Exam Revision

INFR11158/11230 Usable Security and Privacy

Dr. Jingjie Li

02/04/2024

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 THREE A4 pages (6 sides) of notes. CALCULATORS MAY NOT BE USED IN THIS EXAMINATION”
- Past exams online: https://exampapers.ed.ac.uk/

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
- Phishing
- Security and privacy communication (warning, advice, etc.)
- Privacy framework, tools, and policy
- Ethics and consent
- Access control, AI, IoT, at-risk users....

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

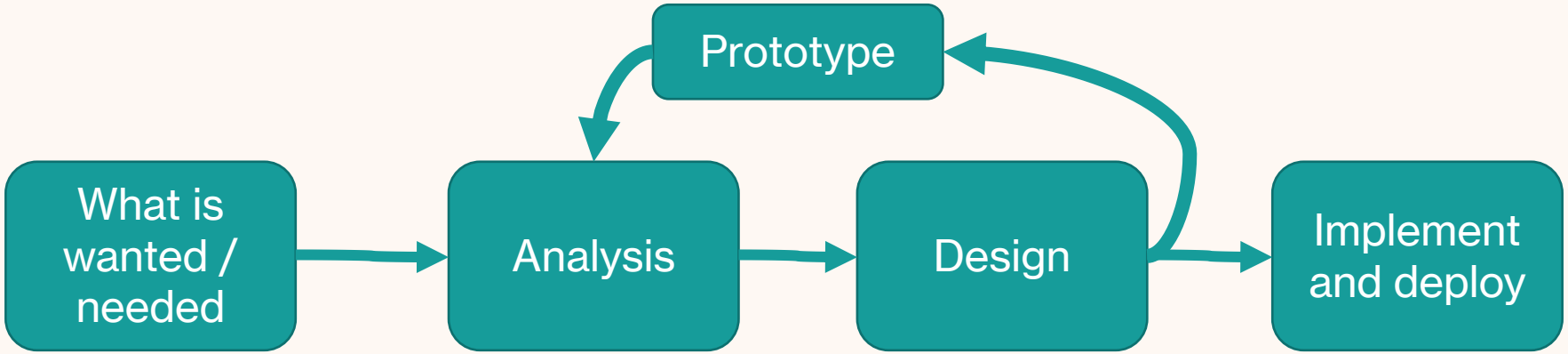
- Computer hardware: phone, laptop, server...
- Computer software: apps, operating systems, database...
- Physical assets: house, car.....
- Information: health record, your profile/identity, business info...
- Emotion, reputation, user experience....

Risk, threat and vulnerability

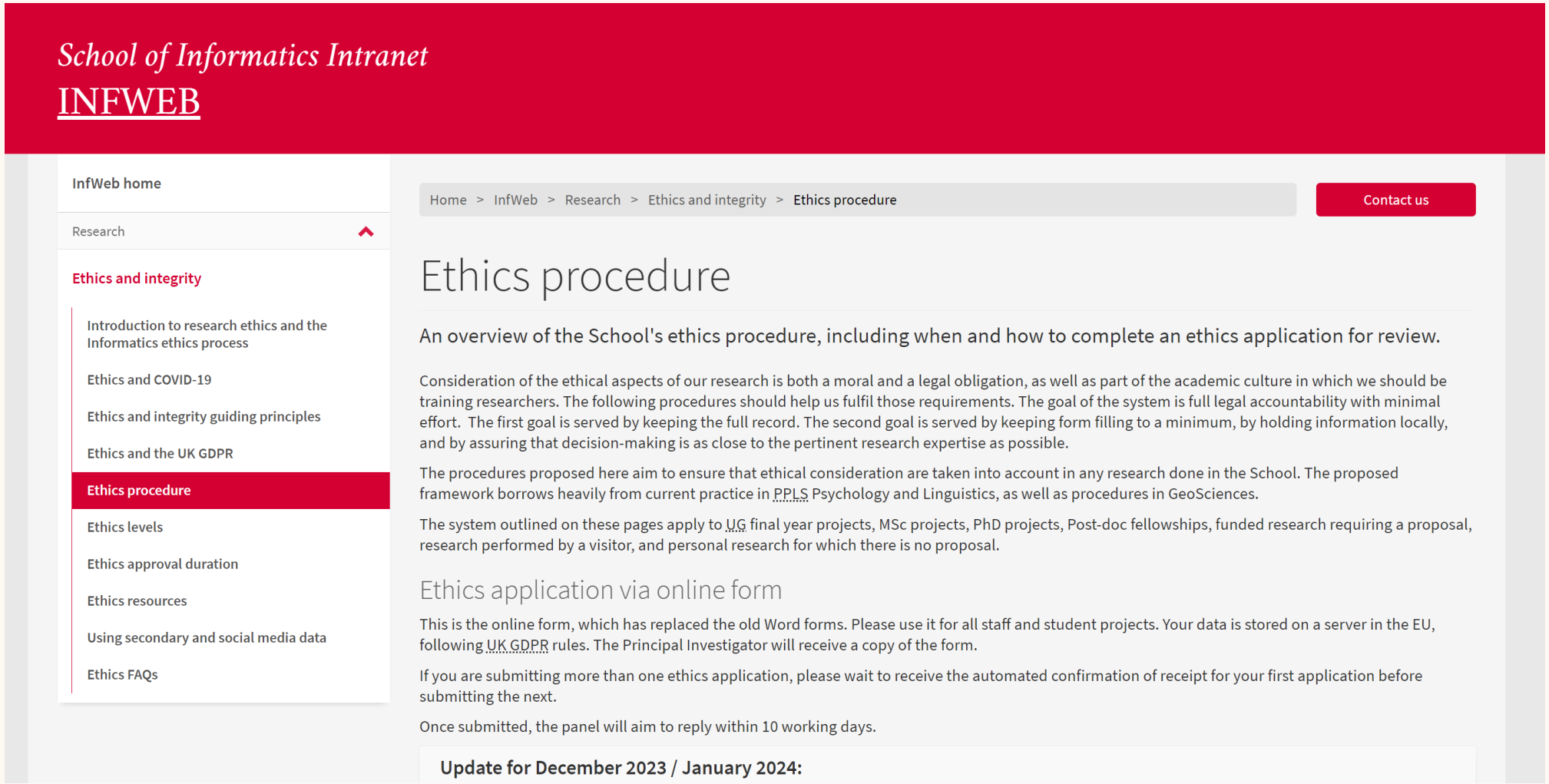
- Vulnerability: the weakness of X (system/human) that can be exploited
  - The program is overprivileged to access things
  - The user reuses their password across applications
- Threat is an action performed by the adversary to damage the asset by exploiting a vulnerability
- Risk = asset X threat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

Study and Analysis Methods

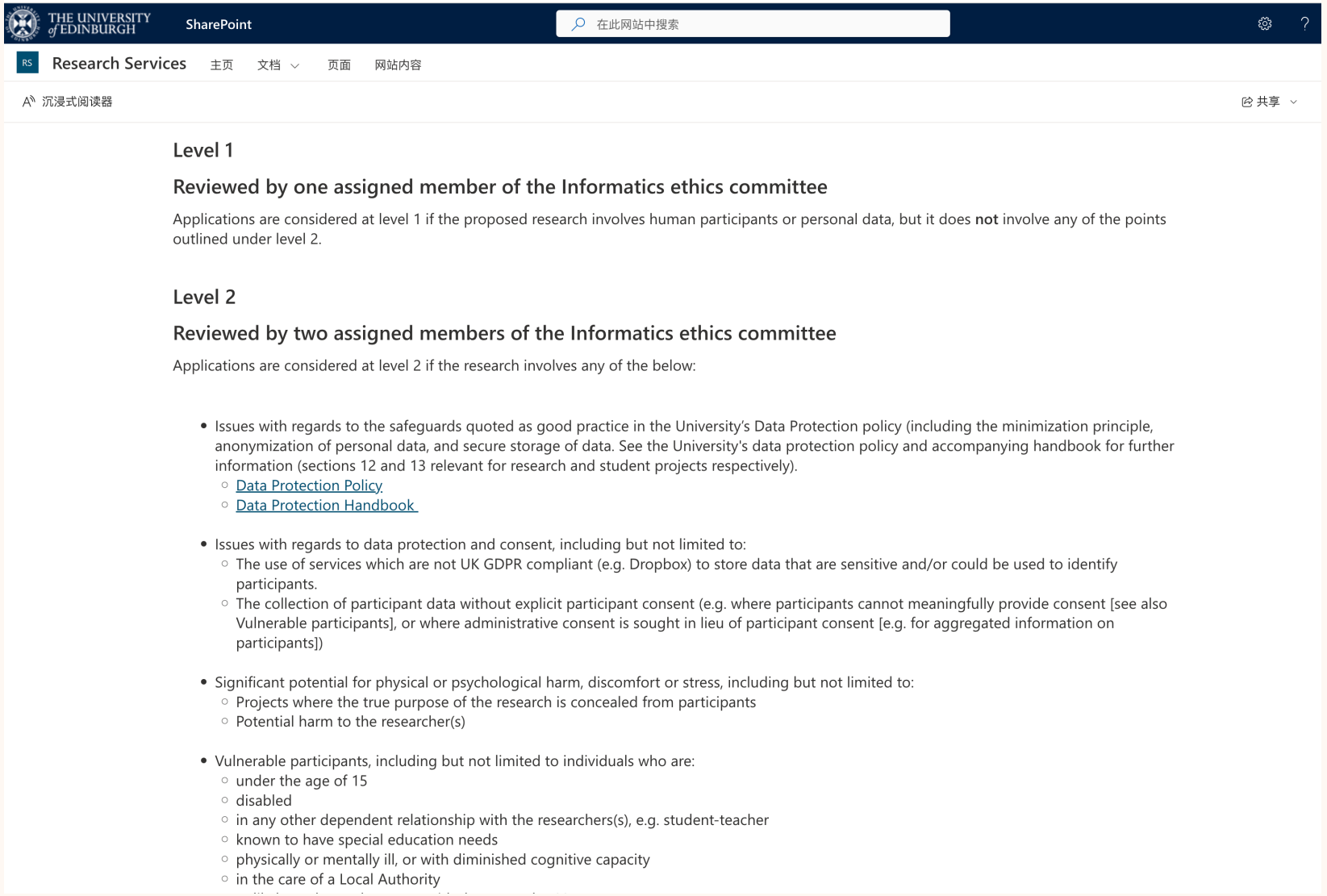
Project lifecycle



Ethics guidelines



Ethics guidelines



Level 1

Reviewed by one assigned member of the Informatics ethics committee

Applications are considered at level 1 if the proposed research involves human participants or personal data, but it does **not** involve any of the points outlined under level 2.

Level 2

Reviewed by two assigned members of the Informatics ethics committee

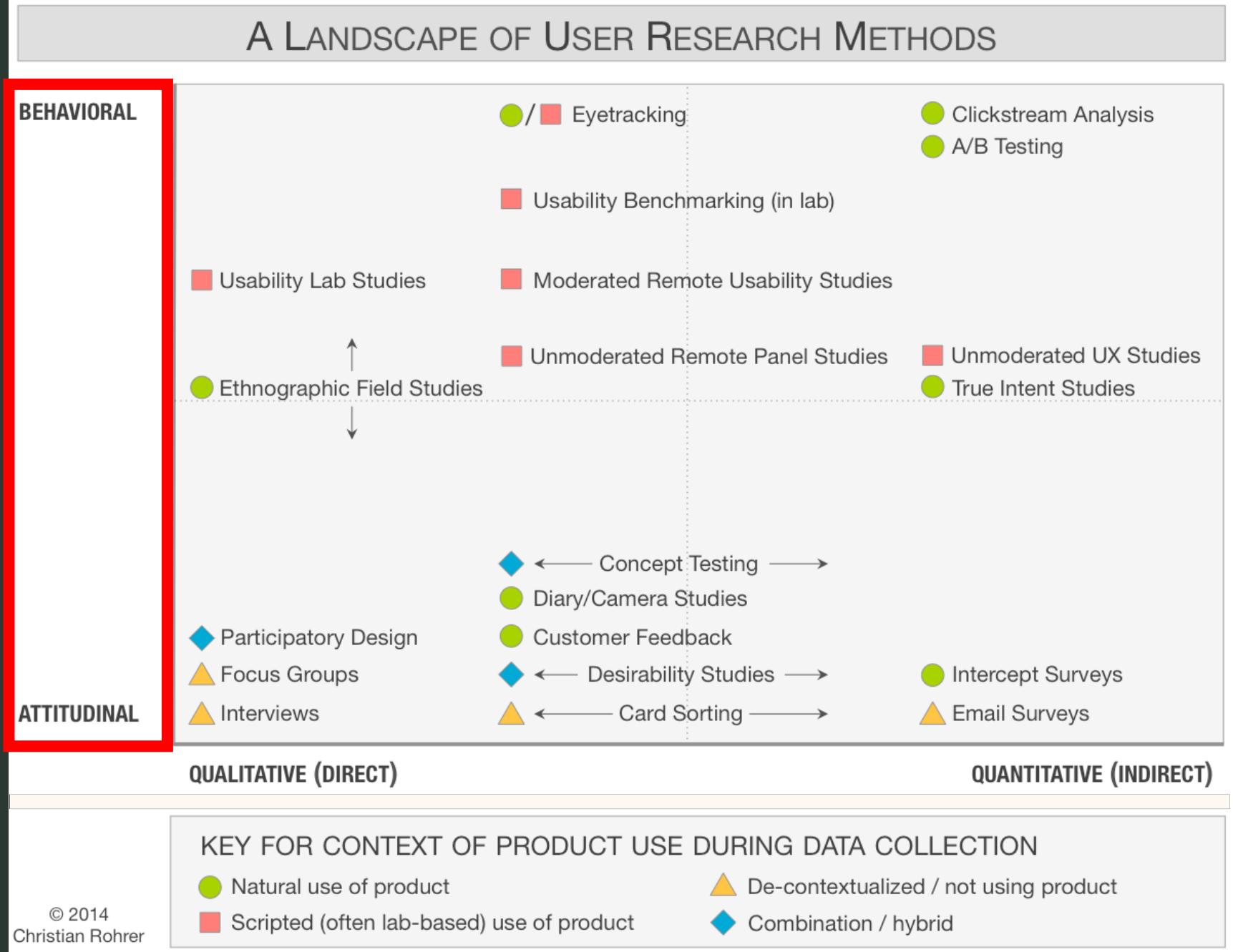
Applications are considered at level 2 if the research involves any of the below:

- Issues with regards to the safeguards quoted as good practice in the University's Data Protection policy (including the minimization principle, anonymization of personal data, and secure storage of data. See the University's data protection policy and accompanying handbook for further information (sections 12 and 13 relevant for research and student projects respectively).
  - Data Protection Policy
  - Data Protection Handbook
- Issues with regards to data protection and consent, including but not limited to:
  - The use of services which are not UK GDPR compliant (e.g. Dropbox) to store data that are sensitive and/or could be used to identify participants.
  - The collection of participant data without explicit participant consent (e.g. where participants cannot meaningfully provide consent [see also Vulnerable participants], or where administrative consent is sought in lieu of participant consent [e.g. for aggregated information on participants])
- Significant potential for physical or psychological harm, discomfort or stress, including but not limited to:
  - Projects where the true purpose of the research is concealed from participants
  - Potential harm to the researcher(s)
- Vulnerable participants, including but not limited to individuals who are:
  - under the age of 15
  - disabled
  - in any other dependent relationship with the researchers(s), e.g. student-teacher
  - known to have special education needs
  - physically or mentally ill, or with diminished cognitive capacity
  - in the care of a Local Authority

https://uoe.sharepoint.com/sites/inf-researchservices/SitePages/Ethics-levels.aspx

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

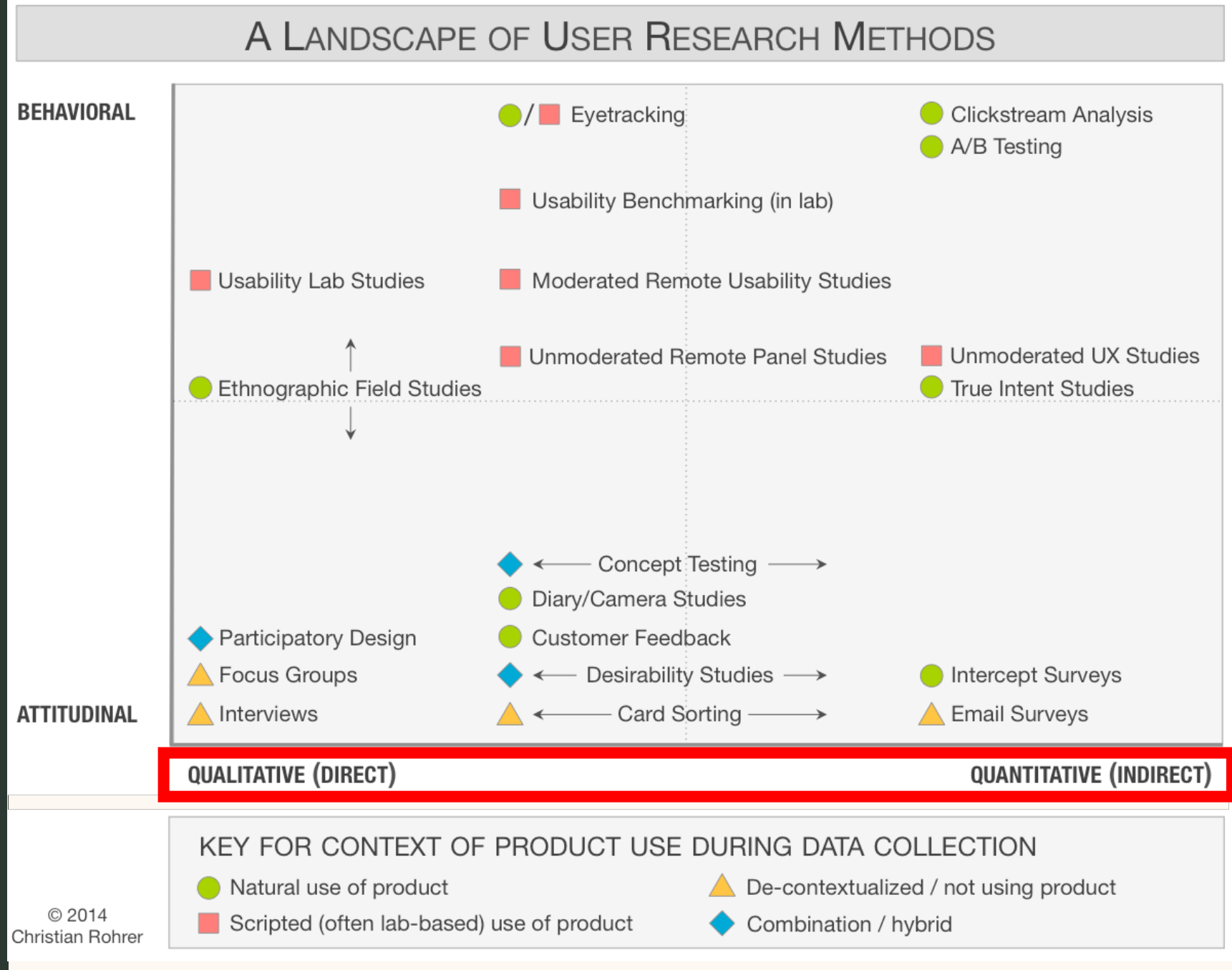
Attitudinal – measures what people say they think or how they say they behave.



https://www.nngroup.com/articles/which-ux-research-methods/

Qualitative – unstructured data such as natural language.

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



https://www.nngroup.com/articles/which-ux-research-methods/

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 unatural
  - (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/

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.

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?

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

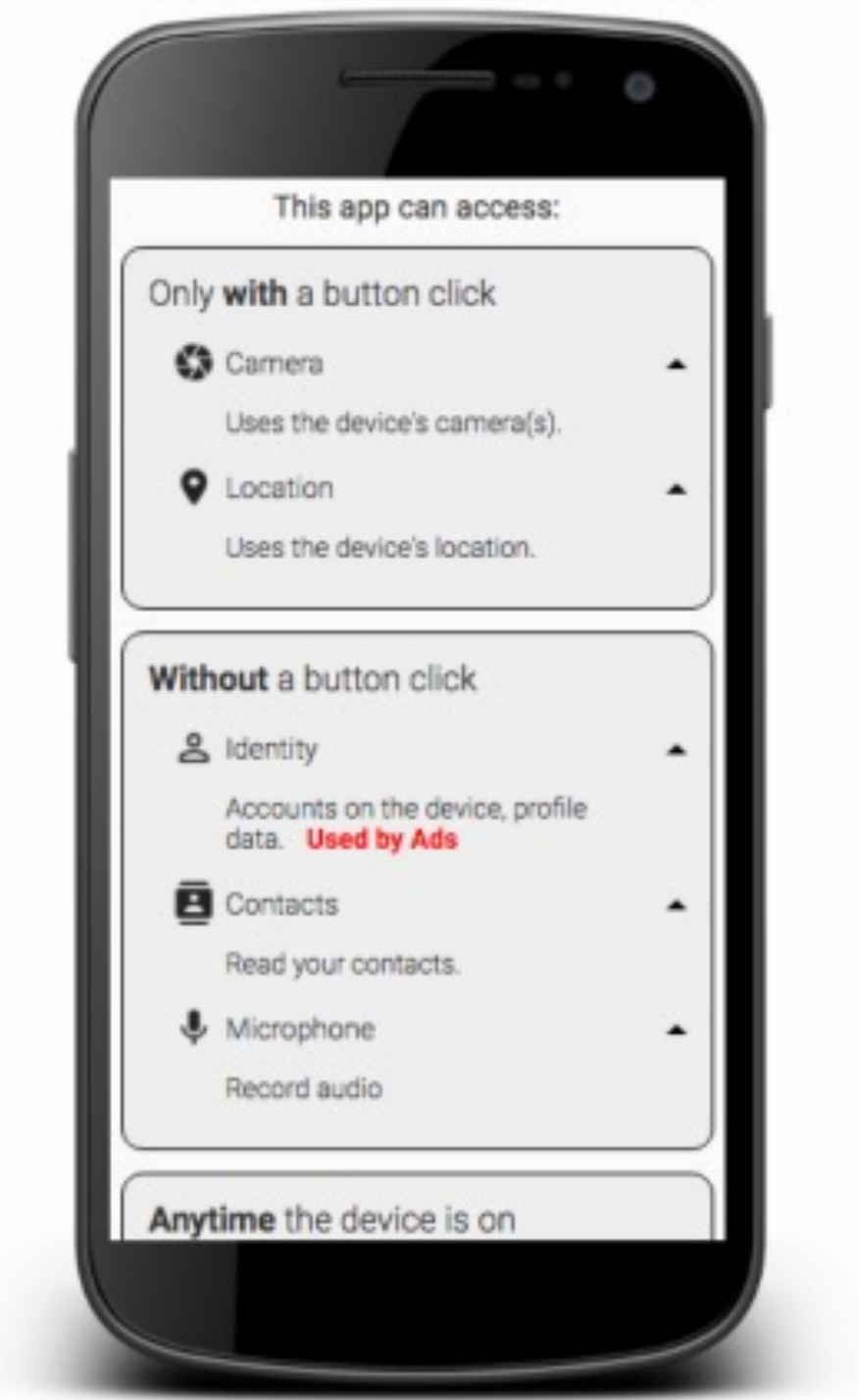
- Numeric
  - **Continuous** – Any value on the range is possible including decimal (1-5)
  - **Discrete** – Only certain values on the range are possible (1,2,3,4,5)
  - **Interval** – Only certain values on the rage are possible and each has equal distance from its neighboring values (strongly agree, 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)



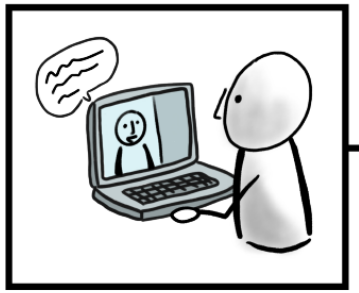
Inductive coding vs deductive coding

- **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)

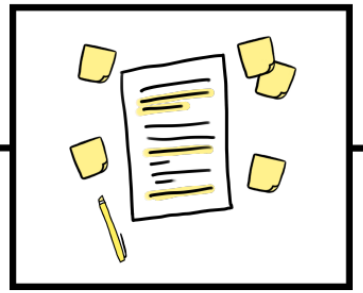
6 Steps to Doing a Thematic Analysis

STEP 1
Gather your data.

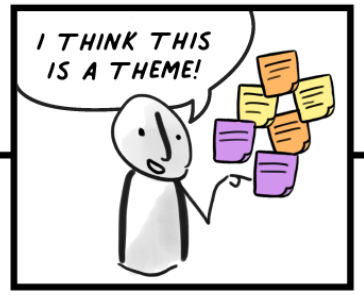


STEP 2
Read all your data from beginning to end.

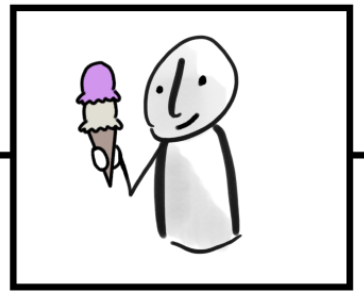
STEP 3
Code the text based on what it's about.



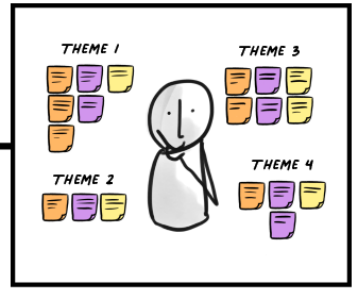
STEP 4
Create new codes to encapsulate potential themes.



STEP 5
Take a break for a day.



STEP 6
Evaluate your themes for good fit.

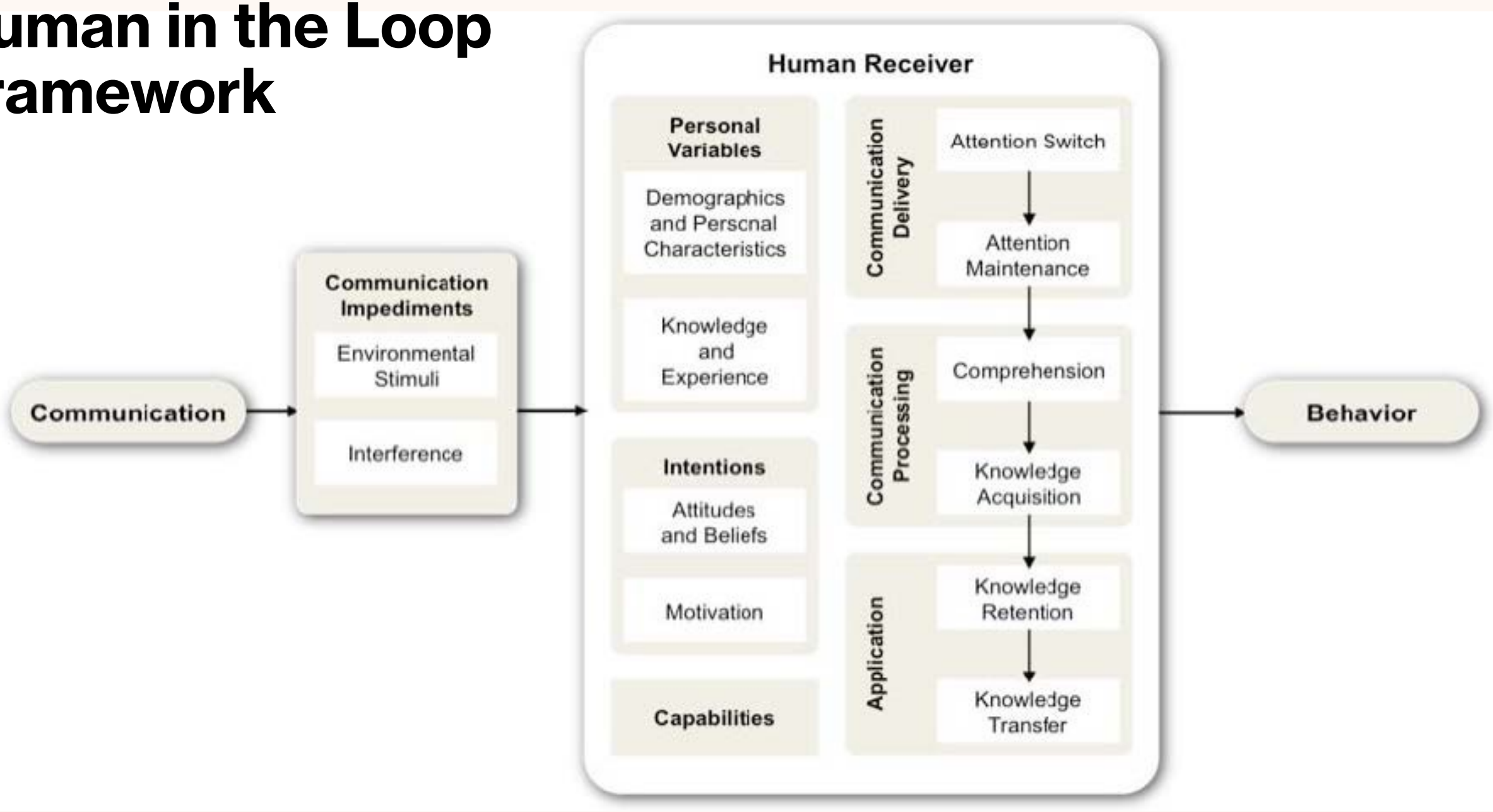


REPEAT AS NEEDED

NNGROUP.COM NN/g

Framework and Topics

Human in the Loop Framework



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

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

- NEAT
- SPRUCE
- Privacy by design
- Contextual integrity
- ....

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

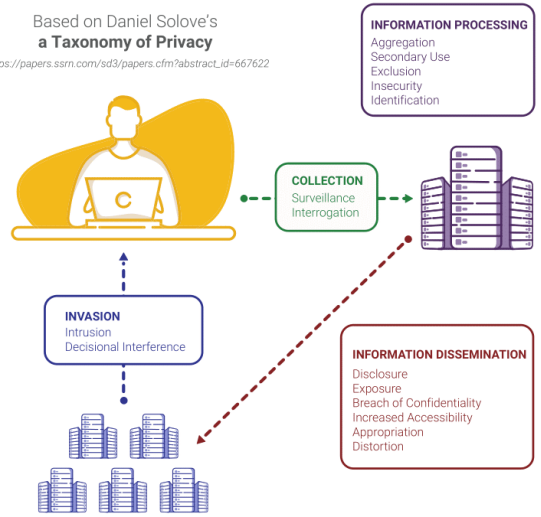
INTRUSION
Disturbing a person's tranquility or solitude

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

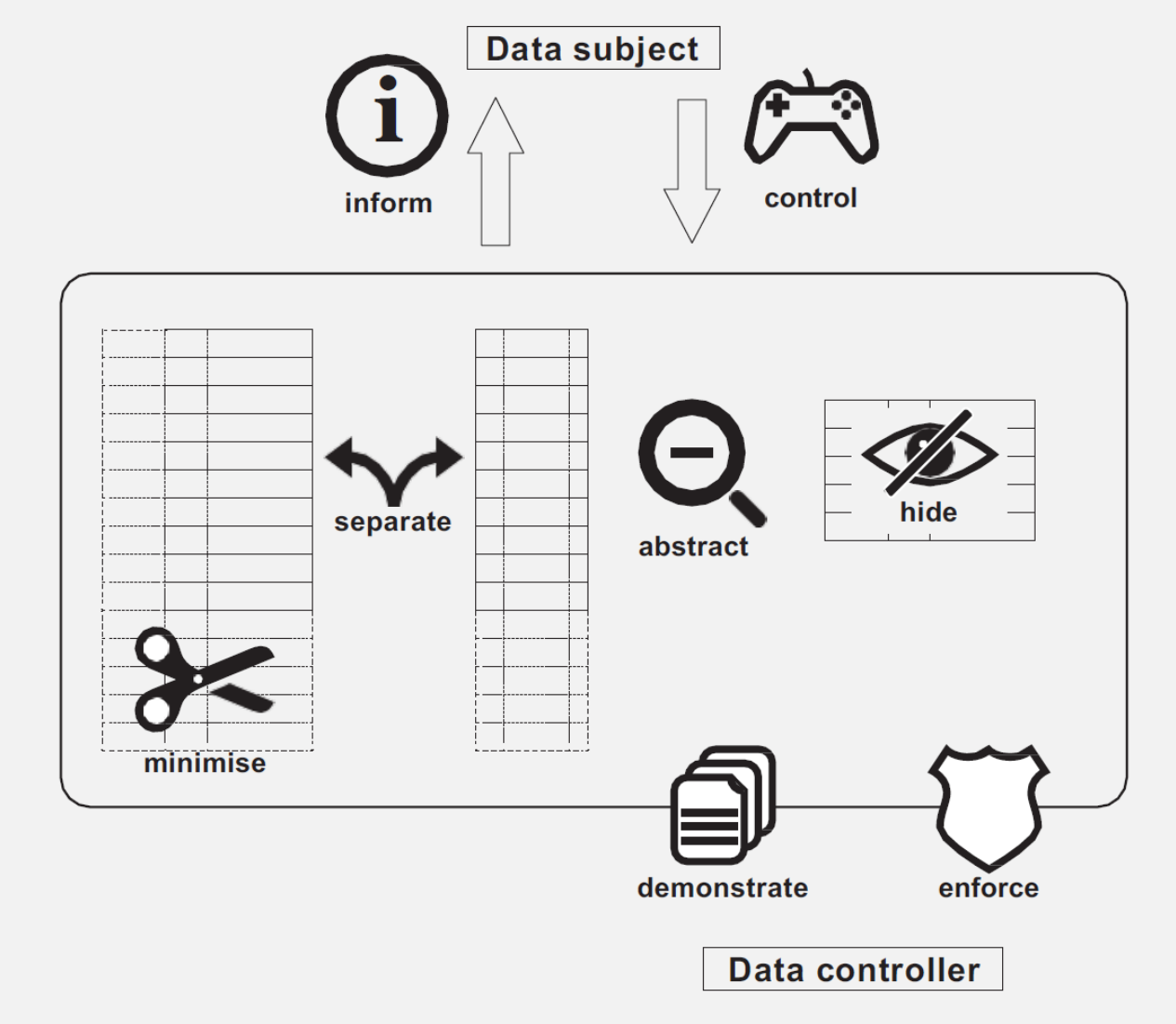
A creditor reporting a paid bill as unpaid to a credit bureau.

Version 6 (2022)

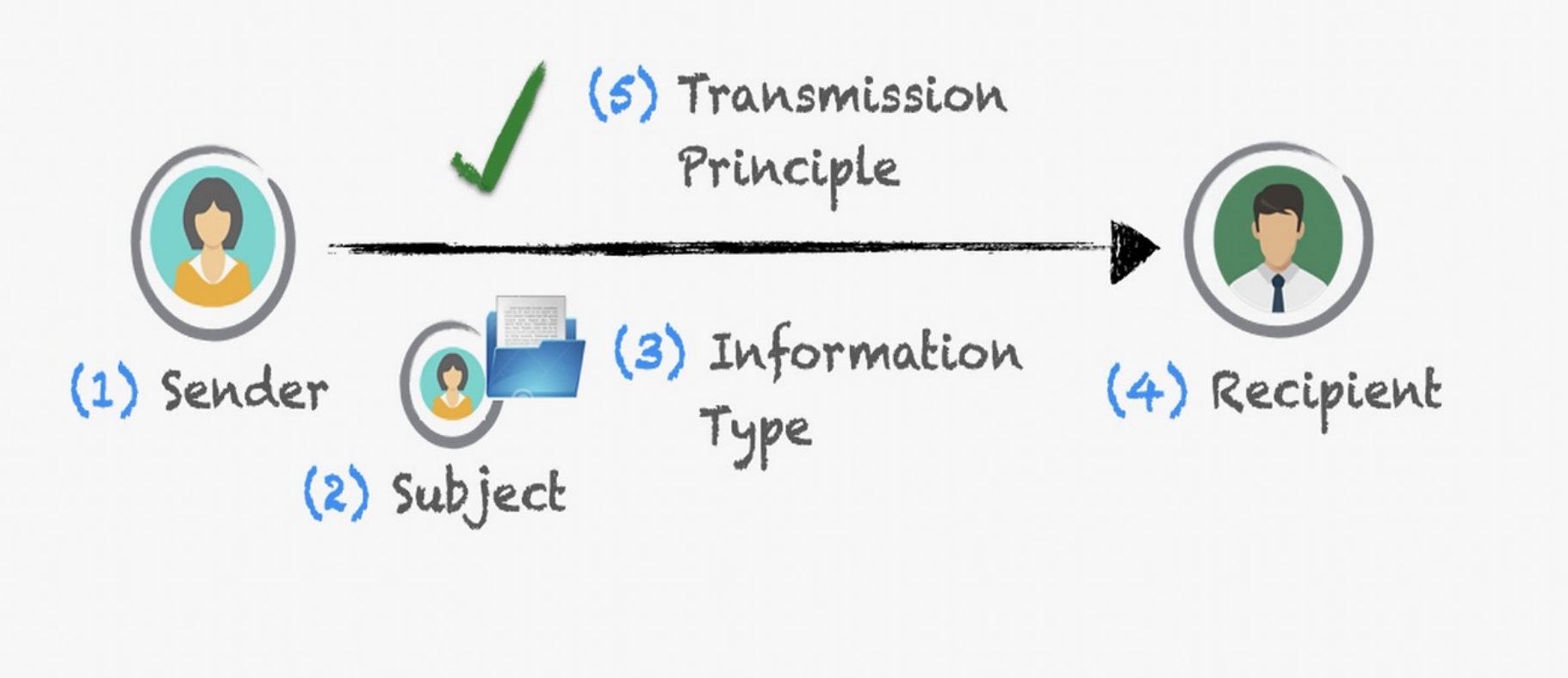
PRIVACY BY DESIGN

https://privacybydesign.training

Privacy by design – strategies

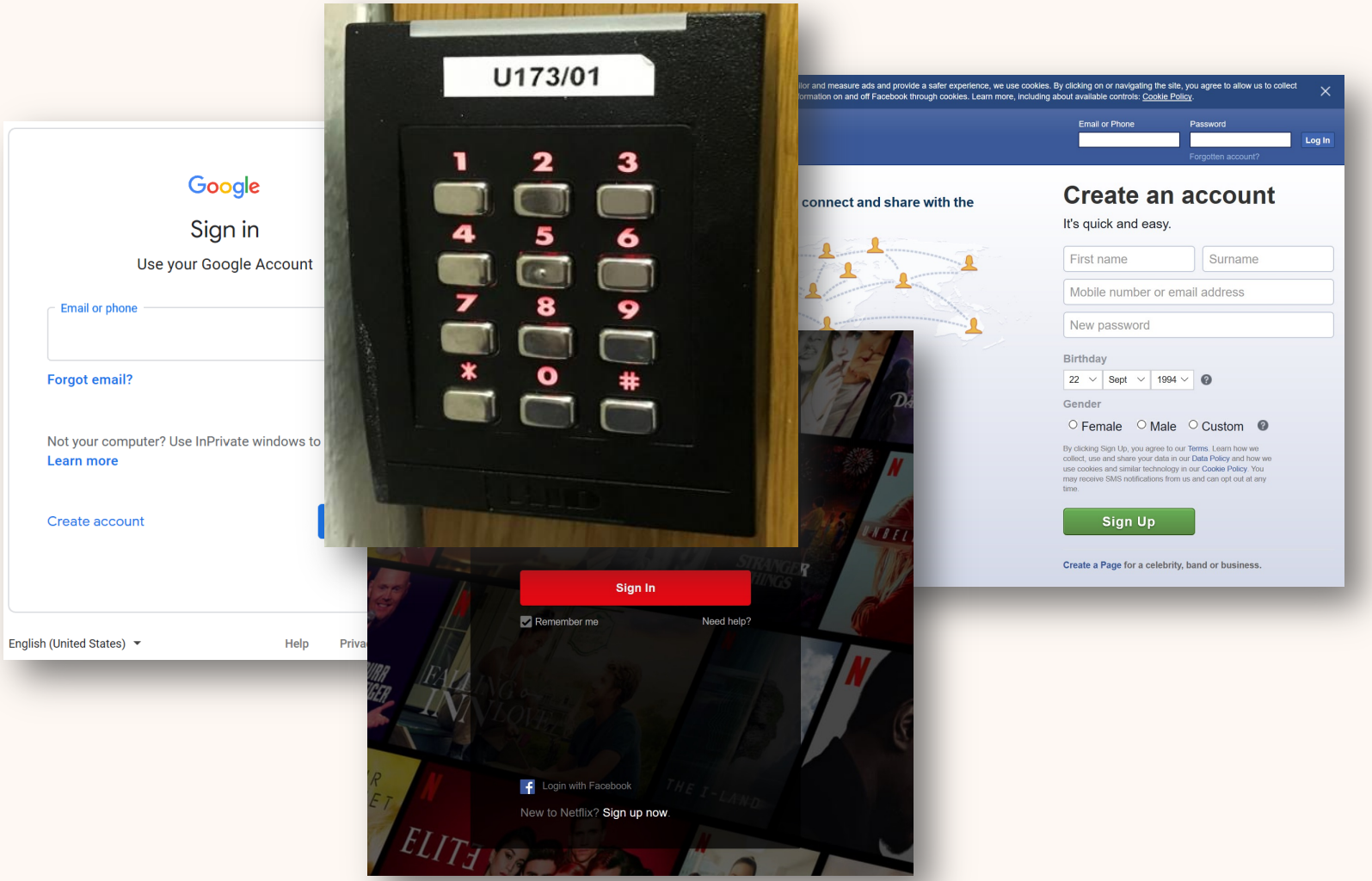


Contextual integrity

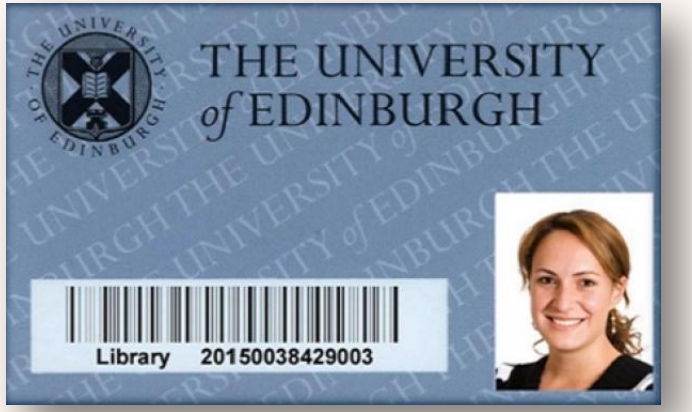


https://www.dli.tech.cornell.edu/post/privacy-policies-as-contextual-integrity-beyond-rules-compliance

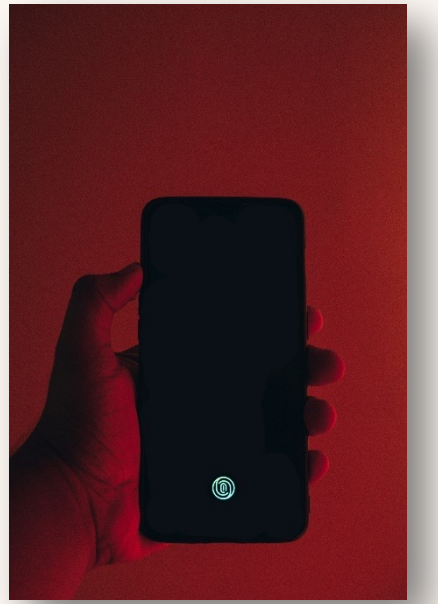
Authentication



What you know



What you have



Who you are

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

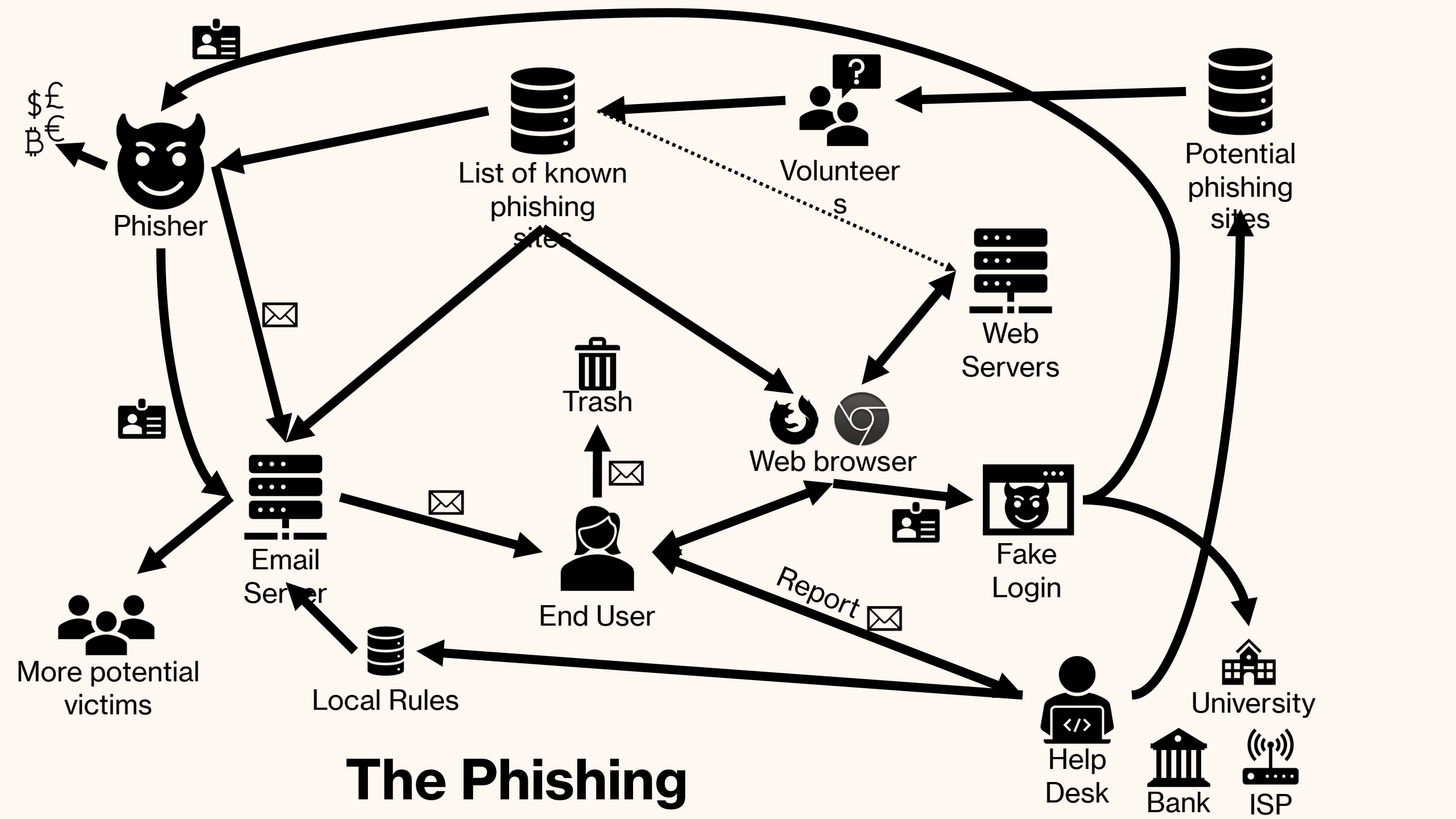
Protects against attacks

- 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

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



The Phishing

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

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

Privacy space framework

Category	Description	Examples
Awareness	Informative	Display information about trackers on current webpage, whether location is being sent
Detection	Actively look for problems	Find trackers on current webpage
Prevention	Used as a precaution	Encryption tools, anonymity tools
Response	Taking action after a problem is detected	Tracking blocker
Recovery	Help you get back to normal	Patching bugs

Benjamin Brunk. A user-centric privacy space framework. In Cranor and Gafinkel, eds. *Security and Usability*. O'Reilly 2005. p. 401-420.

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.”

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!


wemo
Connected to
3G
Attempting to connect, please wait...
1:15
The Internet
Belkin
Other Servers
wemo

The Menlo Report (2012)

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.*

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….

Some ethical practices for social media research

- Follow the terms of use
- Obtain informed consent when possible
- Check our ethics guidelines for more! https://resource.ppls.ed.ac.uk/lelethics/index.php/frequently-asked-questions/research-with-social-media-data/

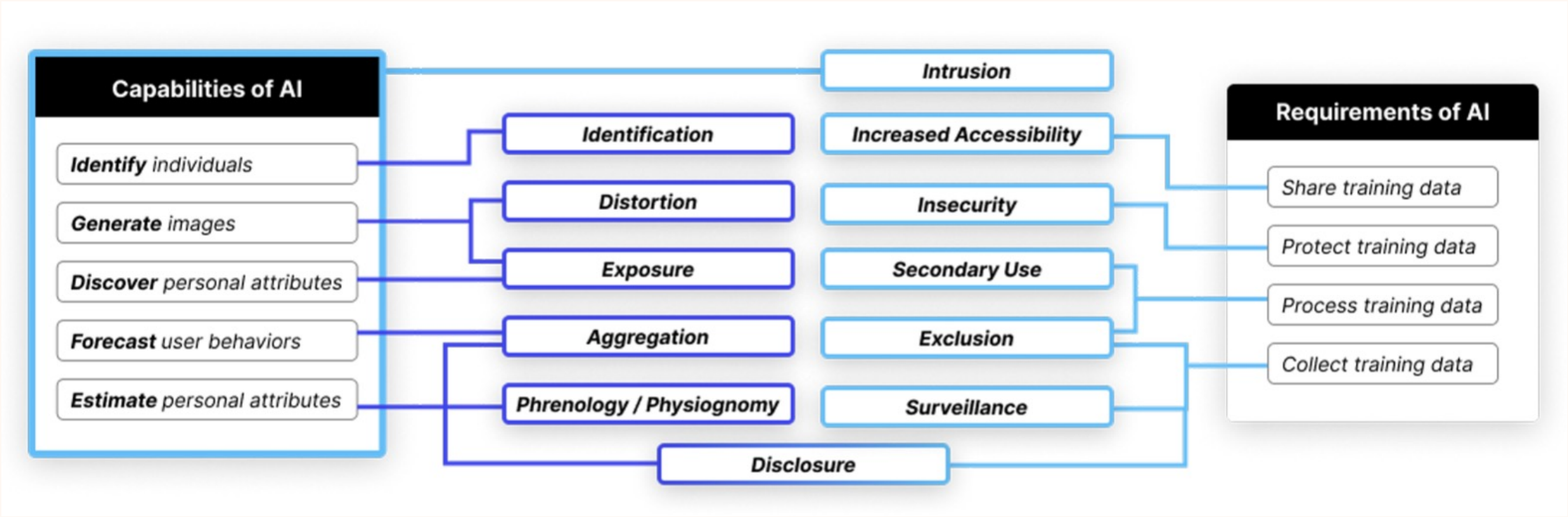
Safe practices for at risk users

Category	ID	Digital-safety practices	Example papers
Professional partnerships & Ethical review	SP1	Elicit expert (academic) opinion on topic area	[17, 31, 67, 70, 82, 83, 112, 132, 136]
	SP2	Form professional partnerships (e.g., support services for at-risk users)	[44, 52, 72, 80, 82, 99, 105, 124, 134, 145]
	SP3	Invite and include an at-risk user to join research team	[17, 83, 97, 112]
	SP4	Seek external (non-institutional) ethical review approval or monitoring	[30, 43, 44, 78]
Positionality & Participant engagement	SP5	Build rapport with participants for understanding digital-safety needs	[1, 33, 34, 38, 73, 91, 97, 113, 137]
	SP6	Conduct pilot studies with general (non-at-risk) users	[5, 30, 33, 64, 67, 95, 101]
	SP7	Conduct studies with proxies for at-risk users (e.g., advocacy groups)	[2, 24, 33, 70, 74, 104, 132]
	SP8	Include researchers whose identities affirm participants'	[2, 6, 38, 64, 97, 110, 112, 113, 132, 134]
	SP9	Practice responsiveness in data collection sessions to potential threats	[3, 38, 49, 89, 100, 101, 124, 127, 128, 132]
	SP10	Provide professional therapeutic support for emotive topics	[7, 11, 30, 48, 95, 100, 101, 115, 144]
	SP11	Train team members in working with digital-safety risks	[7, 38, 115, 121]
Privacy-preserving data collection	SP12	Discourage participant self-disclosure (e.g., personal histories)	[1, 7, 25, 52, 70, 75, 118, 123, 137, 144]
	SP13	Focus data collection on supporting participant safety needs	[24, 34, 38, 66, 81, 97, 120, 121, 123, 129]
	SP14	Do not collect or ask for participant demographic data	[17, 26, 64, 83, 84, 104, 120, 124, 136, 145]
	SP15	Do not collect personally identifiable information on participants	[30, 43, 44, 52, 54, 58, 73, 85, 95, 143]
	SP16	Implement protocols for researchers to prevent stalking by adversaries	[30, 60, 80]
	SP17	Separate potential threats from at-risk users during data collection	[6, 72, 88, 96, 97, 100, 110, 115]
	SP18	Permit participants to contribute false information (e.g., pseudonyms)	[17, 54, 58, 78, 83, 100]
	SP19	Offer participants many modalities to contribute (e.g., audio, notes)	[4, 7, 24, 34, 57, 67, 90, 107, 117, 130]
	SP20	Secure confidentiality and privacy of online and in-person research sites	[6, 24, 30, 43, 44, 77, 100, 113, 134, 139]
Secure data storage & processing	SP21	Implement strict data access control measures for research data	[1, 7, 34, 51, 80, 112, 134, 136, 139, 147]
	SP22	Redact participant information prior to analysis by research team	[59, 86, 95, 107, 114, 128, 130, 140, 143, 156]
	SP23	Use encryption for research data in-transit and at-rest	[52, 60, 75, 85, 86, 87, 101]
	SP24	Use non-encrypted safe storage for research data in-transit and at-rest	[7, 30, 34, 90, 97, 114, 130, 132]
Researcher accountability	SP25	Conduct data collection sessions around participant schedules	[1, 35, 54, 65, 97, 111, 120, 128, 139]
	SP26	Offer formal proof of identity as professional researchers	[70, 82, 97, 112, 114, 115]
	SP27	Only use data from publicly accessible sites (e.g., no authorization)	[11, 32, 40, 97, 103, 138, 147, 155]
	SP28	Provide proportional incentives to participants for contributions	[54, 64, 72, 73, 82, 110, 134, 139, 145, 151]
	SP29	Be transparent with participants about risks incurred by research	[24, 26, 38, 54, 57, 69, 95, 110, 113, 128]
Sharing & evaluating deliverables	SP30	Do not attribute reported data contributions with participant identifiers	[7, 8, 9, 34, 55, 84, 114, 117, 134]
	SP31	Do not report participant demographics in research deliverables	[17, 24, 43, 77, 78, 83, 117, 120, 144, 145]
	SP32	Do not report participant names, pseudonyms, or identifiers	[9, 48, 71, 78, 101, 114, 121, 143, 145, 155]
	SP33	Paraphrase or withhold sources of data (e.g., websites they use)	[2, 9, 17, 40, 59, 69, 78, 123, 136, 155]
	SP34	Evaluate research deliverables for adversarial feedback or education	[34, 38, 44, 59, 82, 113]
	SP35	Selectively edit participant data in research deliverables	[7, 9, 11, 40, 55, 124, 139, 140, 150, 151]
	SP36	Provide participants control of their contributions (e.g., permit redaction)	[7, 47, 54, 75, 91, 113, 114, 117, 136]

Safe practices for at risk users

ID	Strategy title	Description	Example digital-safety practices
S1	Engage experts early	Consult or partner with domain experts from the beginning to inform and help facilitate safe research plans.	SP1, SP2, SP3, SP4, SP10
S2	Assess and mitigate risks by threat modeling	Apply the S&P practice of threat modeling to research protocols, and continuously update threat models to guide ongoing safety mitigations.	SP11, SP16, SP17, SP20
S3	Select the lowest risk method that addresses the research goals	Before soliciting at-risk users for high-touch methods like interviews, consider proxies (e.g., advocates), or indirect methods (e.g., online measurement).	SP6, SP7, SP12, SP14, SP15, SP27
S4	Respect that at-risk users self-manage risk	At-risk users are often experts in managing their safety risks. Give them choice in how they engage with research safety protocols, and respect the choices they make.	SP9, SP18, SP19, SP25, SP26, SP29
S5	Be an advocate for at-risk users' needs	Research, by its nature, can be extractive. Build reciprocity with at-risk users, and work to help them achieve their goals.	SP5, SP8, SP13, SP28, SP36
S6	Handle data and publications carefully	Data collection and analysis should follow security best-practice, and publications should avoid revealing identities or informing adversaries.	SP21, SP22, SP23, SP24, SP30, SP31, SP32, SP33, SP34, SP35

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


Capabilities of AI
Identify individuals
Generate images
Discover personal attributes
Forecast user behaviors
Estimate personal attributes
Identification
Distortion
Exposure
Aggregation
Phrenology / Physiognomy
Disclosure
Intrusion
Increased Accessibility
Insecurity
Secondary Use
Exclusion
Surveillance
Requirements of AI
Share training data
Protect training data
Process training data
Collect training data