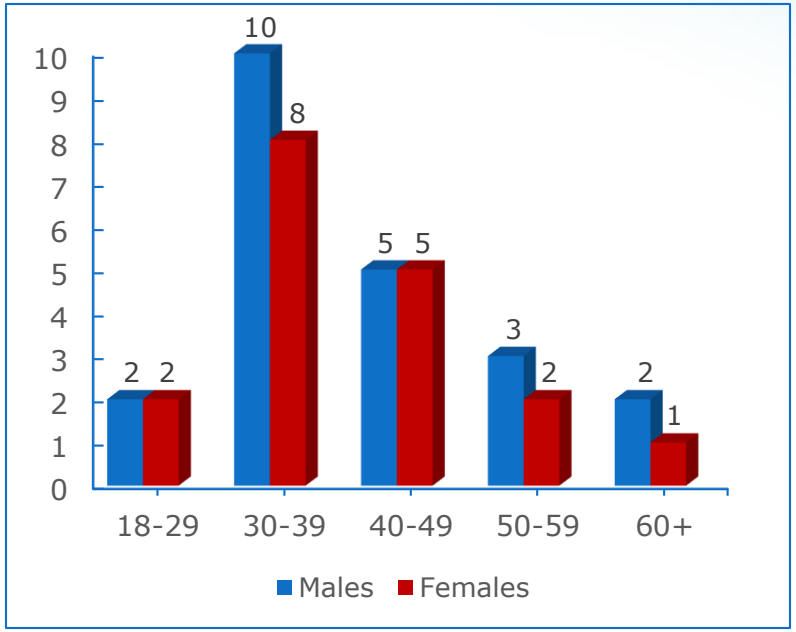


Research Questions

- What are smart home users' privacy and security concerns, if any?
- What privacy/security mitigation actions do users take, if any?
- Who do users believe is responsible for the privacy and security of their smart home devices?
- What is the relationship, if any, between perception of responsibility, concern, and taking mitigative action?

Study Participants

- 40 end users with multiple smart home devices
- Highly educated – 50% with BS/BA, 45% with MS/MA
- 34 live with others
- 32 installers/admins, 8 users



Findings Overview

- Mixed level of concern about privacy and security
- Mitigations to address concerns are often simplistic
- Perceptions of responsibility for smart home device privacy and security do not necessarily correspond to concern level or taking mitigative action

Study Participants' Concerns

Shared Privacy and Security Concerns

Audio and video access

My husband [is] paranoid Google's listening to him about conversations about work. He's worried that if somebody's tapped into one of our Google devices, they're going to hear something they're not supposed to be hearing.

Shared Privacy and Security Concerns

Data Breaches

These big corporations can say they're going to protect your data,…but they really can't protect it…I think if you put your information out there you have to be ready for it to get hacked.

Shared Privacy and Security Concerns

Government Access

Just from a general big brother perspective, I think you're naive to think that we're not being watched and the government is [not] overreaching.

Privacy Concerns

Profiling Household

If somebody has access to this cloud information and they're actually able to associate when you're home and when you're not home based on the sensors and other things you have in your house, they could potentially target you.

Privacy Concerns

Data Collection

You have no idea when it's communicating to the manufacturer or what it's communicating to the manufacturer. And I think the privacy aspects of that are underappreciated.

Security Concerns

Exploitation (hacking) of devices

Each manufacturer is actually just borrowing security APIs instead of creating their own, and the APIs specifically have holes in them. So the same vulnerability is being propagated across vendors.

Security Concerns

Physical Security/Safety

If somebody could hack our system, they could easily open our front door.

Lack of Concern

Not Valuing Information/Privacy Resignation

I feel like you've got people who are pretty talented with computers and can get this stuff… I'm of the mindset, have at it. We don't do anything cool in my house, anyways.

Lack of Concern

Hacking as an Unlikely Possibility

Somebody would have to pluck us at random to really be at risk.

“Willful Ignorance”

I know that it's collecting personal data,… and I know there's the potential of a security leak, but yet, I like having the convenience of having those things.

Study Participants' Mitigations

Mitigations

- Authentication (mostly just setting passwords)
- Limiting audio/video exposure
- Network security (mostly just having secure Wi-Fi)
- Configuring options (but few are available or understood)
- Choosing devices they *think* are secure or that protect privacy

Lack of Mitigations

Lack of Control, Knowledge

I wish we could [limit data collection], but I don't think there'll ever be a way to control it.

I'm not going to educate myself on network security… This stuff is not my forte.

Responsibility

Personal Responsibility

The owners [are responsible]… You're accepting a risk by taking those on in your home.

I think we've realized, sooner or later, your stuff will get breached. It's on you to either put extra restrictions in place or just be okay with the fact that it's going to happen.

Manufacturer Responsibility

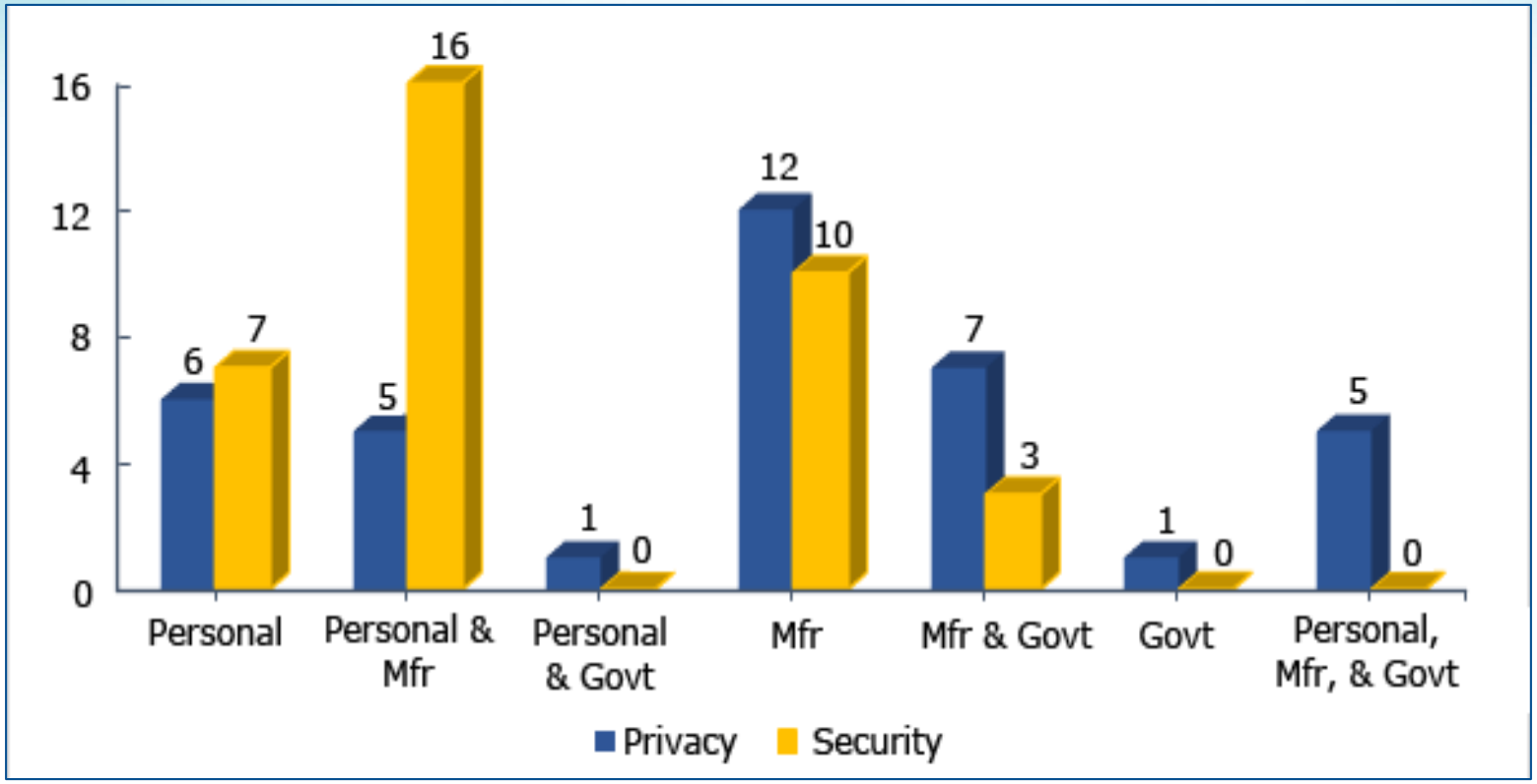
I don’t think they can expect us to be cybersecurity experts. That’s why we bought the product.

If I'm going to buy your product, I think you owe it to me to not abuse that. I did give you money for it.

Government Responsibility

Voluntary consensus on privacy issues is almost impossible to get from the commercial sector… I think they need privacy guidelines at least from the government in order to adhere to them.

Perceptions of Responsibility



Relationships

Correlations

- Moderate correlation between privacy concern and mitigations (but not for security)
- No correlation for personal responsibility and taking mitigative action

Implications

Why the Lack of Relationships?

- Privacy
  - Uncertainty about what is even being collected
  - Participants express the desire to be able to control what happens to their data but don't know what options are available
- Security
  - Incomplete threat model
  - No control over device vulnerabilities
  - Lack the knowledge to implement security mitigations

What can manufacturers do?

- Transparency – what data is being collected, when updates available, what options are available
- Provide privacy and (some) security options, especially at installation
  - Opt-in/out for data collection and usage
  - Secure-by-default as much as possible
  - Better instructions/wizards to help consumers make informed decisions
  - Granular controls for advanced users

What else?

- Best practice guidance
- Consumer ratings for device security and privacy to help in purchase decisions

julie.haney@nist.gov
susanne.furman@nist.gov
https://csrc.nist.gov/usable-cybersecurity