



SP²


SECURITY. PRIVACY. PEOPLE



The Role of Professional Product Reviewers in Evaluating Security and Privacy

Wentao Guo, Jason Walter, Michelle Mazurek

University of Maryland

 wguo5@umd.edu

 @wentaochirps

Choosing safe products: crucial but hard

Internet-connected devices and software expose consumers to harms

But consumers lack time, expertise, and resources to evaluate security and privacy

Eufy's security cameras send data to the cloud without consent, and that's not the worst part

Eufy camera users also learned that their camera streams can be accessed remotely using VLC without encryption or authentication.

Pixel Hunt

Tax Filing Websites Have Been Sending Users' Financial Information to Facebook

The Markup found services including TaxAct, TaxSlayer, and H&R Block

ars TECHNICA

BIZ & IT —

How one rent-a-botnet army of cameras, DVRs caused Internet chaos

Attacks that took down Dyn appear to have been "rented" from multiple botnets.

SEAN GALLAGHER - 10/25/2016, 4:45 PM



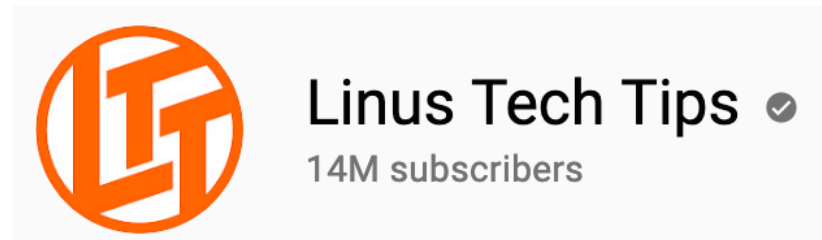
How can professionals help consumers choose safe products?

Who are product reviewers?

Professionals who publish information to help consumers decide what products to use

Product reviewers work at...

- Non-profit organizations
- For-profit media websites
- Independent YouTube channels



Internet-connected devices and software



Smart home
devices



Wearables



Software

Interview research questions

1. What **security and privacy criteria** do product reviewers evaluate?
2. How do **incentives and assumptions** influence their approach?
3. What **techniques and tools** do they use?
4. What are their **challenges and needs**?

Interview format

Virtual semi-structured interviews – 48 minutes

“What are the most important security- and privacy-related criteria you consider when reviewing a product?”

“Has security or privacy ever been the deciding factor in your recommendation?”

Questionnaire – 4 minutes

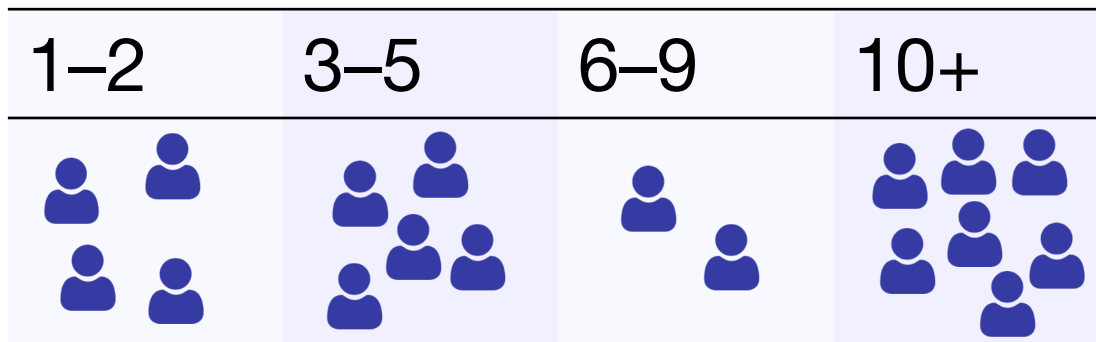
- Security and privacy knowledge
- Demographic and organizational information

Participant information

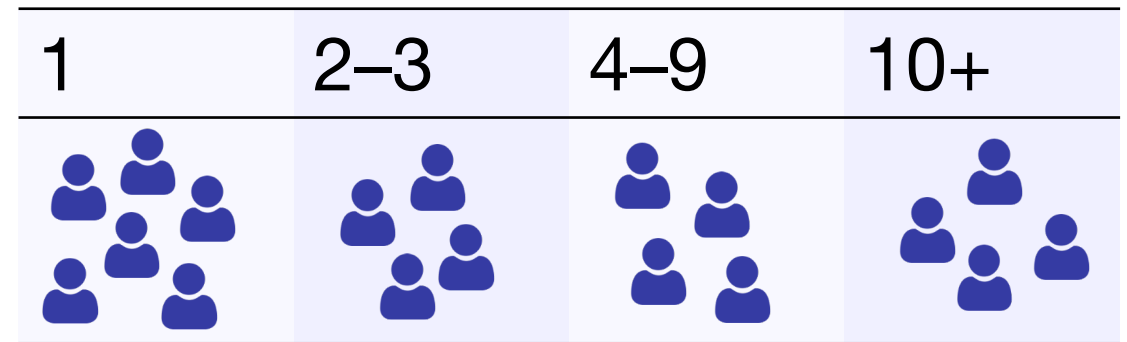
Participants must have published ten reviews

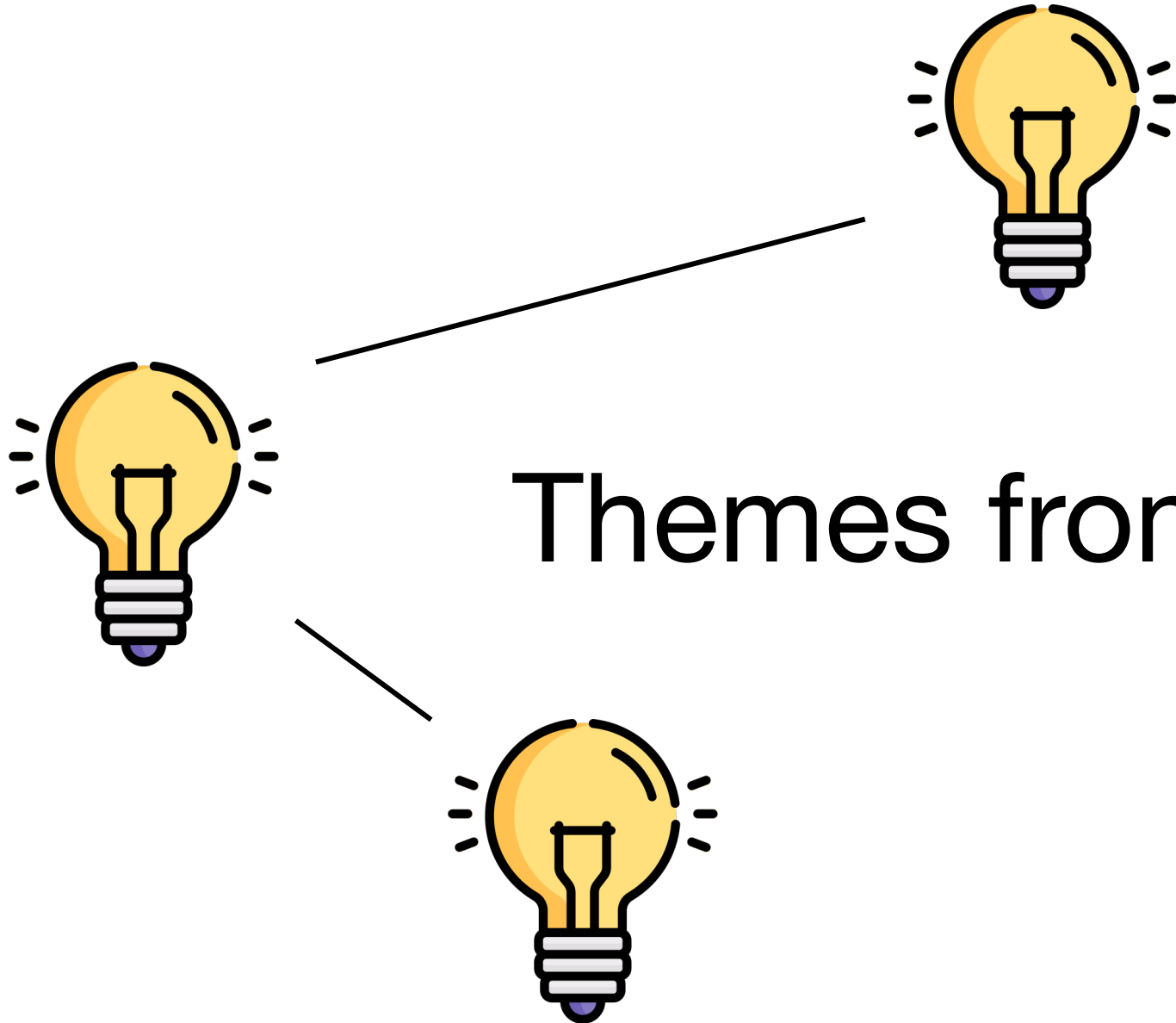
Not primed for security and privacy

years as a product reviewer



product reviewers at organization





Themes from interviews

Some incentives to evaluate S&P

- Reaching different audiences
- Protecting reputation

I would hate to have a glowing review about a product, and then two weeks later, they have a data breach because they didn't encrypt something. **Makes you look bad.**

– P8

Major disincentives to discuss S&P

- Negative reviews are unprofitable
- Audiences perceived as uninterested

If I do a video about [security vulnerabilities], it doesn't get searched for; it doesn't get watched; **nobody cares about it.**

– P11

Disincentives \neq no evaluation of S&P

P6's organization always discusses...

- Two-factor authentication
- Whether data is stored locally
- Whether AI processing is done locally

But that's the type of thing that **we might not write in a review**, because most people shopping for these devices might **not know what that means**. Maybe **people aren't as interested**.

Security and privacy criteria

- Prioritize protection of user data
- Less emphasis on long-term security features

Count	Criterion
11	What data is collected, and how is it shared/used?
7	Reputation of company/product (e.g., breaches)
6	Locale of data storage/processing (local or cloud)
5	Encryption
5	Known vulnerabilities
5	Multi-factor authentication
5	Physical shutters and shut-off switches
4	Data controls
4	Measures to secure data against hacking
4	Transparency about data handling
3	Authentication
3	Data deletion
3	Geographic locale of data storage/processing
3	Justification of data handling
3	Length of data retention
2	Full platform compatibility
2	Security over time
2	Software updates
2	Usable security and privacy features
1	Vulnerability disclosure program
0	Audits

Challenges in evaluating S&P

- Limited time and expertise mean technical tools are often impractical
- Some techniques are feasible but frustrating

I remember my **eyes glossing over** a little bit during **privacy policy reading**.

– P6

Assumptions guide focus

- Free/cheap devices inevitably have privacy trade-offs
- HomeKit devices are trustworthy

With HomeKit, everything is inherently secure.

Stuff runs local; there's no external server calls.

– P3

The role of reviewers in evaluating S&P

Mixed incentives to evaluate S&P, but a unique opportunity to help consumers.

Reviewers cover meaningful criteria, but important areas are left out.

Assumptions are useful but may not be reliable.

How to help reviewers help consumers?

Outreach

- Easy and impactful criteria
- Get out the word on unsafe products

Helpful tools

- Moving beyond evaluative tools
- Help reviewers manage their own S&P

S&P labels

- Facts replace assumptions
- *Bonus*: reviewers interpret labels for consumers