

Introduction to Usable Security and Privacy

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

13/01/2026



THE UNIVERSITY
of EDINBURGH

Overview

- Course overview
- What is usable security and privacy?
- Discussion: Why USEC is challenging?
- Take-home

Sign in

someone@example.com

Password

Sign in

Important
Enter your login name in the format uun@ed.ac.uk,
e.g jbloggs@ed.ac.uk or s1234567@ed.ac.uk

This is the University of Edinburgh's official page for
Your University Login. By using this service you agree
to abide by the University of Edinburgh [Computing
Acceptable Use Policy](#).

[Home](#) [Help](#)

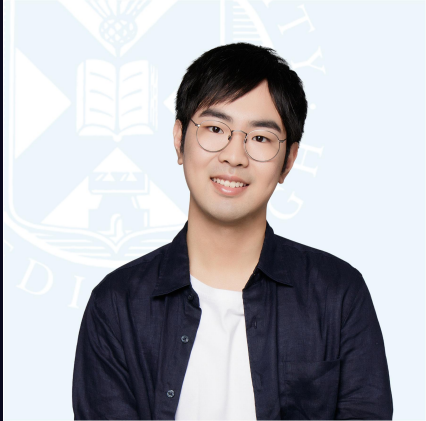
What does “Usable Security and Privacy” mean to you?



wooclap.com

<https://app.wooclap.com/JGUOSU?from=instruction-slide>

JGUOSU



Jingjie Li

jingjie.li@ed.ac.uk

www.jingjieli.me

>Lecturer @ University of Edinburgh, 2023 – now

>PhD @ University of Wisconsin—Madison, 2023

Research focus: Human-centred systems (AI, IoT, AR/VR, etc.), online safety, security and privacy

Developing trustworthy technology for social good

Users & Society

Application

Computing
SW/HW

Pushing the boundaries of human-centred systems



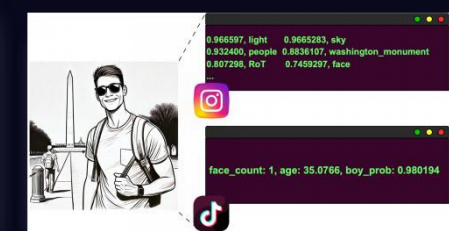
AIoT



Virtual reality



Biometrics



Online community



Course overview

This course is gracefully built on Dr. Kami Vaniea's and Dr. Adam Jenkins's efforts from 2018 to 2023

You will learn about...

- Critical thinking
- Core study design skills (Does X work in Y situation?)
- Reading research papers and extracting meaning
- Applying what you learned into new situations
- Current known best practices in Usable Security and Privacy
-Just how terrifying the real world is

Intersection with HCI, Security, and Privacy

- Human computer interaction
 - Specific examples of how studies are done
 - Critical evaluation of study design and impact on results
 - Real data and analysis
- Computer security and privacy
 - Human–factors issues in security
 - Applied aspects — theory meets practice
 - Ethics and regulations

(Rough) Lecture structure

- 5 min for warm-up, recap, announcement...
- 30 min for course topic (interactive)
- 15 min for further discussion + Q&A
- Course materials on Open Course

Tutorials

- Goal:
 - Practices for **designing, conducting, and analyzing** user studies
 - Experience with real-world examples
- Time: Week 3 – Week 5



Case study coursework (20%)

- Goal
 - Hands-on analysis and design for usable security and privacy techniques
 - Getting ready for research in USEC
- Release: 27 January
- Submission: 23 March

Final exam (80%)

- Goal
 - Assessing the learning outcomes through the semester
 - Applying skills learnt to solve new problems
- Logistics to be finalized

Engagement

- Class participation
- Piazza: open discussion
- Email (please add [USEC] in the subject line)
 - TA: Jiuming Jiang (jiuming.jiang@ed.ac.uk)
 - Jingjie: jingjie.li@ed.ac.uk (feel free to cc me in emails to TA)
- Office hour
 - Tuesday 11am — 11:45am (tentative) @ IF2.04B / online (by appointment via Calendly <https://calendly.com/jingjieli95/30min>)

Questions?

What is Usable Security and Privacy?

Defining security

- **Confidentiality**

- Ensures that computer-related assets are *accessed only* by authorized parties.

- **Integrity**

- Assets can be *modified only by* authorized parties or only in authorized ways.

- **Availability**

- Assets are *accessible* to authorized parties at appropriate times.



<https://www.cambridgeindependent.co.uk/news/giving-gets-easier-for-cambridge-homeless-charity-9051139/>

Is this donation terminal secure?

Defining security

- **Confidentiality**

- Device might collect data from card like name and card number.
- Possibly auto-sign people up for marketing. (Unlikely with GDPR)

- **Integrity**

- How will you be sure that amount charged really is £3?

- **Availability**

- Minimal availability issues, user never loses control of the card.
- Minor risk of fraud alert.



<https://www.cambridgeindependent.co.uk/news/giving-gets-easier-for-cambridge-homeless-charity-9051139/>

Defining security — CIA definition

C onfidentiality	No improper information gathering
I ntegrity	Data has not been (maliciously) altered
A vailability	Data/services can be accessed as desired
A ccountability	Actions are traceable to those responsible
A uthentication	User or data origin accurately identifiable

Defining privacy

- There are many definitions
 - The right to be let alone
 - The right to control one's own data
- Many common security goals overlap with privacy ones
 - Confidentiality
 - Access control of information
 - Protection from unwanted intrusions



Defining privacy

A TAXONOMY OF PRIVACY

INFORMATION PROCESSING



AGGREGATION

Combining various pieces of personal information

A credit bureau combining an individual's payment history from multiple creditors.



SECONDARY USE

Using personal information for a purpose other than the purpose for which it was collected

The U.S. Government using census data collected for the purpose of apportioning Congressional districts to identify and intern those of Japanese descent in WWII.



EXCLUSION

Failing to let an individual know about the information that others have about them and participate in its handling or use

A company using customer call history, without the customer's knowledge, to shift their order in a queue (i.e. "Your call will be answered in the order [NOT] received")



INSECURITY

Failing to protect information

An ecommerce website allowing others to view an individual's purchase history by changing the URL (e.g. enterprivacy.com?id=123)



IDENTIFICATION

Linking of information to an individual. [Sometimes called 'singling out']

A researcher linking medical files to the Governor of a state using only date of birth, zip code and gender.

COLLECTION



SURVEILLANCE

Watching, listening to, or recording of a person's activities

A website monitoring cursor movements of a visitor while visiting the website.



INTERROGATION

Questioning or probing for personal information

An interviewer asking an inappropriate question, such as marital status, during an employment interview.

INVASION



INTRUSION

Disturbing a person's tranquility or solitude

An augmented reality game directing players onto private residential property.

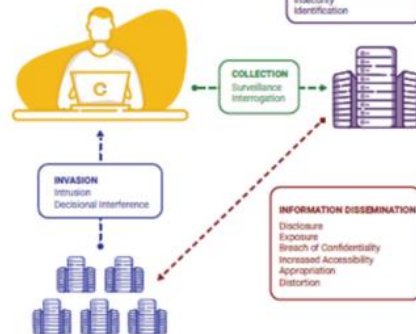


DECISIONAL INTERFERENCE

Intruding into a person's decision making regarding their private affairs

A payment processor declining transactions for contraceptives.

Based on Daniel Solove's
a Taxonomy of Privacy
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=467922



INFORMATION DISSEMINATION



DISCLOSURE

Revealing truthful information about a person that impacts their security or the way others judge their character

A government agency revealing an individual's address to a stalker, resulting in the individual's murder.



EXPOSURE

Revealing a person's nudity, grief, or bodily functions

A store forcing a customer to remove clothing revealing a colostomy bag.



BREACH OF CONFIDENTIALITY

Breaking a promise to keep a person's information confidential.

A doctor revealing patient information to friends on a social media website.



INCREASED ACCESSIBILITY

Amplifying the accessibility of personal information

A court making proceeding searchable on the Internet without redacting personal information.



APPROPRIATION

Using an individual's identity to serve the aims and interests of another

A social media site using customer's images in advertising.



DISTORTION

Disseminating false or misleading information about a person

A creditor reporting a paid bill as unpaid to a credit bureau.

PRIVACY
BY DESIGN



Version 7 (2023)

<https://privacybydesign.training>

Usability and human factors

- **Learn-ability** — The type for typical users to learn the actions relevant to a set of tasks.
- **Efficiency** — How long it takes users to perform typical tasks.
- **Errors** — The rate of errors users make when performing tasks.
- **Memorability** — How users can retain their knowledge of the system over time.
- **Subjective satisfaction** — How users like the various aspects of the system.



Why USEC is challenging?



<https://www.flickr.com/>

- Will people understand encryption?
- What icons work well?
- What is the most important information?
- Does Green/Red have the same meaning world wide?
- Will anyone look at the address bar after loading?
- Will users trust the icon to be accurate?



USEC is challenging because

- Interdisciplinary
- Seemingly familiarity
- Interrelations
- User evaluation
- Ecological validity
- Adversary model
- Technology velocity
- Customer

**Usec is
where
security and
the real world
meet.**

**It is VERY
interdisciplin
ary**



Let's look at one example

Was my message read?: Privacy and Signaling on Facebook Messenger

Roberto Hoyle
Oberlin College
Oberlin, OH
rhoyle@oberlin.edu

Srijita Das
Indiana University
Bloomington, IN
sridas@indiana.edu

Apu Kapadia
Indiana University
Bloomington, IN
kapadia@indiana.edu

Adam J. Lee
University of Pittsburgh
Pittsburgh, PA
adamlee@cs.pitt.edu

Kami Vaniea
University of Edinburgh
Edinburgh, Scotland
kvaniea@inf.ed.ac.uk

ABSTRACT

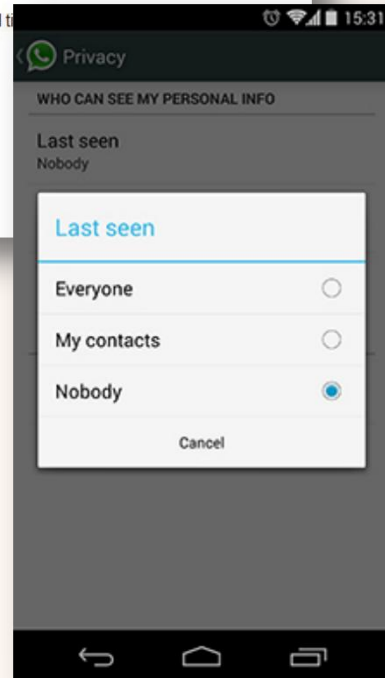
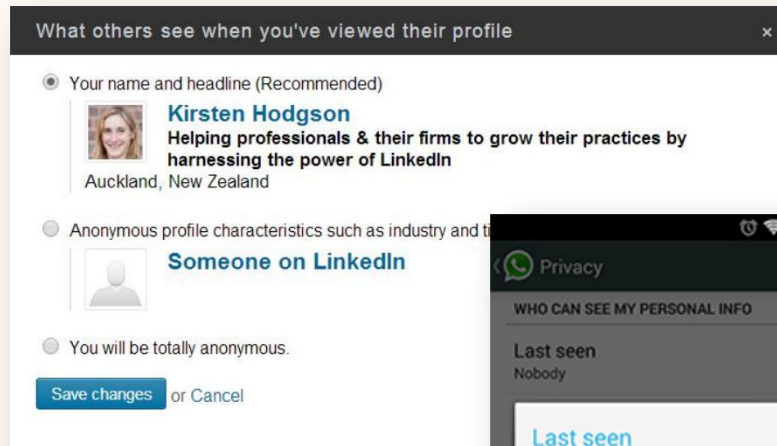
Major online messaging services such as Facebook Messenger and WhatsApp are starting to provide users with real-time information about when people read their messages, while useful, the feature has the potential to negatively impact privacy as well as cause concern over access to self. We report on two surveys using Mechanical Turk which looked at senders' (N=402) use of and reactions to the 'message seen' feature, and recipients' (N=316) privacy and signaling behaviors in the face of such visibility. Our findings indicate that senders experience a range of emotions when their message is not read, or is read but not answered immediately. Recipients also engage in various signaling behaviors in the face of visibility by both replying or not replying immediately.

when a message has been (i) *sent* to the service, (ii) *delivered* to the recipient's device, and (iii) *read* by the recipient.

In general, status about one's availability can create social pressure to be attentive to received messages [13], and also raise privacy concerns about one's visibility [14]. Feedback about whether a message was received or read raises additional privacy concerns and increases social pressure and anxiety for instant messaging viewers. Qualitative studies on the broader use of WhatsApp [3, 11] note such concerns amongst some of their participants although a deeper study of privacy and social pressure is not their focus. More recently, Mai et al. conducted a quantitative study to test specific hypotheses related to how obligated people feel to respond when a message has been read (although they do not study the case

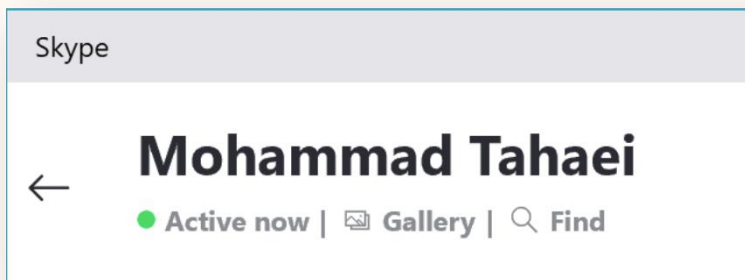
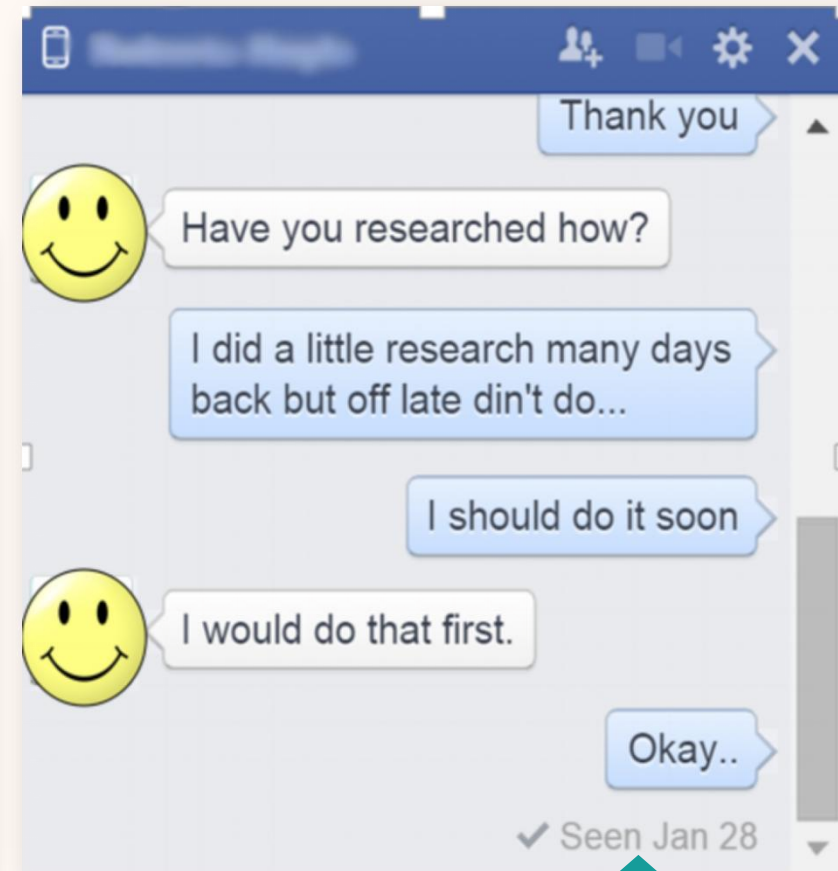
“Seen” visibility in social networks

LinkedIn



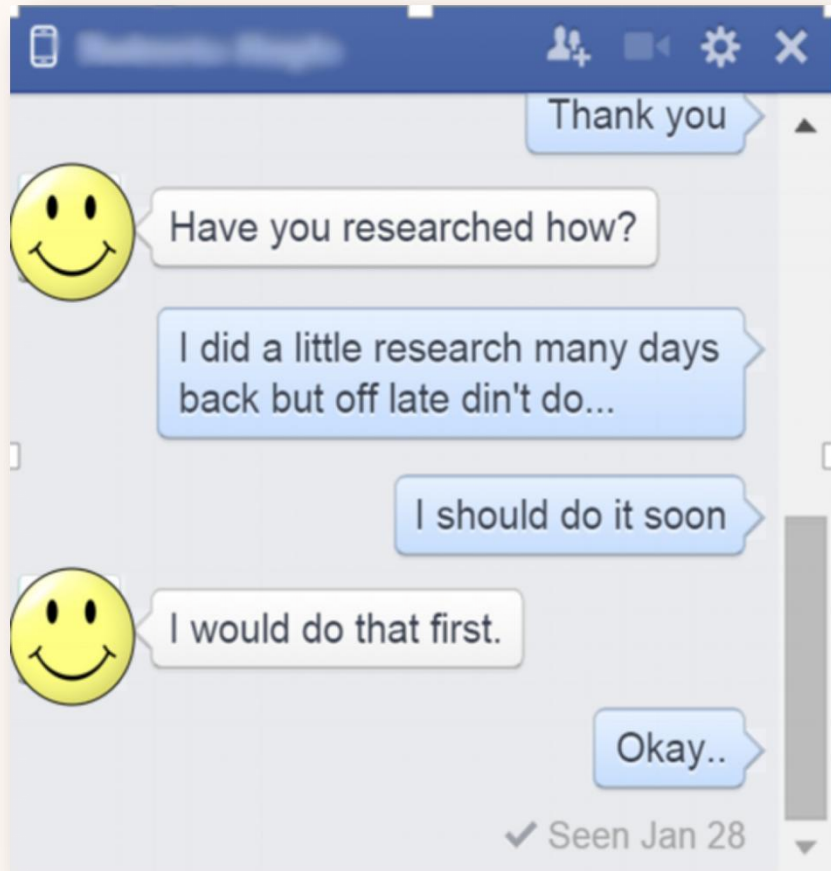
WhatsApp

Facebook Messenger



Skype

Do you like “seen” signal or not?

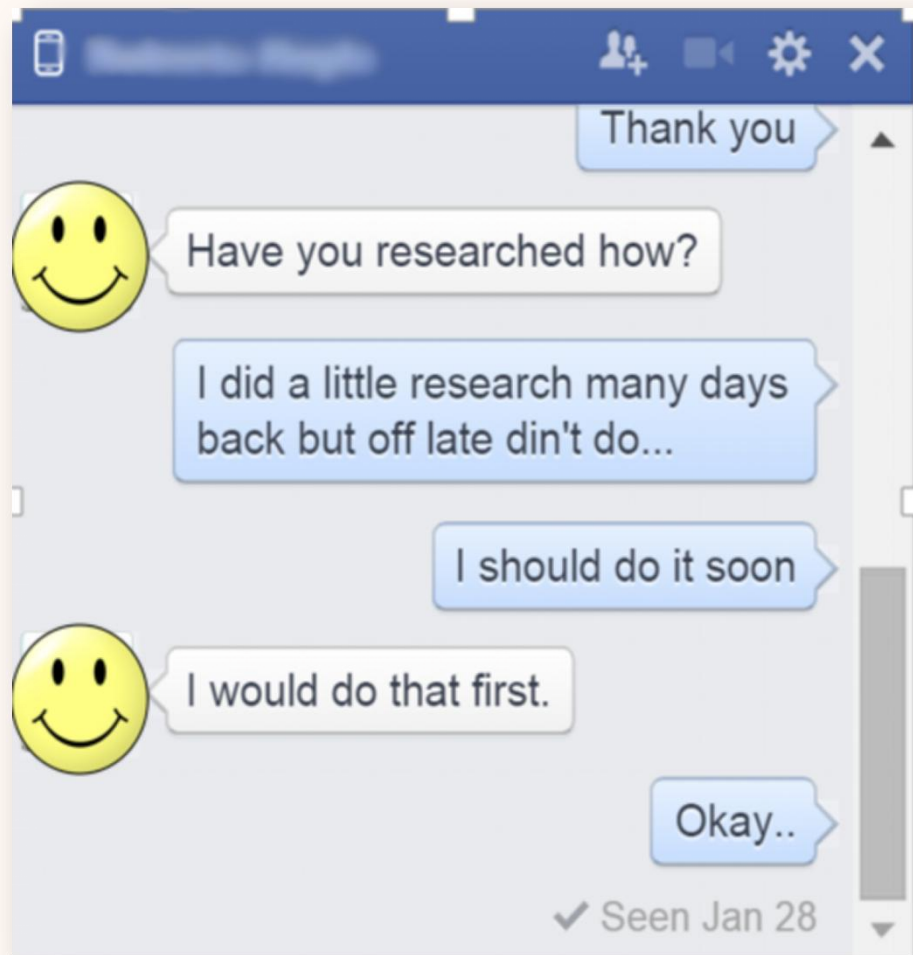


Facebook
(“seen” available)



Wechat
(“seen” not available)

Signaling



- Situational information solves technical problems
- People use these small indicators to signal other information
- People also use them to send other information

**How are people using the Facebook Messenger
“seen” feature for signaling?**

Interdisciplinary

- Social: Boundary management
- Privacy: Chilling effects
- Technical: Access control
- Technical: Network limitations
- HCI: Survey design, question wording, scales
- Statistics: Statistical analysis of the results




Interrelation

- Technologies impact each other
- Researchers need to understand how they interact

What others see when you've viewed their profile

☒ Your name and headline (Recommended)




Kirsten Hodgson

Helping professionals & their firms to grow their practices by harnessing the power of LinkedIn

Auckland, New Zealand

☐ Anonymous profile characteristics such as industry and title



Someone on LinkedIn

☐ You will be totally anonymous.

Save changes

 or Cancel

User evaluation

- Users are good at self-evaluating their own opinions and behaviors
- They are very bad at evaluating the security of something.... So we can't just ask them



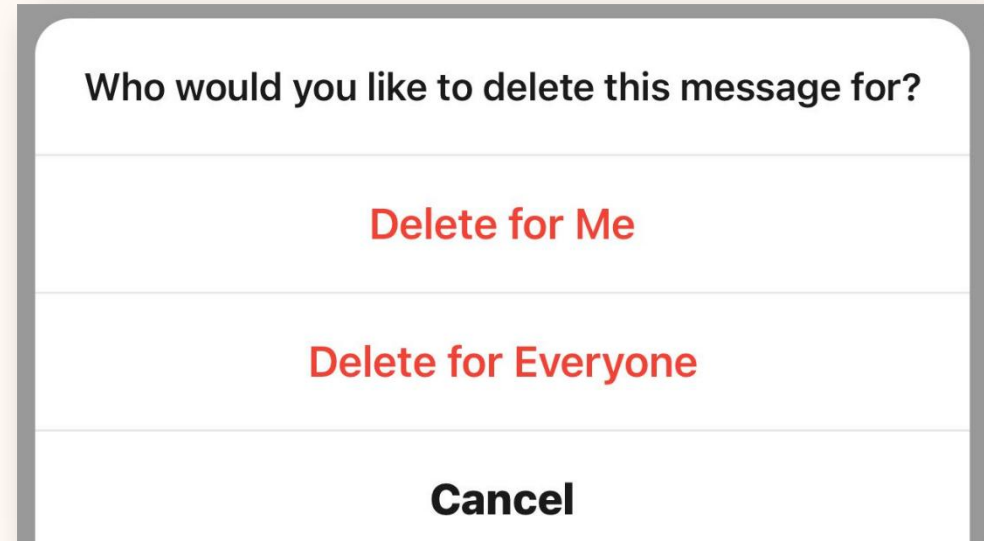
Ecological validity

- If we test something in an experiment, does that mean the same thing exists in the real world?
- Are people changing their answers because they are in a privacy study?

Reason avoided reading a message	Frequency
I wanted to pretend I never saw the message	68.2%
I was too busy with other work and had no time to view the message	45.8%
I hadn't responded to a correspondence from this person and didn't want to let them know I had logged into Facebook	41.3%
I didn't want people to know I am checking Facebook messages at that time of day or day of week	17.9%
I wanted the other person to know I am ignoring them	8.0%
Other	4.0%

Adversary

- Threat models — who and what are we defending against?
- End users would say “everything” but that is not possible
- Researchers need to understand those threats and build technologies that match them

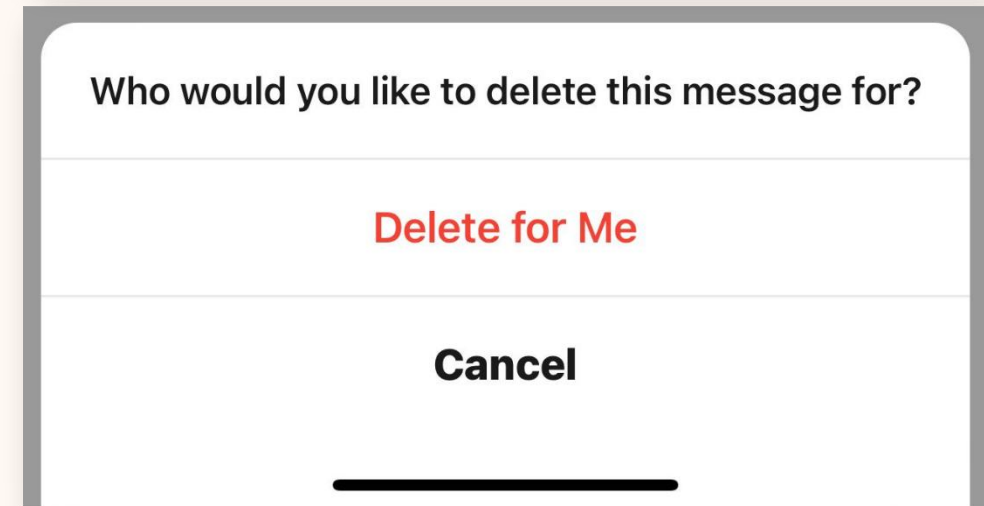


Who would you like to delete this message for?

Delete for Me

Delete for Everyone

Cancel



Who would you like to delete this message for?

Delete for Me

Cancel

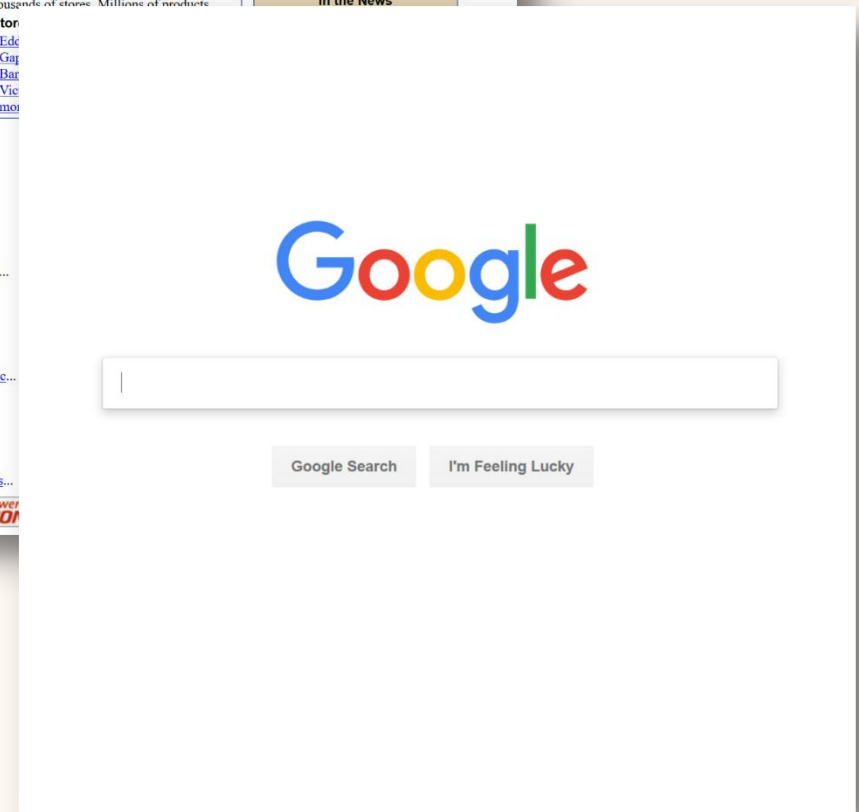
Who are the stakeholders?

- If we prove that the “Seen” feature harms people or violates privacy, who will do anything about it?
- Who will use the research?
- Who will it benefit?











Seemingly familiar

- Incorrect perception that nothing better is possible
- Good solutions look “obvious” in retrospect
- False assumption that creating good interfaces is a gift and not a learned skill



Tech velocity

- Technology changes fast
- Humans like only spending time learning things that will be useful for long time periods

SECURITY NONEXPERTS' TOP ONLINE SAFETY PRACTICES		VS	SECURITY EXPERTS' TOP ONLINE SAFETY PRACTICES	
1. USE ANTIVIRUS SOFTWARE				1. INSTALL SOFTWARE UPDATES
2. USE STRONG PASSWORDS				2. USE UNIQUE PASSWORDS
3. CHANGE PASSWORDS FREQUENTLY			2	3. USE TWO-FACTOR AUTHENTICATION
4. ONLY VISIT WEBSITES THEY KNOW				4. USE STRONG PASSWORDS
5. DON'T SHARE PERSONAL INFORMATION				5. USE A PASSWORD MANAGER

<https://googleonlinesecurity.blogspot.com.au/2015/07/new-research-comparing-how-security.html>

Questions?

Take-home

- Fill out the intro survey (available on Piazza) and say hi
- BBC News – CrowdStrike IT outage affected 8.5 million Windows devices, Microsoft says
<https://www.bbc.co.uk/news/live/cn056371561t>
- BBC News – WhatsApp and other messaging apps oppose ‘surveillance’ <https://www.bbc.co.uk/news/technology-65301510>