Exam Revision

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

24/03/2026

THE UNIVERSITY *of* EDINBURGH

Exam Structure

- Three questions: you must do Question 1 and select either Question 2 or Question 3 to answer
- “NOTES PERMITTED, CALCULATORS NOT PERMITTED examination. Candidates may consult up to ONE A4 pages (6 sides) of notes. CALCULATORS MAY NOT BE USED IN THIS EXAMINATION”

Expectation

- Applying concepts and frameworks learned in the lecture
- Thinking and analyzing critically using logic and examples
  - What are the limitations/tradeoffs?
  - What are the experiment tasks and materials?
  - Any similar cases?
  - ...
- No statistics, calculation, and drawing tested in the exam

Topics

- USEC basics
- Study method and analysis
- Authentication
- Online fraud and phishing
- Security and privacy communication (warning, advice, etc.)
- Privacy framework, tools, and policy
- Ethics and consent
- Access control, vulnerability research, AI, IoT, privacy governance....
- Other coursework-related topics (framework application, dark patterns, etc.)

Example: Bookwork

- Discuss two privacy risks induced by AI and explain how emerging generative AIs may exacerbate the risks with examples in context (hint: you can think about Solove's and Lee's taxonomies we introduced)

Example: Bookwork

- Discuss two privacy risks induced by AI and explain how emerging generative AIs may exacerbate the risks with examples in context (hint: you can think about Solove's and Lee's taxonomies we introduced)
    - What are the framework components?
    - How do you interpret it in context? Can you discuss within a real-life application as example? For example, how generative AI may enable new ways to aggregate information and misrepresent people on social media and autodigest?

Example: Case Study

- Alex is a moderator for an online social community on Discord (an instant messaging social platform that allows text messaging, video calls, and third-party plugins in a group chat). The community focuses on topics related to mental wellbeing. The community organises weekly online activities, such as reading groups, group exercises, and gaming, which may happen within Discord or apps connected to Discord. The community is public facing, and it accepts anonymous members to join.
    - As the community grows, Alex receives more recent complaints about inappropriate interactions between group members. Name three types of online safety harms that may occur within this community.
    - Name and discuss three specific Privacy by Design Strategies (other than ``Hide" and ``Demonstrate") that apply Privacy by Design principles reasonably to develop and deploy the above AI assistant. Explain how they help mitigate possible privacy risks in the related application context.

Example: Design and evaluate

- Online scams pose significant threats to the users of social media platforms such as Facebook, X (Twitter), and TikTok that leverages different human vulnerabilities and platform features. You are a security researcher, and you are interested in understanding people's experiences of online scams on social media platforms and designing solutions to mitigate such online scams. Answer the following questions in constructing a research study regarding this topic.
    - Propose a solution to address online scams on social media platforms and describe the challenges or trade-offs when implementing the solution. You can discuss the solution and challenges to one type of scams more specifically.
    - Design a user study to evaluate your solution. Describe and justify your study method. What are your dependent and independent variables?

USEC Intro

Defining security – CIA definition

Confidentiality	No improper information gathering
Integrity	Data has not been (maliciously) altered
Availability	Data/services can be accessed as desired
Accountability	Actions are traceable to those responsible
Authentication	User or data origin accurately identifiable

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.

USEC is challenging because

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

Threat Modelling: Adversaries

- Malicious actors
  - Hacker
  - Users (your family, your friend, your customer, etc.)
- Service providers
  - Company
  - App developers
- “Big brother”
- ... (depending on your position)

Assets

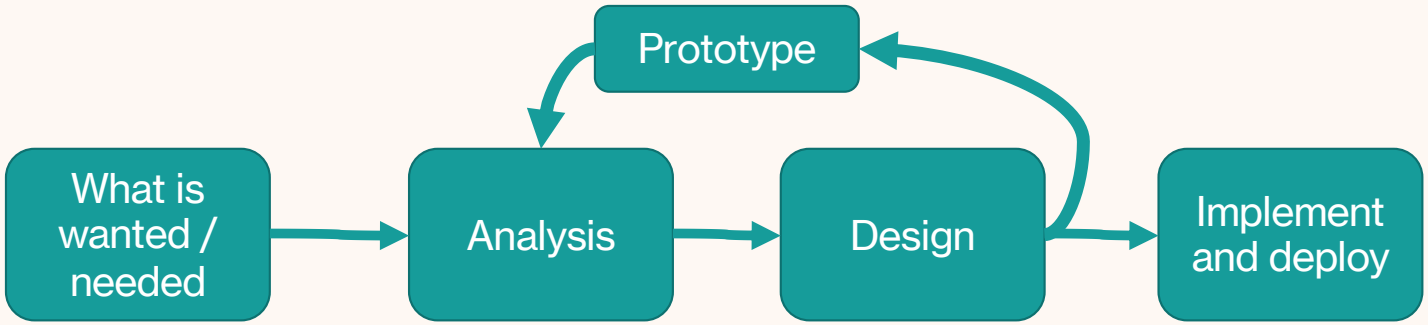
- Computer hardware: phone, laptop, server...
- Computer software: apps, operating systems, database...
- Physical assets: house, car.....
- Information: health record, your profile/identity, business info...
- Emotion, reputation, user experience....

Risk, threat and vulnerability

- Vulnerability: the weakness of X (system/human) that can be exploited
  - The program is overprivileged to access things
  - The user reuses their password across applications
- Threat is an action performed by the adversary to damage the asset by exploiting a vulnerability
- Risk = asset X threat X vulnerability

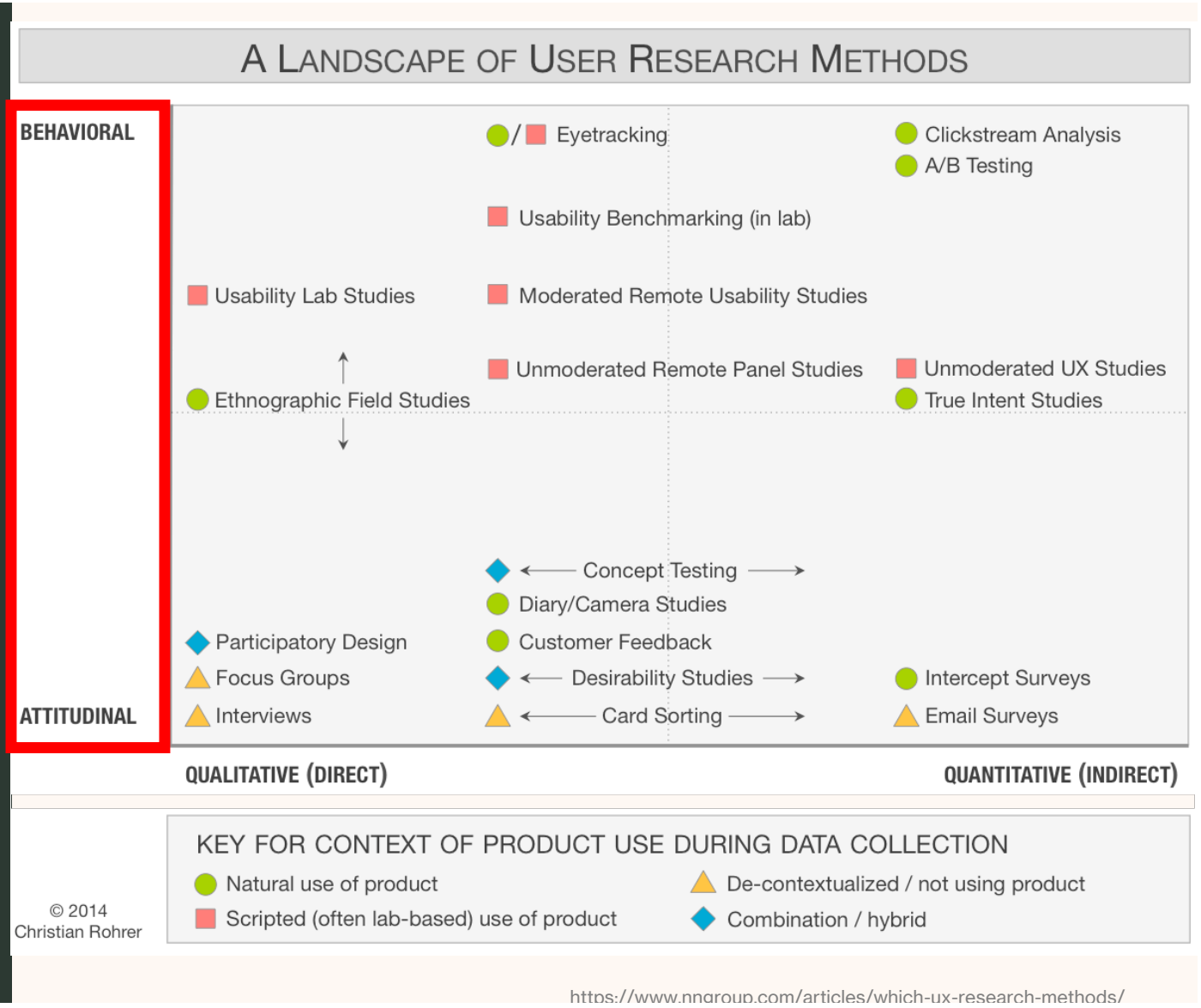
Study and Analysis Methods

Project lifecycle



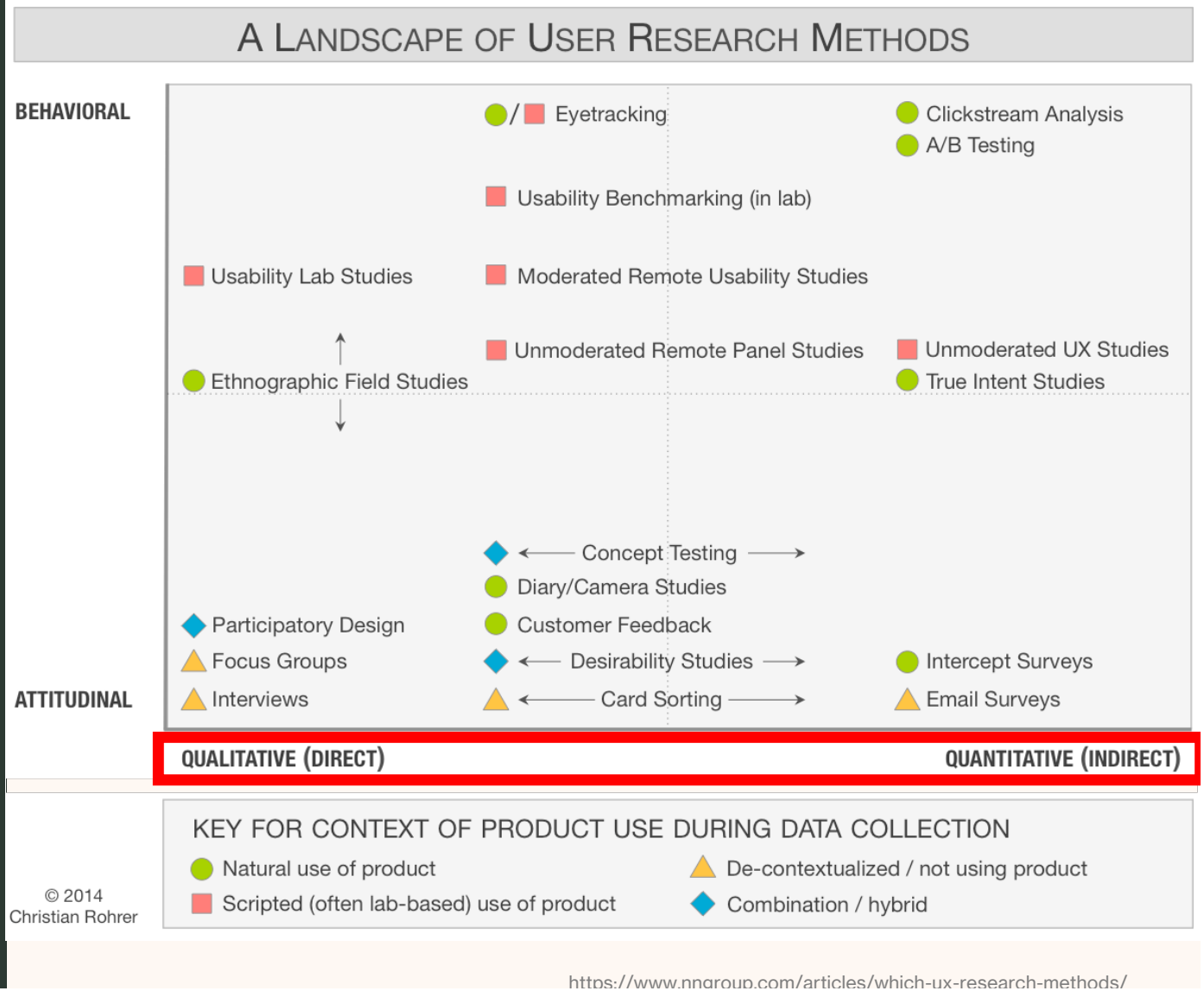
Behavioral – measures how people actually behave, what they do.

Attitudinal – measures what people say they think or how they say they behave.



Qualitative – unstructured data such as natural language.

Quantitative – numerical data. Anything that can be counted or measured with numbers.



Lab Study

- Basic idea: Have a participant come to a physical place (lab) and interact with the interface there
- You setup the lab so it mimics the situation you want to test
- Pros
  - Full control over the environment so limited confounds
  - Detailed data from each subject
  - Ability to ask them why they did something
- Cons
  - Small sample sizes
  - Being in the lab changes user behavior. They feel safer and their normal distractions are gone. That can be bad for deception studies.

Think aloud

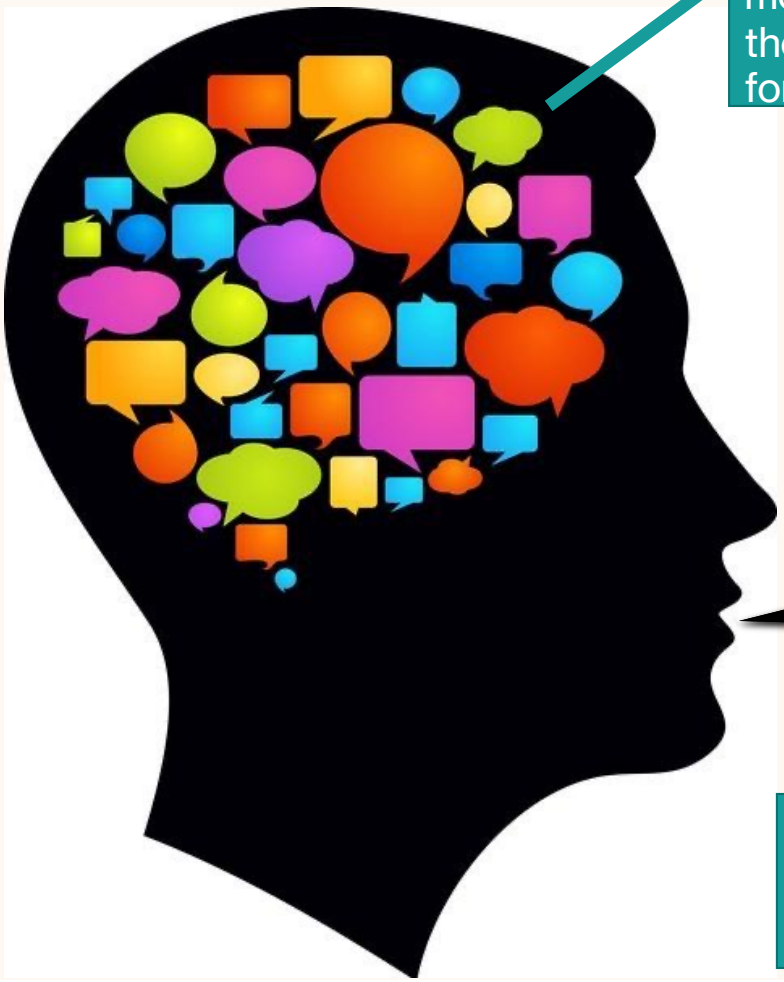
- Basic idea: Have a participant use the interface and speak aloud while they do so
- Think aloud is a very versatile, can be long or short, detailed or minimal, planned or ad-hoc
- Pros
  - Learn what the user is trying to do and why they click on some things
  - Very detailed information
  - Testing with about 5 users will find the majority of major (usability) issues
- Cons
  - Biasing user behavior, making the situation unnatural
  - (Concurrent) Talking aloud changes how long a user spends on tasks so this method cannot be combined with timing

https://www.nngroup.com/articles/thinking-aloud-the-1-usability-tool/

Think-Aloud aims to measure **what is in the person's head** at that moment, even if those thoughts are poorly formed.

If we ask the user to **"explain"** their thoughts then they have to convert the jumble in their head into a linear English sentence.

Converting thoughts to sentences forces users to think more and **changes their behavior**.



Hm... I'm thinking about what I need to say next... Maybe this button is the one I need.

We ask users to "talk aloud" and we do not interrupt them so that they behave just as they would normally. If you interrupt or ask them to explain it changes their behavior.

- Think about what tasks you will ask users to do
  - E.g., Log in to UoE's VPN; store a new password via Apple's password manager
- Design how you can instruct the users in an experiment, avoid jargon and bias
  - Bad example: *Today we will be studying the fact that Android devices take a long time to log in. I will be asking you to log into a provided Android phone several times in front of a camera to see if you can log in quickly*
  - Good example: *This study is about the usability of Android phone login screens. Today I will be asking you to log into a provided Android phone several times in front of a camera. We are using the camera so that we can identify small issues that make the login screen harder to use*

Activity 1: Intro script revisit / write down (3 mins)

Activity 1: Share your intro script (2 mins)

Task and subtask

Primary and secondary tasks

- A “primary task” is basically something **someone wants to do**. It is typically high level and expresses some state or activity that user wants to achieve.
  - Determine if I need to buy anything fridge-related from the store.
  - Spend an hour playing not-too-challenging games
  - Play the song I just thought of.
- A “secondary task” or “subtask” is a **smaller task that the user must accomplish to complete** the primary task.
  - What was the name of the song I’m thinking of?
  - Which music service is likely to have it?
  - There are two versions, which one do I want to play?

Planning a survey

- Surveys normally answer **multiple research questions**. With each research question tied to one or more survey questions.
- **Descriptive** – learn something about the whole population.
  - How many people have heard of the term “phishing”?
  - What words do people use to describe cookie tracking?
- **Testing for correlation or causation** – show that two things are related or one thing causes the other thing.
  - If someone has been trained on phishing in the past, are they better at differentiating phishing emails?
  - We have three training options, each user goes through one training, which training causes people to identify phishing emails the best?

Survey scales

- Basic idea: A set of questions that have been previously shown to measure a property.
- Pros
  - Easy to copy-and-paste into a survey.
  - Allows you to measure hard-to-measure concepts like risk seeking behavior or attitude towards privacy.
- Cons
  - Making a new scale is very challenging.
  - Can contain an annoyingly large number of questions.

Testing: Correlation vs. Causation

- Correlation
  - Two things tend to behave in a way that seems inter-related, where if one thing changes the other thing will also change in a related way.
  - For example, if the price of rice goes up at the same time as the price for beans.
- Causation
  - When one thing changes it causes the other thing to change.
  - For example, when the weather gets cold more people wear coats. Cold weather causes more people to wear coats.

Testing: What are you going to measure?

- In statistics there are classically two types of measurements (variables): dependent and independent
- Dependent
  - Also known as the **outcome variable**
  - “Dependent” on the study
  - Measures the usability **goal**
- Independent
  - Anything **you are directly manipulating**
  - An element of the study which is under your control
  - A pre-existing feature of your participant

Testing: Between vs. Within subjects

- Between subjects
  - Your study only shows one interface to one person
  - You are measuring how well the people randomly assigned to the A interface did compared to the people randomly assigned to the B interface
  - **Lots of variability with this method**
- Within subjects
  - Your study shows all interfaces to all people
  - You are measuring the difference in how they do on the two interfaces
  - **Less variability (same person) but more learning effects and priming**

Testing: Types of data

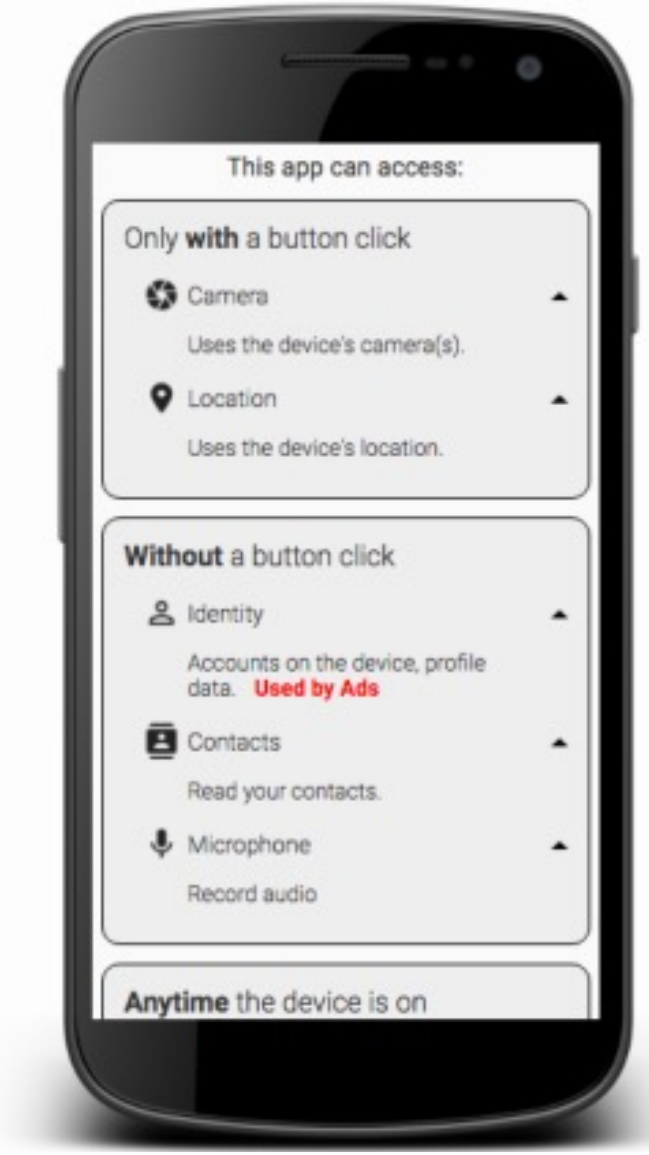
- Numeric
  - **Continuous** – Any value on the range is possible including decimal (1-5)
  - **Discrete** – Only certain values on the range are possible (1,2,3,4,5)
  - **Interval** – Only certain values on the rage are possible and each has equal distance from its neighboring values (strongly agree, agree, neutral, disagree, strongly disagree)
- Categorical
  - **Binary** – Only two possibilities (true, false)
  - **Ordinal** – The values have an ordering (slow, medium, fast)
  - **Nominal** – The values have no ordering (apple, pear, kiwi, banana)

Some research questions:

- Can people differentiate between a subdomain and a domain when reading a URL?
- Does [my new system] help people differentiate between malicious URLs and safe ones?
- Can users use [my new password manager] faster and with less errors than [the old password manager]?
- Does knowing how an app will use its permissions impact app installation decisions?
- What factors impact end-users' willingness to update software?
- Using [website], can users successfully opt-out of cookie tracking without forming inaccurate mental models?

Study design

- RQ: Does [my new interface] enable people to accurately determine what permissions an app will use?
- A/B test between the existing and new interface
- Between subjects
- 10 Tasks shown in the same order to all participants
- Dependent variables
  - Accuracy on task
- Independent variables
  - Which interface (A or B)

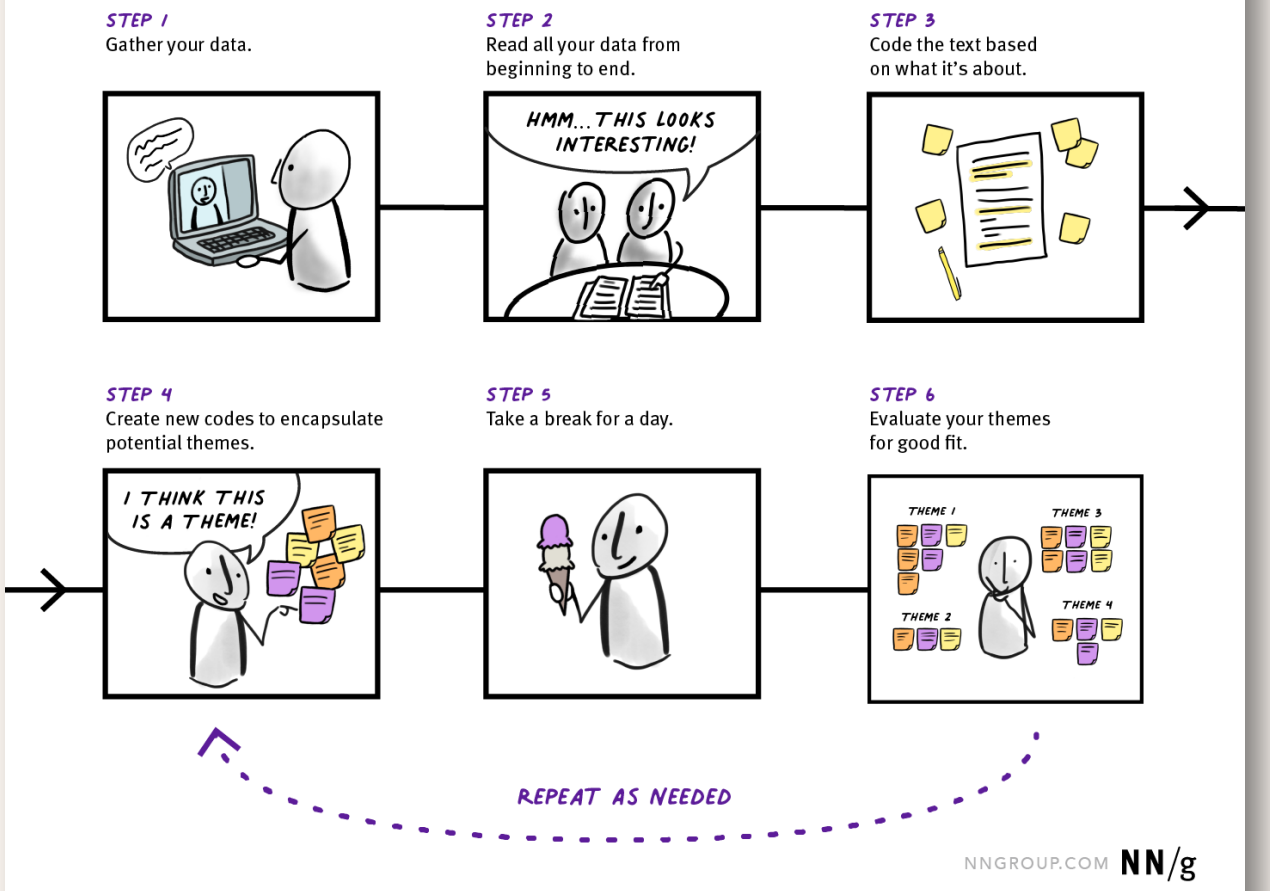


Inductive coding vs deductive coding

- **Inductive (bottom-up):** look for any ideas that interest you from different aspects
    - Snapshot of an app on a phone
    - Child playing with dog
    - Edited picture
    - Motion detection enabled
    ....

- **Deductive (top-down):** start with some hypothesis
    - Children being monitored by app (privacy concern)
    - Camera placed in the living room (place of the scene)

6 Steps to Doing a Thematic Analysis



Frameworks

A good authentication method:

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

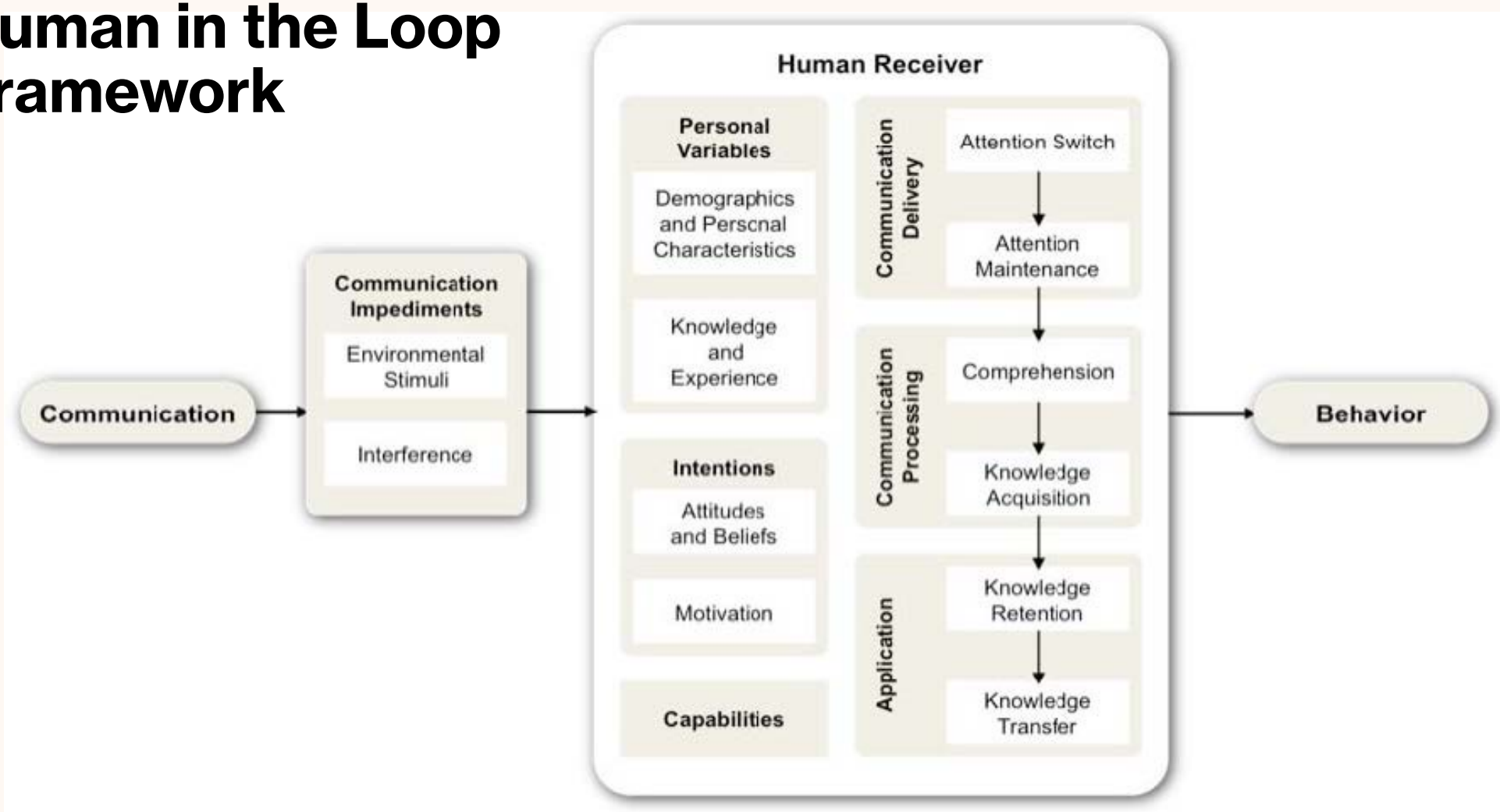
Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Human in the Loop Framework



https://medium.com/@ezgineer/usable-security-and-privacy-introduction-d676abc8c61d

A TAXONOMY OF PRIVACY

INFORMATION PROCESSING

AGGREGATION
Combining of 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

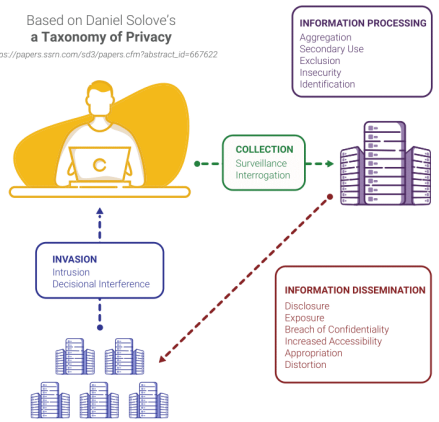
INTRUSION
Disturbing a person's tranquility or solitude

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/sd3/papers.cfm?abstract_id=667622



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.

Version 6 (2022)

PRIVACY BY DESIGN

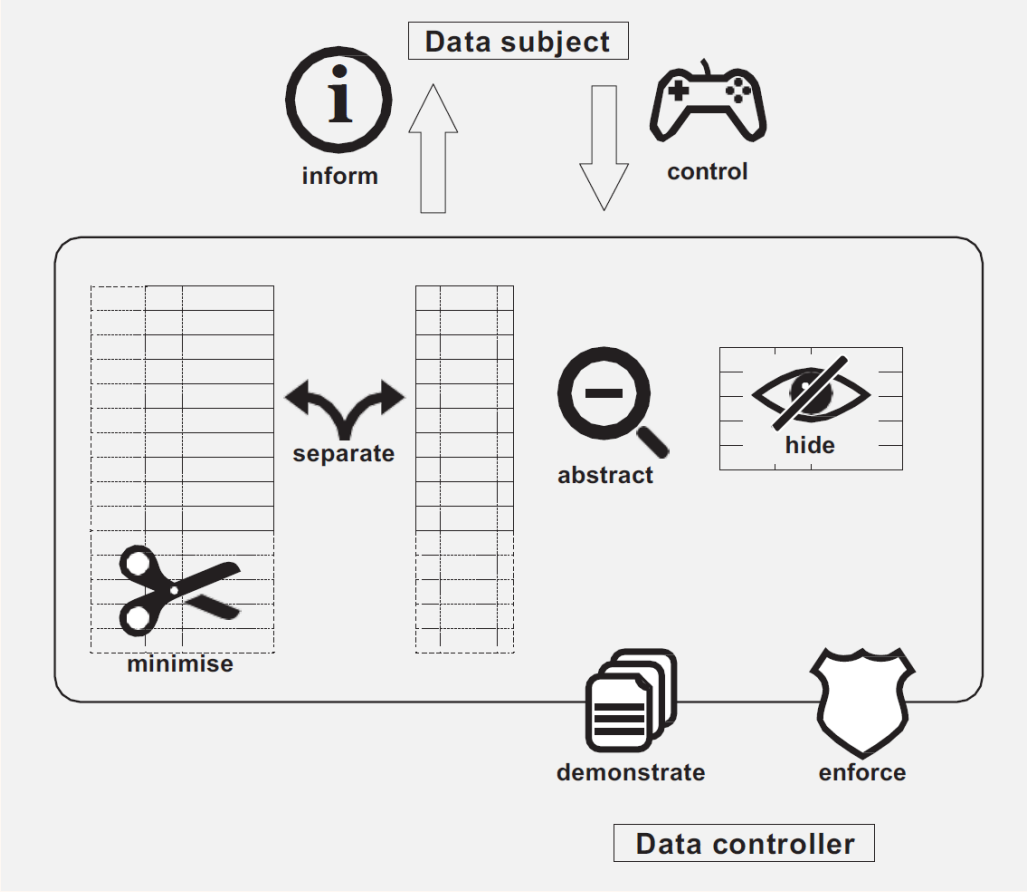
https://privacybydesign.training

Privacy by design – definition

Framework for building privacy proactively into new systems, proposed in 2009.Widely accepted as an international standard for good privacy engineering. GDPR also basis some of its principles on Privacy by Design.

- **Proactive** not Reactive; **Preventative** not Remedial
- Privacy as the **Default**
- Privacy **Embedded** into Design
- **Full** Functionality – Positive-Sum, not Zero-Sum
- End-to-End Security – Lifecycle Protection
- Visibility and Transparency
- **Respect** for User Privacy

Privacy by design – strategies



Other Frameworks: What are they used for, and how to use them?

- NEAT
- SPRUCE
- Privacy by design
- Fraud Taxonomy...
- ....

The Menlo Report (2012)

- Res
- Ber
- Jus
- Res

Principle	Application
Respect for Persons	Participation as a research subject is voluntary, and follows from informed consent; Treat individuals as autonomous agents and respect their right to determine their own best interests; Respect individuals who are not targets of research yet are impacted; Individuals with diminished autonomy, who are incapable of deciding for themselves, are entitled to protection.
Beneficence	Do not harm; Maximize probable benefits and minimize probable harms; Systematically assess both risk of harm and benefit.
Justice	Each person deserves equal consideration in how to be treated, and the benefits of research should be fairly distributed according to individual need, effort, societal contribution, and merit; Selection of subjects should be fair, and burdens should be allocated equitably across impacted subjects.
Respect for Law and Public Interest	*Engage in legal due diligence; Be transparent in methods and results; Be accountable for actions.*

Stakeholder-based ethics analysis

- **Stakeholders:** You are expected to consider all possible stakeholders (people, including the research team and society at large, and entities including companies) that may be impacted by your research. You are expected to detail how each stakeholder may have been impacted by the research procedures you undertook and how those stakeholders may be impacted by the publication of your research now and in the future.
- For example, who are the stakeholders involved in a vulnerability disclosure?

https://www.usenix.org/conference/usenixsecurity26/call-for-papers#ethics

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

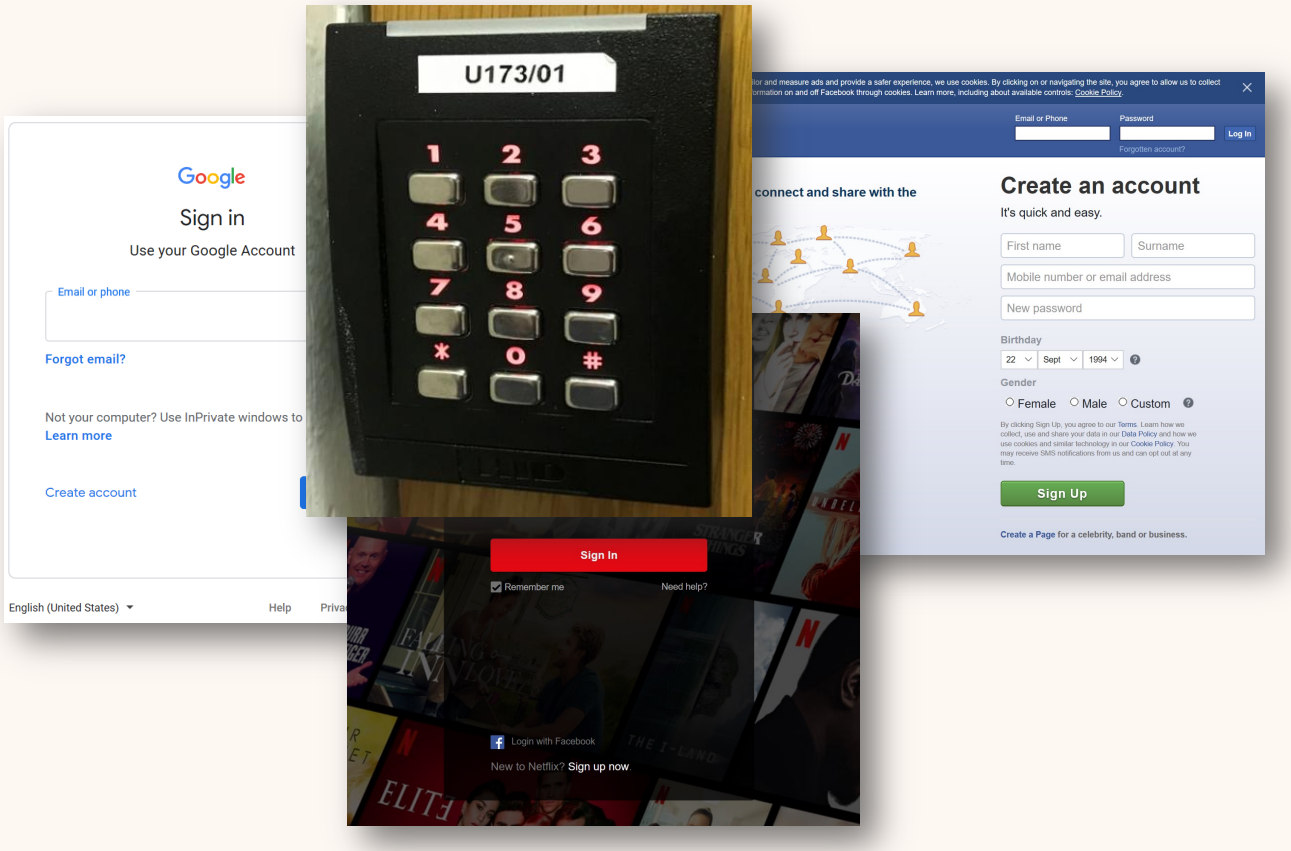
Unique – Knowledge the user has – Tell the user what information they bring to the decision regarding the context

Choices – List available options and clearly recommend one

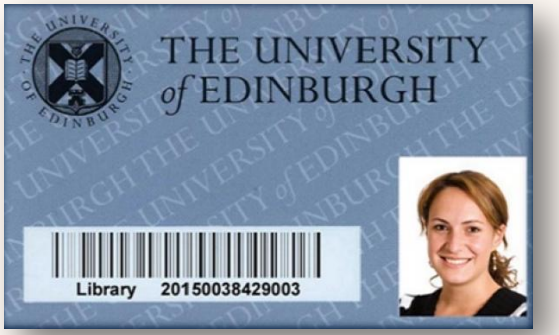
Evidence – Highlight information the user should factor in or exclude in making a decision

Topics (not exclusive)

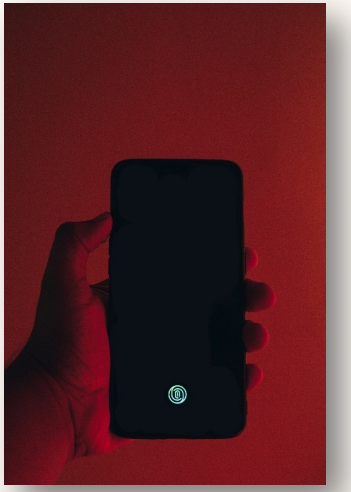
Authentication



What you know



What you have



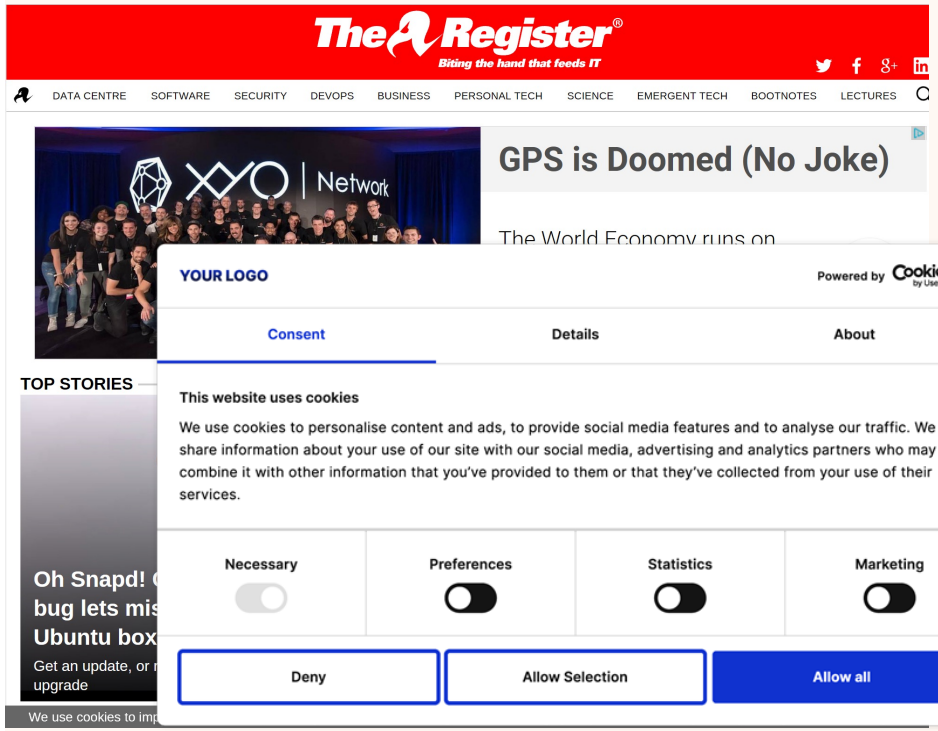
Who you are

Attributes of a “good” biometric feature

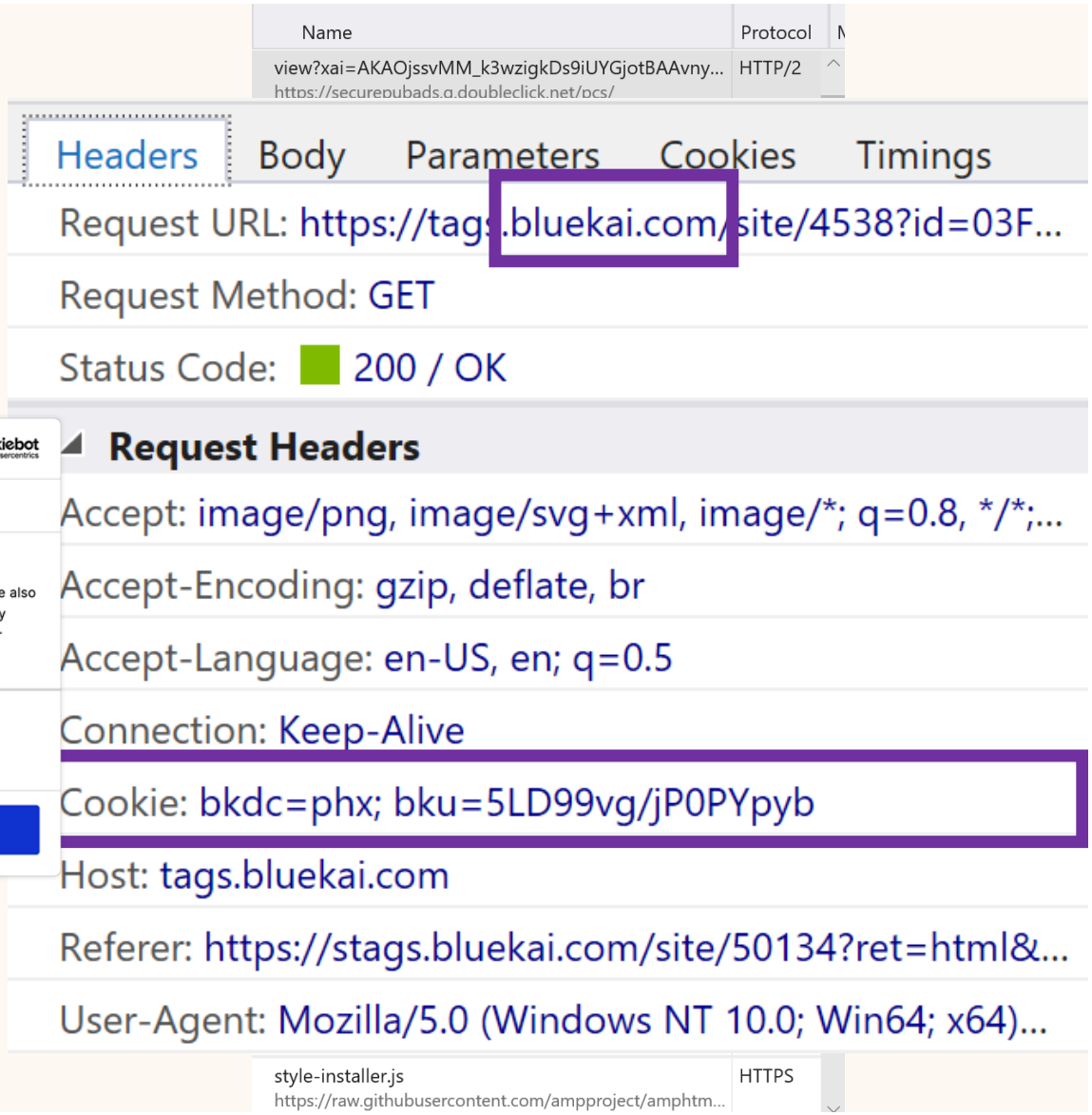
1. **Universality:** Does everyone have it?
2. **Distinctiveness:** Is it different for everyone?
3. **Permanence:** Does the feature change over time/age?
    - bad: face, good: fingerprint
4. **Collectability:** How easy it is to collect/measure the feature?
    - Very hard: DNA, relatively easy: fingerprint
5. **Performance:** How difficult to match?
6. **Acceptability**
7. **Circumvention:** How easy to spoof?
    - Voice recognition

https://www.cse.msu.edu/~rossarun/pubs/RossBioIntro_CSVT2004.pdf

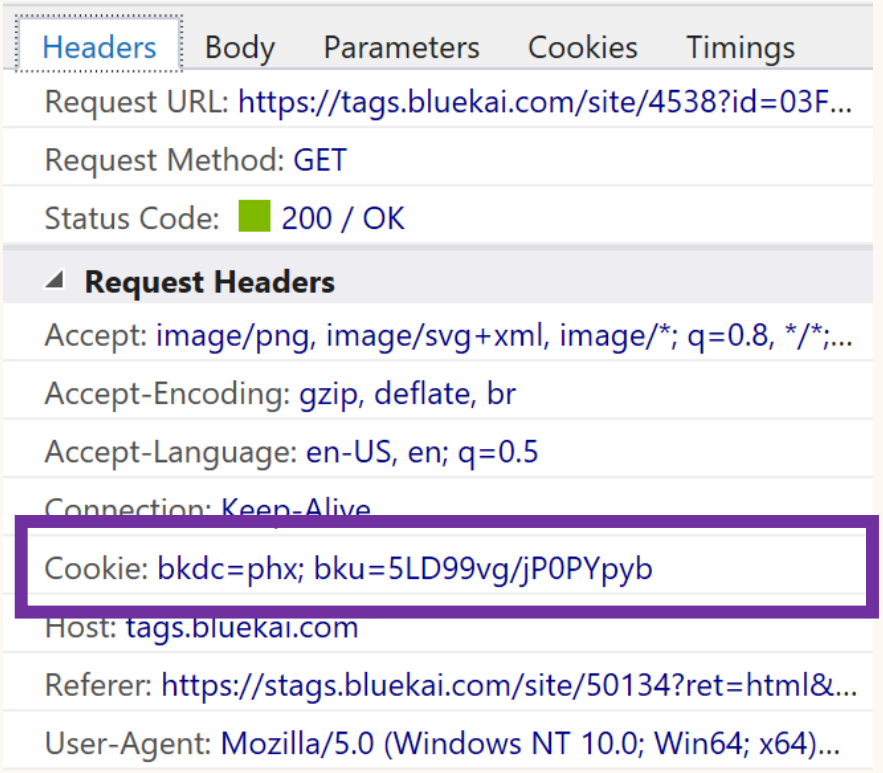
Cookie



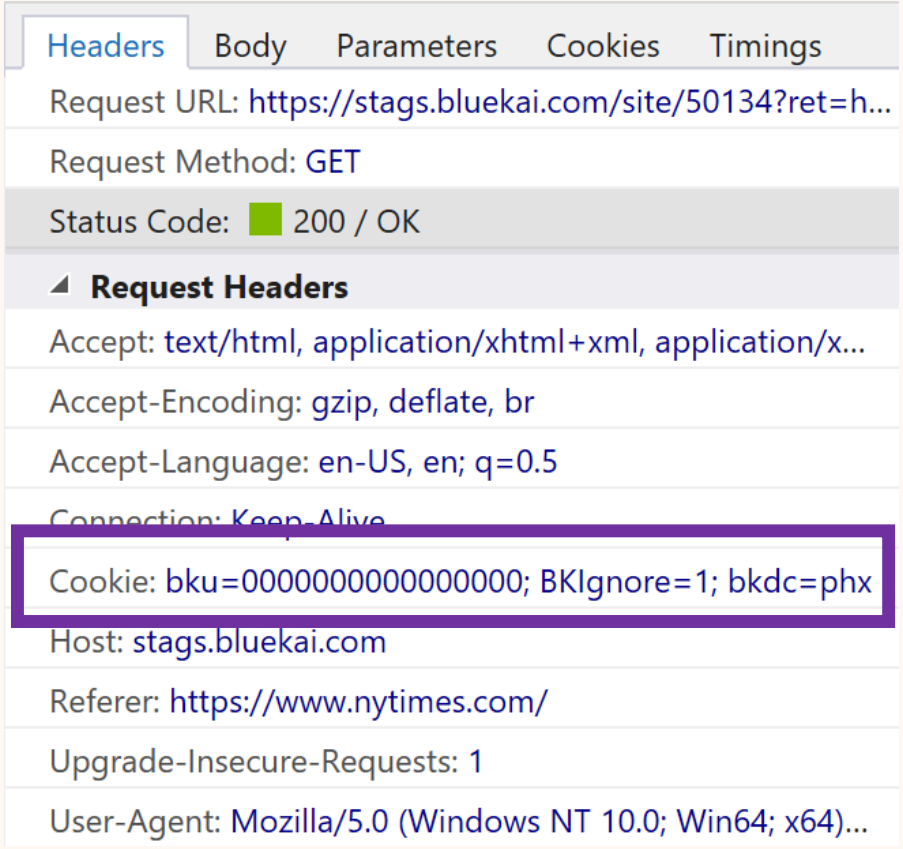
https://ico.org.uk/for-organisations/direct-marketing-and-privacy-and-electronic-communications/guide-to-pecr/cookies-and-similar-technologies/

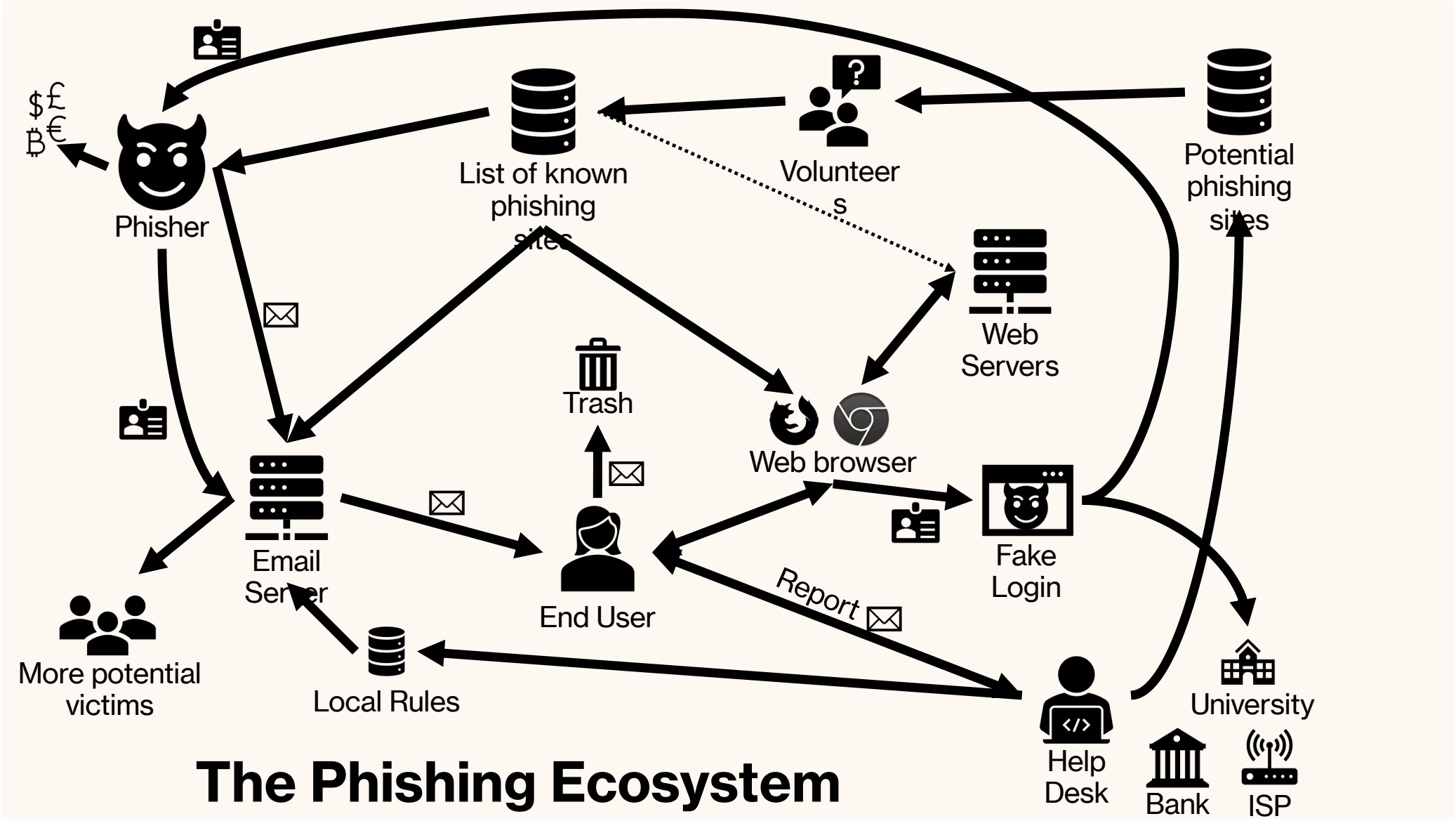


BEFORE OPT-OUT



AFTER OPT-OUT




$£
฿€
Phisher
List of known phishing sites
Volunteers
Potential phishing sites
Web Servers
Trash
Web browser
Email Server
End User
Fake Login
Report
More potential victims
Local Rules
Help Desk
University
Bank
ISP
The Phishing Ecosystem

Common phishing elements

- **Automated** – Typically directed against many people.
- **Impersonation** – Communication claims to be from someone trusted or that they are not. For example, from a bank.
- **Direction to a website** – Links that look like they go somewhere legitimate but in fact go somewhere controlled by the attacker.
- **Contain an attachment** – Attachment asks for information to be sent back or contains malicious code.
- **Authentication info requested** – The communication aims to get authentication information.

Main “solutions” against phishing

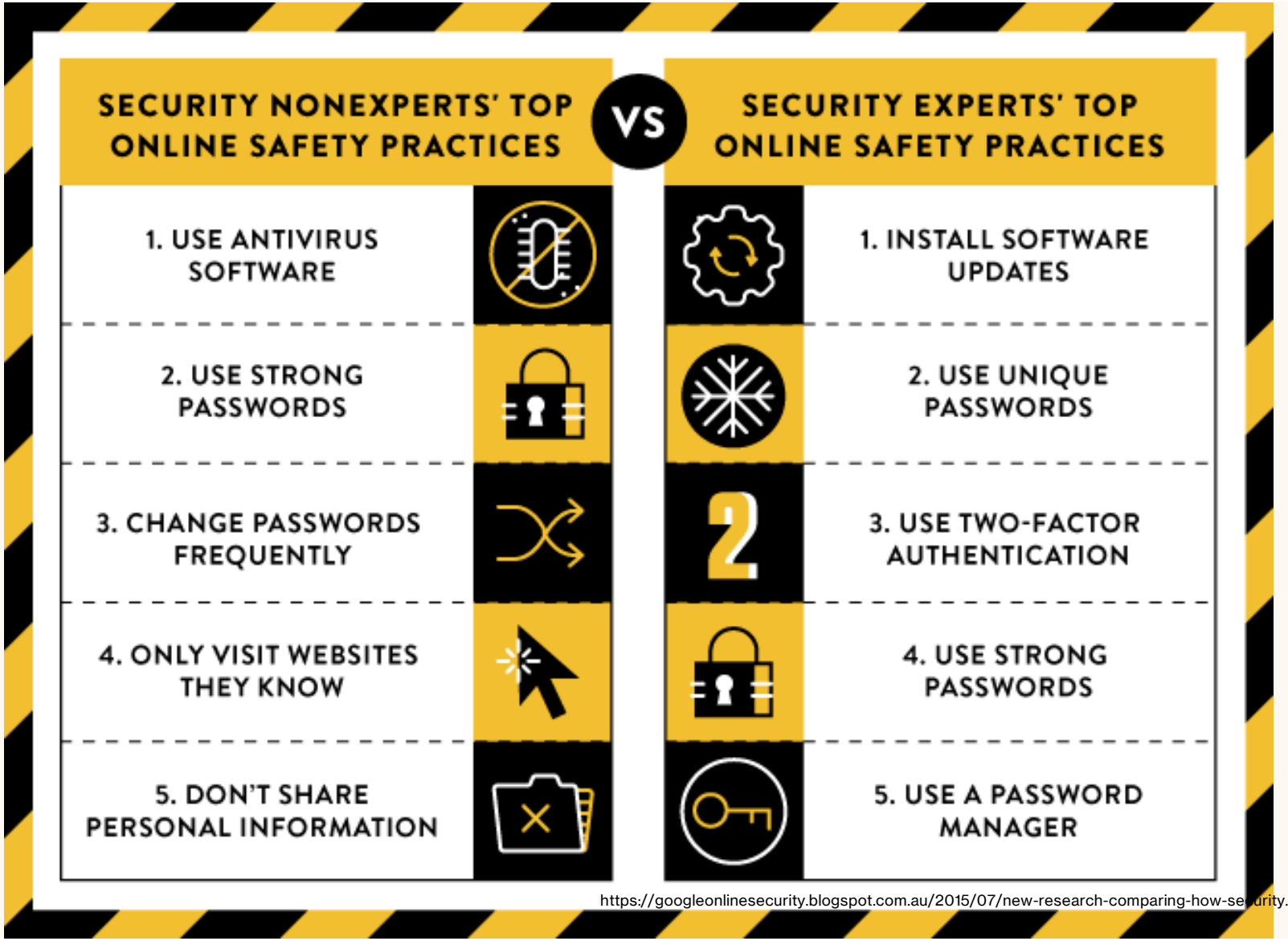
- **Automatically block attacks using filters**
- **Train users**
- **Support users**
- **Improve protection of authentication credentials**

Overview of Stanford Fraud Taxonomy

- Consumer Investment Fraud
  - Securities fraud
    - Equity investment fraud
      - Penny stock fraud
      - ...
    - ...
  - ...
- Consumer Products and Services Fraud
  - ...
    - *Phishing websites/emails/calls*
- Employment Fraud
- Prize and Grant Fraud
- Phantom Debt Collection Fraud
- Charity Fraud
- Relationship and Trust Fraud

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.”



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

Access Control Matrix

Objects (files)

Subjects (users)

	a	b	c	d	e
jingjie	r,w	-	r,w, own	-	r
bob	-	-	r	r	r,w
alice	w, own	r	r	-	-
eve	r	r,w	r,w	-	r

Permitted operations

[Lampson, Graham, Denning; 1971]

Could be a very huge table to store and access!

ACL vs. Capabilities

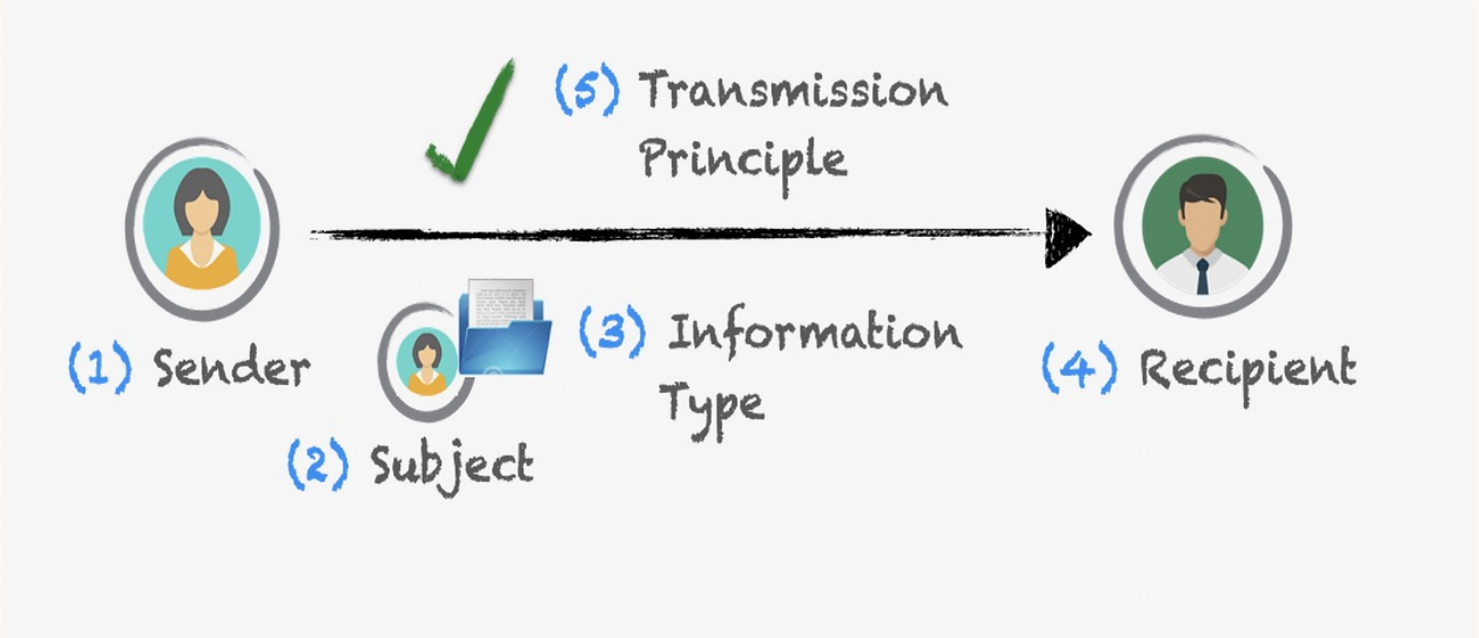
ACL

- Each file contains lists of user ids with their permissions (column in AC matrix)
- Check user/group against ACL
- Relies on authentication
- Inefficient run-time security checking

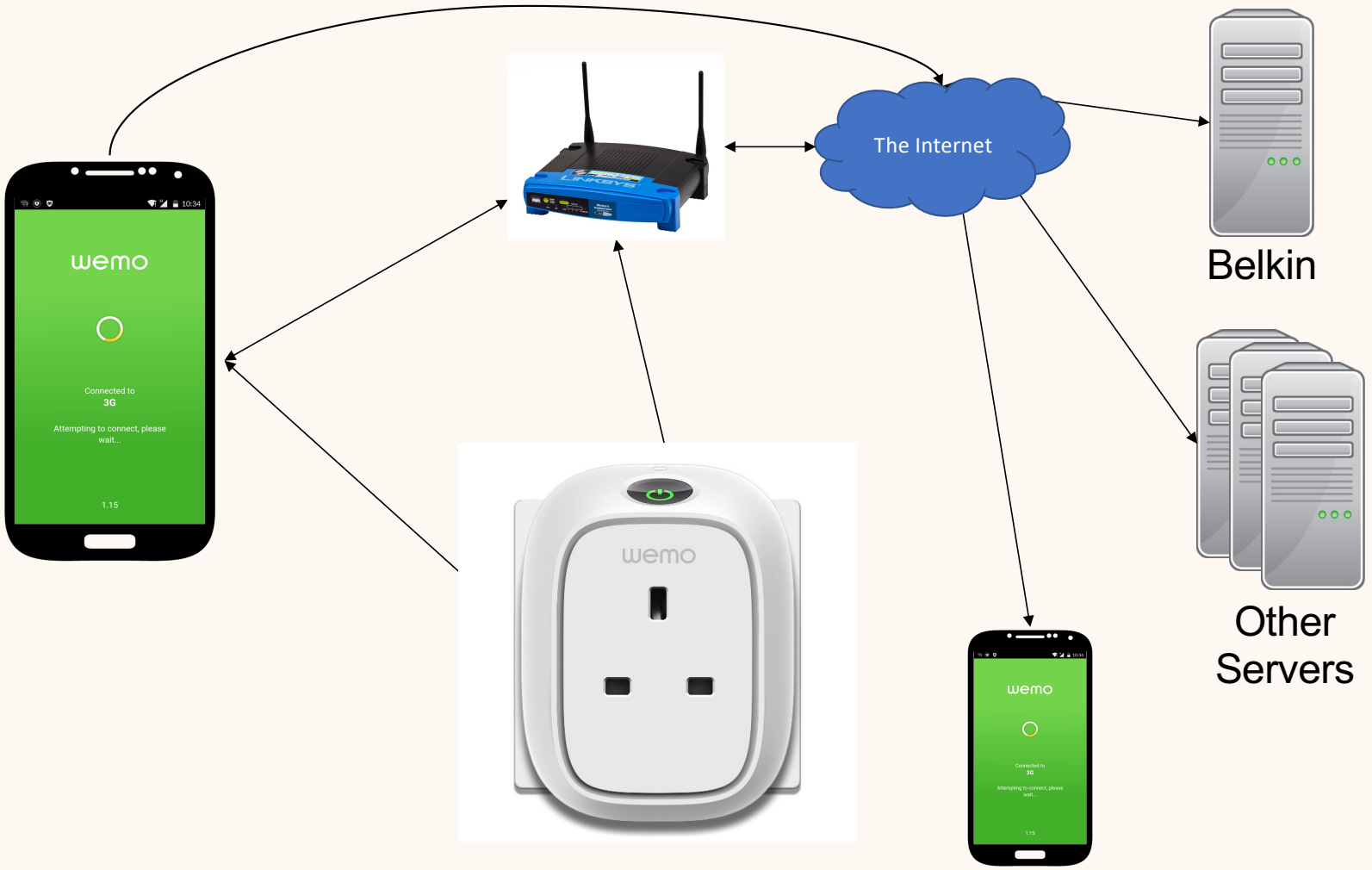
Capabilities

- Stores each user's capabilities (row in AC matrix)
- Check validity of capability
- Can be easily passed to other subjects (delegation)
- Hard to change a file's status globally, e.g., revocation

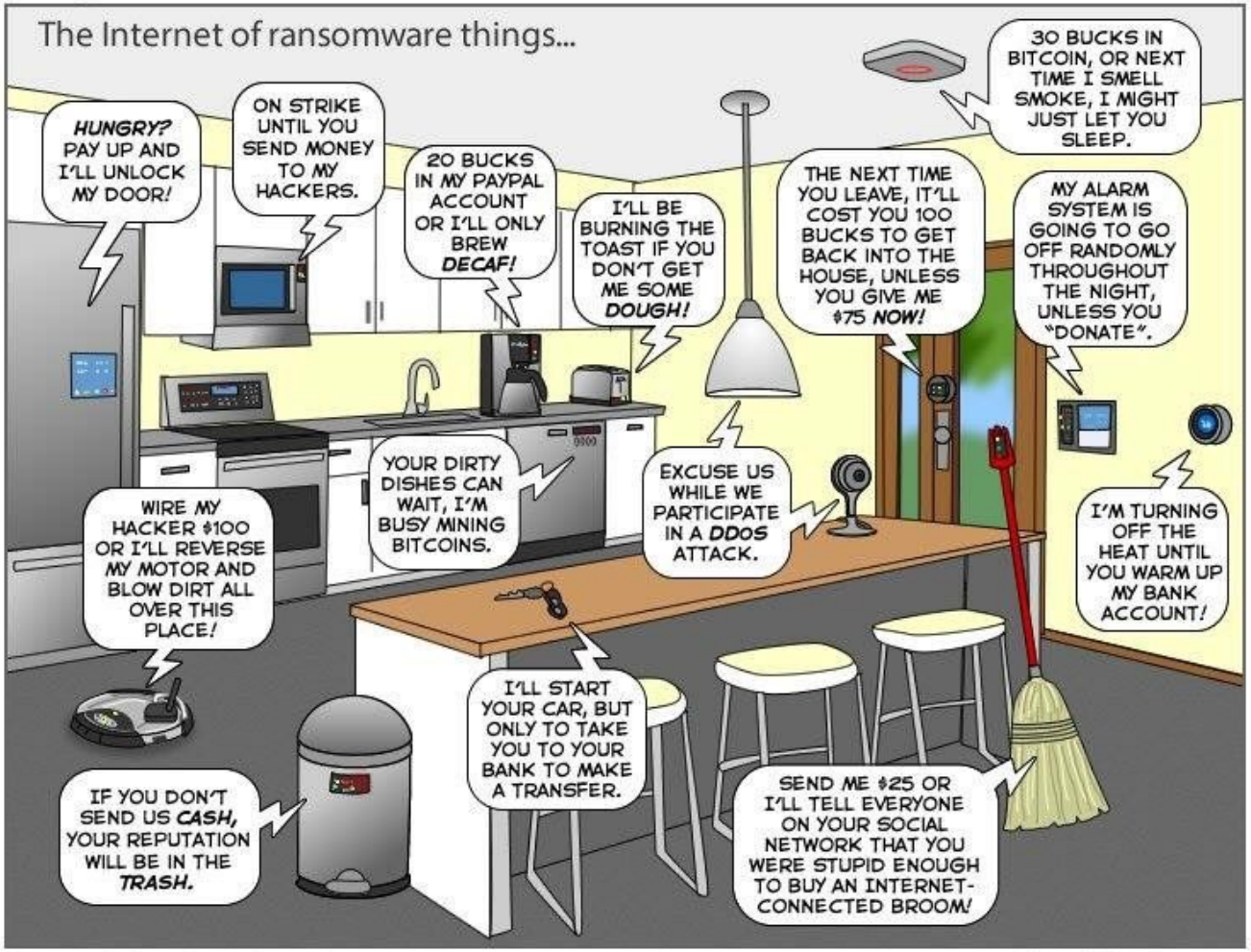
Contextual integrity



https://www.dli.tech.cornell.edu/post/privacy-policies-as-contextual-integrity-beyond-rules-compliance


wemo
Connected to
3G
Attempting to connect, please wait...
1.15
The Internet
Belkin
Other Servers
wemo

The Joy of Tech™ by Nitrozac & Snaggy



joyoftech.com

Consent in General Data Protection Regulation

The basic requirements for the effectiveness of a valid legal consent are defined in Article 7 and specified further in recital 32 of the GDPR. **Consent** must be freely given, specific, **informed** and unambiguous. In order to obtain freely given consent, it must be given on a voluntary basis. The element “free” implies a real choice by the data subject….

1998 Act:	GDPR:
Principle 1 – fair and lawful	Principle (a) – lawfulness, fairness and transparency
Principle 2 – purposes	Principle (b) – purpose limitation
Principle 3 – adequacy	Principle (c) – data minimisation
Principle 4 – accuracy	Principle (d) – accuracy
Principle 5 - retention	Principle (e) – storage limitation
Principle 6 – rights	No principle – separate provisions in Chapter III
Principle 7 – security	Principle (f) – integrity and confidentiality
Principle 8 – international transfers	No principle – separate provisions in Chapter V
(no equivalent)	Accountability principle

Some examples of at-risk groups

“We define a user(s) as being at-risk if they face an elevated likelihood of an attack to their digital safety, have factors that influence or exacerbate their chances of being targeted, and/or experience heightened harm as a result of a digitally-mediated attack”

- Survivors of intimate partner violence
- Political activist
- Identity based marginalization (e.g., queer, women, people of color....)