

Security and Privacy Advice 2

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

01/03/2024



THE UNIVERSITY
of EDINBURGH

Overview

- Recap
- Security and privacy advice: why challenging?
- Framework & advice
- Take-home

NEAT

Necessary – Can you change the architecture to eliminate or defer this user decision? Interrupt users only when necessary.

Explained - Does your user experience present all the information the user needs to make this decision? Explain the decision users need to make with information (**See SPRUCE**)

Actionable – Have you determined a set of steps the user will realistically be able to take to make the decision correctly? Give steps in all scenarios (e.g., benign vs malicious)

Tested – Have you checked that your user experience is NEAT for all scenarios, both benign and malicious? Have you tested it on a human who is not a member of your team? Do usability testing.

SPRUCE

Source – State who or what is asking the user to make a decision

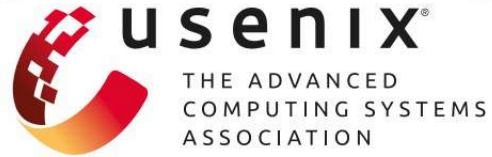
Process – Give the user actionable steps to follow to make a good decision

Risk – Explain what bad thing could happen if they user makes the wrong decision

Unique – Knowledge the user has – Tell the user what information they bring to the decision regarding the context

Choices – List available options and clearly recommend one

Evidence – Highlight information the user should factor in or exclude in making a decision



A Comprehensive Quality Evaluation of Security and Privacy Advice on the Web

Elissa M. Redmiles, Noel Warford, Amritha Jayanti, and Aravind Koneru, *University of Maryland*; Sean Kross, *University of California, San Diego*; Miraida Morales, *Rutgers University*; Rock Stevens and Michelle L. Mazurek, *University of Maryland*

<https://www.usenix.org/conference/usenixsecurity20/presentation/redmiles>

**This paper is included in the Proceedings of the
29th USENIX Security Symposium.**

August 12–14, 2020

978-1-939133-17-5

Contribution

- Taxonomy of security and privacy advice
- Quality evaluation of security and privacy advice

Contribution and method

- Taxonomy of security and privacy advice
 - Online scraping of 2780 pieces of advice; human annotation and analysis
- Quality evaluation of security and privacy advice
 - Survey and evaluation with 1586 User and 41 experts

Identifying advice

- How do people get advice online -> crowdsourcing search queries for security and privacy advice
- Where experts find and recommend advice? -> asking security experts
- Result: 1264 out of 1896 documents after cleaning

Topics of advice

Table 1: The 12 categories of security advice we identified.

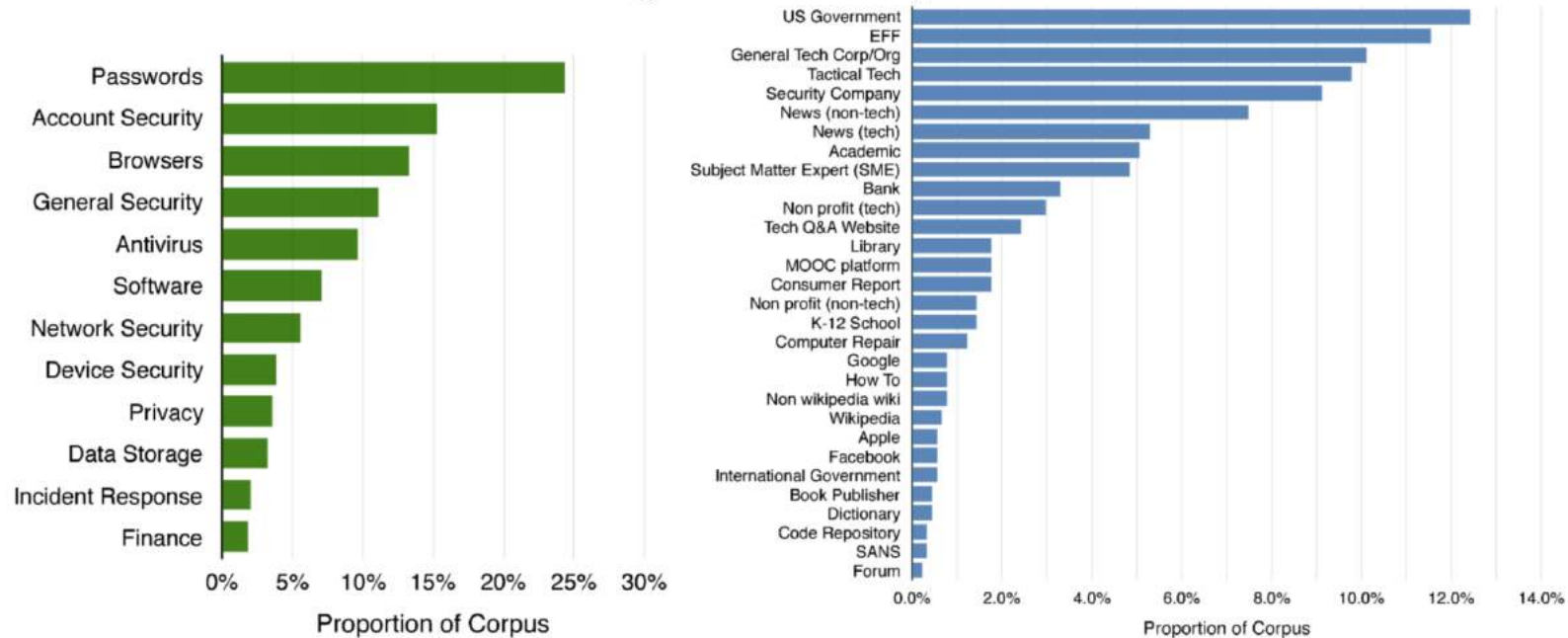


Figure 1: Distribution of topics (left) and domain categories (right) across the corpus.

- Qualitative coding and analysis

Evaluating advice: metrics

- Perceived actionability
 - **Confidence:** how confident users can implement it
 - Time consumption: how time consuming people think it would take to implement
 - **Disruption:** how disruptive people think when implementing it
 - **Difficulty:** how difficult people think it is to implement
- Scale: 4-point Likert from “Not at All” to “Very”
- Framework: building on Protection Motivation Theory and Human in the Loop model

Evaluating advice: metrics

- **Perceived efficacy:** whether the experts believe that a typical user would experience an improvement or not
- **Comprehensibility:** multiple measures for evaluating text comprehension, e.g., “How easy is this document to read?”

Results

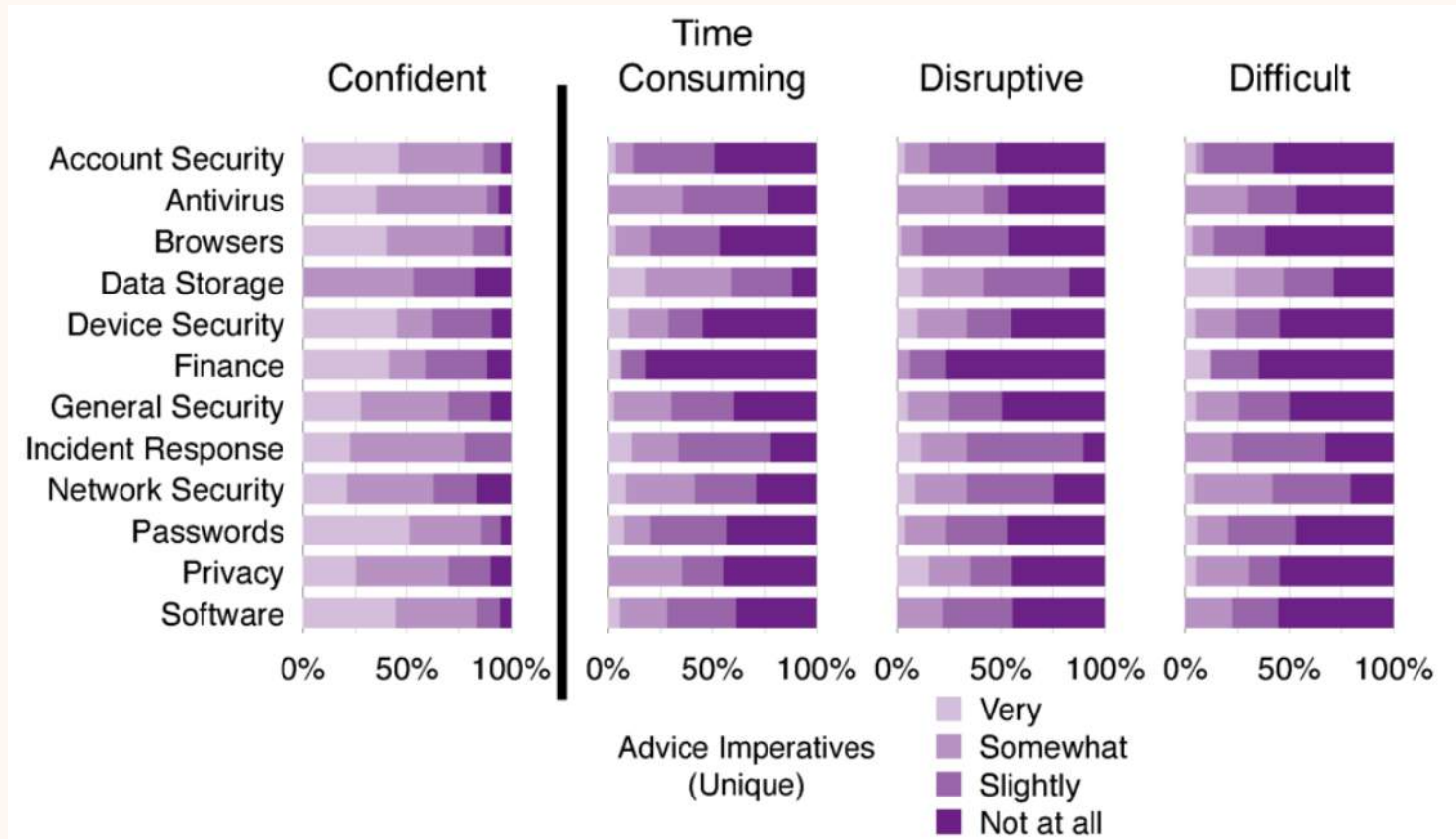


Figure 3: Advice actionability by topic across 374 unique advice imperatives.

Results

Advice	Not Confident	Very Time Consuming	Very Disruptive	Very Difficult	Efficacy	Risk Reduced
Apply the highest level of security that's practical	X	X		X	All Accurate	50%
Be wary of emails from trusted institutions	X				All Accurate	25%
Beware of free VPN programs		X		X	All Accurate	30%
Change your MAC address	X				Majority Accurate	32.5%
Change your username regularly		X	X	X	Majority Useless	NA
Consider opening a credit card for online use only	X				All Useless	NA
Cover your camera			X		Majority Accurate	30%
Create a network demilitarization zone (DMZ)	X				Majority Accurate	27.5%
Create keyboard patterns to help remember passwords		X	X	X	Majority Useless	NA
Create separate networks for devices	X	X	X	X	Majority Accurate	40%
Disable automatic download of email attachments		X			All Accurate	40%
Disable Autorun to prevent malicious code from running	X	X			All Accurate	50%
Disconnect from the Internet	X				All Accurate	25%
Do online banking on a separate computer				X	All Accurate	32.5%
Encourage others to use Tor			X	X	Majority Accurate	25%
Encrypt cloud data	X			X	Majority Accurate	45%
Encrypt your hard drive	X		X	X	All Accurate	5%
Isolate IoT devices on their own network	X	X	X	X	Majority Accurate	20%
Keep sensitive information on removable storage media		X			Majority Accurate	22.5%
Leave unsafe websites		X	X		Majority Accurate	22.5%
Limit personal info being collected about you online	X				Majority Accurate	15%
Lock your SIM card in your smartphone	X	X	X	X	No Consensus	NA
Not blindly trust HTTPS	X				Majority Accurate	20%
Not change passwords unless they become compromised	X				All Harmful	-30%
Not identify yourself to websites	X				Majority Accurate	30%
Not let computers or browsers remember passwords	X				Majority Accurate	45%
Not overwrite SSDs	X	X	X	X	All Accurate	45%
Not send executable programs with macros			X	X	All Accurate	20%
Not store data if you don't need to				X	All Accurate	40%

Results

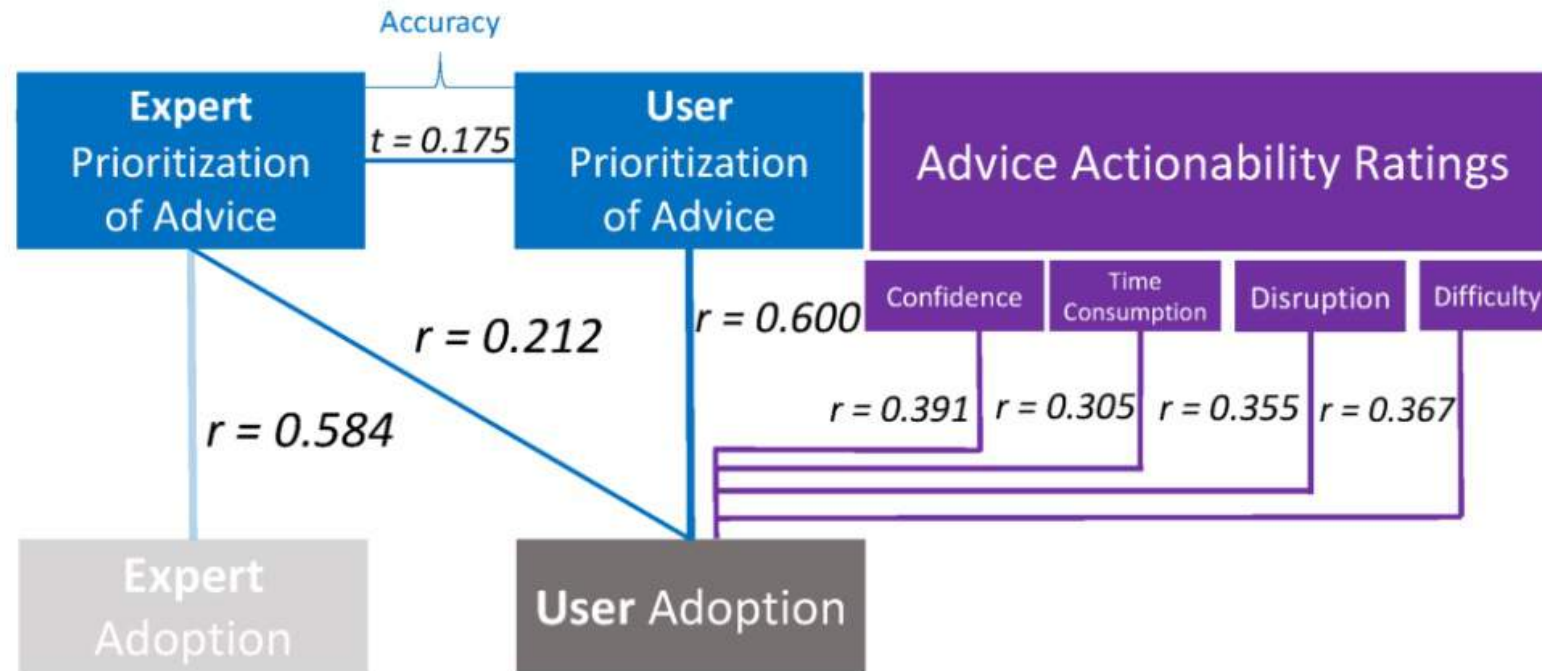


Figure 6: Correlation between security advice adoption, actionability, and priority rankings.

Previously we talked about phishing and we talked about advice.

Start thinking about what advice we give people, how we give it, and how to deliver it effectively.



**Caution
Mind the step**



WHO'S GIVING

**YOUR
BAG**



THE EYE

DON'T LET A THIEF GET AWAY WITH IT!



**METROPOLITAN
POLICE**

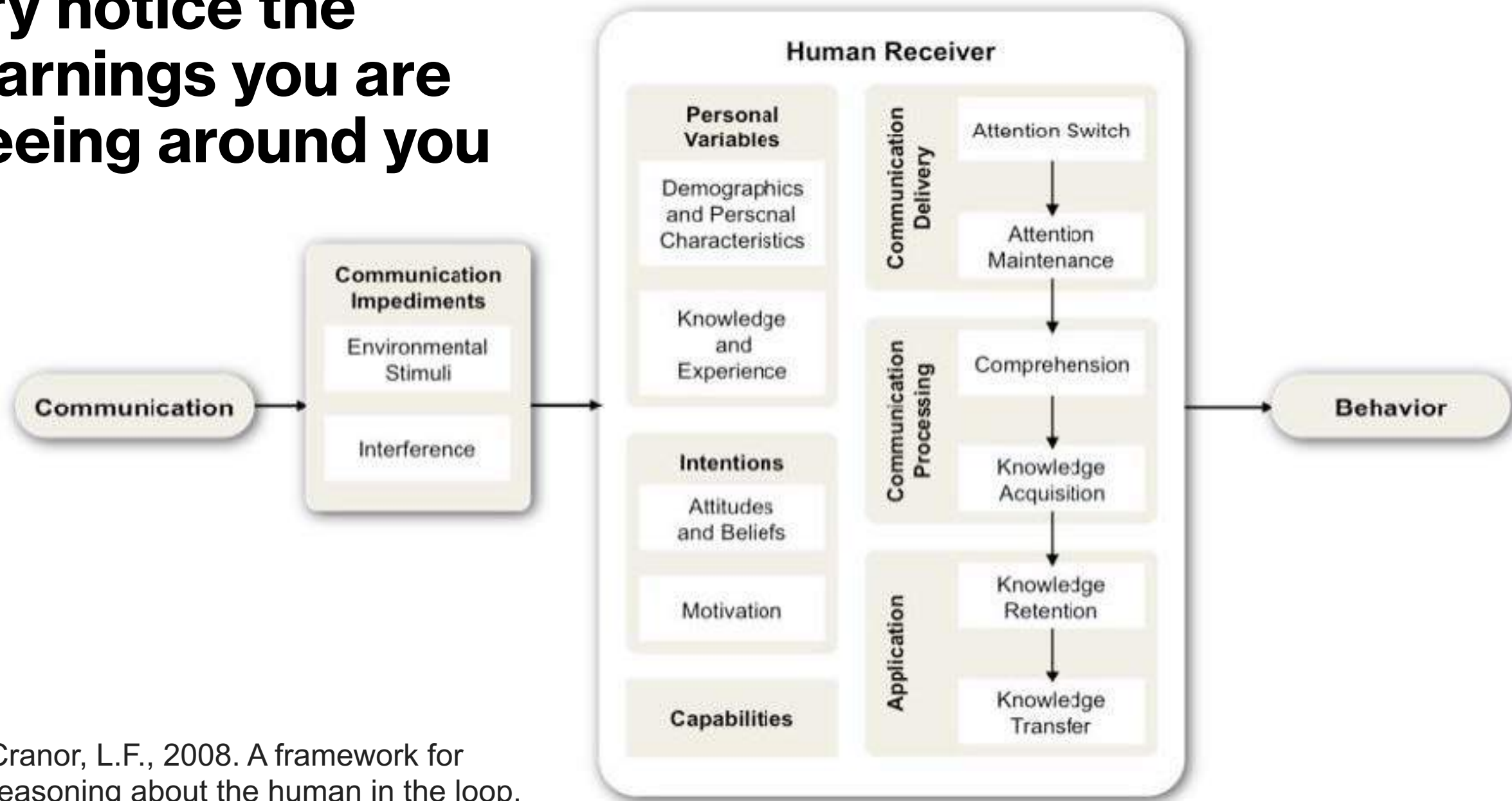
Working together for a safer London

In the next few slides I want to make three points:

1. People give other people piles of advice all the time
2. The advice being given out can tell you a lot about what people think is important or what is broken about a situation
3. Warnings are a type of advice



Try notice the warnings you are seeing around you



Cranor, L.F., 2008. A framework for reasoning about the human in the loop.

Human in the Loop: Communication Impediments

- **Environmental stimuli** (either related or unrelated) may divert users' attention away
- **Interference** prevents communication from being received as intended (can be malicious)

**If you want
to find
usability
problems,
look for
signs.**

DISHWASHER
IS
ON !!!

Human in the Loop: Human Receiver

- **Communication delivery:** should pay attention long enough to process it
- **Communication processing:** comprehend and acquire knowledge
- **Application:** retent the knowledge and knows when it's applicable and to apply it

First reaction: Pull

Sign says: Push



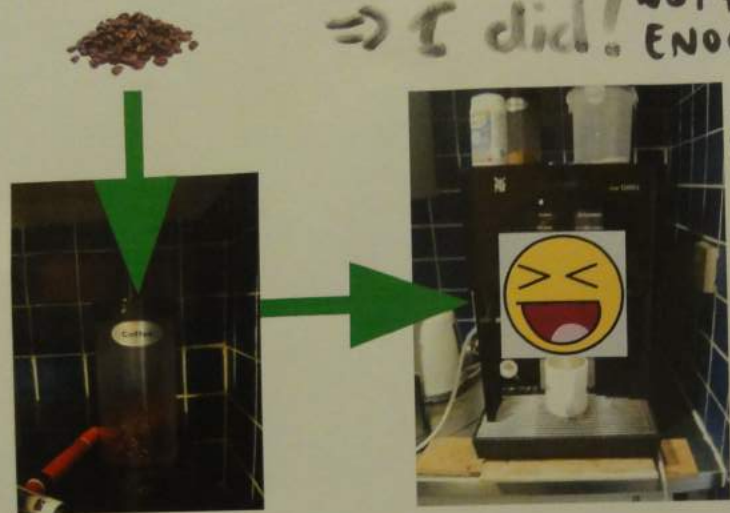
Human in the Loop: Human Receiver

- **Personal variables**, e.g., demographics, personal characteristics, knowledge , etc. – ability to comprehend and apply communications
- **Intentions** like attitudes, impacting the decision of whether to pay attention on a communication
- **Capabilities** to take proper actions

Maybe something is not obvious

Please do not make the coffee machine sad.

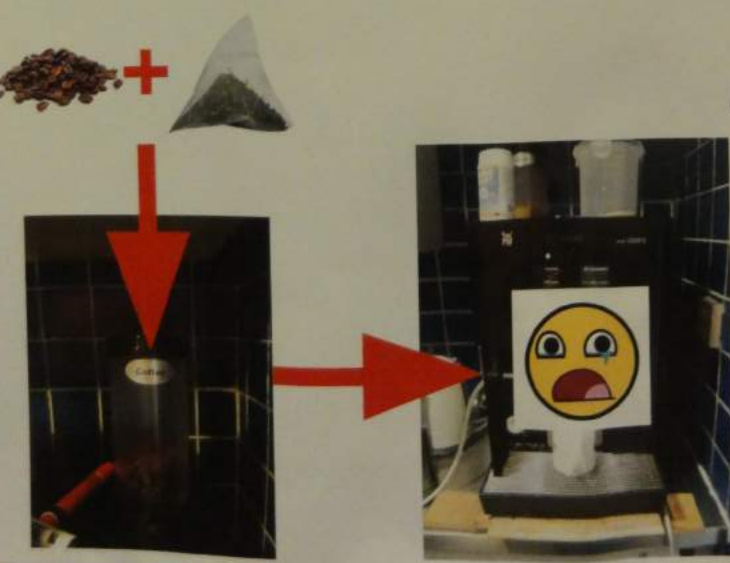
⇒ vote remain
⇒ I did! NOT HARD ENOUGH!



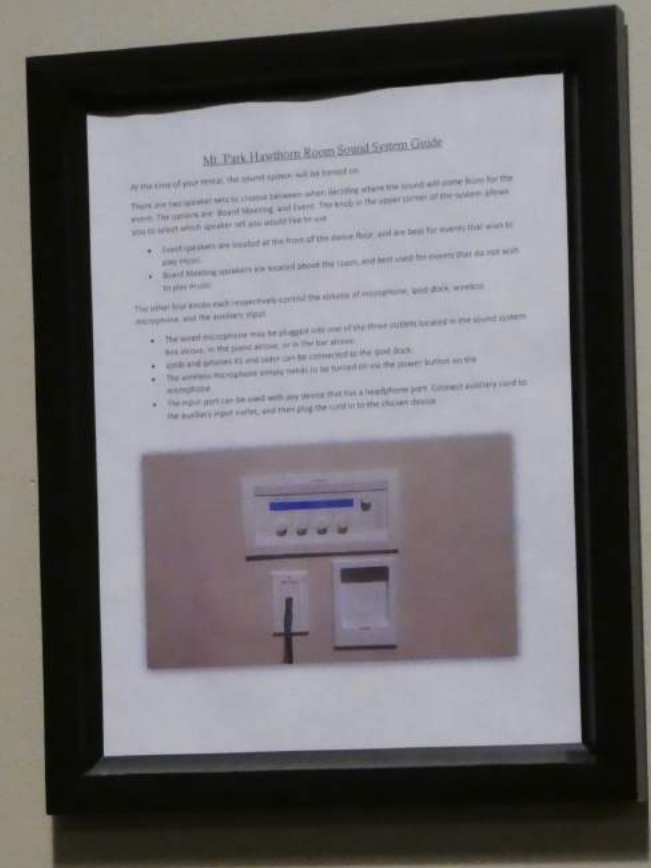
I think the pencil! isn't that mad funny?

NOPE. IT'S AN I SECRETLY WANTED BETTER PASTURE!

+



Maybe the tool is too
confusing to use
without explanation



Maybe people have an attitude that certain warnings don't apply to them or are not actually relevant



Signs highlight common problems people in a space are experiencing.



Intention – **tradeoff** happens here, but not always in a very rational way

“It’s up to the Consumer to be Smart”:
Understanding the Security and Privacy Attitudes of Smart Home Users on Reddit

Jingjie Li¹, Kaiwen Sun², Brittany Skye Huff¹, Anna Marie Bierley¹,
Younghyun Kim¹, Florian Schaub², and Kassem Fawaz¹

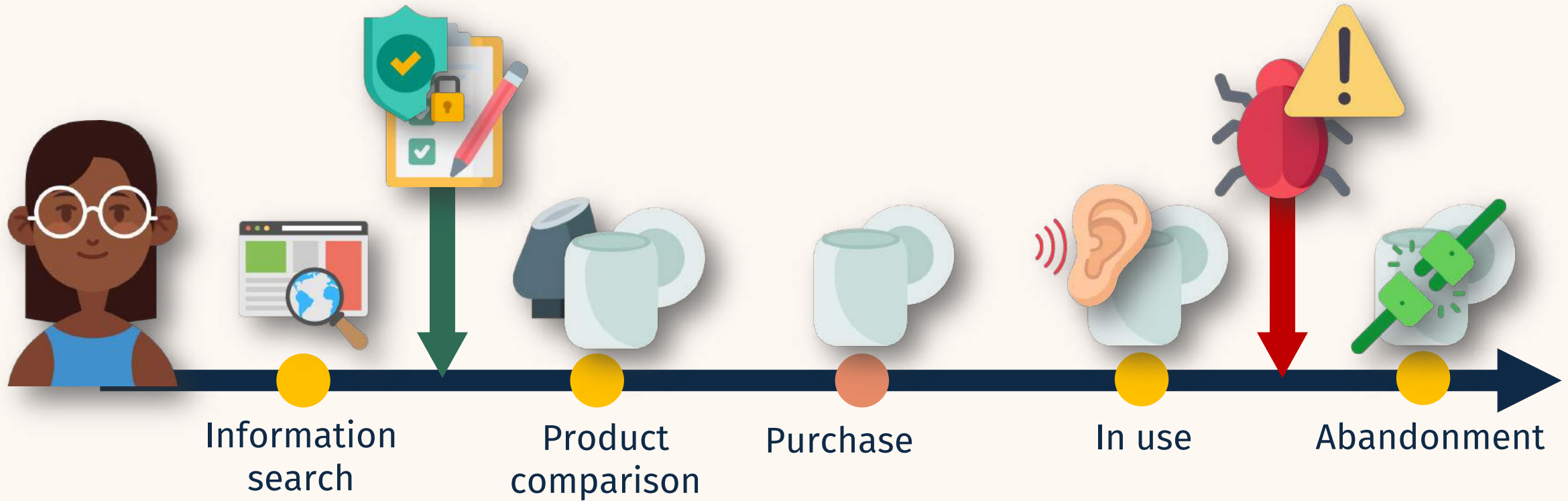
¹University of Wisconsin–Madison, {*jingjie.li, bshuff, bierley, younghyun.kim, kfawaz*}@wisc.edu

²University of Michigan, {*kwsun, fschaub*}@umich.edu

Abstract—Smart home technologies offer many benefits to users. Yet, they also carry complex security and privacy implications that users often struggle to assess and account for during adoption. To better understand users’ considerations and attitudes regarding smart home security and privacy, in particular how users develop them progressively, we conducted a qualitative content analysis of 4,957 Reddit comments in 180 security- and privacy-related discussion threads from /r/homeautomation, a major Reddit smart home forum. Our analysis reveals that users’ security and privacy attitudes, manifested in the levels of concern and degree to which they incorporate protective strategies, are shaped by multi-dimensional considerations. Users’ attitudes evolve according to changing contextual factors, such as adoption phases, and how they become aware of these factors. Further, we describe how online discourse about security and privacy risks and protections contributes to individual and collective attitude development. Based on our findings, we provide recommendations to improve smart home designs, support users’ attitude development, facilitate information exchange, and guide future research regarding smart home security and privacy.

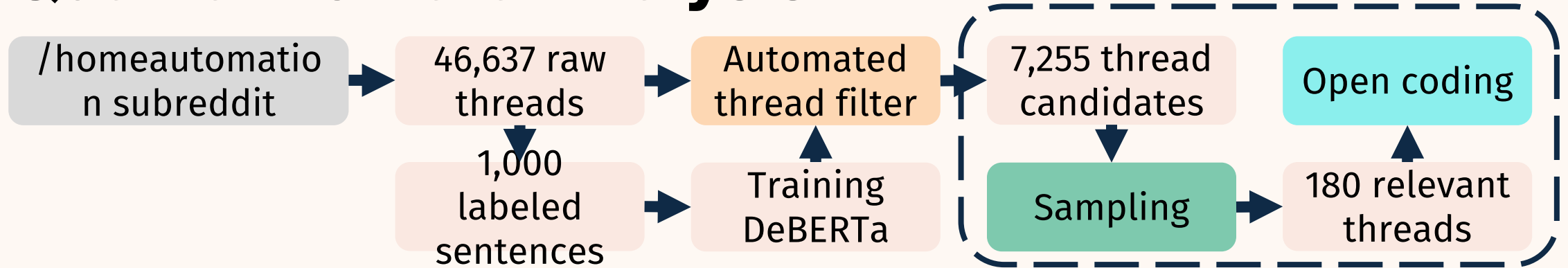
varying S&P attitudes and concerns [25], [44]. While existing studies on users’ S&P perceptions of smart home have primarily focused on singular timepoints in the adoption journey and are often conducted in controlled contexts using methods such as interviews and surveys [28], [33], [85], [88]; these studies may miss the rich dynamics when users develop their S&P considerations and attitudes over time. Meanwhile, little research has investigated and holistically understood how users organically develop varying S&P considerations and attitudes throughout their adoption journey.

Recently, researchers have started leveraging online communities to study users’ attitudes, including those on S&P-related topics, in vivo [48], [73], [74]. Online communities provide venues for many smart home users to seek product information and exchange S&P ideas. Members of such online communities collectively drive the topics and discussions based on their interests. As such, we choose a smart home-related online discussion forum to investigate *how smart home users develop S&P considerations, which shape their S&P attitudes during the adoption of smart home products*. We investigate our main research objective through three research questions:



How do users **develop** security and privacy attitudes organically?

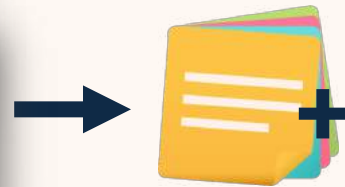
Qualitative Data Analysis



- Our team with broad knowledge (S&P, computer science and engineering, information science, psychology, and legal studies) performed **qualitative coding** and **thematic analysis**
- Inter-rater reliability = 0.74 (substantial)



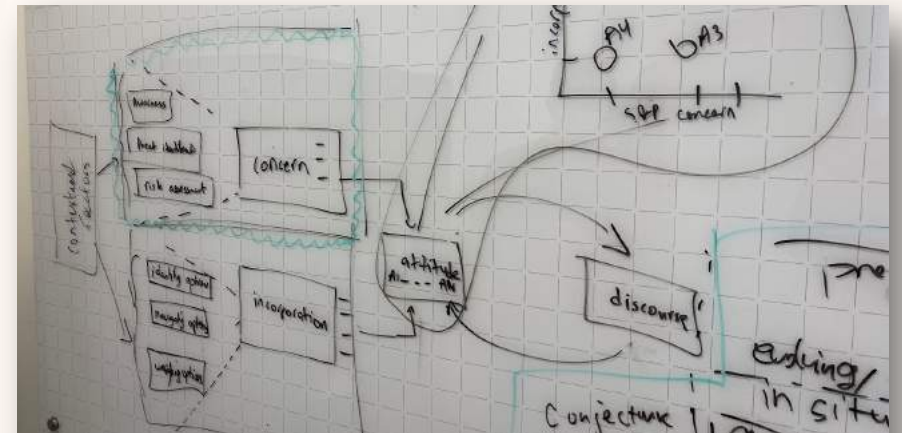
**Reddit
comments**



Themes



Codes



**Our framework under
construction (2021)**

Findings: Contextual Factors Related to S&P



Users' understanding and requirements differ and are constraint by diverse contextual factors

Findings: S&P Attitudes

But I don't really care about people eavesdropping me.



Dismissiveness
(44/255 users)

Incorporating protective strategies



I'd definitely like to hear what other people have to say.

Exploration (111/255 users)

People are walking around with a cellphone 24/7!

Resignation (13/255 users)

I value convenience over complete privacy

Positive pragmatism (71/255 users)

Personally I would and have layered the devices in 3 layers for security...

Devotion (65/255 users)

Low

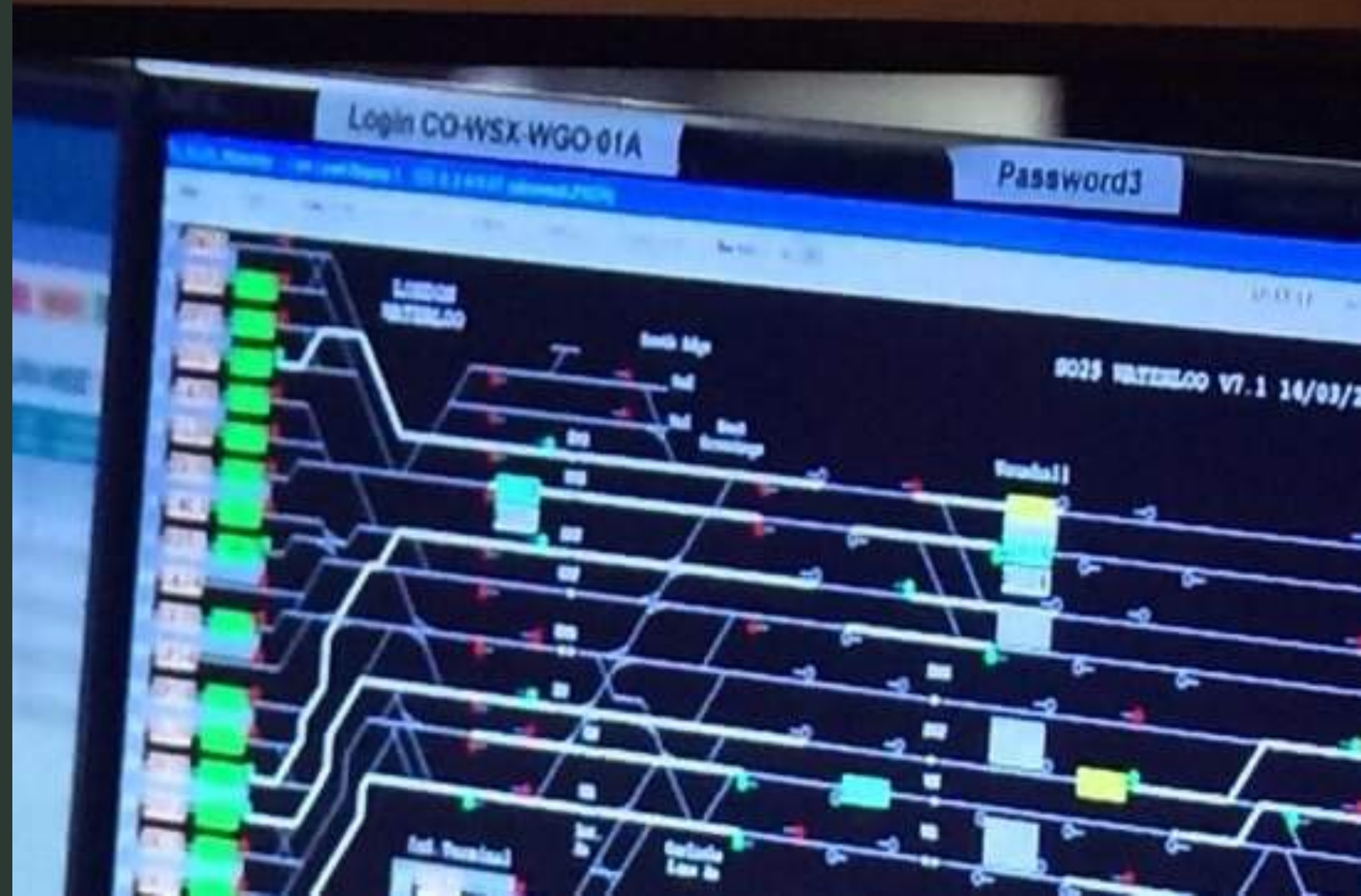


High

Concern

Users' attitudes are contextual and evolve, despite preconception

Just wandering around with your eyes open will tell you a lot about the culture, norms, and problems of a space.



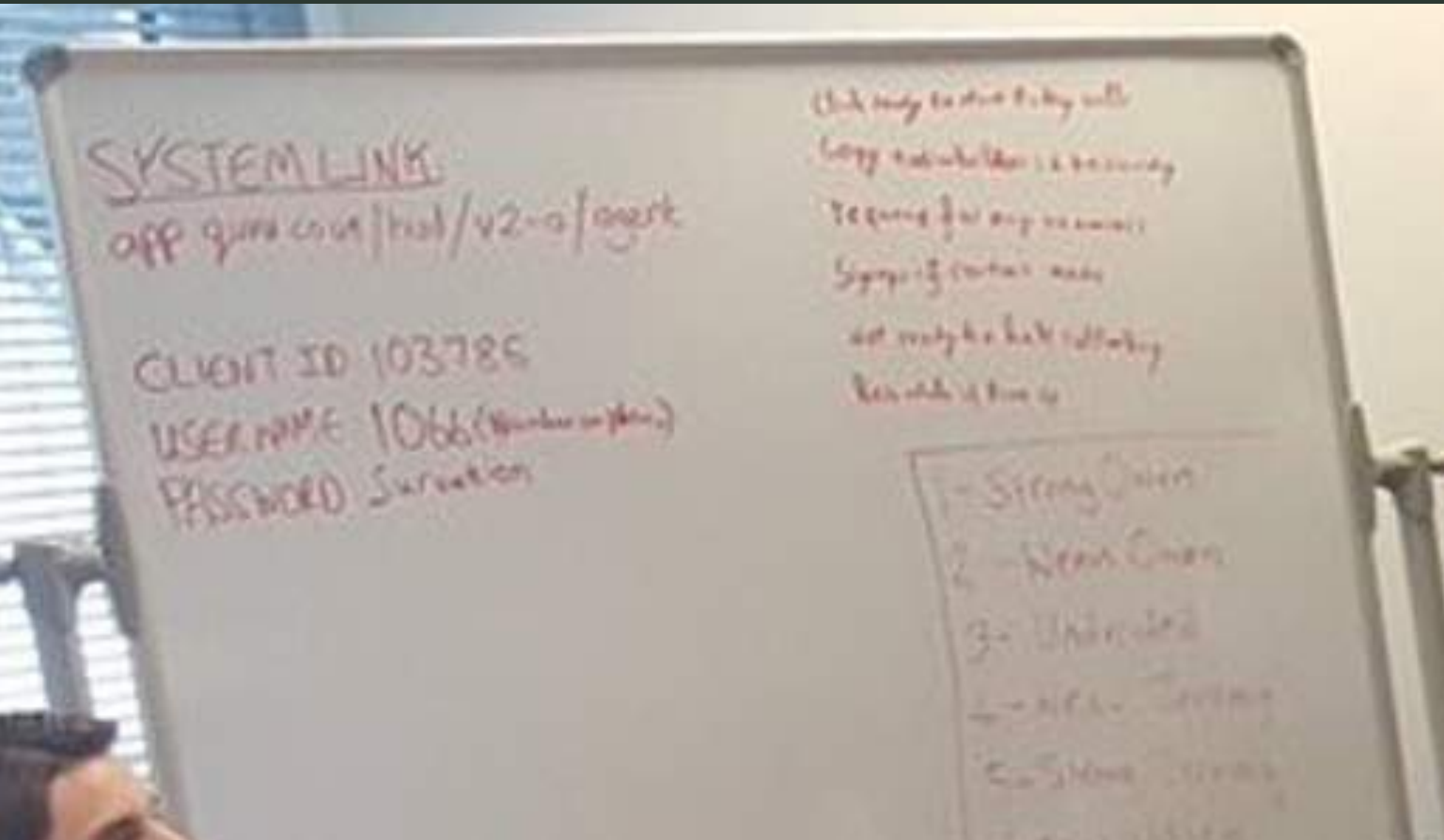


Photo shared by Owen Smith's own social media team



Notice the passwords behind him?



**Why do we
involve
users in
decisions?**



Because they have **contextual** knowledge the computer doesn't have.



Think: **when** do we need to involve users in decision?

“Easy” to
dismiss by
hitting X ...

Except that
hitting X
means “I
accept”

Review our cookie policy

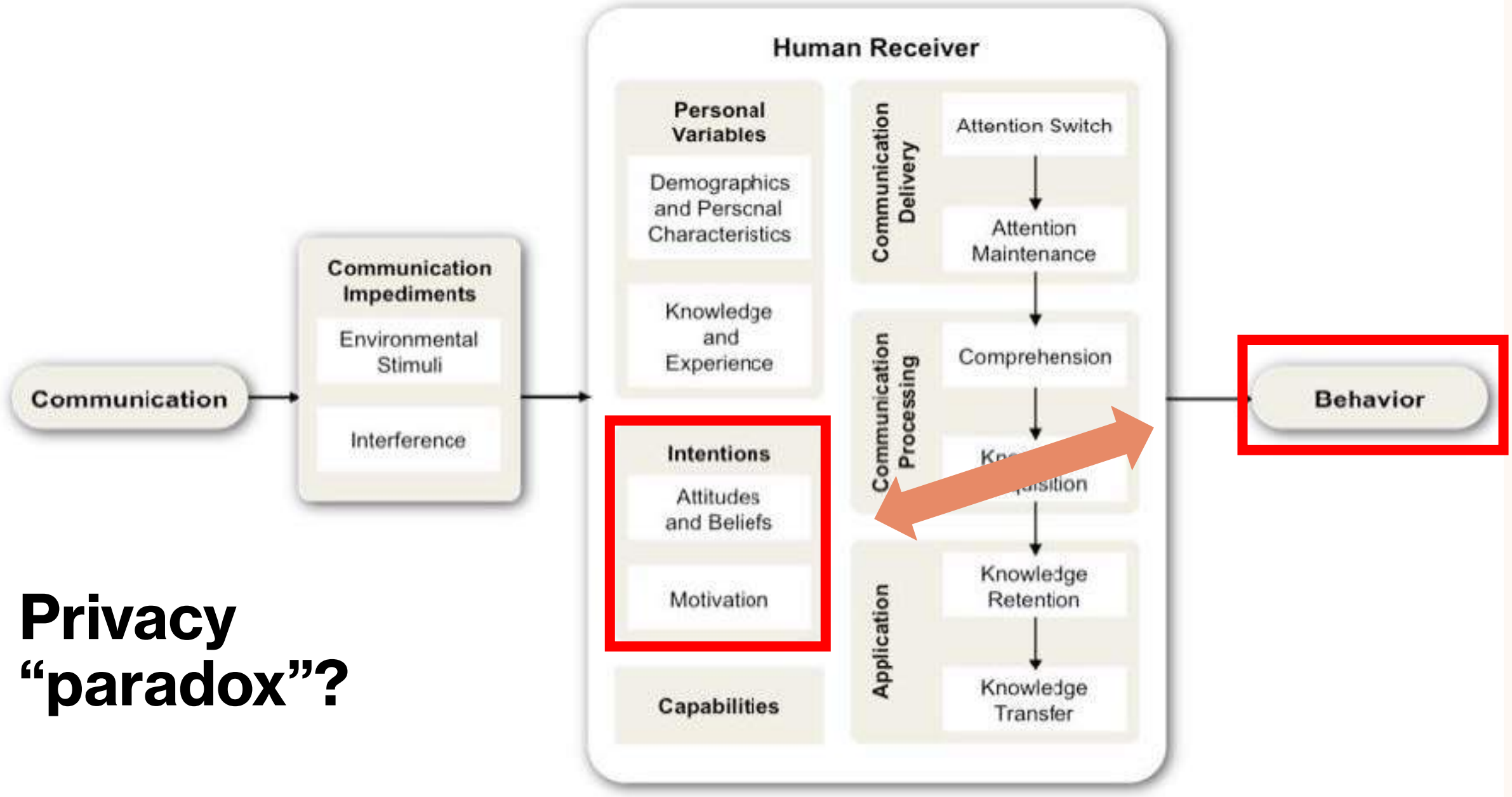


What do we use cookies for?

We use cookies and similar technologies to **recognize your repeat visits and preferences**, as well as to **measure the effectiveness of campaigns and analyze traffic**. To learn more about cookies, including how to disable them, view our [Cookie Policy](#).

By clicking "I Accept" or "X" on this banner, or using our site, you consent to the use of cookies unless you have disabled them.

I ACCEPT



**Privacy
“paradox”?**

My Point:

Good security decisions are contextual and require balancing **risks with benefits**. Good advice/warnings help users to do that.

The elements in the framework interplay with each other

All sorts of things need to be communicated to users

- **Questions** – “did you log in from this location?”
- **Warnings** – “the website has malicious software”
- **UI passive indicators** – the lock icon on the browser
- **UI active indicators** – “You need to generate a key”
- **Task-relevant information** – “Passwords should be 8 characters long and must have a capital letter.”
- **Educational** – “10 security behaviors you should do to protect yourself online”
- **Awareness** – “This phishing email has been going around, don’t fall for it.”

The goal of today's lecture is teach you to create useful communications with users on security topics.

NEAT

Necessary – Can you change the architecture to eliminate or defer this user decision? Interrupt users only when necessary.

Explained - Does your user experience present all the information the user needs to make this decision? Explain the decision users need to make with information (**See SPRUCE**)

Actionable – Have you determined a set of steps the user will realistically be able to take to make the decision correctly? Give steps in all scenarios (e.g., benign vs malicious)

Tested – Have you checked that your user experience is NEAT for all scenarios, both benign and malicious? Have you tested it on a human who is not a member of your team? Do usability testing.

Necessary

Explained

Actionable

Tested



UNIVERSITY

ORDINANCES REQUIRE
BICYCLES & MOPEDS BE
PROPERLY REGISTERED,
LOCKED & PLACED ONLY IN
BICYCLE RACKS TO AVOID
IMPOUNDMENT
MOTORCYCLE PARKING
PROHIBITED

Necessary
Explained
Actionable
Tested

The image shows a screenshot of an American Express account page. At the top, there is a navigation bar with a 'Menu' button, the 'AMERICAN EXPRESS' logo, and links for 'Help' and 'Log Out'. Below the navigation, the user's name 'KAMI' and membership details 'Member Since 2018' and 'The Preferred Rewards Gold Card® (-91000)' are displayed. A gold American Express card is shown on the left. A modal window is open in the center, titled 'British Airways Data Breach'. The modal contains the following text: 'We are proactively monitoring the updated British Airways data breach', 'We will contact you if we suspect fraudulent activity on your Account. There is no need to take any action at this time. You will not be liable for any fraudulent charges and you can continue to use your Card. You can sign up for free fraud and account activity notifications via SMS and email.', and a blue button labeled 'Sign up to Alerts'. At the bottom of the page, there are three buttons: 'Balance details', 'Make a payment', and 'Use your points'.

Menu

AMERICAN EXPRESS

Help Log Out

Good evening, KAMI Member Since 2018
The Preferred Rewards Gold Card® (-91000)

AMERICAN EXPRESS
3759 874573 21001
C. F. FROST

Accounts (1)

your

ance

Visit the
everyday

No
Check Spending Power

Balance details

Make a payment

Use your points

British Airways Data Breach

We are proactively monitoring the updated British Airways data breach

We will contact you if we suspect fraudulent activity on your Account. There is no need to take any action at this time. You will not be liable for any fraudulent charges and you can continue to use your Card. You can sign up for free fraud and account activity notifications via SMS and email.

Sign up to Alerts

Questions

Take-home

- **(Blog)** Gabriele, S. and Chiasson, S., 2020, April. [Understanding fitness tracker users' security and privacy knowledge, attitudes and behaviours](#). In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (pp. 1-12).
- **(Blog)** Guardian - [The privacy paradox: why do people keep using tech firms that abuse their data?](#)