Graduation Thesis

2025

Envisioning future experience for online data privacy

Author
Haoyue Sheng

Master thesis
Msc. Design for interaction
Faculty of Industrial Design Engineering
Delft University of Technology

Graduation Committee
Chair
Prof. Giulia Calabretta
Faculty of Industrial Design Engineering

Mentor
Dr. Davide M. Parrilli
Faculty of Industrial Design Engineering

Phd. Michelle Winkelsdorf
Faculty of Industrial Design Engineering

August 2025

Preface

The past few months for me with this project have been a winding, challenging, and studying road. It was a journey full of uncertainty, reflection, and persistence. It has also been an unforgettable process, one that not only deepened my academic understanding but also pushed me to grow personally as a designer. I'm happy to share the outcome of this project.

First and foremost, I would like to express my complete heartfelt gratitude to my supervisors, Giulia and Davide. Without your dedicated coaching, encouragement, and patience, I would not have been able to finalize this project. Thank you for constantly reminding me to look at the bigger picture, helping me capture the essence of my ideas, and supporting me through the ups and downs of the writing process. I am fortunate to work with my empathic chair and mentor.

Secondly, I would like to thank all the participants who contributed to this research. Your insights and great feedback were invaluable. I sincerely appreciate the time and openness you gave me. The voices shaped this project in profound ways.

Besides, I am deeply grateful to my beloved family and all my friends for lifting me when I doubted myself and simply for being there. The encouragement and companionship kept me going.

Lastly, to everyone who has helped me along the way during my master's studies: thank you! I will carry your kindness with me as I move forward.

Take a step toward a better world in online data privacy, no matter how small that step might be. What we need most is continuous reflection, learning, and improvement, and I hope this work contributes to that ongoing journey.

Enjoy reading!

Author
Haoyue Sheng

Master thesis
Msc. Design for interaction
Faculty of Industrial Design Engineering
Delft University of Technology

Graduation Committee
Chair
Prof. Giulia Calabretta
Faculty of Industrial Design Engineering

Mentor
Dr. Davide M. Parrilli
Faculty of Industrial Design Engineering

Phd. Michelle Winkelsdorf
Faculty of Industrial Design Engineering

August 2025

Summary

Data privacy has become increasingly complex and critically urgent in today's digital society. As individuals engage with various online services, vast amounts of personal data are continuously collected and analyzed through different digital platforms and services. Even with the protection of GDPR in the EU, privacy risks persist in everyday life, which could become more subtle and complex due to the rapid development of the socio-technological context.

While privacy goes beyond mere compliance, it's about empowerment. Privacy threats are deeply embedded in everyday digital experiences, often invisible, making it difficult for individuals to recognize them. Besides, privacy is inherently subjective, meaning its significance and interpretation vary widely among individuals. Traditional privacy research, often grounded in legal or technical compliance, tends to overlook these personal, situated experiences. **This project argues that it is crucial to help people become aware of and reflect on privacy, as it is essential to developing more nuanced understandings of the concept.**

Additionally, speculative design and future studies played a key role in this project, which were used to challenge conventional thinking and propose a range of alternative futures. Future design and speculative design are used to open up new possibilities for the transformation and innovation of services. In doing so, the work contributes to an evolving body of research that views design as a tool for critique and change, inspiring various future possibilities. **The project advocates for future design practices rooted in individual empowerment and reflective experience.**

Based on these, the study focuses on two interrelated and progressive **objectives**:

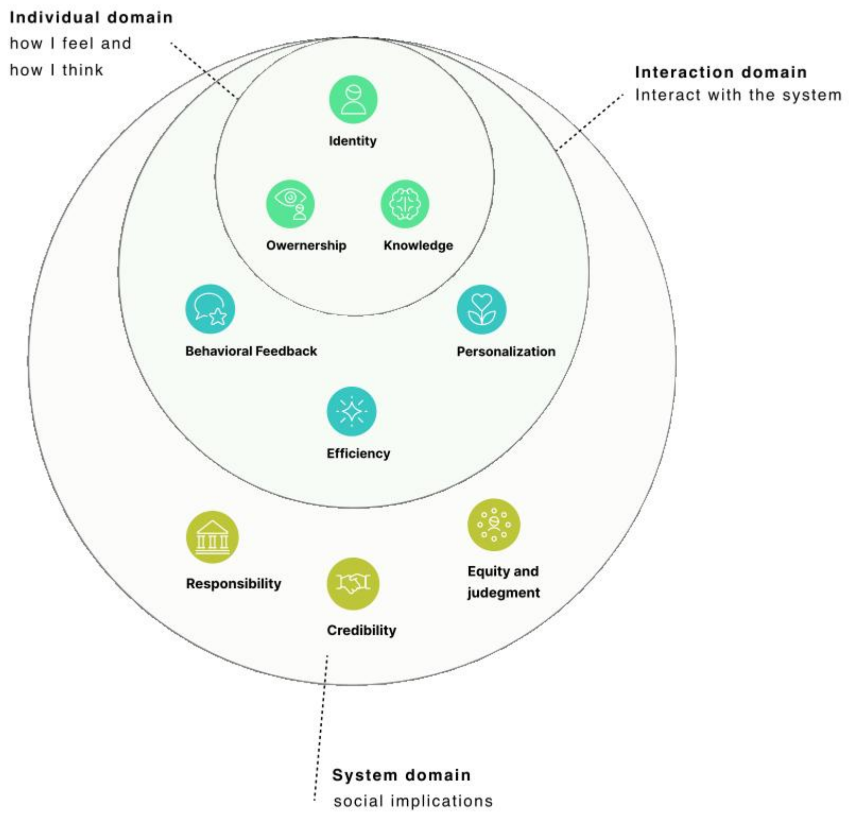
- Raise awareness and gather collective insights
- Envision the alternative future intervention of online privacy in users experience

To achieve these goals in the research, the research unfolds in **three primary phases**:

- **Grounding privacy risks in context**: Understanding the risks within the current socio-technical context of online privacy. The findings include privacy threats towards individuals developed from the theories, case study grounding in real-world risks, and individual concerns, as well as insights from an auto-ethnography study.

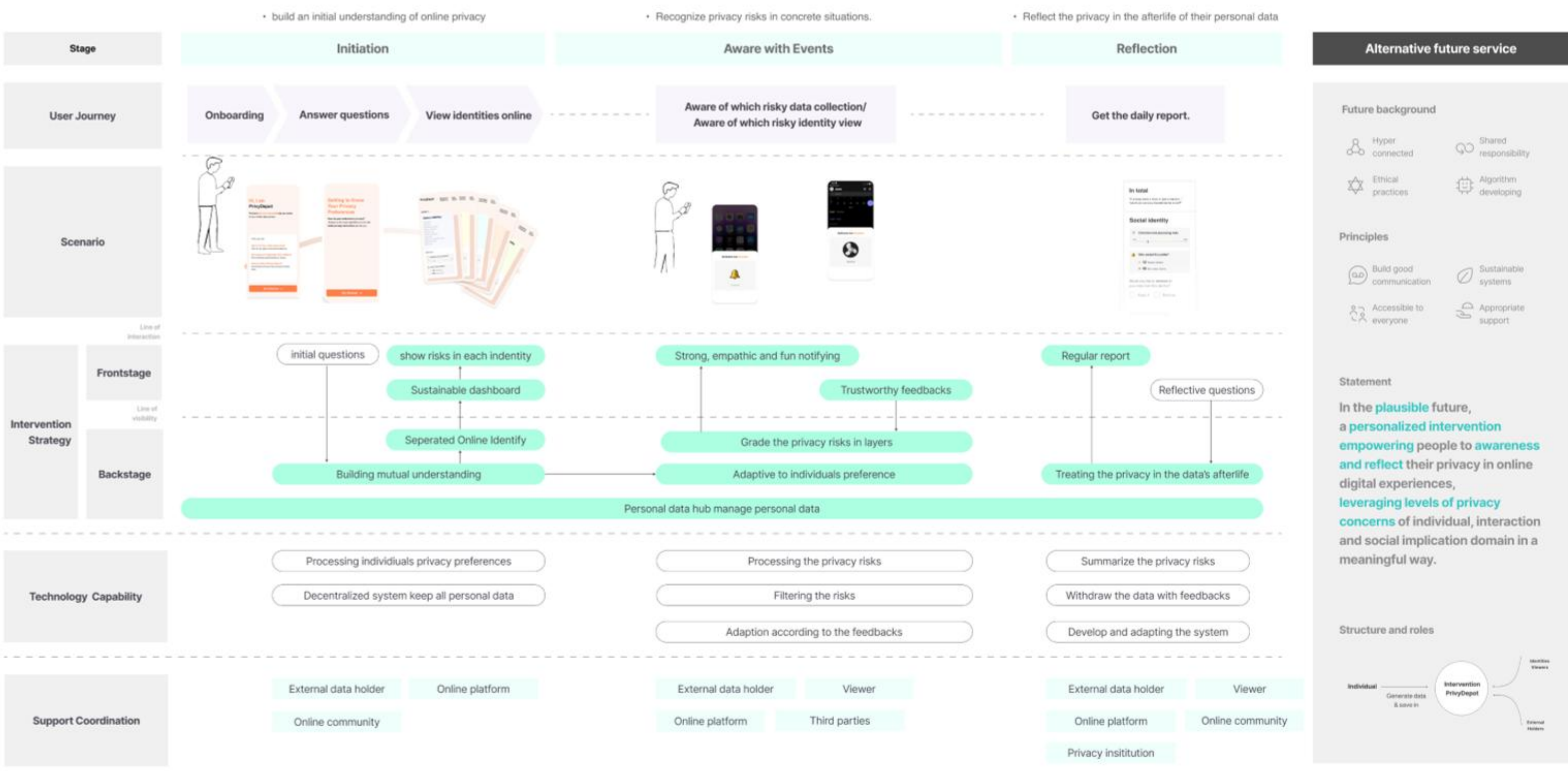
- **Raise awareness**: we expand the research by exploring "preposterous futures" in the collection, processing, and storage stages of data practice. Set in "preposterous futures", three speculative design artifacts were developed based on the collection, processing, and storage stages of data practice, with follow-up participatory workshops to raise awareness. The findings reveal collective concerns about individual future privacy, which helped us build a deeper understanding of online privacy.

- **Towards a meaningful future intervention**: Leveraging collective insights, we explore plausible future possibilities, where insights collected from individuals are translated into concrete future service and design concepts. In this phase, the alternative future intervention "Echoes of Privacy" is developed. Set in a near-future world, this intervention envisions a new paradigm of sustainable privacy that, with the proper structure, could empower individuals. The alternative service can be accessed by participants with a tangible prototype and a future narrative.



Collective findings: Privacy concerns map

Figure 1 : "preposterous futures" artifacts and the follow-up workshop findings



In the plausible future, a personalized intervention empowering people to awareness and reflect their privacy in online digital experiences, leveraging levels of privacy concerns of individual, interaction and social implication domain in a meaningful way.

Figure 2: "Plausible futures" service blueprint

Content

01

Introduction

This chapter provides an overarching introduction to this project, which includes the following parts:

- General background
- Opportunity
- Research question
- Approach
- Project journey

General Background

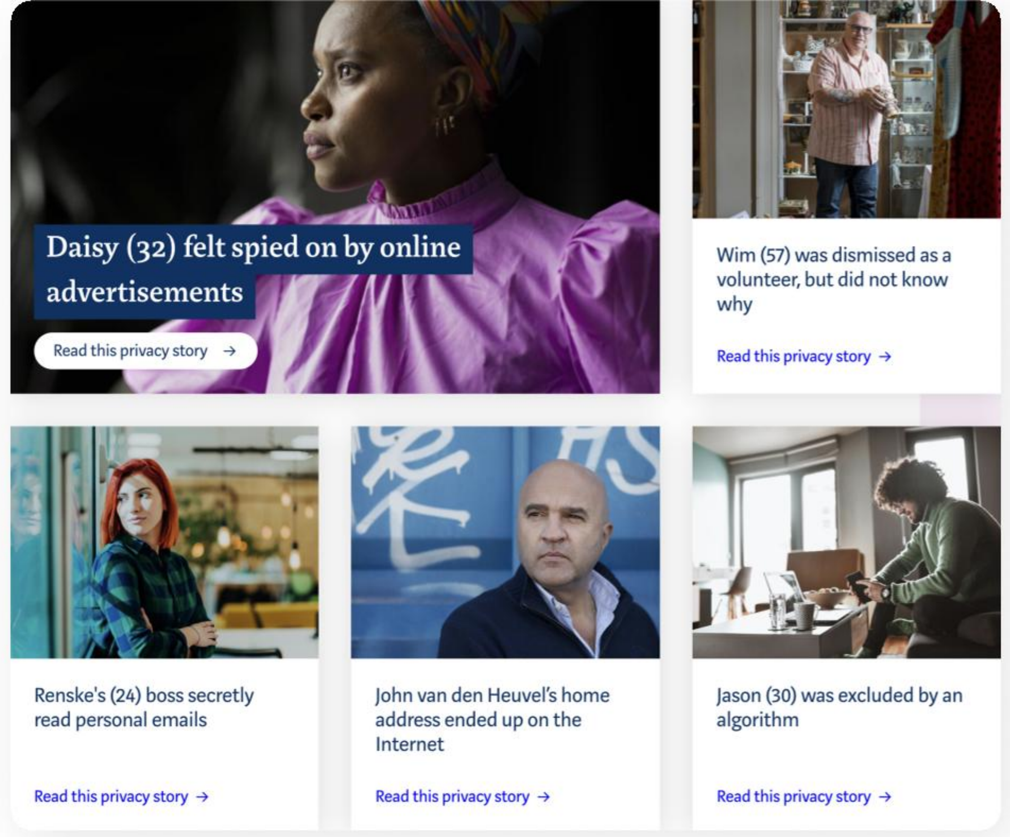
Online privacy in EU

Online digital services, eg, social media, e-commerce platforms, streaming apps, and e-health systems, have become deeply embedded in our everyday lives. These services are aimed at online users, which individuals offer, offering convenience and personalization, yet they continuously collect and process vast amounts of personal data behind the scenes. The paradox of modern life is that our daily participation in these systems fuels a data-driven infrastructure whose workings pose broadly privacy risks (Yu, S., 2016).

The context of this project is online digital privacy in the European Union. The legal protection of digital privacy is primarily grounded in the General Data Protection Regulation (GDPR,2018). The GDPR grants individuals a set of robust data rights, including the ability to access, correct, delete, and limit the processing of their data (GDPR, 2018).

Despite the support from legal foundations, online digital privacy violations remain widespread in practice. Personal data continues to face significant risks. We use the cases in the Netherlands as examples. According to reports from the Autoriteit Persoonsgegevens (AP), the Dutch Data Protection Authority, over 25,000 personal data breaches were officially reported in 2023 alone. These violations have ranged from targeted online cyberattacks by hackers who intend to steal personal data to accidental leaks by some online companies, government institutions, or public institutions. The individual rights of online data privacy have been harmed in practice. Another notable case occurred in 2024, when CoronaLab, a primary COVID-19 testing provider, exposed a serious personal data incident due to a misconfigured database. This time, an online data breach affected more than 1.3 million individuals, posing a risk of exposing sensitive personal and health-related information (Fowler, 2024). In society, there is a strong resistance to individual surveillance in the EU. One example is the 2018 public referendum against the "Sleepwet" (the Intelligence and Security Services Act), where a majority of voters opposed expanded surveillance for intelligence agencies. The SyRI case (System Risk Indication) also demonstrates the violation of using personal data collection and analysis (Meuwese, 2018). In 2020, the Dutch institution AP ruled that the government's use of predictive algorithms to detect welfare fraud violated individuals' rights and could have a significant, unintended impact on low-income communities, with negative consequences for both individuals and society (IAPP, 2020).

Overall, these cases reveal a considerable gap between regulatory ideals of online data privacy and actual risks to individuals in practice. **In this project, we go beyond legal and technical compliance with online privacy and consider how we can empower and impact individuals in real-world settings.**



Daisy (32) felt spied on by online advertisements

Read this privacy story →

Wim (57) was dismissed as a volunteer, but did not know why

Read this privacy story →

Renske's (24) boss secretly read personal emails

Read this privacy story →

John van den Heuvel's home address ended up on the Internet

Read this privacy story →

Jason (30) was excluded by an algorithm

Read this privacy story →

Figure 1.1: Online privacy cases shows on the Persoonsgegevens (AP) website

Opportunity

Individual awareness

While current society consistently expresses concern about online data privacy, a significant lack of awareness persists about the actual risks people face when using digital platforms and online services. The widespread adoption of digital services, especially among younger populations, has normalized constant data exchange, often with a limited understanding of its consequences. Numerous studies have shown that **users interact with websites and apps without being aware of how their data is collected and processed** (Kokolakis, 2017; Graeff & Harmon, 2002; Pötzsch, 2008).

According to preliminary literature findings, a lack of privacy awareness is not simply a personal neglect, it is a structural issue deeply ingrained in online data systems. We can see several factors linked to this lack of individual awareness. Some aspects are interrelated and could lead to more severe consequences in terms of privacy invasions (Pötzsch, 2008).

Inherent complexity of modern data systems.
One significant factor contributing to unawareness is the complexity of modern data systems, where the data flow is often invisible and the risks are interrelated within this system. The flow of personal data in digital ecosystems is non-linear, continuous, and largely invisible to online end users(Mai, 2016). Unlike physical objects, data leaves no tangible trace; users are often unaware that their data has been collected and processed.

Normalized online experience for individuals
The online experience is embedded in the current online structure, where issues that arise from more profound structural asymmetries, such as information asymmetry (where platforms possess far more knowledge than users) and service providers have significantly more understanding and control over data flows than users (Li, Y., 2012). Over time, these create a normalized user experience (Smith & Johnson, 2022; Li, Y., 2012), leading users to accept terms without critically engaging with them. There are also intended nudges and manipulations from the current online service design. These manipulative interface nudge strategies, known as dark patterns (Nelissen et al., 2022), include techniques such as hiding unsubscribe buttons, using default opt-in checkboxes, or creating misleading wording around consent (Nelissen et al., 2022). These designs are crafted to subtly encourage users to share more personal information in their experience than they might otherwise choose, often without realizing they are doing so.

Research paradox in individuals expressing privacy
There is a persistent inconsistency between the attitudes of end users and their actual behaviors regarding privacy. Even when users care about privacy, they often fall into the “privacy paradox,” a phenomenon widely recognized as such (Pitt & Lunt, 2006). In other words, people claim to value privacy, but often engage in intrusive practices, share sensitive information, or overlook privacy settings in real-world interactions with digital platforms. While there is no unifying theory to explain this, factors such as lack of awareness and information asymmetry between users and current online data collection systems are plausible explanations (Kokolakis, 2017).

Overall, these interrelated factors shape the lack of awareness. The contextual nature of the online system, individual experiences, and the expression of privacy are all reasons that could contribute to the lack of awareness. **In this project, we use individual (online users) awareness as a critical starting point, with design help empowering individuals on online data privacy.**

The lack of privacy awareness is not just a personal neglect, it is a structural issue deeply embedded in online data systems.

In this project, we use **individual (online users) awareness** as a critical starting point for **empowering individuals on online data privacy.**

Understanding privacy

In this project, another core area related to understanding privacy is explored. Before delving into this project, we need to clarify what “privacy” means.

Firstly, there is no fixed or universal terminology to define privacy. In theoretical studies, privacy is a multidimensional concept. According to Solove (2008), privacy is conceptualized as a separate domain encompassing “the right to be alone,” “limited access to self,” “control over personal information,” “personality,” “intimacy,” and “safety.” The studies are critical in privacy, legal, and technical compliance. Others, such as Karwatzki et al. (2022), outline privacy risks in the psychological, social, professional, legal, and political domains, and note that privacy violations can have various significant consequences. Nissenbaum’s (2009) contextual integrity theory posits that privacy is not about secrets, but rather about maintaining an appropriate flow of information within a specific social context. In real-life practice, people’s explanations of privacy can extend beyond these conceptual and theoretical domains (Solove, 2008).

Secondly, understanding privacy is highly subjective and varies from person to person. Privacy can be related to personal value, which differs from person to person, and people may have different concerns and attitudes towards privacy (Solove, 2008).

Thirdly, privacy is highly contextual. Privacy is a relational experience shaped by interactions, context, and various aspect. In the digital age, privacy is contextual (Nissenbaum, 2009) when people interact with an online service . The context also implies that privacy is a personalized experience, applicable to multiple scenarios and fields.

Based on the various aspects of understanding privacy, it is valuable for this project to **research the opinions of different people**. It is helpful to **create a space for individuals to express their views on their experience regarding online data privacy.**

Individual engagement towards future design

Raising individual awareness of privacy is essential for protecting personal data rights and serves as a driving force for the sustainable and healthy development of a digital society (Mavroeidi, Kitsiou, & Kalloniatis, 2020). One example is Rossi et al.’s research (2022), in which policymakers anticipate specific scenarios using generative design materials to investigate people’s views on future-proof privacy regulations.

Futurists research and predict various potential futures, adopting a more engaged and participatory approach where preferred futures are actively imagined and shaped in the present (Inayatullah, 2013). The project is conducted with a focus on envisioning future privacy. Design plays a critical role in this process by prompting reflection and encouraging individuals to actively engage with privacy issues, transforming them from passive recipients into proactive participants.

Montgomery (2020) draws the landscape of speculative design for designers. Through the map of the future study landscape, we are positioning our design in this project at two points on the map: **from critical design points towards future design points.**

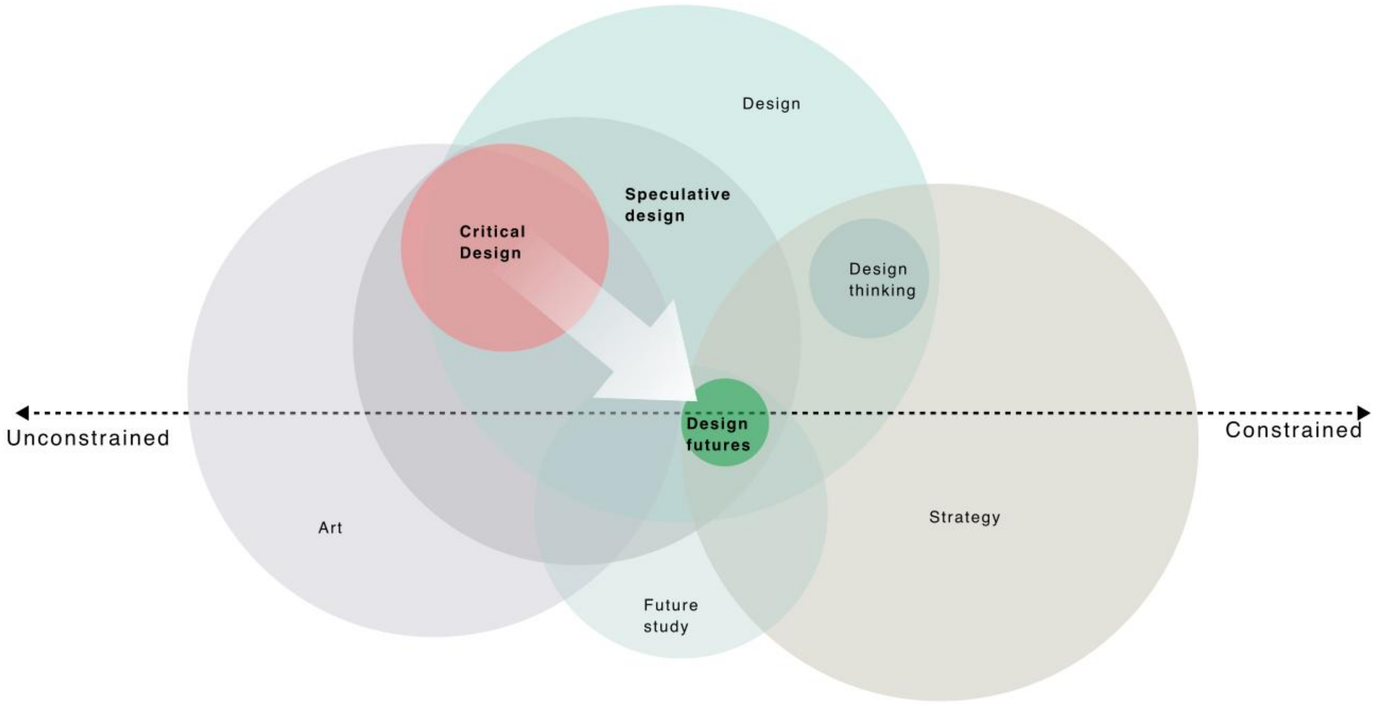


Figure 1.2: Landscape of speculative design V2.0 (Montgomery, 2020)

Research question

Based on all these opportunities, we have raised the overarching question for this project and two related goals.

The main research question is:
- **How can design empower individuals to reflect on and envision their online digital privacy?**

The two **objectives** for the project are:
- Raise awareness and gather collective insights
- Envision the alternative future intervention of online privacy in users experience

To elaborate on these two goals, two sub-research questions are raised:
- **Raise Awareness: How could design help provoke individual awareness of online data privacy?**
- **Envision alternative futures: How can design leverage the collective opinions into meaningful and plausible futures?**

Methodology

This project adopts a mixed-method research strategy, combining reflection. Three key approaches are highlighted in the following, which are essential methodologies for building the key blocks of the research.

- **Speculative Design**
- Speculative design (Dunne & Raby, 2013) is a key method employed in this research. Speculative design is particularly suited for exploring digital privacy (Rossi et al,2022), where many risks remain abstract, invisible, or normalized through daily interaction. In the project, speculative design is employed in two valuable directions, challenging dominant narratives and imagining alternative futures. In the direction of challenging dominant narratives, we aims to invite individuals to debate, allowing them to reflect on their digital experiences and privacy concerns. Speculative design produces provocative artifacts, such as actionable prototypes and narratives, that expose hidden assumptions and spark dialogue. In the direction of imagining alternative futures, we use speculative design to envisioning plausible futures and make it communicative and tangible towards people.

- **Research-through-Design (RtD)**
- Research through design (Stappers & Giaccardi, 2017) serves as the overarching methodology in this project, RtD positions design as a means of generating knowledge. With participants involved, RtD is conducted to raise awareness and explore potential future interventions. Through prototyping and conceptual exploration, this approach enables the investigation of complex, abstract issues for online digital privacy in a practice-led way.

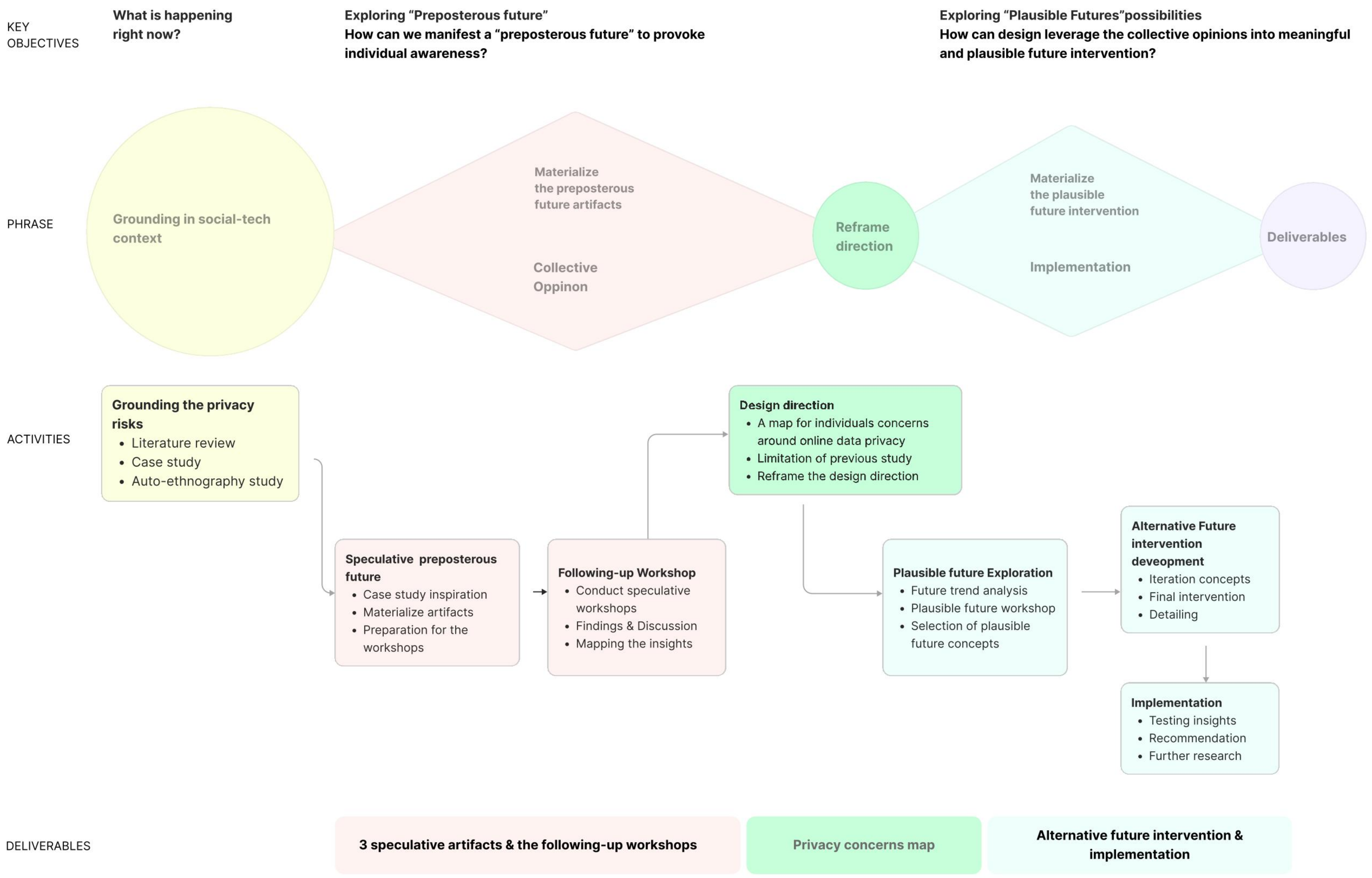
- **Auto-ethnographic study**
- Auto-ethnography, originally from sociology, refers to a design research method that approaches the research through the researcher’s first-hand experience (Schouwenberg, L., et al., 2021). Through self-reflection and critical documentation of one’s digital experience, this method enables the researcher to bridge theory and practice, offering first-hand insights that humanize abstract concepts of privacy.

Project journey

The key research journey is shown in the following map, which follows three iterative phases:
- Grounding the online data privacy risks in the social-tech context
- Exploring the preposterous future in speculations that help raise awareness of privacy risks
- From the collective insights of individuals to envision future interventions. The three key phrases that help us understand “what is happening right now”, “what are concerns towards the individual ”, and “what could happen in the alternative future”.

The delivery for this project included two parts:
- Several preposterous speculative artifacts and the follow-up workshop findings
- Alternative future intervention with implications.

Project journey map



KEY OBJECTIVES

What is happening right now?

Exploring "Preposterous future"
How can we manifest a "preposterous future" to provoke individual awareness?

Exploring "Plausible Futures"possibilities
How can design leverage the collective opinions into meaningful and plausible future intervention?

PHRASE

Grounding in social-tech context

Materialize the preposterous future artifacts

Collective Oppinon

Reframe direction

Materialize the plausible future intervention

Implementation

Deliverables

ACTIVITIES

Grounding the privacy risks
- Literature review
- Case study
- Auto-ethnography study

Speculative preposterous future
- Case study inspiration
- Materialize artifacts
- Preparation for the workshops

Following-up Workshop
- Conduct speculative workshops
- Findings & Discussion
- Mapping the insights

Design direction
- A map for individuals concerns around online data privacy
- Limitation of previous study
- Reframe the design direction

Plausible future Exploration
- Future trend analysis
- Plausible future workshop
- Selection of plausible future concepts

Alternative Future intervention deveopment
- Iteration concepts
- Final intervention
- Detailing

Implementation
- Testing insights
- Recommendation
- Further research

DELIVERABLES

3 speculative artifacts & the following-up workshops

Privacy concerns map

Alternative future intervention & implementation

Figure 1.3: Project journey map

02

What is happening right now?

Grounding the social-tech context of online data privacy

Before envisioning the future, we need to ground ourselves in what is happening right now.
This chapter presents a comprehensive overview of **capturing online privacy risks in the social-tech context** through three methods: a literature review, a case study, and an auto-ethnographic study.
The findings are highlighted in the context of our understanding of online digital privacy risks and factors.

Overview

Capture “complexity and invisibility”

Given the intangible and often invisible nature of privacy risks in everyday data practices, this chapter opens with the central question: **How can we effectively ground the social-tech context of online data privacy risks?** To achieve this, we adopt a three-pronged approach that is complementary to each other, enabling us to grasp the risks, which encompass both theoretical depth and real-world insight. This approach bridges the abstract world of data privacy with grounded and lived experiences.

- **Theoretical study**: We begin with a literature review to examine how privacy risks emerge through data flows and how existing privacy taxonomies define the complex relational structures between individuals and their data. This lens provides a conceptual foundation for understanding the evolving definitions of privacy in both technological and social terms.

- **Case Study**: With theoretical support, we employed a wide range of case studies of real-world incidents involving data privacy risks to complement the theoretical perspective. This method addresses the limitations of theoretical study and grounds abstract models in the complexity of lived reality. In other words, case studies help translate theoretical online data privacy risk categories into understandable and relatable contexts, enabling clearer engagement for readers.

- **Auto-ethnography study**: Finally, we incorporate an auto-ethnographic method, placing the researcher’s experiences at the center and as the first-hand expression. It helps articulate the often unspoken feelings associated with privacy in practice. This method clarifies the researcher’s reflective position within the study and fills an experiential gap often left by structural or case-study approaches.

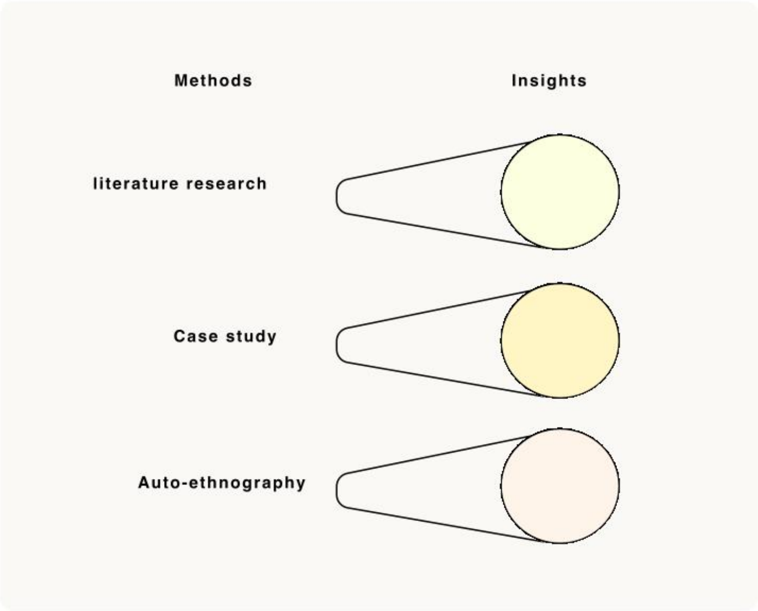


Figure 2.1: Method for grounding invisibility

Theoretical study

Before we analyze the privacy risks, we should first understand what online data practices are and how they shape the privacy issues in the current online environment.

What is data practice?

Data as a living and dynamic entity

Data serves as the smallest and most essential unit of online activities and related privacy practices. From Floridi’s (2005) ontological view, data is the foundational unit of digital environments, shaping how users are represented, interpreted, and acted upon within online systems and infrastructures. Similarly, theory around the personal data pratice(Lupton, 2016; Lupon, 2017), emphasizes the central role of data in our daily lives. Data can be seen as a more-than-human entity that coexists with us and shapes our relationships with both online and offline ecosystems. Data practices not only influence how we approach privacy but are also shaped by our online activities (Lupin, 2016). Research on dynamic data practices is therefore valuable for understanding how privacy operates in this context.

Types of Data are collected

According to the current EU privacy regulation, GDPR, three types of data are highlighted: personal data, sensitive data, and aggregated data (GDPR, 2018; Voigt & Von, 2018).

Personal data refers to any information that can be used to identify an individual . This category can encompass a wide range of information, including basic identity details, financial records, and educational backgrounds. These categories are often varied and overlapping, open to individual interpretation, and can differ among legal experts and privacy specialists(Finck & Pallas, 2020) .

Sensitive data is a specific subcategory of personal data. If exposed, it may pose significant risks to individual privacy or involve highly sensitive issues. Examples include sexual orientation, political beliefs, or religious affiliations (GDPR, 2018). While sensitive data is critical, privacy specialist Solove (2023) suggested that regulation should focus on privacy risks themselves rather than the sensitive data categories alone.

Aggregated data refers to collective information derived from multiple individuals. It enables new interpretations. (GDPR, 2018). For example, targeted advertising may use aggregated data to display ads based on total sales or consumer behaviors within a specific region.

Take away: Various data is collected from peoples and generate ranges of privacy issues in levels.

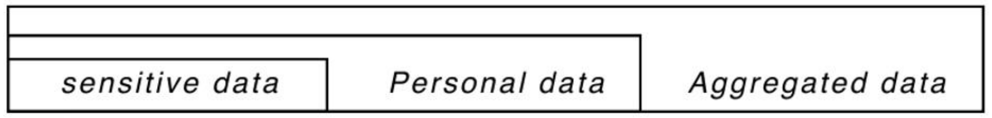


Figure 2.2: Type of data collected

Data connectivity

The Data, Information, Knowledge, and Wisdom (DIKW) Hierarchy, initially formulated by Russell L. Ackoff (1989), serves as a foundational framework for understanding how raw data collected from individuals evolves into meaningful insights through connection and interpretation (Berlinger, 2004).

Data alone is symbolic and has limited meaning without context. Information results from linking raw data into forms that are more useful and actionable. Information answers the fundamental questions of who, what, where, and when (Berlinger, 2004), allowing individuals or systems to interpret data in a more structured way.

For deeper insight, information is transformed into knowledge. Knowledge involves recognizing patterns of individuals and can be used as actionable input to create tailored online services (Berlinger, 2004).

Wisdom belongs to humans (Berlinger, 2004) and is grounded in values. In practice, the hierarchy is not strictly linear; instead, it illustrates how individual data is continuously used and transformed within online services.

Raw data has limited meaning and low value on its own. However, as data becomes increasingly centralized through personal devices and online platforms, it gains significance. For example, a single piece of location data might seem trivial in isolation. However, when combined with other seemingly harmless information, it can reveal sensitive details such as an individual's home address, daily routines, or even health conditions. With this interconnectedness of personal data, both opportunities for value creation and new vulnerabilities emerge for individuals.

Take away: The term 'data' here refers to the raw data collected from users. When processed, organized, centralized and interpreted through a service, data become information and knowledge, providing context and understanding for people, which could help inform decisions and strategies for individuals, online services, and other parties (Chen et al., 2009). In this project, for simplicity, we use "data" to represent all variants of connected data.

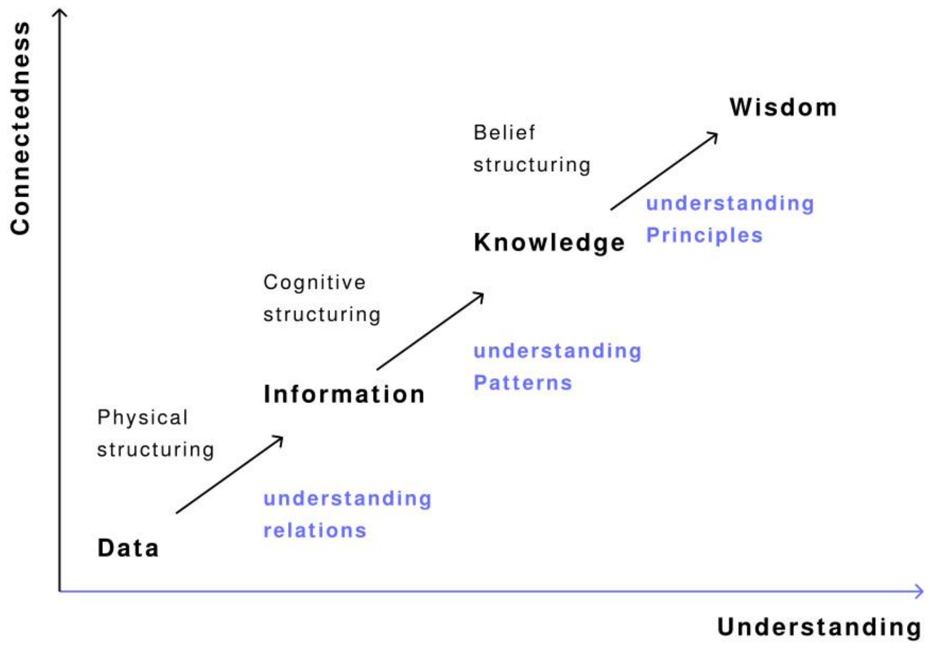


Figure 2.3: DIKW Hierarchy(Berlinger,2004)

Main insights:

1. **Dynamic data practice** raises issues of online privacy. Viewing privacy through a data-centric lens is valuable, as it helps define specific risks and reveals how data shapes relationships between individuals and their surrounding environment.

2. **Types of data collection** related to online privacy. Identifying and categorizing different types of data collection allows us to understand better how privacy risks emerge and affect individuals in varying ways

3. **Data connectivity, centralization and processing shape** the environment of online privacy understanding. Privacy issues arise within interconnected systems where data is continuously connected, processed, and transformed through interactions between individuals and online platforms. As data is linked and analyzed, new contextual understandings are generated, which simultaneously add value to personal data while increasing potential risks.

What is privacy in data practice?

Privacy taxonomy

Solove (2008) developed a classification system that highlights different types of privacy risks. This taxonomy, widely applied in privacy law and regulation, also contributes to the technical design of privacy. As shown in the figure, the taxonomy identifies risks associated with data collection, processing, dissemination, and invasion.

Among these categories, both invasion risks and data collection risks involve the transfer of data from individuals to data holders. In this flow, data generated by physical devices is transmitted to online entities. To maintain coherence and simplify our study, we propose combining "collection" and "invasion" into a single category, which we collectively refer to as the "collection" phase. This adjustment enables us to highlight three primary categories on the map, each representing a crucial data flow within data practices.

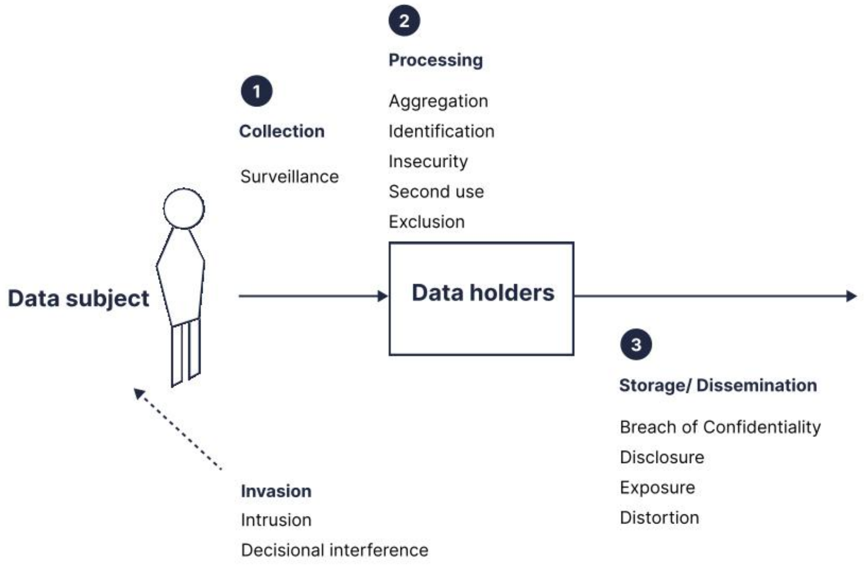


Figure 2.4: Privacy taxonomy (Solove, 2008)

System: Identify key roles and key flows

Based on this analysis and recombination within our study context with Solove (2008), we develop a model for online privacy in this study, which reveals three key flows related to the individual side, providing a fundamental understanding of how individuals interact with online privacy. Through Karen Barad's theory (2007), we understand that online privacy is not a static concept, but rather a dynamic and relational concept emerging from the "intra-actions" of roles. Inspired by these theories, the individuals, the holder, and the reviewers are mutually constituted through their interconnectedness. This map illustrates the concept of privacy in the flow linked to individuals and how current data practices mediate the experience of privacy.

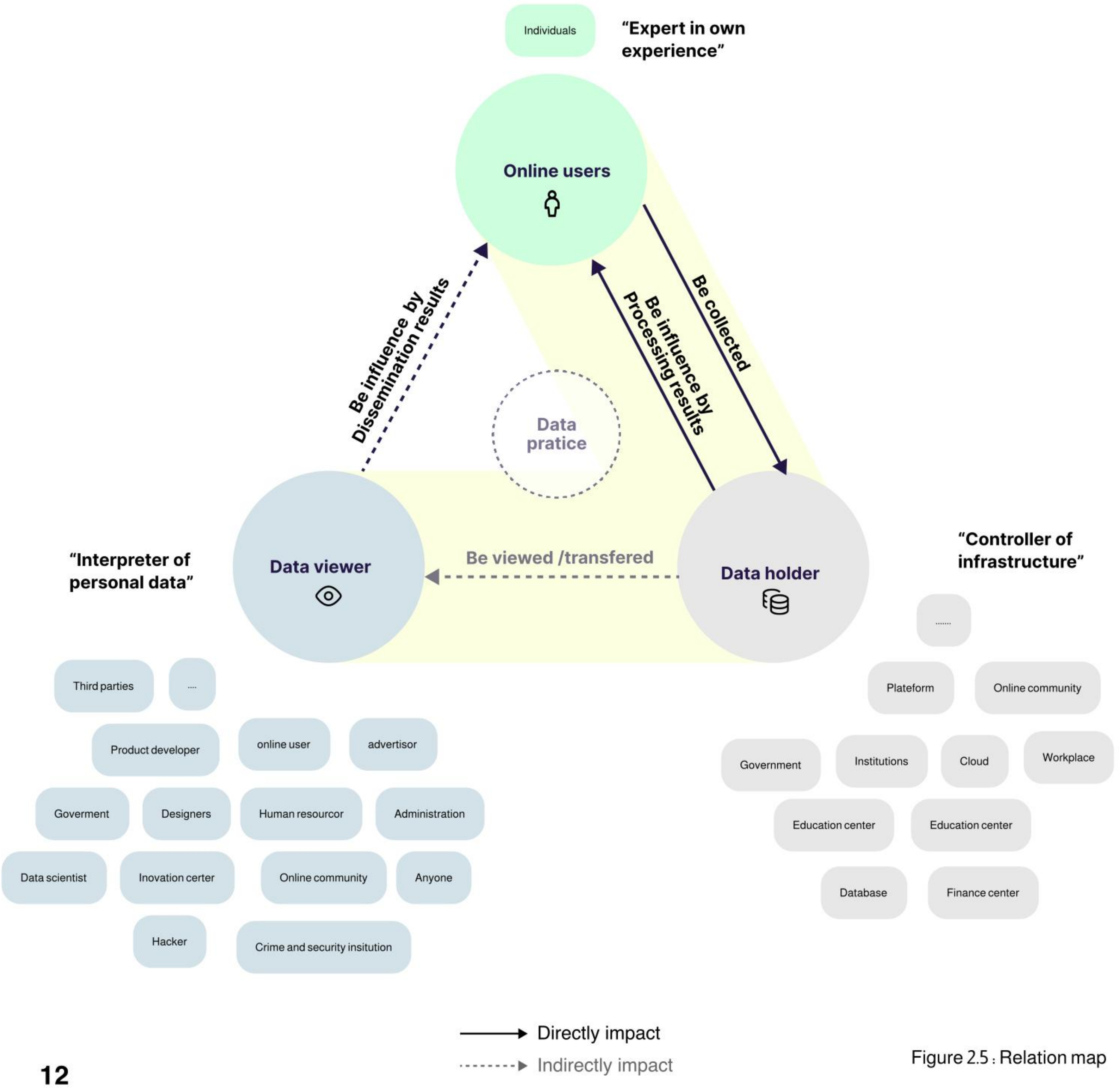


Figure 2.5 : Relation map

What are the key roles?
It is crucial to understand that individual privacy are dynamics flow through various roles in the current online community. We identified three key roles in the online data privacy context, which included individuals as online users, data holders, and data reviewers.

- **Individuals (online user):** They are the subjects of data privacy, interacting with digital services (in our context, online individuals). They are the expert of their own online experience. Individuals, as online users, are the primary focus of this project.
- **Data holders:** The digital platforms, services, or apps that collect and centralize users' data, which could be considered data holders. In this map, the Data holders play a role in infrastructure control, where they store personal data and add understanding through processing, serving as the bridge between individuals and data viewers. (Solove, 2008)
- **Data viewers:** In the real world, the collected and processed data can be shared with anyone, allowing them to interpret the personal data. Data viewers can be other online users, online platforms, institutions, or the government. Data viewers play a key role in interpreting our online data. In a real-world setting, the data viewers could be the same as the data holders, such as online services, or they could be any online users or institution, including other online users, advertisers, data analysts, or government agencies(Solove, 2008).

What are the key flow?

- **Collection:** This flow illustrates the movement from the individual to the data holder. This includes both voluntary actions (such as filling out a profile or uploading a photo) and involuntary tracking (such as voice surveillance and online behavioral monitoring).
- **Processing:** The processing results show what is inside the holder and reviewers which can be expanded towards everywhere. The processing is facilitated by technology and supported by a data connection. Individuals could not see the processing progress, but the results could have an impact on them(Solove, 2008).
- **Storage and dissemination:** The storage refers to the afterlife of personal data. The dissemination is embedded in the storage phrases and has been transferred from the holder to the viewers. At the same time, the result of the dimension can influence the individuals(Solove, 2008).

The three key flow as key phrases are fundamental to this study, which also shows relational and dynamic powers changing through the roles in the curent online community. In the model, the flow of the data collection and storage/dimension is communicated through the individual data holder or the viewers.

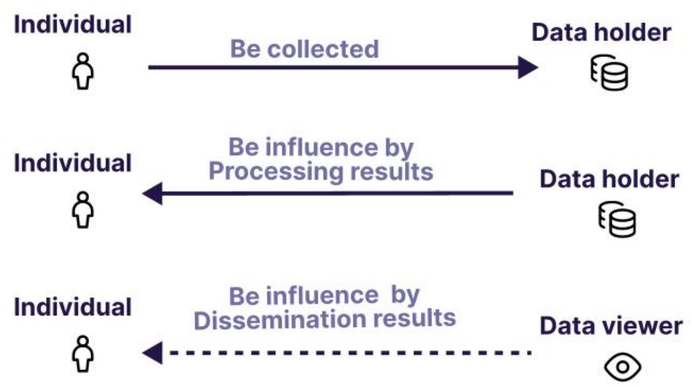


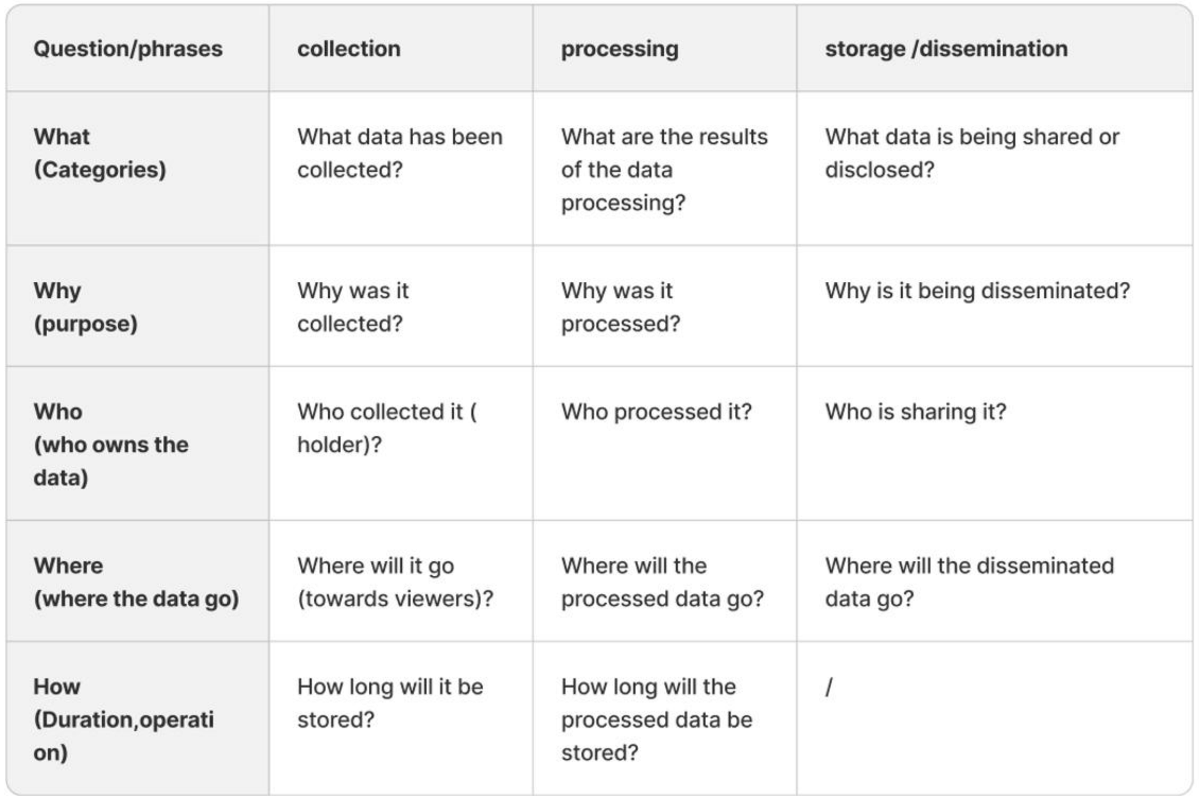
Figure 2.6 : Key flow map

How could we interpret these flows towards individuals?

After creating a relational map, it's crucial to analyze the flow of information among them. Acquisti et al. (2017) state that "incomplete information" is used to identify the limited information provided to individuals, which could be one reason for harming individuals' privacy.

To identify what types of information are exchanged between these roles, we drew inspiration from Acquisti et al. (2017), who examined how visual instructions help individuals understand privacy-related information. For example, Rossi and Palmirani (2019) developed a set of data protection icons that classify data practices based on processing purposes, agent roles, operations, and subcategories. Similarly, Pins et al. (2022) visualized key moments in the user's data access journey. These, along with Solove's (2010) privacy taxonomy, guided us in creating a structured model for analyzing information flow.

Individuals often lack awareness of the information flowing within these systems, so we use questions to help analyze the system and identify what kind of information is lacking for individuals. These questions help us build a systematic understanding of information flows and question the privacy rights in the system. We grouped these ideas into thematic clusters and summarized them in a table to help clarify what specific information flow is lacking in this system, which prevents individuals from understanding the system. These questions were developed from a table, allowing us to ask questions across three key stages: collection, processing, and storage, to identify the lack of information for individuals in awareness.



Question/phrases	collection	processing	storage /dissemination
What (Categories)	What data has been collected?	What are the results of the data processing?	What data is being shared or disclosed?
Why (purpose)	Why was it collected?	Why was it processed?	Why is it being disseminated?
Who (who owns the data)	Who collected it (holder)?	Who processed it?	Who is sharing it?
Where (where the data go)	Where will it go (towards viewers)?	Where will the processed data go?	Where will the disseminated data go?
How (Duration,operation)	How long will it be stored?	How long will the processed data be stored?	/

Figure 2.7: question the flows

Take away: From these analysis, it is clear that privacy risks can impact individuals at every stage. By analyzing what is lacking for individuals, we can better understand how to raise their awareness across various phases, ultimately empowering them within the system.

Dynamics among roles

Defining the dynamic of individuals, viewers, and holders in the system, as explored in the literature shows how information asymmetry exists, and also provides a evidence for privacy issues exists in the power dynamics. Evidence suggests that the system is driven mainly by data holders and viewers, who have access to and control over individual data. In contrast, individuals who generate this data and live with the consequences of its use often cannot participate in the flow of information and have little influence over their data (Quach et al., 2022).

Personal data provides significant value to data holders and is used for a variety of purposes across different contexts, such as human resources, goods and services provision, scientific research, financial administration, healthcare, crime and national security, security and surveillance, marketing, customer relations, authorization management, judicial processes, education, automated decision-making, and fraud detection and prevention (Rossi & Palmirani, 2019).

Online users often desire to protect themselves from threats in their digital experiences, but they cannot do so frequently. Their opinions are commonly overlooked in existing models. The literature highlights that the current structure exploits: (1) users' lack of awareness or concern, (2) users' incapability of recognizing risks, and (3) users' inability to resist and protect themselves, all of which increase privacy risks for individuals (Bongard-Blanchy et al., 2021).

Take away: Therefore, from the current state to the future, a long journey remains ahead in researching individuals' privacy. Key goals include: (1) raising awareness among individuals, and (2) empowering individuals to resist and protect themselves in the future.

Criticism of taxonomy

The relation map is developed from the privacy taxonomy. Despite its widespread adoption in legal, Solove's framework has received several notable critiques.

- Angel and Calo (2024) argue that the taxonomy lacks a clear definition of privacy, which risks blurring the boundaries between privacy harms and other legal domains such as consumer protection or anti-discrimination.
- Barocas and Nissenbaum (2014) add that the taxonomy does not provide a system of normative prioritization, making it difficult to determine which harms are most urgent or harmful in practice.
- Moreover, the model may fail to address emerging, emotional risks, such as those related to predictive profiling or identity distortion (Angel and Calo, 2024).
- Another criticism is that, in practice, Solove's categories are difficult to translate into actionable strategies.

Take away: Therefore, Solove's taxonomy is not treated as an endpoint. two critical lenses supplement it:

- A case-based analysis of real-world digital privacy incidents,
- An individual-centered inquiry grounded in auto-ethnographic reflection.

Main insights:

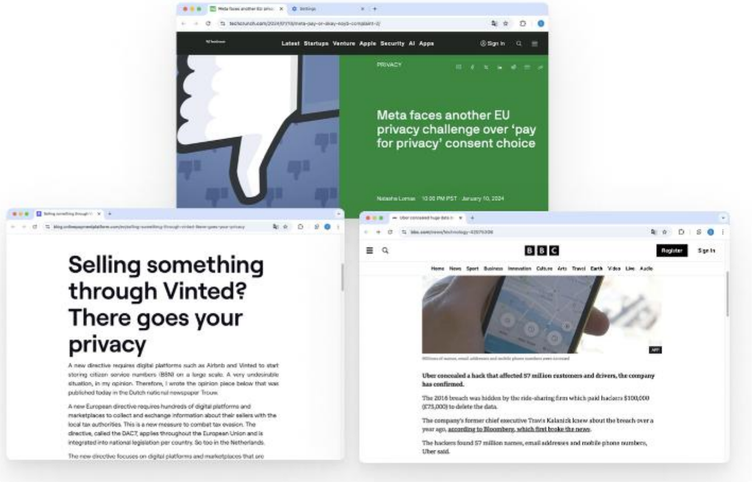
The privacy taxonomy provides the foundation for this research, helping us gain an overview of privacy risks. It illustrates how different categories of privacy concerns arise across the phases of data practice and highlights the roles involved.

For this project, we identified key roles and data flows by creating a series of diagrams that visualize relationships within data practices. These diagrams highlight three key flows between **individuals, data holders, and data viewers.** Within these flows of **collection, processing, and storage**, we can observe how information is transmitted, where it is lacking for individuals, and how value is assessed differently for each actor. The diagrams demonstrate how these roles collectively co-shape the online data privacy system.

The limitations of the taxonomy prompt us to examine the real-world implications of privacy for individuals. Considering these theoretical constraints, the taxonomy should be complemented with contextual and experiential insights. This integration will be addressed in the subsequent phases of our research.

Case study

To investigate how digital privacy risks manifest in real-world contexts and bridge the gap between privacy theory and real-world dangers, we conducted a targeted review of news reports and public case studies. This exploration aims to move beyond theoretical definitions of privacy and examine how privacy violations are experienced in the real world. In the case of searching, we used search keywords such as "data privacy," "data threat," "personal data breach," and "digital surveillance" to locate relevant articles. The sources were drawn primarily from EU-focused technology news platforms, such as TechCrunch and The Verge. Additionally, since privacy is global issue, that the personal data could leak out of EU(Greenleaf, 2012). we included international outlets, eg. The New York Times to gain a broader, global perspective on digital privacy incidents.


Latest Startups Venture Apple Security AI Apps
Sign In
Home News Sport Business Innovation Culture Arts Travel Earth Video Live Audio
Register
Sign In

PRIVACY

Meta faces another EU privacy challenge over 'pay for privacy' consent choice

Natasha Lomas · 10:00 PM PST · January 10, 2024

Selling something through Vinted? There goes your privacy

A new directive requires digital platforms such as Airbnb and Vinted to start storing citizen service numbers (BSN) on a large scale. A very undesirable situation, in my opinion. Therefore, I wrote the opinion piece below that was published today in the Dutch national newspaper Trouw.

A new European directive requires hundreds of digital platforms and marketplaces to collect and exchange information about their sellers with the local tax authorities. This is a new measure to combat tax evasion. The directive, called the DAC7, applies throughout the European Union and is integrated into national legislation per country. So too in the Netherlands.

The new directive focuses on digital platforms and marketplaces that are

Uber concealed a hack that affected 57 million customers and drivers, the company has confirmed.

The 2016 breach was hidden by the ride-sharing firm which paid hackers $100,000 (£75,000) to delete the data.

The company's former chief executive Travis Kalanick knew about the breach over a year ago, according to Bloomberg, which first broke the news.

The hackers found 57 million names, email addresses and mobile phone numbers, Uber said.

Figure 2.8: case study website example

Taxonomy	Description	Case example	source/ authors	key factors
Collection/ Invasion Risks				
Intrusion	Actions that disturb one's solitude in physical space	In 2018, a Spanish case exposed the **workplace surveillance using hidden microphones** and cameras amounted to an **intrusive violation of employee's private life.**	(European Court of Human Rights, 2018)	boundaries of personal space
Decisional interference	Interfering with a person's private decisions or actions, often by others (e.g. governments)	In 2018, Cambridge Analytica harvested Facebook users' data without consent to **create psychological profiles**, which were then used to **influence voter decisions** in major political events	(Cadwalladr, 2018)	Decision-making
Surveillance	Watching, listening to, or recording of an individual's activities	Signal, a privacy-first messaging service, launched a bold advertising campaign to **reveal how Facebook target users using personal data.** The ads mimicked targeted ad formats but explicitly listed the exact traits Facebook had used to target the user. e.g., "You got this ad because you're a newlywed Pilates instructor and you're cartoon crazy."	https://signal.org/blog/the-instagram-ads-you-will-never-see/	presence of personal devices
Processing Risks				
Aggregation	combining various pieces of data about a person to make inferences beyond what is explicitly captured in those data	One of classic examples is the 2012 target incident in the U.S. where the company's **predictive analytics algorithm identify a teenage girl was pregnant based on her shopping behavior** (unscented lotion, vitamin supplements).	(Hill, 2012)	sensitive information, misinterpretation
Identification	linking specific data points to an individual's identity	In 2022, it was reported that platforms such as **Airbnb and Vinted were storing Dutch citizens' BSN**s (Burgerservicenummer)	https://blog.onlinepaymentplatform.com/en/selling-something-through-vinted-there-goes-your-privacy	identification
Secondary use	The use of personal data collected for one purpose for a different purpose without end-user consent	In 2024, it was reported PayPal's plan to build an advertising network lerveraging on the customer transaction data in the stores and online.	https://www.theverge.com/2024/5/28/24166381/paypal-building-ad-network-transaction-data	Purpose
Insecurity	Carelessness in protecting collected personal data from leaks and improper access due to faulty data storage and data practices	In 2016, Uber experienced **a massive data breach** in which hackers accessed the personal data of approximately 57 million users and drivers worldwide. The compromised information included names, email addresses, phone numbers, and in some cases, driver's license numbers.	https://www.uber.com/en-CH/newsroom/2016-data-incident/	identification
Storage/ Dissemination Risks				
Exclusion	The failure to provide end-users with notice and control over how their data is being used	In 2025, it is reported that the LinkedIn "quietly" introduced a privacy setting, automatically **using personal data to train AI**	https://www.bbc.com/news/articles/cdxevpzy3yko	controllability
Breach of Confidentiality	Breaking a promise or obligation to keep someone's information private.	In 2021, Mozilla evaluated the privacy practices of 25 **dating apps** and found that 22 of them had serious privacy issues, collecting more and increasingly intrusive data than ever before.	https://www.mozillafoundation.org/en/blog/everything-but-your-mothers-maiden-name-mozilla-research-finds-majority-of-dating-apps-more-data-hungry-and-invasive-than-ever/	Unpredictability
Disclosure	Revealing and improperly sharing data of individuals	In 2020, it was reported that Zoom illegally shared users' personal data with Facebook, even **when users did not have a Facebook account.**	https://technewsdaily.com/zoom-facebook-privacy	Unpredictability
Exposure	revealing sensitive private information that people view as deeply primordial that we have been socialized into concealing	Allo is an instant messaging app first launched in 2017 allows the Google to read users' chats.	https://www.bbc.com/news/technology-37429849	Unpredictability
Distortion	Disseminating false or misleading information about people	Criminal Use of Deepfake technology for harassing or humiliating individuals online.	https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/	Fake information

Figure 2.9: case study analysis

Analysis with privacy Taxonomy (Solove, 2008)

To contextualize privacy taxonomical risks, we link the real-world case to the theoretical frame. In figure 2.9, we show one case for each category. By analyzing these cases in the table, we can see that there are key elements as factors linked to each phrase. We explain these key factors in detail.

Collection

- **Personal device intrusion:** A personal device is the first point of contact for individuals to generate personal data. Individuals can be tracked privately when using any personal device in the environment, including smartphones, laptops and any IoT technology could be in the future.(Lupton, 2017)
- **Personal actions generate consequences:** With each action taken, whether clicking, tapping, or typing ,personal data can be generated and collected.
- **Persnal space and boundaries:** The boundaries between public and private domains are increasingly blurring, for example, between office space and private space, which raises the risk of surveillance.
- **Individuals' agency and decision-making:** online nudges that guide and shape user decisions.

Processing

- **Identification:** Even if identification are not be collected directly, they can be identified through the data connection and processing.
- **Misinterpretation:** People's actions or preferences can be misunderstood when taken out of context.
- **Sensitivity:** Not all data is equal. Details about someone's health, emotions, or beliefs can carry significant risks, and mishandling this kind of information can be deeply personal.

Storage/ Dissemination

- **Controllability:** Once data is collected, it cannot be taken away. People do not know what is happening behind the scenes. It can be reused, reshaped, or combined with other data in ways they never imagined (Kokolakis, 2017).
- **Broken access:** Data ends up being used in ways people did not expect, or never intended to access. This can be viewed as a breach of promise for individuals.
- **Unpredictability:** Once data is shared, it is challenging to determine where it ends up. People cannot take it back or stop it from spreading, and they cannot predict future risks. (Lupton, 2016)
- **False Information:** If incorrect information is shared, such as deepfake news. This can impact how others perceive a person, as well as how they perceive themselves.(Lazer et al., 2018)

Main insights:

Analysis using the privacy taxonomy framework revealed the key factors in each phrase, helping us contextualize the phrases and prioritize the key elements that could have a significant impact on individual privacy. During the data collection phase, critical factors included **the presence of personal devices, the role of rights in decision-making, and the blurred boundaries of personal space**. During processing, critical factors are tied to **identification, the misinterpretation, and the handling of sensitive information**. In the dissemination phase, the critical factors included a lack of **controllability, broken promises regarding data usage, unpredictable future use, and the influence of false information**.

New themes emerged

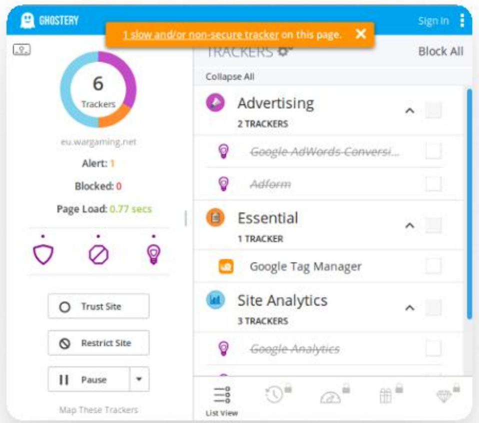
From the case study, several **new themes also emerged**. We clustered these themes into distinct categories to gain a deeper understanding of how technological and social factors shape privacy risks and influence individuals. These themes complement the existing privacy taxonomy and help reveal how risks exist across all phases in the online context.

Technology communication capability

Technologies inherently carry moral and social values (Verbeek, 2008). In the context of online data privacy, technology serves as an intermediary between individuals and platforms, shaping how privacy threats are framed and understood.

A persistent gap exists between technical systems and human understanding, which can be described as an unintended or original attribution of technology (Verbeek, 2008). The initial development of technological advancements often overlooks a human-centered perspective.

When facing these challenges between humans and technologies, some **current services or tools** have emerged to bridge the gap and provide a more humanized way for online users to visualize what is happening to their online privacy.



1 slow and/or non-secure tracker on this page.

eu.wargaming.net

Alert: 1

Blocked: 0

Page Load: 0.77 secs

Figure 2.10: Ghostery shows the tracker on each page

Cases from add-ons and plug-ins on the website to help the ethical use of online data through **visualizing the data practice**. One case study example is the privacy visualization add-on for Firefox called Lightbeam, which offers an interactive website that visualizes the flow of personal information between services, making invisible data practices visible and accessible. Another example is Ghostery, an independent, privacy-focused browser extension that alerts users to trackers embedded on every page they visit, helping them understand the scope of online tracking in specific services.

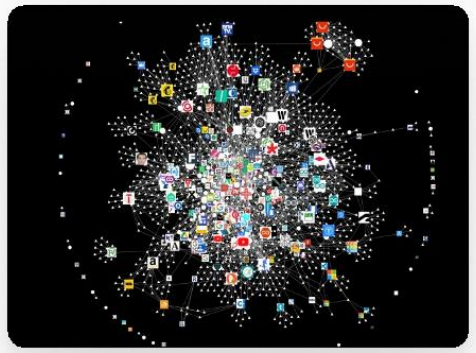


Figure 2.11: Site connection on the lightbeam

Another case for online services is more **ironic**. The messaging app signal launched a campaign visualized exposing Facebook's targeted advertising practices by displaying ads such as, "You saw this ad because you are a newlywed Pilates instructor and you are cartoon crazy." Although Facebook quickly shut down the campaign, it demonstrated how technology can engage users more morally and communicate privacy risks in ways that are tangible and approachable.

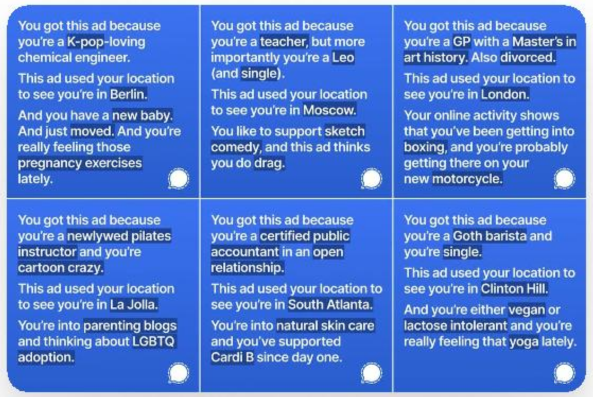
Those cases demonstrate a trend to enhance the communication capabilities of technology, making privacy risks more visible.

Algorithm bias and discrimination

Technology is not neutral (Miller, 2021). The algorithm generates bias and privacy issues.

Bias appears in **data-driven decision-making**. Take target ads as an example. One significant example is that the company's algorithms can track everyday shopping patterns, such as purchases of lotion, vitamins, fragrance-free soap, or cotton balls, and calculate a "pregnancy prediction" score for customers. The system could even estimate due dates with remarkable accuracy. While marketed as personalized advertising, this kind of predictive profiling intrudes on privacy (Hill, 2012).

Another cases illustrate how biases are generated through the exploitation of **sensitive personal information.** Maya, a menstrual tracking app with over 5 million downloads, asks users to log intimate details about their cycles, moods, symptoms, and sexual activity. Investigations revealed that all of this data, along with users' in-app actions, was shared with Facebook and CleverTap (Privacy International, 2020). By turning deeply personal health information into a commodity, third parties can profit from users' vulnerabilities through targeted advertising. These risks are heightened because technology often advances faster than legislation can keep pace.



You got this ad because you're a K-pop-loving chemical engineer.

This ad used your location to see you're in Berlin.

And you have a new baby. And just moved. And you're really feeling those pregnancy exercises lately.

You got this ad because you're a teacher, but more importantly you're a Leo (and single).

This ad used your location to see you're in Moscow.

You like to support sketch comedy, and this ad thinks you do drag.

You got this ad because you're a GP with a Master's in art history. Also divorced.

This ad used your location to see you're in London.

Your online activity shows that you've been getting into boxing, and you're probably getting there on your new motorcycle.

You got this ad because you're a newlywed pilates instructor and you're cartoon crazy.

This ad used your location to see you're in La Jolla.

You're into parenting blogs and thinking about LGBTQ adoption.

You got this ad because you're a certified public accountant in an open relationship.

This ad used your location to see you're in South Atlanta.

You're into natural skin care and you've supported Cardi B since day one.

You got this ad because you're a Goth barista and you're single.

This ad used your location to see you're in Clinton Hill.

And you're either vegan or lactose intolerant and you're really feeling that yoga lately.

Figure 2.12 : signal exposing target ads

Figure 2.13: HaveIBeenTrain tool

Privacy issues can further amplify bias and perpetuate **harmful stereotypes**. The controversial "Gaydar" model claimed it could predict sexual orientation from facial images, and other research attempted to predict criminality using facial recognition. These models risk legitimizing discrimination and reinforcing societal biases (New Yorker, 2017).

Algorithm development plays a central role in these issues, often **operating in grey areas in protection**. A notable case is the German Luca app: designed initially for COVID-19 contact tracing, it was later repurposed by law enforcement to track potential witnesses to crimes. This example illustrates how tools designed for one purpose can stretch ethical boundaries when used in new contexts (Washington Post, 2022). **The use of personal data could expand beyond its original purpose.**

At the same time, **identity-related risks could be more threatened**. According to Signicat's Battle in the Dark 2025 report, fraud attempts rose by 88% in just four years, with identity fraud alone increasing by 69% (SC, 2025). The theft and misuse of personal identities create new opportunities for bias and exploitation.

Some tools try to aware people from this processing and potential risks of bias. The HaveIBeenTrained website allows individuals to check whether their faces have been included in massive AI training datasets, such as Midjourney, highlighting how personal data can be collected and used without their knowledge or consent (Pulitzer Center, 2024).

Exclusion of some people or groups

In the current social context, privacy protections are not equally available to all individuals.

The exclusions often leave **vulnerable groups** lacking both awareness and the resources to detect or respond to privacy violations. Certain groups, such as children and teenagers, are particularly vulnerable to privacy violations by large digital platforms. For example, TikTok has been fined for failing to protect minors' data (European Commission, 2023)。

These exclusions are also further reinforced by **data monetizatio**n. The rise of "pay-for-privacy" models, which include Meta's 2024 premium privacy subscriptions, has sparked ethical criticism. We argue that privacy is a fundamental right, and that requiring payment to avoid surveillance undermines the principle of equal access to information. For individuals who cannot afford these services, the consequence is a two-tiered internet, one in which wealthier users can shield themselves from tracking, while others remain exposed.

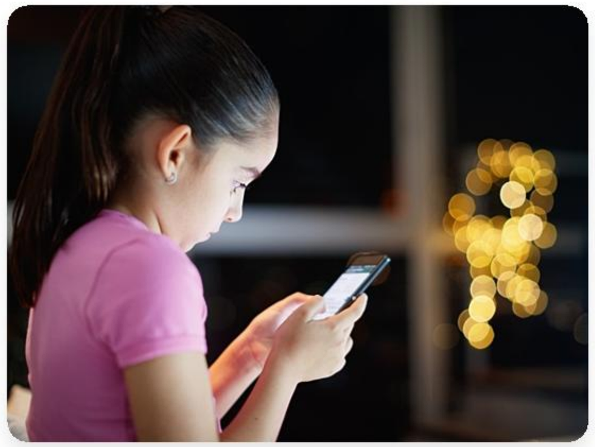
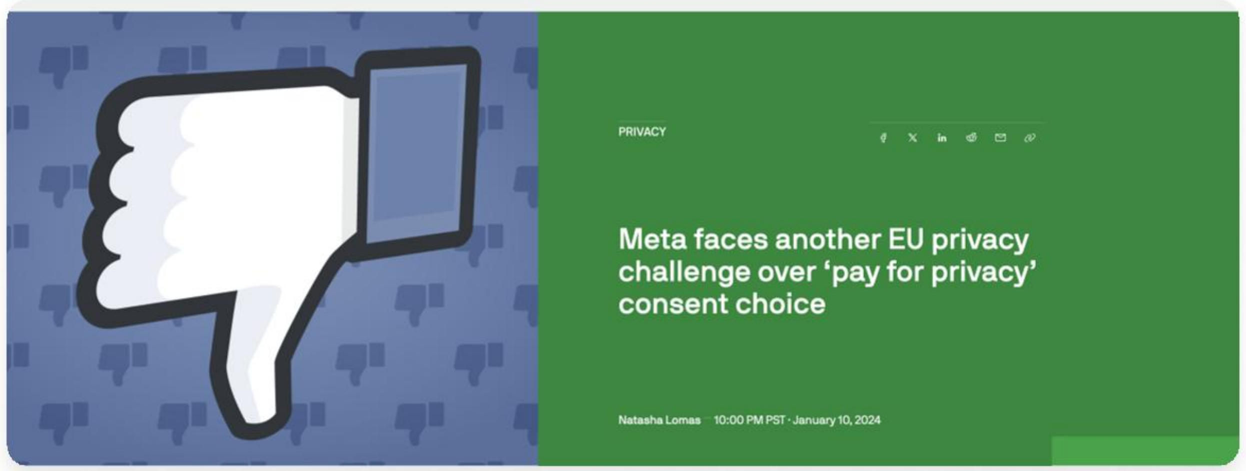


Figure 2.15: vulnerable groups like children



PRIVACY

Meta faces another EU privacy challenge over 'pay for privacy' consent choice

Natasha Lomas 10:00 PM PST · January 10, 2024

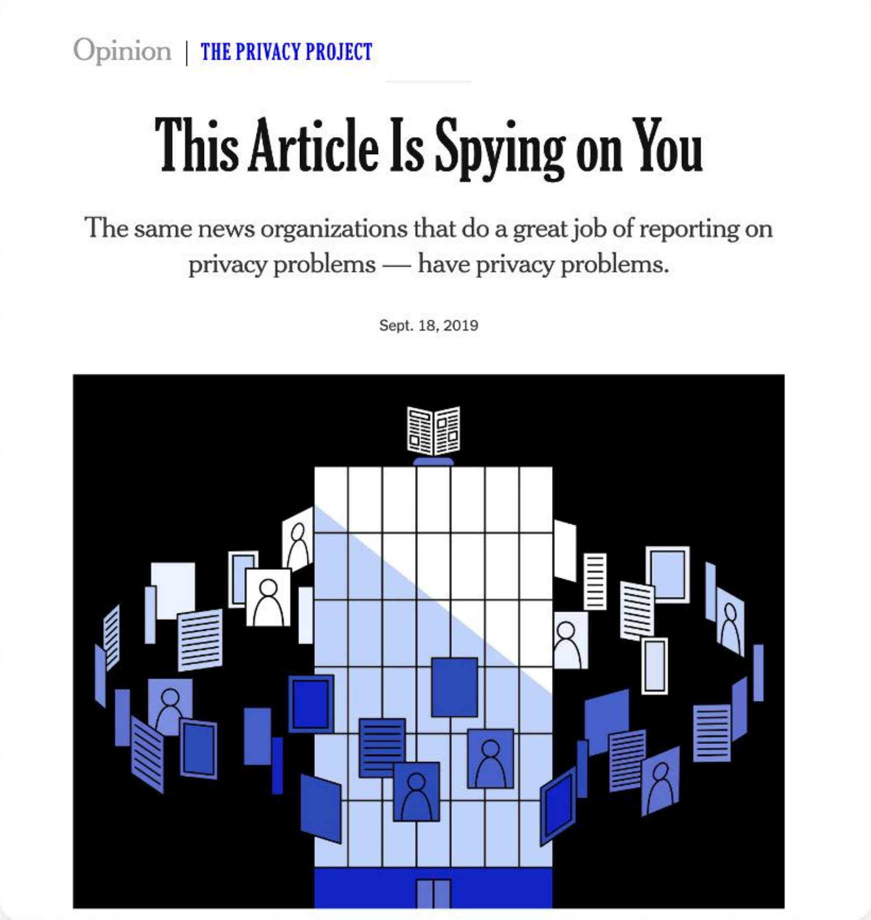
Figure 2.14: News fromTechChurch" pay for privacy"

Individual psychological influence

From the case study, we know that privacy risks have psychological impact on individuals. One Reddit user reflected, “Privacy concerns are ruining the enjoyment of useful technology” (u/CCPareNazies, 2013). This comment highlights a phenomenon: When individuals are that a persistent lack of privacy can erode a person’s sense of safety and stress, anxiety, and fatigue(Choi, Park, & Jung, 2018) .

Case studies illustrate the impact of **psychological unpreparedness on people when facing risks** that are totally outside their expectations. For instance, the New York Times article “This Article Is Spying on You” (Harris, 2019) reports that even platforms designed to inform readers about privacy issues can still track users and collect personal data, which collects data about readers’ political beliefs, health interests, and personal behavior, and could be shared with the government. In this case, readers assumed that simply engaging with privacy-aware content would protect them, yet their personal information was still being harvested. Another case that is In 2024, dutch privacy authority give a fines for Uber for unlawfully transferring drivers' personal data to the United States, which could cause potential more severe privacy diffusion without the regulation of GDPR, and the transformation couldn’t be informed users. their privacy risks can go globally without unpreparedness,. Such scenarios reveal that individuals are often ill-equipped to anticipate or respond to privacy risks, which could amplify feelings of negative feelings, for example distrust, powerlessness, and frustration(Kalia, 2022).

The implication for psychological influence also includes that privacy risks can influence people’s attitudes and behaviors, creating a kind of feedback loop between people and technology: our attitudes and behaviors affect how we use technology, and technology, in turn, influences our attitudes and behaviors over time.



Opinion | THE PRIVACY PROJECT

This Article Is Spying on You

The same news organizations that do a great job of reporting on privacy problems — have privacy problems.

Sept. 18, 2019

Figure 2.15 : the New York Times article “This Article Is Spying on You”

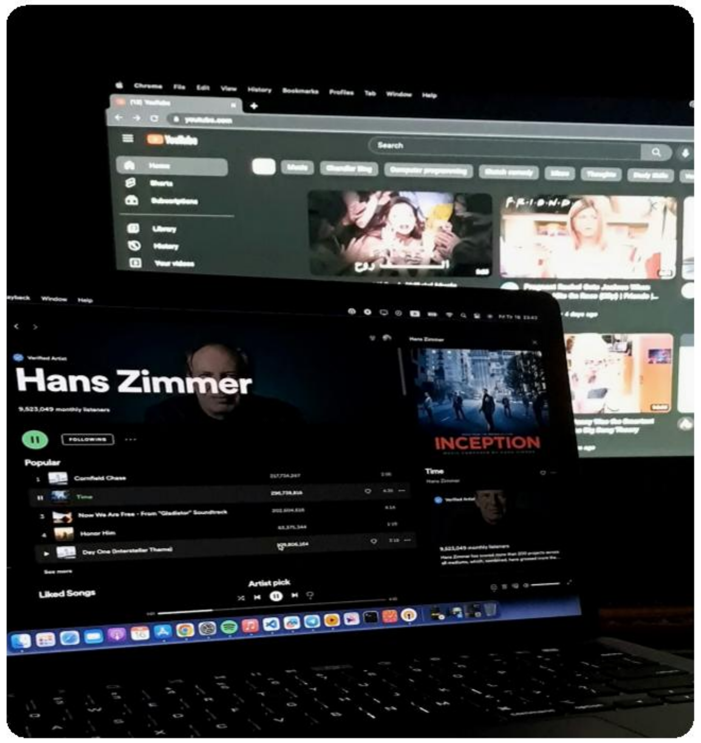


Figure 2.16 : 6 connected service

Accessibilities on technology

The accessibility of digital and connected technologies to individuals makes online privacy vulnerable.

The case examples shows that organizations are increasingly adopting advanced monitoring tools in the name of safety and efficiency. One example is in Australia, companies are testing SmartCap, a brainwave-monitoring device that **tracks workers’ fatigue to reduce accidents and improve productivity(**Regan, 2020).

Another case shows that the availability of consumer technologies shows how surveillance c**apabilities have entered everyday life**. According to the Surveillance Studies Centre at Queen’s University, there are currently more than 400 types of wearable devices on the market, with fitness trackers and smartwatches dominating through body-sensing functions(Regan, 2020). Even clothing has become a medium of connectivity: Levi Strauss, in collaboration with Google’s Jacquard project, developed a tech jacket that allows wearers to answer calls and control music simply by touching the sleeve(Regan, 2020).

These cases illustrate **how easily technology integrates into personal spaces, which is considered seamless and invisible.**

Hyper-connected space and online communities

Online communities have become an essential part of daily life for both individuals. In today’s “permanently online and permanently connected” (POPC) world, people, devices, and systems are continuously linked. The vision of Society 5.0, promoted by Japan, aims to create a “super-smart society” that integrates cyberspace and physical space (Helbing, 2023). In this context, individuals’ data flows seamlessly across platforms and devices, from wearable sensors to social media and AI-driven services. While this connectivity offers convenience and efficiency, it also increases the risk of personal data being shared beyond its intended context.

On the positive side, online communities foster belonging, mutual support, and resilience, enhancing well-being and personal growth. They provide spaces for self-expression, knowledge sharing, and collaboration, helping individuals feel part of something larger and strengthening social ties (Erfani, Abedin, & Blount, 2015). **However, being active and present in online communities almost always involves disclosure**, which keeps individuals continuously engaged but also exposes them to privacy risks (Rainie & Anderson, 2014).

Isolation strategies do not work

The case study shows that companies like Google Maps are changing how they handle personal data eg. personal location data used in the map. Instead of backing it up to the cloud, they will store it locally on the user’s device. This aims to reduce online exposure and limit the personal data created through overuse (Acquisti, Brandimarte, & Loewenstein, 2017).

Some people try to protect their privacy by isolating themselves online (Rainie & Anderson, 2014). They may avoid certain websites or limit their digital activity, using tools that restrict time on social media. These strategies can offer short-term benefits, but they are not effective or should be recommended.

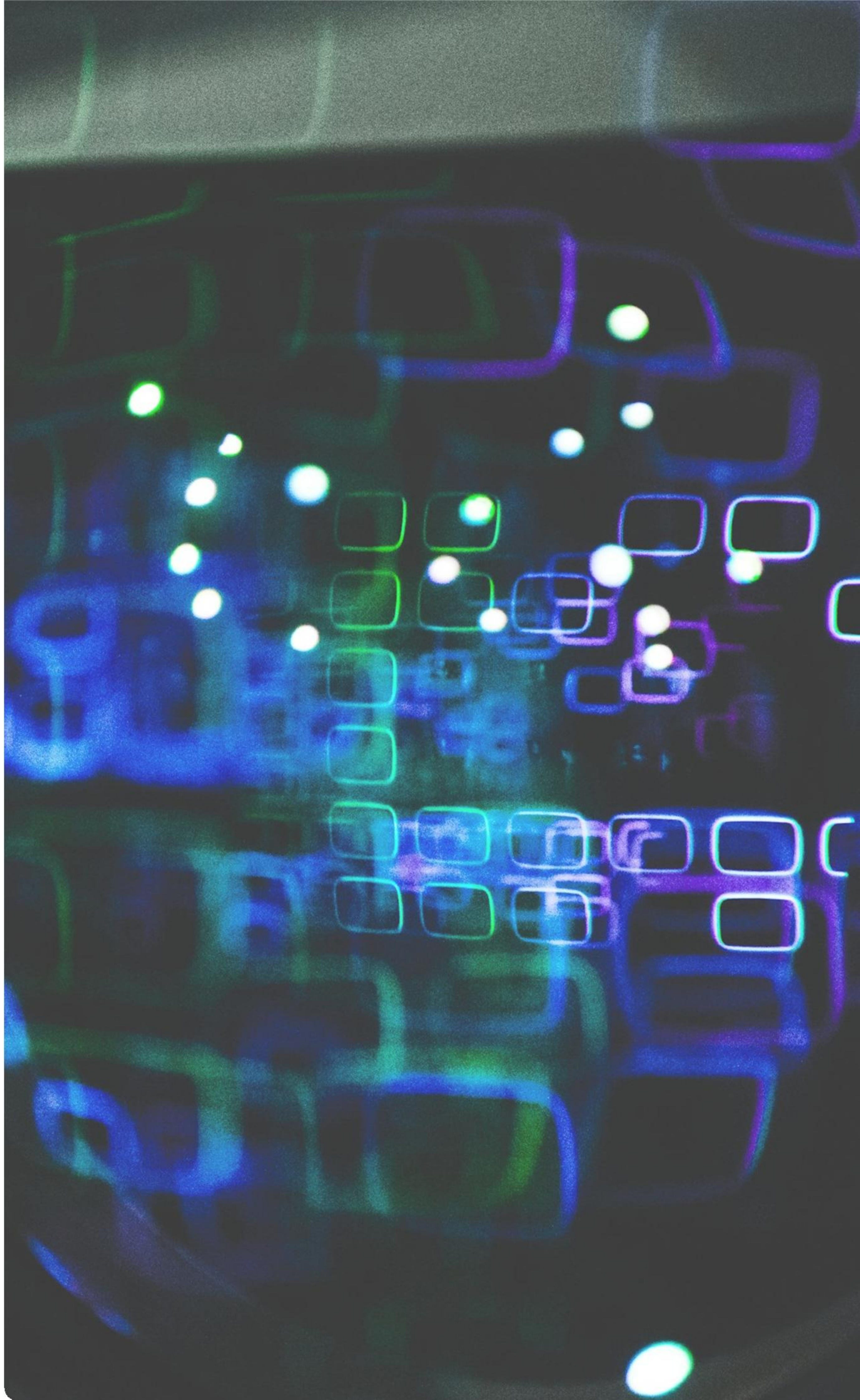
Isolation can also **reduce personal agency** by limiting access to online opportunities and social connections, which are important for well-being(Erfani, Abedin, & Blount, 2015). Privacy should not mean completely withdrawing from online life.

We argue that privacy should not be equated with isolation. Instead, it should focus on creating a digital presence that is balanced allowing individuals to engage online without excessive exposure. In other words, protecting online privacy should not require giving up digital rights or the ability to participate fully in online society.

Main insights:

Through the analysis of the case study, new themes are emerging considered more general factors influencing all the phrases of data practice in the online context, which linked to the social and technology aspects.

- Technology communication capability
- Algorithm bias and discrimination
- Accessibilities on devices and new technology
- Exclusion of some people or groups
- Psychological influence
- Hyper-connected space and online communities
- Isolation strategies do not work



Auto-ethnography study

Goal: contextualize privacy risks in online personal experience

Can individual aware of privacy risks in everyday life? The **goal** of this study is to **contextualize privacy risks with individuals experiences in everyday life.**

The **reason of using this method** is that social is subjective and built on various perspectives. Everyone is the expert of their experience(Chang, 2008).Since the privacy concerns are different from person to person and lack of clues or traditional methods to gather it, it is better to start from the researcher's first-hand experience and generate creative materials through the researcher's expertise to expand the research perspective further.Besides, auto-ethnography methods, allows the researcher to actively record their experience and reflect on their ideas, forming thinking models and insights (Schouwenberg & Kaethler, 2021). These results help to generate creative material and gather more insights.

Process

Four days of contextual observation and dairy logging

1. Observing clues: The researcher observes the real-world privacy issues with specific events experienced in everyday life. Based on the researcher's experience, the activity was repeated over days .

2. Diary of My one-day online data privacy experience

To facilitate quick record, the researcher used an online diary for logging events, allowing for notes-and screenshots. The recording captures the researcher personal concerns the privacy issues in the context.

3. Informal Conversations

During the days of study， informal conversations also took place in parallel. The informal interview included a cybersecurity engineer (online), a digital product manager (online), and the researcher's friends. These conversations are pretty casual and open, lacking the structured question support typically found in formal interviews.

These conversations aim to help deepen the reflection. These talks served as contextual extensions to help deep auto-ethnographic reflection . The informal conversation provided input from various viewpoints, offering comparative insights that enriched understanding of the context of online privacy in this study.

4. Reflectivity: "Reflect in action"

To facilitate timely and regular reflection, the researcher engaged in continuous, parallel analysis, as "Reflection-in-action" (Yanow & Tsoukas, 2009). With the support of online diaries, recurring issues and significant moments began to emerge through this iterative process. Reflecting on these patterns and themes gradually shaped the foundation for the researcher's narrative.

5. Summary analysis

After completing the four-day auto-ethnography, these insights were initially expressed through visual tools, such as graphic language and relationship maps, to facilitate internal reflection.

Findings from the Auto-ethnography study included:

- Six key insights: explore personal concerns and gain first-hand insight around online data privacy.
- Privacy-related experience: This is a summarized finding based on the personal concerns we can conceptualize privacy experience in the real world
- Privacy in domain: This is a summarized finding based on the personal concerns we can conceptualize privacy in domains

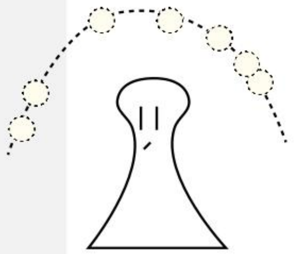
Key insights

1. Privacy risks does not only influence online
2. Lack of connection of personal data
3. Identity-based concerns
4. "Who is viewing" & "who is collecting" concerns
5. Who's responsible for privacy?
6. The burden of self-awareness and management

1."Risks does not only influence online"

One overarching understanding is that online privacy issues not only influence a person in the totally digital and virtually space sphere. For example, the researcher expressed greater concern about possibility suvilliance while at home than when in a café. Since the home is perceived as an intimate, protected space, whereas a café is already a semi-public environment where others are physically present, this suggests that online privacy risks could be embodied, depending on the location, the character of the space, and the presence of other people. This aligns with Palen and Dourish's (2003) theory that privacy is dialectical: the same surveillance can trigger vastly different emotional and cognitive responses in individuals depending on the situational context.

Another key evidence is that in current connected online environments, privacy issues can be inherently linked to the privacy of others in shared digital spaces. For instance, when we are in an online meeting, the privacy of each participant, such as their face, voice, and any materials they share, is interconnected with that of all other members. In such online settings, the boundaries of privacy can blur, as one person's exposure may inadvertently reveal aspects of another's. These findings are linked to the theory that privacy is collective and contextual in the digital age (Sarigol et al., 2014).



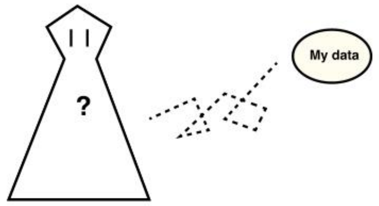
"Risks does not only influence online"

2. Lack of connection of personal data

A significant personal concern throughout the study is the sense of losing control over personal privacy in the online environment, which could lead to a decline in attention to personal privacy. Our personal information continues to move across multiple services, countries, and contexts without our knowledge.

Upon analysis, one key reason for this disconnection and ownership is the seamless experience offered by online platforms. With minimal “friction” (which refers to the extra effort required by users in their experience) and almost no clear signals, it is easy for people to forget that privacy risks exist (Sheahan et al., 2024). The smoothness of the experience is intended to be designed by online service and technology development.

These observations point to a key finding: as digital experiences become more effortless and efficiency is valued, there is less friction in the user experience, which could hinder users’ awareness and engagement with privacy.

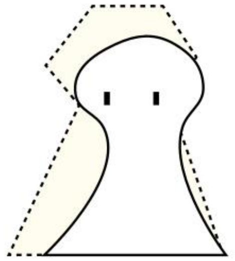


Lack of connection of personal data

3.Identity-based concerns

During informal discussions, we repeatedly highlighted identity-related issues as one of their biggest concerns. These concerns are particularly prominent during the phases of data processing and dissemination.

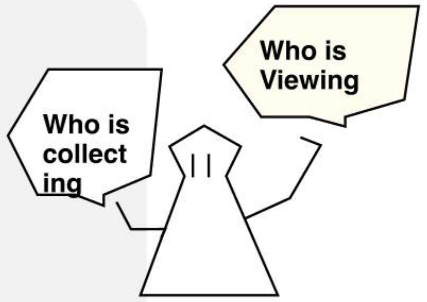
Beyond the invasion of identity, there is an added layer of concern: once identity is established, systems can act to control individual choice, often without their awareness. For example, targeted advertising leverages personal profiles to deliver highly tailored suggestions, nudging people toward specific products or behaviors. These findings indicate a shift in deep concern in online privacy: from “the service knows me” toward a more profound unease over “the service could decide who I am.”



Identity-based concerns

4. “Who is viewing” and “who is collecting” concerns

Another key finding from the study highlights the concerns over who collects data and who views or interprets it. However, the device could collect personal information without the user’s awareness. The personal concern is that the person viewing these collected data could generate a more harmful impact than what is collected. Raw data has limited meaning, but once it is processed and interpreted, it can generate far greater implications about individuals.



“Who Is Seeing Me?” vs“Who is collecting”

5. Who’s responsible?

Another concern is that, despite individuals' ability to make informed choices about their online behavior, their influence over systemic privacy practices remains minimal. This problem becomes even more frustrating after a privacy violation, or one may feel a sense of wrongdoing.

There is ongoing concern about who should be held responsible for privacy violations in various contexts, including individuals, platforms, service providers, and the government. Individuals might have no choice but to protect their privacy with the current structure.

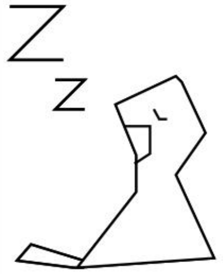
Whose responsibility?

6. The burden of self-awareness and management

Online services and apps offered users the ability to delete or manage their data. Currently, management and awareness mainly involve accepting or declining cookies on websites, reviewing app permissions, responding to data breach notifications, updating privacy settings across multiple platforms, and evaluating terms of service changes(O’Byrne,2025)

However, in practice, researchers have found that individuals often face significant challenges： 1. lack a clear understanding of what privacy truly entails in these complex self-management systems. 2. Individuals are expected to manage it themselves. These management tasks can be time-consuming, confusing, and exhausting. 3. Tools exist to support privacy management, such as cookie banners and privacy centers, which are typically standardized, failing to reflect the dynamic nature of privacy. For example， collection is often treated as a one-time action, such as accessing “I agree” on a website once. In reality, the lifecycle of data continues long after consent is given.

Overall, the current system provides limited support for building privacy awareness.



The burden of self-awareness and privacy managenent

Figure 2.18 : 6 personal concern insight

Summarized findings

Privacy-related experience

This summary shows that what the online privacy-related experience is like in the real life.

- **Privacy risks are pointless in real life.**
  - Privacy risks exist everywhere, 24 hours/7days.
  - Even when we are offline or not engaging directly with a platform. There is little touchpoint for us to aware of the risks of privacy.

- **Privacy could be perceived through specific interaction.** As Goffman (1959) describes “interactional incidents”. These events do not announce privacy risks themselves through alarms. Example from the reflections illustrate this: People can feel continual privacy threats emotionally, even when nothing seems to be happening. The example is sometimes feeling an inexplicable unease while filling out a form.

  - **Perceive risks from the clues:** From personal experience, small signals can suggest privacy risks and the need for privacy protection, such as being asked for a password again or noticing that the voice icon on a computer is active. However, these clues are often subtle and unclear, which aligns with the theory that people interpret privacy through contextual clues (Tang et al., 2022).
  - **Perceive risk through event results**: Compared to these tiny clues, privacy awareness becomes significantly stronger when people directly experience the results of a privacy breach. One example is the moment when an AI assistant unexpectedly calls someone by their name, revealing that the system has access to personal information. Another example is that the researcher received a targeted ad that referred to her student status, while this is something she had never directly disclosed to the website.

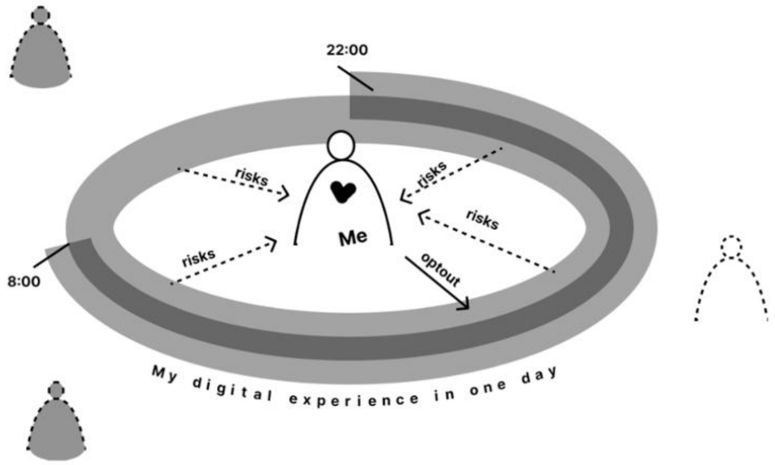


Figure 2.19: Event based experience

Privacy risks in domains

As explored further, we consider that privacy can overlap various domains. Inspired by the interlinked domains of a psychology of privacy framework (Stuart et al, 2019), we identified three interconnected domains that define how we might perceive and respond to privacy risks in various domains. They are included

- **Personal domain:** This refers to the internal space of emotions, memory, and embodiment. .In this domain, privacy is deeply tied to a sense of self. The domain that people “feel”For example, people's willingness to cope with privacy issues and their attitude towards privacy can influence the agency and controllability in this domain.

- **Interaction / experience domain:** This is where interactions occur. For example, the physical and digital spaces where people interact with physical devices and the invisible data generated in the digital space.

- **Social-inferred domain:** This is not about what happens, but what we believe others might think, know, or assume based on our digital privacy practices. This domain highlights how privacy is deeply social and relational in nature. For example, social connections can occur in these domains.

How people treat privacy in these areas could reflect their values. The domains can tie to an individual’s core beliefs, which helps us classify privacy concerns in the collective insights presented in the following chapters.

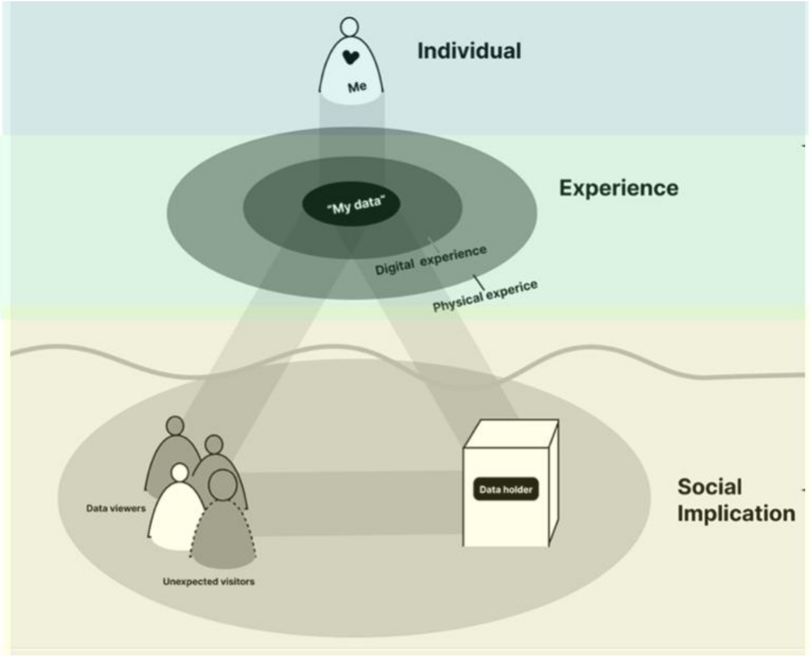


Figure 2.20: privacy risks in domains

Take away

How to use the findings?
In this section, we treated privacy as a lived experience. We represent how privacy in the currently experience could be and how privacy could be understood in everyday life, which helps us expand the research in the following phrases.

“Event-based experience” provide us an comprehensive understanding of privacy-related experience, which could used for envision the potential future experience in the next chapters.

“Privacy in domains” helps us understand how privacy concerns differ across levels of areas. This findings give us possibilities of locating and mapping concerns in layers.

Personal concerns insights
With the personal concerns support, we gain firsthand insights into how people experience the current online environment. This helps us develop speculative artifacts in the next chapter, which in turn helps us expand on the key insights.
Besides, we use of the results is to expand personal reflection by generating reflective material. With these insights, we designed and produced a sensitizing booklet intended to serve as a generative tool for the next stage of participant engagement.

Mapping the context

In this chapter, we answer the question: **What are the online privacy risks in the current social-technology context?** From literature review, cases study and auto-ethnography study There are many factors that we map our findings. We cluster them again in the cross-analysis map.

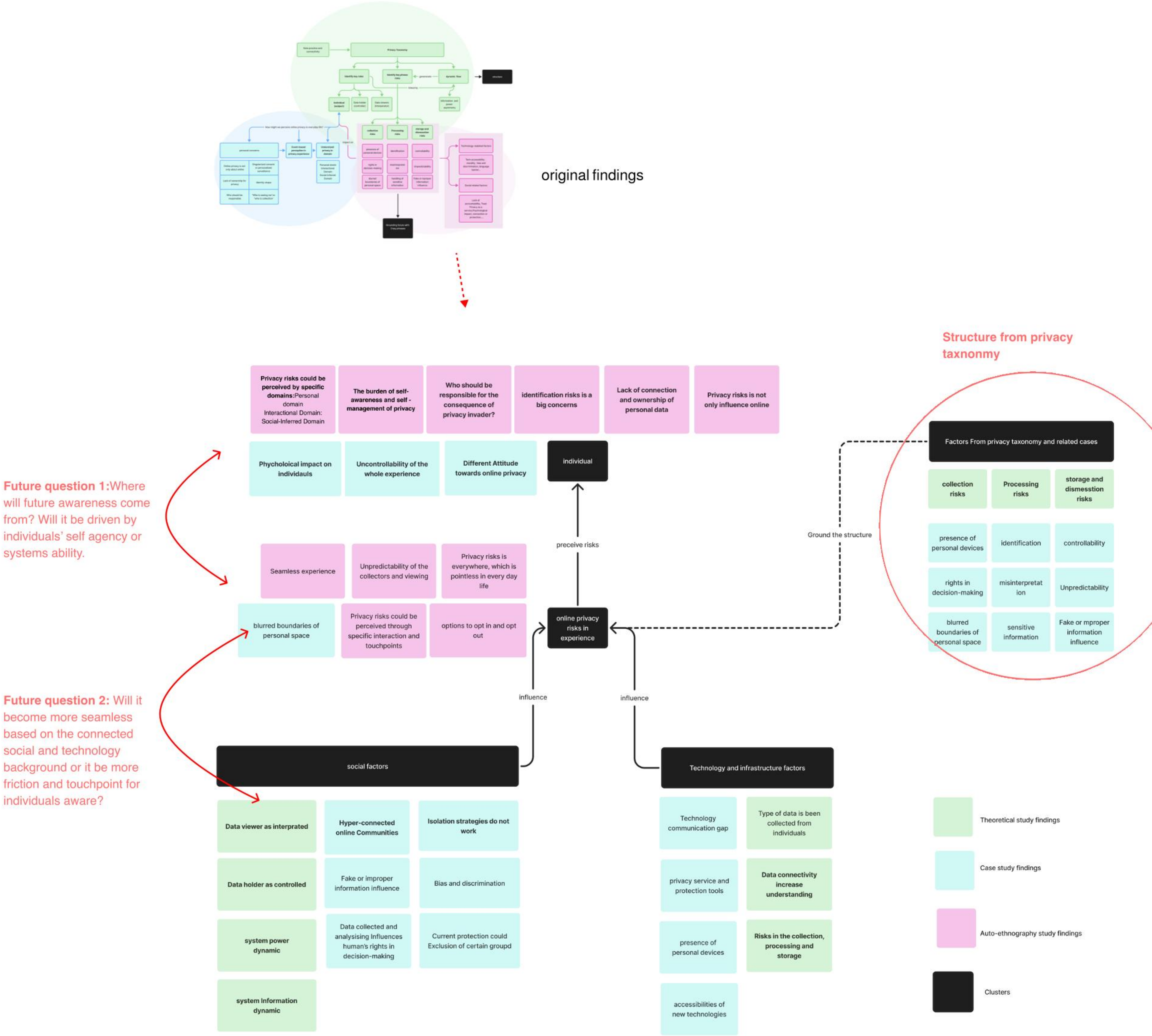
From our study, the **structure of the privacy taxonomy is highlighted as the foundation.** Data serves as the smallest and most essential unit of privacy. Each phase of the data lifecycle (collection, processing, and storage) carries privacy risks. By focusing on data activities in each phase, we can better link individual experiences of privacy with infrastructures in the digital life.

The factors could be levels from individual, social, technological, and online experience aspects introduce uncertainty and prompt us to question the future.

There are also two fundamental questions build for future envisioning:

Future question 1: **Where will future awareness come from?** Will it be driven by individuals' self-agency or systems' support ability?

Future question 2: **What kind of future privacy-related experience could be?** Will it become more seamless based on the connected social and technological background, or will it be more friction and touchpoints for individuals aware?



original findings

Structure from privacy taxnonmy

Future question 1: Where will future awareness come from? Will it be driven by individuals' self agency or systems ability.

Future question 2: Will it become more seamless based on the connected social and technology background or it be more friction and touchpoint for individuals aware?

Privacy risks could be perceived by specific domains: Personal domain Interactional Domain: Social-Inferred Domain

The burden of self-awareness and self - management of privacy

Who should be responsible for the consequence of privacy invader?

identification risks is a big concerns

Lack of connection and ownership of personal data

Privacy risks is not only influence online

Phycholoical impact on individauls

Uncontrollability of the whole experience

Different Attitude towards online privacy

individual

preceive risks

Seamless experience

Unpredictability of the collectors and viewing

Privacy risks is everywhere, which is pointless in every day life

blurred boundaries of personal space

Privacy risks could be perceived through specific interaction and touchpoints

options to opt in and opt out

online privacy risks in experience

Ground the structure

Factors From privacy taxonomy and related cases

collection risks

Processing risks

storage and dismesstion risks

presence of personal devices

identification

controllability

rights in decision-making

misinterpretat ion

Unpredictability

blurred boundaries of personal space

sensitive information

Fake or mproper information influence

influence

influence

social factors

Data viewer as interprated

Hyper-connected online Communities

Isolation strategies do not work

Data holder as controlled

Fake or improper information influence

Bias and discrimination

system power dynamic

Data collected and analysising Influences human's rights in decision-making

Current protection could Exclusion of certain groupd

system Information dynamic

Technology and infrastructure factors

Technology communication gap

Type of data is been collected from individuals

privacy service and protection tools

Data connectivity increase understanding

presence of personal devices

Risks in the collection, processing and storage

accessibilities of new technologies

🟩 Theoretical study findings

🟦 Case study findings

🟪 Auto-ethnography study findings

⬛ Clusters

Figure 2.21: Map the context of privacy risks and related factors

Conclusion

Overall, this chapter helps us ground the context of online privacy risks and identify the key factors. We can conclude our understanding in the following statement:

- There is a gap in people's awareness of their privacy in the current context, which characterized by asymmetric information and power. When people encounter privacy risks, they often struggle to recover and maintain resilience in the face of these risks. Some individuals are excluded from protection altogether. Privacy risks can affect individuals in various ways, often in unexpected ways. From the infrastructure of data collection, processing, and storage, these risks can also reinforce bias and discrimination, impact personal psychological well-being, attitudes towards privacy, and even behavior and decision-making.

- With the presence of devices, the hyperconnected environment, and communities, these influences are not confined to online spaces; they can extend offline and be shared across groups. Regarding responsibility for risks, there are unclear boundaries about who should be accountable for privacy breaches. Technology and communication can exacerbate the gap in people's understanding of online privacy, thereby intensifying existing privacy issues.

- There is also a persistent lack of connection and ownership for people and their own data, which prevents people from fully understanding their privacy. When considering people's privacy perceptions, limited interactions make it difficult for individuals to aware of online privacy, which can be understood in terms of individual experiences and social implications.

- Existing tools and strategies aim to assist individuals, including privacy management systems and external tools that visualize connections to mitigate privacy risks, as well as isolation measures. However, these solutions are not always effective and have limited impact. As online experiences become increasingly seamless, the responsibility for individuals to maintain self-awareness and manage their data effectively increases.

Considering the current risks of online privacy, it is important to raise awareness these privacy threats and spark conversations about the future. In the next chapter, we utilize our findings, with speculative design support, we expand our findings and deepen our understanding of online privacy.

03

Preposterous future

How could manifest privacy risks into speculative artifacts ?

The future is built on diverse opinions. Based on the initial findings of understanding the social-tech context of online privacy, this chapter serves as a transition point, **aiming to expand the privacy concerns by investigating various perspectives from people.**

In this chapter, we introduced **speculative design and three speculative artifacts** as probes for the preposterous future, which could raise awareness and spark discussions in the following up workshop.

Speculative design

Building on the initial understanding of privacy developed in the previous chapter, we use those findings as a foundation to gather further insights from diverse individuals. In this chapter, we translate our perspective into three tangible speculative artifacts, each situated within future scenario. These artifacts serve as provocations, designed to raise awareness, stimulate reflection, and spark critical discussions about digital privacy.

In this phrase, speculative design used as a powerful approach getting opinions for the online privacy issues. Speculative design can be overlapped with “critical thinking”, “critical design”, and “design fiction”(Malpas，2017). This design approach extends beyond traditional problem-solving methods to critically analyze their potential effects.

In contrast to design practices driven by commercial goals and immediate user requirements (Johannessen, Keitsch, & Pettersen, 2019), speculative design can question of normative cognitive and behavioral patterns. More importantly, the speculative design helps spark conversations among individuals about the potential outcomes of future possibites.

New voice

Speculative design does not adhere to a single set of approaches. Instead, it uses a variety of methods and objects to stimulate ideas and spark conversations. Here are some case studies of speculative design and critical design related to data privacy from the past. Here are some representative cases as follows:

The episode “black mirror: The Entire History of You” crafts a thriller story set in the near future, where everyone has access to a data implant that records everything they do, see, and hear. The permanent data story raises questions about its benefits and offers related reflections.

Figure3.1: Black mirror: The Entire History of You

A notable example is the centralization of data (Sinha, 2019). This interactive web-based project visually demonstrates how data is collected and what types of data are extracted, thereby helping to show the perceived value of personal information.

Figure 3.2:Visual material of Centralization of data

Another example is Who is Surveillance, which employs physical interactive installations to reshape the relationship between users and service providers, which helps individuals visualize what happens on the personal data collected by various online websites and regain control over data (Liu, 2021)

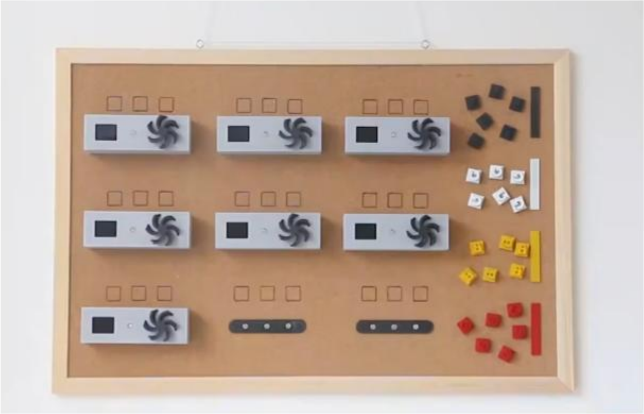


Figure 3.3: Physical installation of Who is Surveillance

These cases are new voices for the online privacy future, offering individuals vivid experiences of the speculative future and inspiring us to learn how we can utilize speculative narratives to build the future.

Preposterous future building

To raise awareness of individuals most effectively, here we use the stand of a preposterous future(“impossible! future”) in the speculative cone(Dunne & Raby, 2013).
To craft these alternative futures and make them tangible, we followed these steps:

- Scenario building using a future matrix
- Mapping possible directions
- Selecting ideas based on criteria and iterating through feedback tests
- Materializing three future artifacts

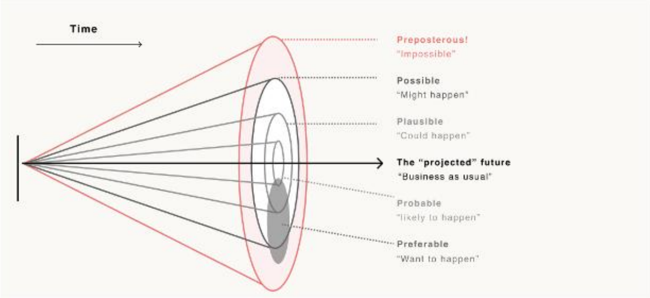


Figure 3.4：“preposterous future”(Dunne & Raby, 2013)

Scenario building using a future matrix

To envision the preposterous future, we employed a future matrix approach (Rhydderch, 2017), a tool for generating future scenarios. The future matrix was structured with horizontal and vertical axes, each representing a key uncertainty identified within the system. This framework enabled the exploration of possibilities.

Based on the findings from the previous chapter, we used two critical future questions as the axes in the matrix and mapped the future ideas. These questions help define the most uncertain aspects of the future as identified in the study presented in the last chapter.

- **Axis 1: Where will future awareness come from?** Will it be driven by individuals' self-agency or systems' ability?
- **Axis 2: What kind of future experience could be?** Will it become more seamless based on the connected social and technological background, or will it be more friction and touchpoints for individuals aware?

For each phase of the data process: collection, processing, and storage/dissemination. We applied a separate future matrix to guide exploration, resulting in three matrices corresponding to these phases. Using three distinct matrices allowed us to identify the preposterous future within each phase and to envision such futures more comprehensively.

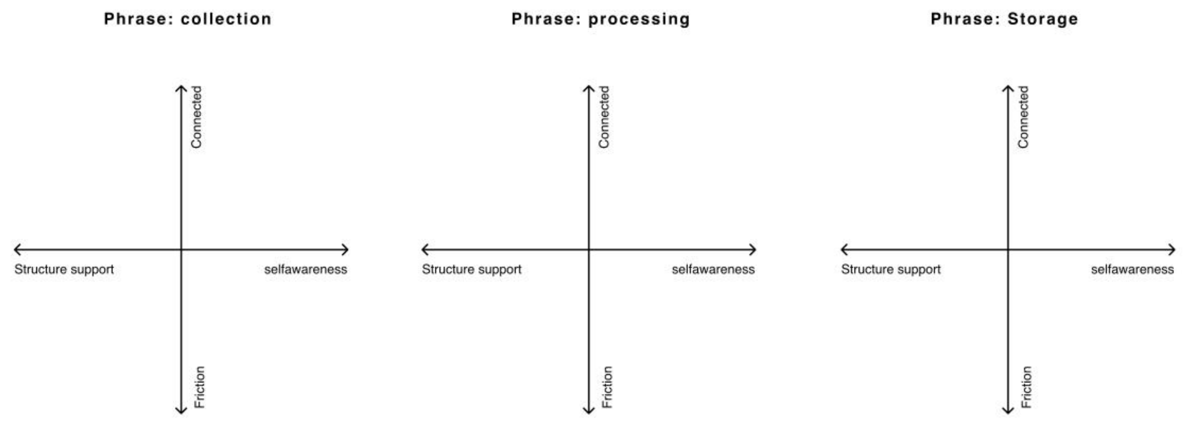


Figure 3.5: Future matrix building

Mapping possibilities

After building the future matrix, we explored a range of ideas and uncertainties through the future quadrants. From each matrix, we selected one representative scenario that best illustrated the core future risks and raised awareness of that specific phase.

Since there were many ideas, we applied several criteria, grounded in the literature and previous research findings, to select those that fell under the "preposterous future" category and could effectively envision such futures.

Criteria

To select the artifacts under "preposterous future", we highlight several criteria grounded in the literature and the previous research findings:

The artifacts should support the three phases of the data lifecycle separately.

Each artifact was designed to correspond to a distinct phase of the data practice lifecycle: data collection, data processing, and data storage. This alignment was intended to ensure coherence across the speculative exploration and to surface differentiated privacy risks at each stage.

The artifacts should have the ability to inspire critical thinking.

The artifacts were evaluated for their potential to provoke critical reflection and public debate, rather than provide answers. This aligns with Dunne and Raby's (2013) vision of speculative design as a tool for challenging assumptions and encouraging audiences to imagine alternative realities. The goal was not consensus, but productive discomfort, a state that fosters deeper dialogue. The artifacts should have the ability to inspire critical thinking.

The artifacts could evoke intense emotion.

Selected artifacts were also assessed based on their capacity to evoke emotional responses in a preposterous future, which could have made abstract data risks have a personally impactful effect, potentially leading to meaningful personal experiences (Dunne, 2013).

The artifacts could have ambiguity to open the discussion.

Lastly, the artifacts should convey intentional ambiguity, allowing for multiple interpretations that depend on the individuals' various backgrounds, values, and lived experiences. Ambiguity is a valuable quality in speculative design, used to open up space for broad discussion (Dunne & Raby,2013).

Materializing prepostous future

Considering all the criteria, three preposterous speculative scenarios were ultimately selected. We began prototyping speculative artifacts and objects to bring these future scenarios to life. Rounds of quick pilot tests were conducted to assess the clarity and effectiveness of each concept's narrative. After discussions with the supervisory team and quick feedback from two master's students in the DFI program, we refined the initial set of speculative narratives. We narrowed the focus to three final artifacts. This selection process was both iterative and reflective, balancing the objectives of the scenarios with participant feedback to ensure a comprehensive approach.

The reason for using interactive prototypes is that interaction enables people to immerse themselves in and engage with concrete, everyday scenarios, bringing the preposterous futures to life. These artifacts act as "hooks," prompting participants to reconsider their position in data practices while also reflecting on broader implications.

Eventually, three artifacts were developed, each representing a plausible future within the phases of data collection, processing, and dissemination.

Artifact: Collection

#Always wearable privacy#

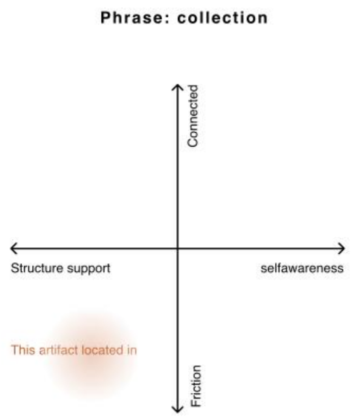
Data Box Belt

As more and more personal data is collected in the future, something begins to change. People start to wear a new type of object on their body: it is called the “Data Box Belt.”

This small belt goes everywhere with people. Inside, the data box belt stores various types of personal information, including location, health, and shopping habits. More importantly, it cold give people personal choice. In a world where data is constantly being taken, the Data Box Belt is a quiet way to take back control. It let people choice that when to share and when to take back their personal data.

When people walk near a shop, they reach into their belt and remove a small “location card.” Just by taking it out, and their location can no longer be tracked. In every environment and every step， people can fully decide whether to opt in or opt out of their data. At every moment, people must make a decision: do I want my data to be collected or not? What type of data do I want to collect, and which type should not be collected?What if you have full abilities to control of your personal data online?

The artifact is intended to highlight the risks in the collection phase.



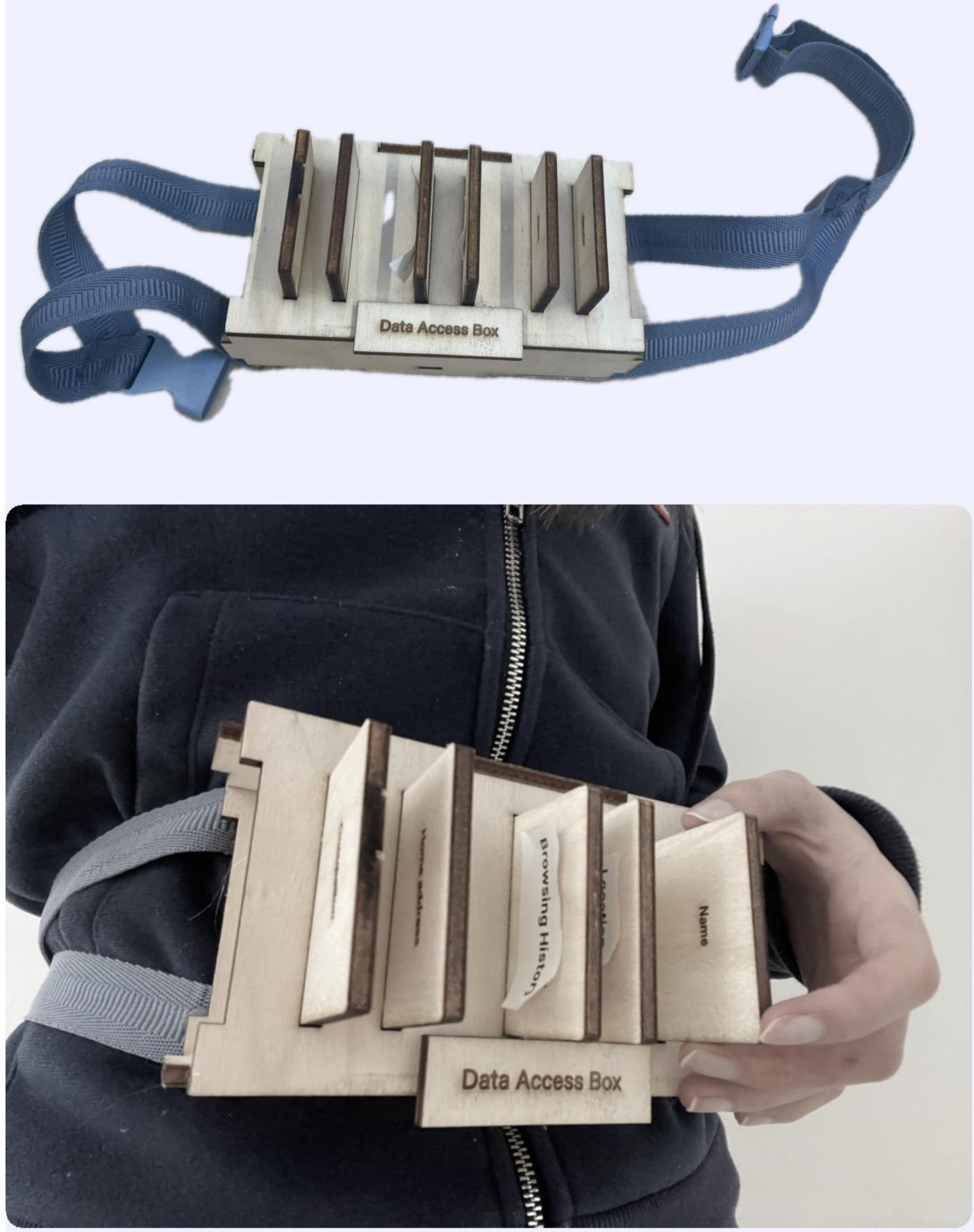


Figure 3.6: Data box belt

Artifact: Processing

#Radical transparency privacy#

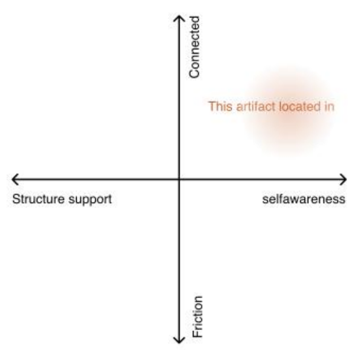
Interactive Dark web

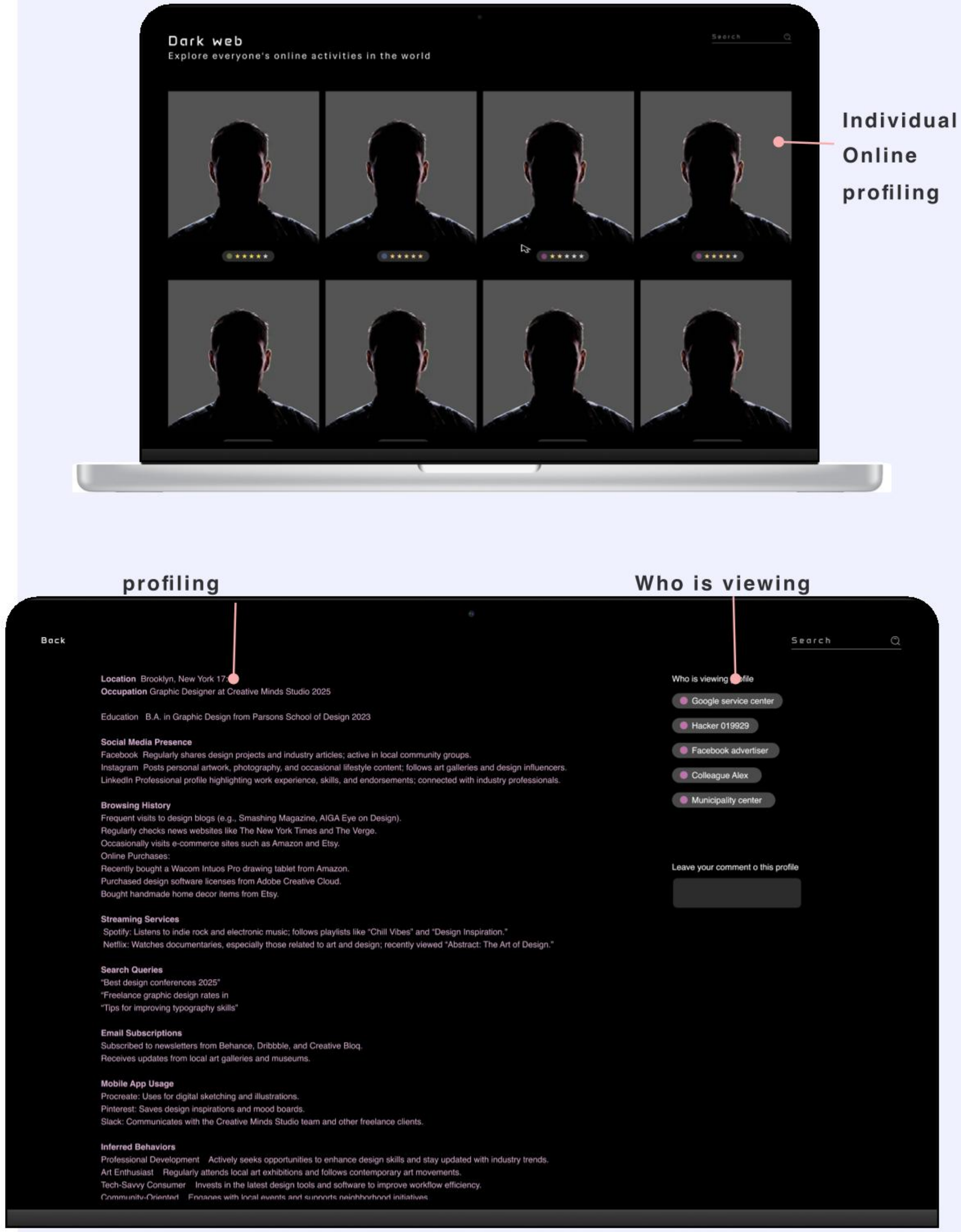
With the advancement of algorithmic technologies and the hyper-connectivity of global systems, a new platform has emerged called the “Dark Web,” where everyone’s data can be found on the interactive platform. If people want, they can easily visit the magical site by searching and viewing anyone’s online profile on it. These profiles provide details about the user’s location history and online purchases, as well as what they are seeing, and offer a prediction of their specific hobby or interests.

These profiles not only include the person themselves, but also those of friends, family, employers, and even hackers. Their profiles can be found on the website. Through the dark web, you can see and access anyone’s profile in the world. At the same time, others could also see your profiling in reverse. On the other side of the platform, a live activity feed shows who is currently viewing your data. They could be your boss, a friend, a stranger, any company or persons on the other side of the globe.Could you also play a roles as a data reviewer? What if processing results of every piece of your personal data is visible to everyone?

The artifact is intended to illustrate the risks in possessing phrases.

Phrase: processing




Dark web
Explore everyone's online activities in the world
Search
Individual Online profiling
profiling
Who is viewing
Back
Search

Location Brooklyn, New York 17:
Occupation Graphic Designer at Creative Minds Studio 2025

Education B.A. in Graphic Design from Parsons School of Design 2023

Social Media Presence
Facebook Regularly shares design projects and industry articles; active in local community groups.
Instagram Posts personal artwork, photography, and occasional lifestyle content; follows art galleries and design influencers.
LinkedIn Professional profile highlighting work experience, skills, and endorsements; connected with industry professionals.

Browsing History
Frequent visits to design blogs (e.g., Smashing Magazine, AIGA Eye on Design).
Regularly checks news websites like The New York Times and The Verge.
Occasionally visits e-commerce sites such as Amazon and Etsy.
Online Purchases:
Recently bought a Wacom Intuos Pro drawing tablet from Amazon.
Purchased design software licenses from Adobe Creative Cloud.
Bought handmade home decor items from Etsy.

Streaming Services
Spotify: Listens to indie rock and electronic music; follows playlists like “Chill Vibes” and “Design Inspiration.”
Netflix: Watches documentaries, especially those related to art and design; recently viewed “Abstract: The Art of Design.”

Search Queries
“Best design conferences 2025”
“Freelance graphic design rates in
“Tips for improving typography skills”

Email Subscriptions
Subscribed to newsletters from Behance, Dribbble, and Creative Bloq.
Receives updates from local art galleries and museums.

Mobile App Usage
Procreate: Uses for digital sketching and illustrations.
Pinterest: Saves design inspirations and mood boards.
Slack: Communicates with the Creative Minds Studio team and other freelance clients.

Inferred Behaviors
Professional Development Actively seeks opportunities to enhance design skills and stay updated with industry trends.
Art Enthusiast Regularly attends local art exhibitions and follows contemporary art movements.
Tech-Savvy Consumer Invests in the latest design tools and software to improve workflow efficiency.
Community-Oriented Engages with local events and supports neighborhood initiatives

Who is viewing profile
● Google service center
● Hacker 019929
● Facebook advertiser
● Colleague Alex
● Municipality center

Leave your comment o this profile

Figure 3.7: Interactive dark web

Artifact: Storage

Persistent reminders privacy#

Diagnose Kit

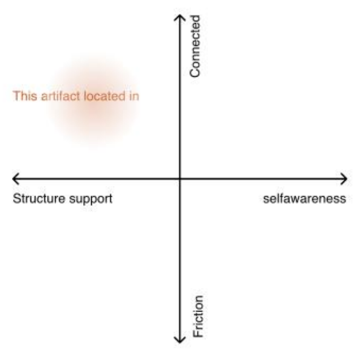
In the future, a new product for individuals will be launched: “a diagnosis kit”. This is a personal artifact designed to help individuals test the status of their digital storage across all devices, which can also be viewed as an “afterlife” of data usage.

Once people activate it, the artifact emit a tone and light to indicate that their data is being dissemintation. The more vulnerable your data is, the more urgent the alert becomes. The device monitors all traces around your health apps, financial trackers, social media logs, and more. For example, at your home, the artifacts sit on your desk, you hear red light pulses, and the voice speaks from the kit:

“Your health data has been accessed by a third party in an unknown jurisdiction. “Your data has been transferred outside the EU. We are unable to verify its current jurisdiction or status.”The ambiguity warning is intended. People are often informed that their data is being moved, is vulnerable, is being watched, or is even being sold, with no control. What if every piece of your data moving flow is visible to you?

The artifact is intended to illustrate the risks in the storage phase.

Phrase: storage



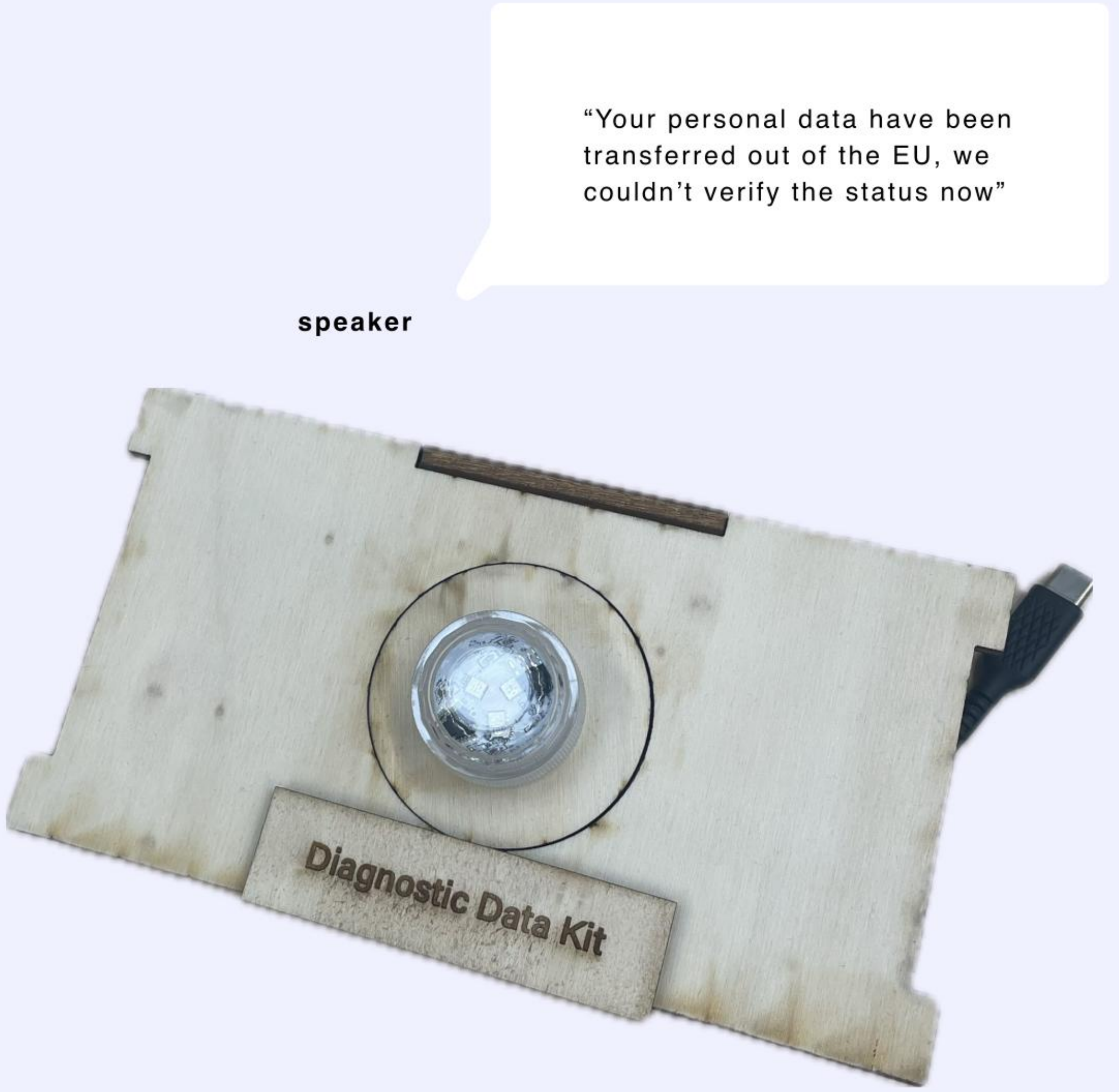

“Your personal data have been transferred out of the EU, we couldn’t verify the status now”
speaker
Diagnostic Data Kit

Figure 3.8: Diagnose kit

Conclusion

Three speculative artifacts in the preposterous future

These three artifacts were carefully selected and served as an entry point for discussion and reflection. They not only stand for the researcher's initial insights from the previous study but also resonate with Watts' (2008) assertion that "telling stories of the future is always a social, material, and political practice. It always has effects, which is always non-innocent." Through rich interaction scenarios and layered, ambiguous expressions, these pieces are used to reveal potential threats to data privacy.

Building with a future matrix.

The future matrix utilized the findings from the ground phase, which included the tension between individual awareness and structural/system support, as well as the prospect that the future will involve more risks or that all risks could be brought under control. Through the analysis of manifesting the risks in each stage, we have identified the three most provocative scenarios to inform our artifacts.

Gather insights in the following discussion.

This chapter serves as a transition to the three proposed artifacts, which act as initial points for understanding privacy. These were used in the follow-up speculation session to expand the discussion and gather collective insights during group discussions.

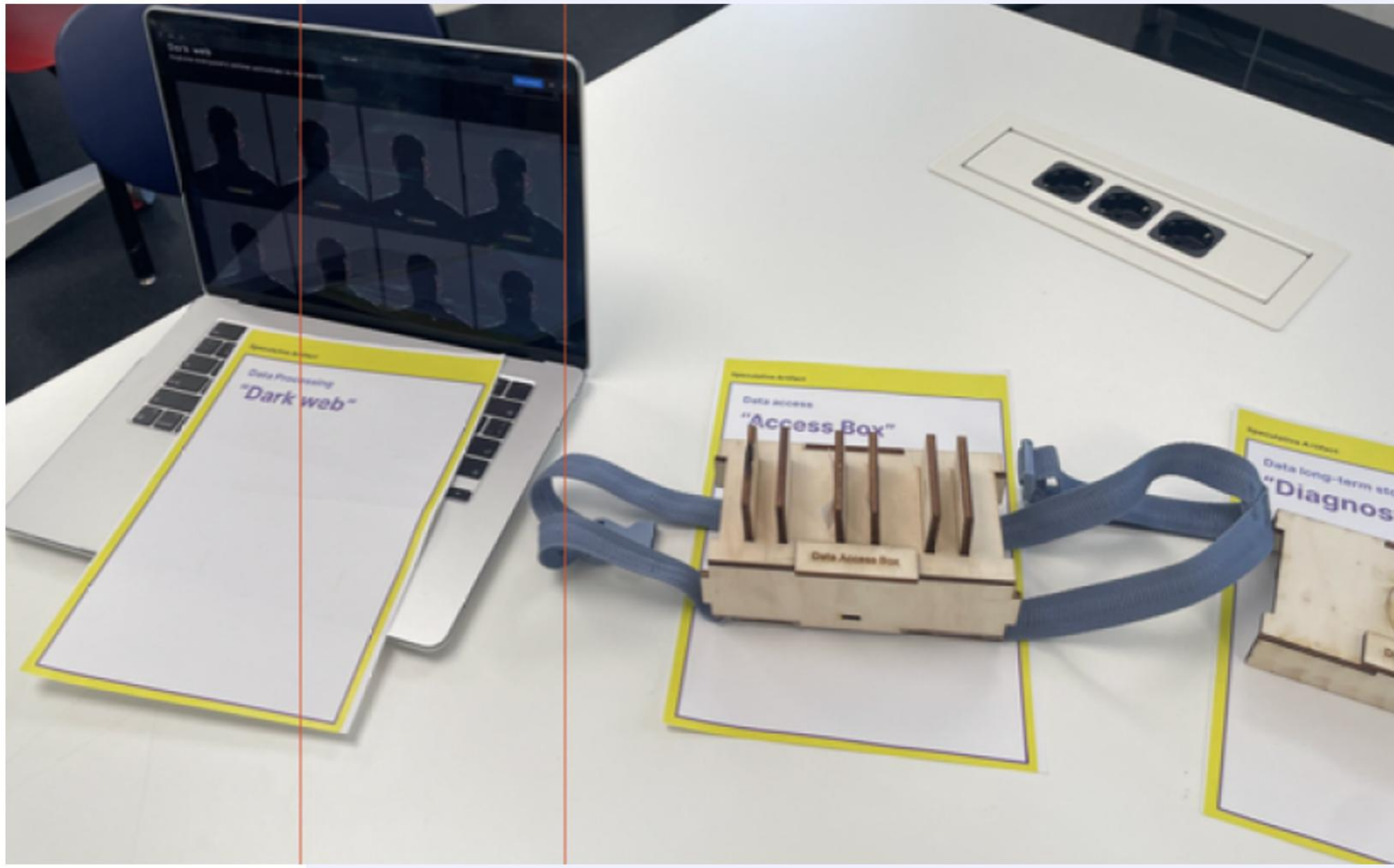


Figure 3.9: 3 artifacts

04

Raising awareness co-speculating workshop & insights

With speculative artifacts, we conducted a workshop **aimed at raising people's awareness of online privacy risks and gathering practical opinions on online privacy.**
After the workshops, we identified **nine concerns** that represent the concerns of people about the future of online privacy.

Workshop: Are you aware of your online privacy?

In the previous chapter, we introduced three speculative artifact probes materializing the “preposterous futures.” Each represents a phrase, including collection, processing, and storage. By making the risks visible, these artifacts have the potential to investigate people’s diversity and privacy concerns. In this chapter, we apply those probes within a participatory workshop setting to gather collective insights on people’s opinions on privacy.

Goal

We clarify that the goal of the workshop is to raise people’s awareness and understanding of people’s concerns about online privacy throughout the three speculative artifacts in the preposterous future.

Why do we conduct a participatory workshop format?

- The workshop is a bottom-up approach that enables open-ended exploration. Workshops create a shared space for dialogue, debate, and the exchange of ideas. This format not only allows for the collection of diverse and layered viewpoints but also helps reveal how individuals negotiate, compare, and co-construct their understanding of privacy in a group setting.

- Workshops also offer participants value for understanding privacy for themselves beyond research goals. They are mutually beneficial spaces where participants are not only responding, but learning, becoming moreaware of online privacy. Through speculative storytelling and interactive discussion, the probes serve both as research tools and educationalinstruments, increasing participants’ critical awareness and stimulating meaningful reflection.

- Furthermore, compared to a 1v1 interview, the collective nature of the workshop facilitates the emergence of conflicting opinions, and shared emotions for these “preposterous future”, which are often absent in individual interviews.

Setting

1. Recruiting participants

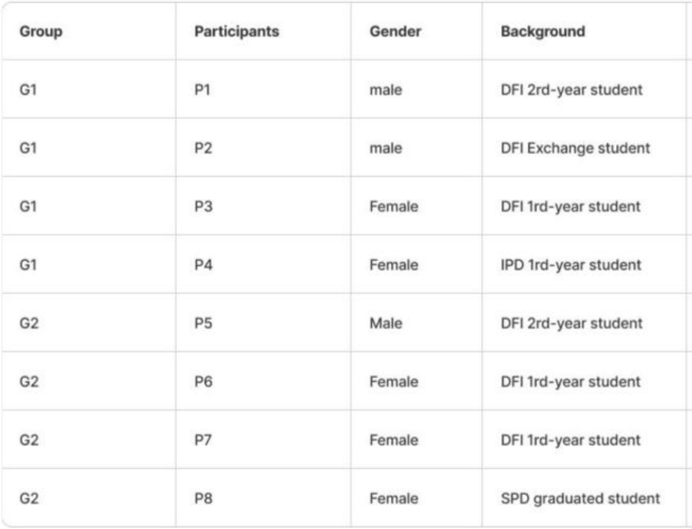
Eight participants were recruited through both online and offline methods. Recruitment was advertised via WhatsApp channels commonly used by students, as well as through physical posters placed around the Faculty of Industrial Design Engineering (IDE) at TU Delft. These posters included a brief project description and a QR code linking to a sign-up form, allowing interested individuals to register conveniently. A total of eight participants were recruited based on their expressed interest in data privacy. The participants were divided into two smaller groups, each consisting of four participants, to encourage active discussion and group dynamics. To have a mix of perspectives, the backgrounds in each group ensure that there are non-DFI students involved.

2. Sensitizing

Based on the context mapping, the Sensitizing booklet is to help participants and the researcher better prepare the workshop. This booklet is designed to engage participants in a reflective journey, similar to an auto-ethnography, a highly personal journey. The sensitive booklet introduces the context of the workshop and helps participants start reflecting on their online privacy. Sensitizing the booklet involves four steps that participants must complete within four days before the workshop.

3. Set up for the workshop.

The workshop took place in a studio room at the Industrial Design Engineering (IO) building at TU Delft. Before the workshop, participants receive a confirmation email from the group and the participant (Appendix). The sensitizing materials were also attached to this email, inviting people to complete them. Each group participates for approximately one hour, following a structured procedure designed to engage participants in speculative thinking about online privacy.



Group	Participants	Gender	Background
G1	P1	male	DFI 2rd-year student
G1	P2	male	DFI Exchange student
G1	P3	Female	DFI 1rd-year student
G1	P4	Female	IPD 1rd-year student
G2	P5	Male	DFI 2rd-year student
G2	P6	Female	DFI 1rd-year student
G2	P7	Female	DFI 1rd-year student
G2	P8	Female	SPD graduated student

Figure 4.1: Participants recruited for the workshops: Are you aware of your online privacy?

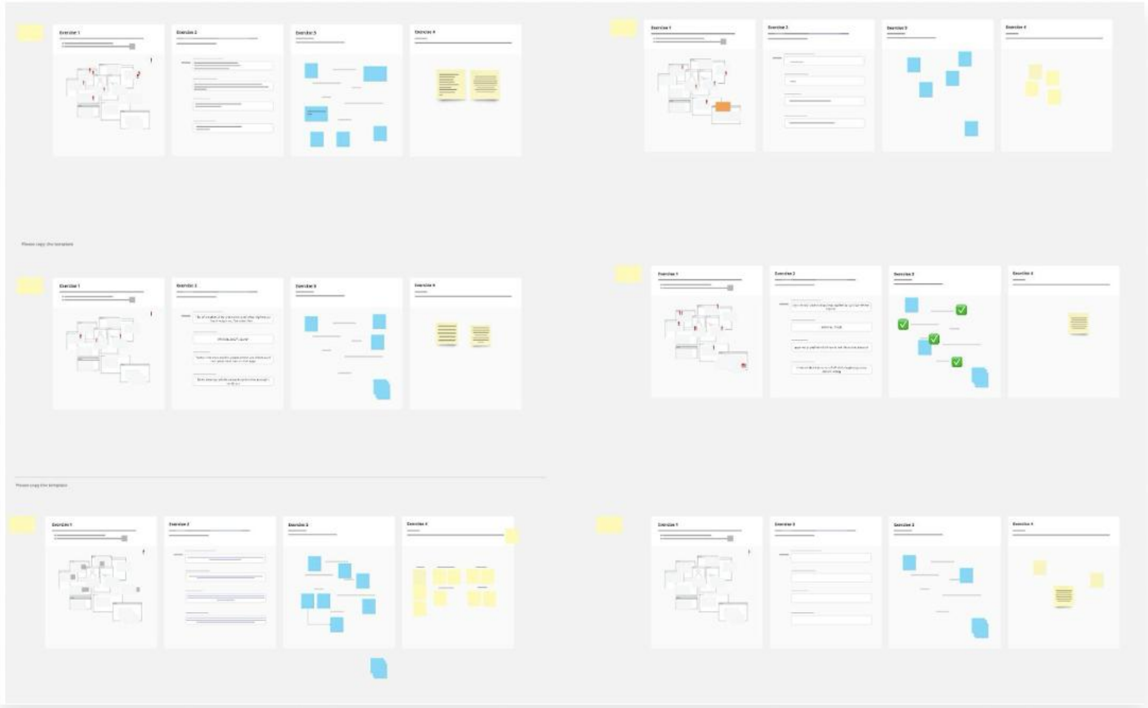


Figure 4.2: sensitizing booklet

Procedure

This workshop procedures is designed and iterated with the two rounds and here we shows that final version of workshop implement in the second workshop, which included these following steps:introduction, talking about speculative artifacts,talking about speculative futures,

Step 1: Welcome and Introduction (10 mins)

The goal of this part is to welcome and immerse participants in the workshop.

Firstly, participants were welcomed with refreshments and encouraged to engage in casual conversation to create a comfortable atmosphere. The purpose of the study and the workshop procedure were explained in detail. A consent form was provided to participants, which emphasized that participation was voluntary and that they could choose not to answer any questions or withdraw from the study at any time without providing a reason.
After these, people can freely share some writings from the sensitive booklet, which helps them recall the context and provides a warm-up for group discussion.

Step 2: Talking about Speculative Artifacts (30 mins)

At the beginning, participants were introduced to speculative prototypes through an audio guide, creating an immersive experience and evoking emotions.

The narratives include the introduction of future contexts and stories of speculative artifacts, which were designed to illustrate possible future data privacy challenges, prompting participants to share their thoughts and emotions.

After hearing the audio guide about these artifacts, people can interact freely with the three prototypes and begin to share their opinions about them. To help them express themselves, a ProEmo tool was provided to assist participants in articulating their emotions and nuanced feelings towards the future (Desmet, 2019). The questions provided to individuals are:

- What is your impression of these artifacts?
- What are your feelings after experiencing these artifacts?
- What do these artifacts mean to you?

At this stage, participants engage in open discussions and reflections on the artifacts and fictional scenarios.

Step 3: Talking about Speculative Futures(30 mins)

The goal of this step is to speculate about what the future may hold with these artifacts. After engaging with the speculative artifacts, participants engaged in a group discussion about what online privacy might look like in the future. They use physical stickers to write down their opinions about the future and share them with others. There are also some questions provided to help people express their opinions about the future.

- What is your opinion on this future?
- What are your concerns?
- What can you envision for the future?

First, each participant conducted individual brainstorming using stickers (5 mins). This was followed by a group discussion (20 mins) to explore and discuss ideas.

Step 4: Wrap-up (10 mins)

The goal of this part is to help reflect the workshop process and add value for participants. After the general reflection on the workshop process took place, gathering the findings of the workshops and
Participants were asked:

- How did you feel during the workshop?
- What do you gain from the workshop?

At the end of the session, participants received metal bookmarks as a token of appreciation for their time and effort.

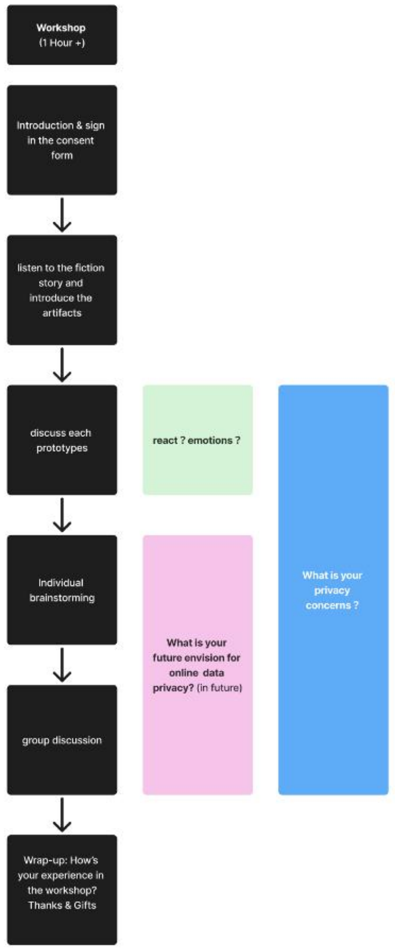

Workshop (1 Hour +)
Introduction & sign in the consent form
listen to the fiction story and introduce the artifacts
discuss each prototypes
react ? emotions ?
What is your privacy concerns ?
Individual brainstorming
What is your future envision for online data privacy? (in future)
group discussion
Wrap-up: How's your experience in the workshop? Thanks & Gifts

Figure 4.3: Developing the workshop procedure

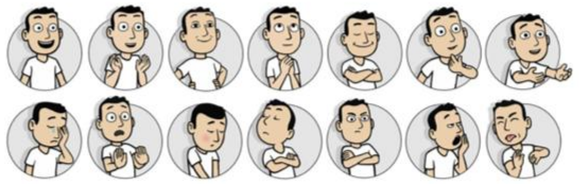
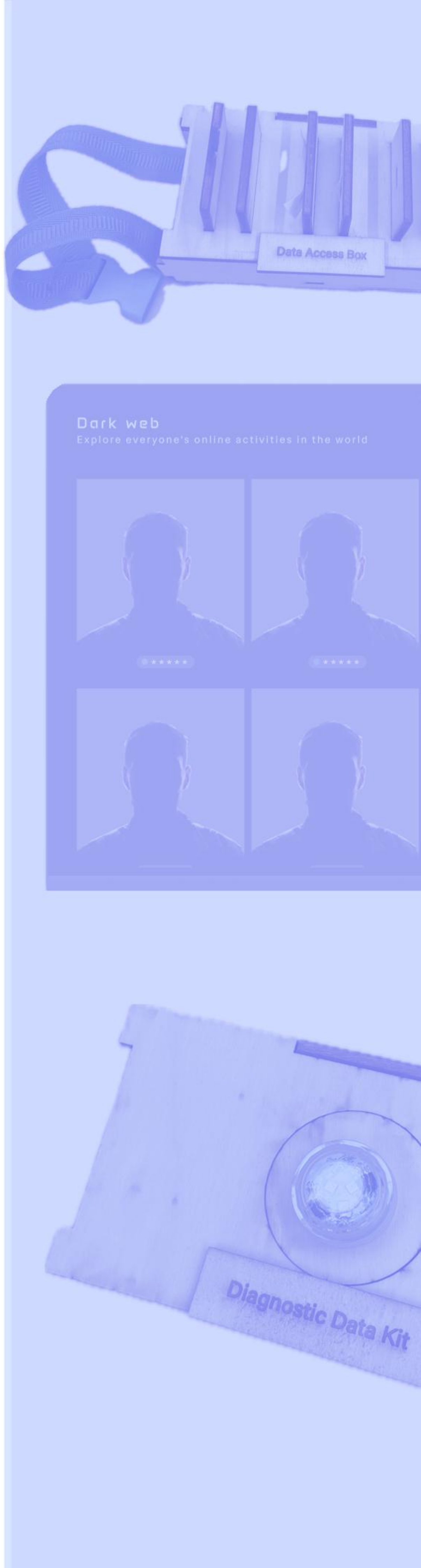
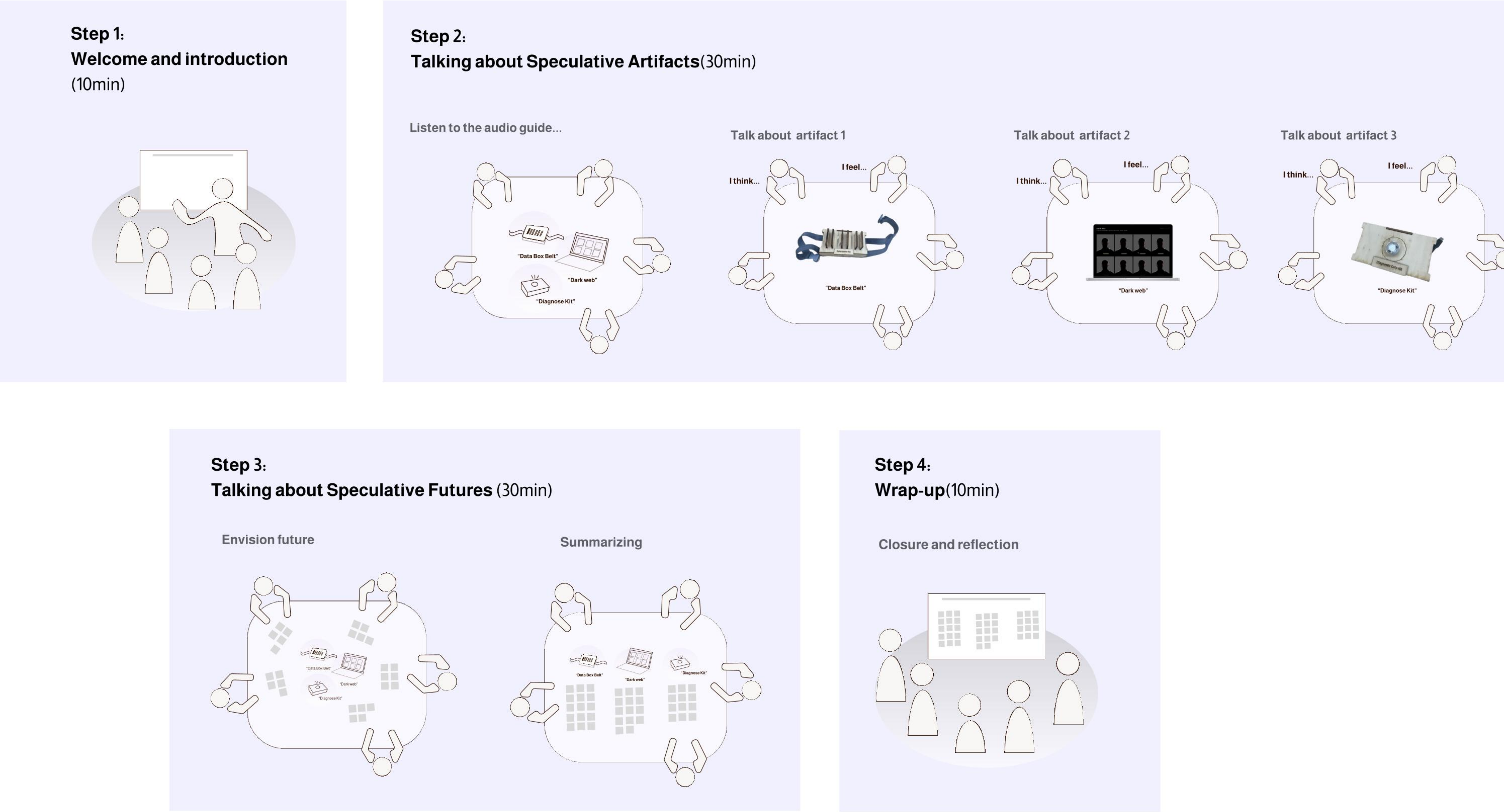


Figure 4.4: ProEmo (Desmet, 2019) to identify the emotion

Figure 4.5: Audio guide



Procedure



Step 1:
Welcome and introduction
(10min)

Step 2:
Talking about Speculative Artifacts(30min)

Listen to the audio guide...

Talk about artifact 1

Talk about artifact 2

Talk about artifact 3

Step 3:
Talking about Speculative Futures (30min)

Envision future

Summarizing

Step 4:
Wrap-up(10min)

Closure and reflection

Figure 4.6: visualize workshop procedure

Analysis

Preparation: Audio recordings from the sessions were transcribed. Relevant participant quotes were anonymized and documented on a FigJam for further analysis.

Coding: Identify the quotes with the statements card. The coding system was developed based on the context-mapping skills(Sanders & Stappers, 2013), where each quote was examined and tagged with relevant codes to categorize into insightsJ

Themes development: Groups of related codes were clustered into overarching themes. These themes were linked back to the goal (privacy concerns), providing a structured interpretation of the participants' insights.

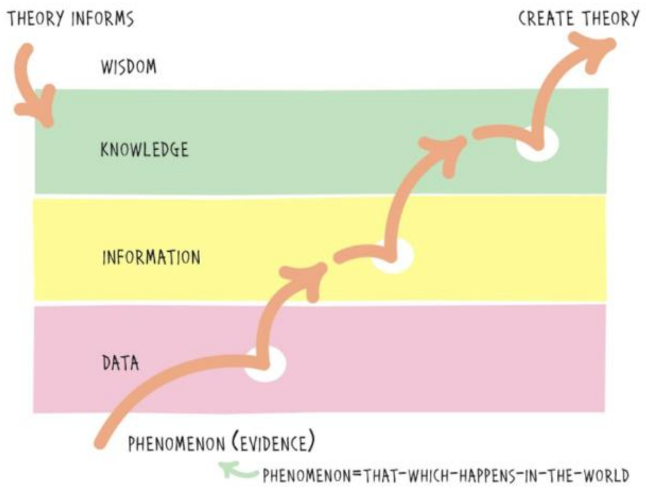


Figure 4.7: analysis method (Stappers and Sanders, 2019)

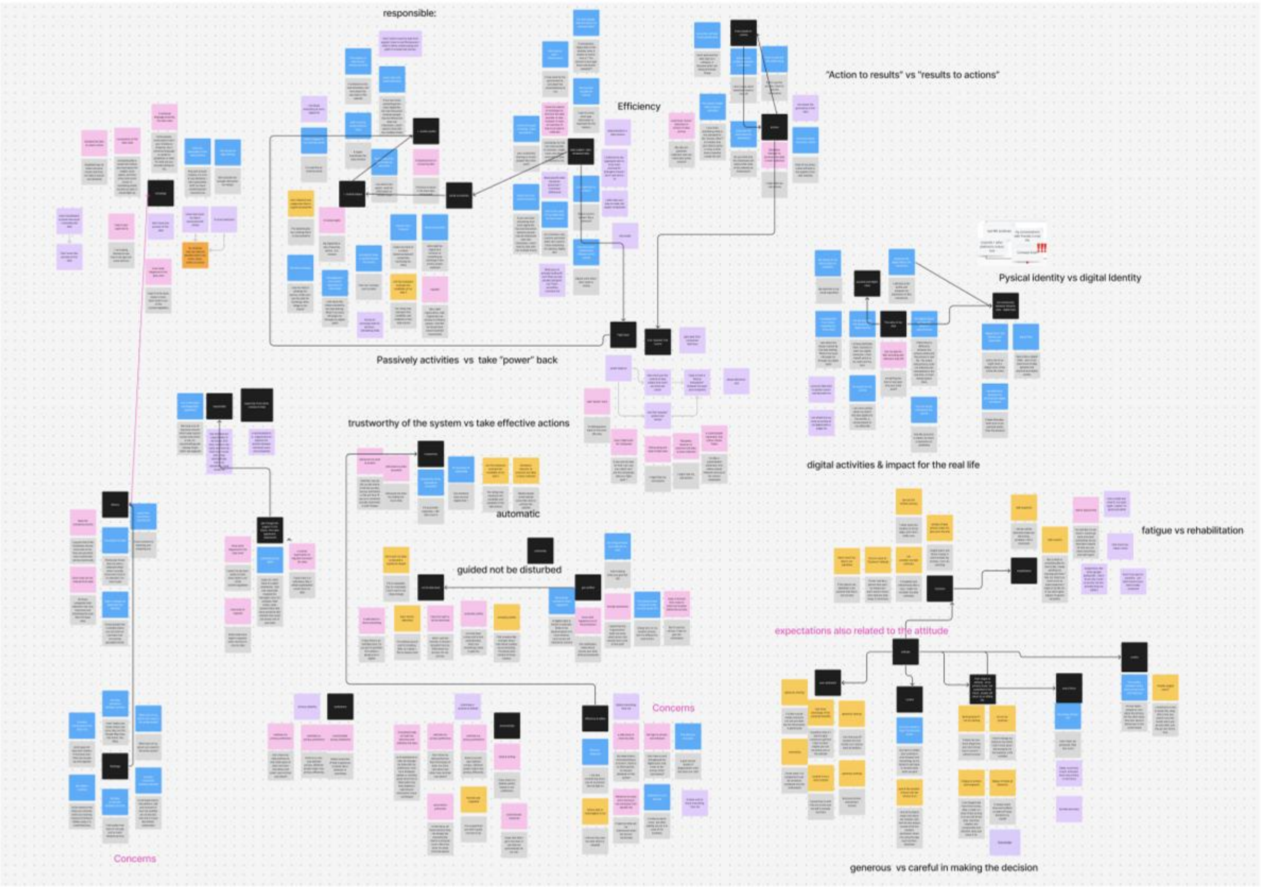

responsible:
"Action to results" vs "results to actions"
Efficiency
Pysical identity vs digital identity
Passively activities vs take "power" back
trustworthy of the system vs take effective actions
digital activities & impact for the real life
automatic
guided not be disturbed
fatigue vs rehabilitation
expectations also related to the attitude
Concerns
Concerns
generous vs careful in making the decision

Figure 4.8: Theme development

Themes

Concern1: Lack of privacy knowledge and literacy

Participants conceded their worry about their own privacy **knowledge and literacy limitations**. While they were aware to some extent, they identified themselves as not being privacy experts, especially on technical aspects."Previously I knew that my data was collected, but when I actually realized how much was collected, it became more scary.""I know someone is watching and analyzing me."

They also express that they would like to **understand the intention, what was behind this surveillance**, what companies were looking for and what kinds of inferences were being made from their data.

"All these categories that infer behavior are very important and interesting for sure, even more so than the input data."

They admitted that their present conception of how the companies use their data is **founded on their assumptions and not on what takes place.**

"I assume that if the companies access more data about me, they can technically provide more customized services."

Participant was worried about the **degree of granularity of data collection**, in addition to what occurs following the simple data collection. All these categories that infer behavior are very important and interesting for sure, even more so than the input data."

There is a desire for a more universal and standardized way to understand privacy-related knowledge: "Like a universal language, model, guideline, or style that clearly communicates what data you are actually taking from me."

Concern 2: Association between the specific behavior and consequences

Another concern shows that the gap between their **actions and the consequences:**

"What does each of my actions cause?"

This gap could be attributed to the inherent nature of data . Since data is interconnected and utilized across platforms in the background, it is difficult for users to grasp how these processes reinforce the disconnect between their behavior and its outcomes."In the back end of the platform, your account or even two profiles are still connected.""I did realize how one app could pull so many website services." "I don't perceive data types as categories, it includes everything I am doing."

At the same time, a struggled to **identify specific measures** they could take to strengthen their control over data privacy or determine which behaviors led to certain outcomes:

"I don't know which websites I need to turn off."

Concern 3: Digital identity and its connection to real-life identity

Another concerns exists between **their digital identity and their real-life identity**. They feared that if their digital identity were fully exposed, it could lead to negative judgments from others based on their online data: "I am afraid that my boss might judge me based on my digital data." "I am concerned that fake data could spread rumors and discredit me."

There was also a discussion about the **potential of having a "digital twin"**, a representation of one's entire life online:It could feel more comfortable if their digital identity was not closely tied to the real-life identity. They noted that online visibility felt more comfortable than offline: "It feels friendlier, feels nicer to be watched online than in the physical world."

There also an envision for make the digital identity and real-life identity could be clearly separated : "I wish my digital activities could be completely separated from my real-life activities."

Concern 4: The relationship between the data provider and the reviewer

Participants also discuss need of transparency data sharing between data providers (individuals) and data reviewers (companies, platforms, or others).
“As a reviewer, why do I need to see this data? Do I need to know everything about a person’s digital life?”
Participants were also concerned that the ability to access someone’s full digital life could affect the quality of real-life interactions.
“If you can know everything from someone’s digital life, the real interaction between people may be influenced. There would be less real interaction; I don’t need to chat with him multiple times.”
The envision around have more control over what data is shared, stressing the importance of setting boundaries on how much of their digital life is exposed. They wanted transparency not only from data providers but also from data reviewers.

Concern 5: Responsibility for decisions

Currently, privacy responsibility primarily **falls on users**, requiring them to read privacy policies and manage their privacy settings using available tools. However, participants found it challenging to navigate these decisions, especially given the complexity of data practices.

There is a desire for privacy responsibility is towards the direction shift away from individuals, **making privacy protection more automated and regulated:**
“Less and less our responsibility in the future. Just like how my front door comes with a lock automatically, that’s not something I need to plan for.”
“When I use the internet, I shouldn’t have to think about my privacy. It’s my privacy.”
Participants also emphasized the need for **stronger legal regulations** to define clear boundaries on data usage:
“There need to be more laws to regulate when and how to use our data.”
“I just need to know what happened in the grey area.”

Concern 6: The social equality impact

Another concern is about i**nequality in data privacy**, particularly regarding who has control over data and how it impacts different social groups. They worried that those with technical expertise (eg. web-developers) might have ways to protect their own data, while others remain vulnerable:“If someone is a web developer, will they be able to block their own data from these websites?”
This imbalance could lead to deepening social divides, **where certain groups benefit from data protection while others face increased exposure.**
“I worry about bad actors using my information to commit fraud.”
Some participants even associated corporate data collection with exploitative behavior, comparing it to a form of “**violence” or power imbalance:**
“When companies access my data without my control, it feels like a violent act.”
The idea of data monetization raised further questions about **fairness**. Participants noted that they exchange their personal data for services, but questioned whether they could use their data as a valuable asset for other exchanges in the future:
“I use my data to exchange for services, but can I exchange it for something else in the future?”
There is an envision for a shift is translating the individual from **a passive role to an active one**,where individuals have more power over their data, rather than simply surrendering it to companies:
“If companies use my data for free, can I use their data in return?”
“Can I access companies’ data as a fight-back?”

Concern 7: Personal preference
Participants noted that privacy concerns vary from person to person, as individuals have different thresholds for what they consider acceptable. Some are willing to trade certain aspects of their personal data for better services if they perceive minimal risks to their privacy.However, the current system collects data indiscriminately, without considering these personal differences.
There are envisions for customizable privacy framework that could be linked to their identity, allowing them to define their own data-sharing boundaries. This expectation highlights a need for more individualized control over data sharing, rather than a one-size-fits-all approach.
“Can I show my data preferences, what types of data I care more about and what I’m less concerned about?”
“I’d like to define what kind of data I’m comfortable sharing, like a personal statement or setting.”

Concern 8: Efficiency in the protection

The concerns rise from the intrusiveness of current privacy mechanisms, particularly **non- user-friendly mechanisms**, such as cookie consent pop-ups and long aggreements. From a user experience perspective, these measures disrupt online activities, prioritizing legal compliance over take the shoes of the user:
“I don’t want my data to become a burden to myself.
“I also don’t want to be constantly interrupted with reminders, especially if there’s nothing I can actually do about it.”
Participants also discuss the **measurements** in the digital experience compares to the physical spaces，which is harder to detect:
“In digital spaces, it’s harder to estimate my exposure, whereas in physical spaces, I can feel and aware when I’m being tracked by a camera.”
Instead of frequent disturbed, participants wanted a **more efficient and intuitive approach** to aware the privacy . They envisioned a **safety and controlled** space will be provide for data: “Can I have a single card that stores all my digital identities, only inserting it into services when necessary?”
“I hope for an invisible cloak, something I can put on and become invisible, both physically and digitally.”
“ When I use the internet, I shouldn’t have to think about my privacy. It’s my privacy.”

Concern 9: credibility of the system

One concerns about whether privacy protection measures implemented by companies truly ensure security. They discussed around that whether the existence of privacy-protection way. One example is the strong and automatic password:
“If the system were truly secure, would these tools even be necessary?” “Does this approach actually guarantee privacy protection?”

Also, participants reflected on a news report about companies **offering premium services for enhanced privacy protection,** effectively turning privacy into a paid privilege. They felt this violates users’ fundamental privacy rights and expressed skepticism about whether these paid services truly guarantee data security
“Even if I spend extra time and money on these companies, I still can’t guarantee that my data is safe or that my privacy won’t be violated.”

Overall, these concerns led to **doubts about automated privacy protections**, making participants question whether they would still trust the system’s security even if such measures were in place:
“If there were truly automatic protection measures in place, would I still trust the system?”

Discussion

Attitude

From the study, we observed that participants approach privacy with different attitudes, which we can categorize based on their dialogues.

- Naively optimistic. People were forthcoming in providing personal information and showed little concern for the outcome. For instance, one of the participants, referring to some cultures, said that" it was common for everybody to know each other's salary", and people enjoy the full rewards of the potential benefits. Others were even looking forward to being a "data reviewer," with anticipation of being able to view what data is available about themselves, as one commented, "I would love to see what data is out there about me."

- Careful with their data privacy. They emphasized the importance of keeping their information private, such as deleting cookies from their browsers periodically and ensuring that they only enable location access when using a specific service. They suggest an active method of safeguarding privacy, implying that individuals must carefully consider any actions that could potentially infringe upon their data.

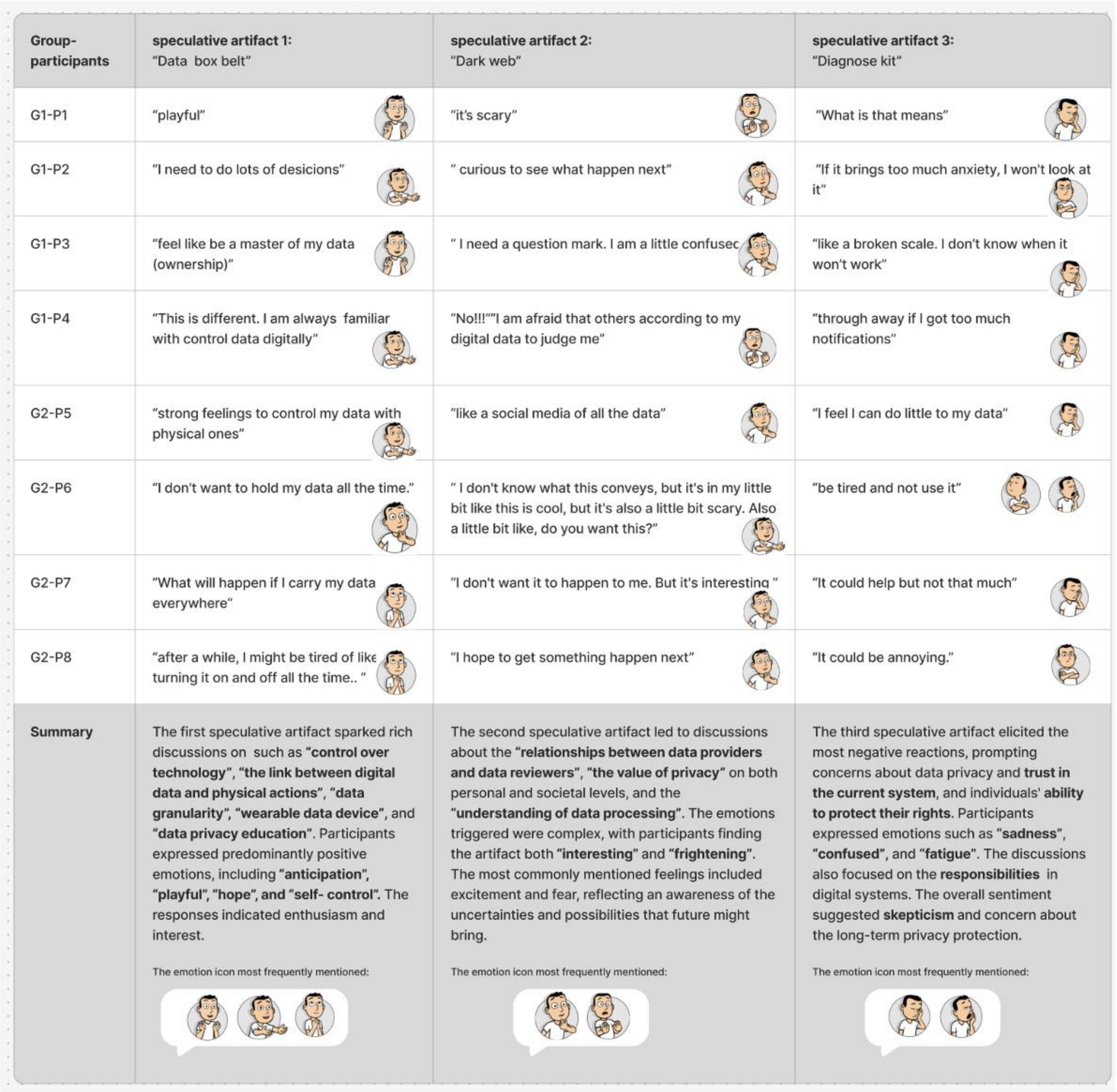
- Negative and "cynicism" (Hoffmann et al., 2016) in privacy protection. There is a feeling of helplessness regarding the state of data privacy. A few of the participants expressed frustration, with comments such as, "I feel frustrated because there is nothing I can do," or "It is not my business."The concept of self-surrender privacy was also introduced, where individuals felt they had no control over their data. As one of the participants pointed out, "If the data is not identifiable, I can pretend that this is not my data,".

These varying attitudes shape their opinions toward the future. More importantly, **the findings suggest that potential future interventions should take personal perspectives into account and be adaptable to the diverse needs and attitudes of different individuals.**

Artifacts

The study introduces speculative prototypes based on three fundamental phases of data practice: access, processing, and storage. While these stages are conceptually distinct, they are deeply interconnected in real-world applications. Participants' reactions to these prototypes varied widely. Concepts such as the "Data Box Belt" and the "Dark Web" were met with a more positive outlook, as they sparked discussions about how future technologies might empower users by enhancing control over their data. In contrast, attitudes toward "diagnose" were significantly more apprehensive.

Although these artifacts were intended to situate them within a fantastical future, the feedback reflected both utopian and dystopian perspectives, sparking debates and argumentation during group discussions. These prototypes also triggered unexpected associations beyond their intended design. For example, discussions around the "Access Box" led participants to reflect on contemporary tracking mechanisms, such as cookies. At the same time, the "Dark Web" prototype evoked concerns about surveillance technologies, including voice and physical tracking. These reactions further illustrate that the three phases of data practice(collection, processing, and storage) are not perceived as isolated, but as deeply interconnected aspects of digital privacy.



Group-participants	speculative artifact 1: "Data box belt"	speculative artifact 2: "Dark web"	speculative artifact 3: "Diagnose kit"
G1-P1	"playful"	"it's scary"	"What is that means"
G1-P2	"I need to do lots of desicions"	" curious to see what happen next"	"If it brings too much anxiety, I won't look at it"
G1-P3	"feel like be a master of my data (ownership)"	" I need a question mark. I am a little confusec	"like a broken scale. I don't know when it won't work"
G1-P4	"This is different. I am always familiar with control data digitally"	"No!!!""I am afraid that others according to my digital data to judge me"	"through away if I got too much notifications"
G2-P5	"strong feelings to control my data with physical ones"	"like a social media of all the data"	"I feel I can do little to my data"
G2-P6	"I don't want to hold my data all the time."	" I don't know what this conveys, but it's in my little bit like this is cool, but it's also a little bit scary. Also a little bit like, do you want this?"	"be tired and not use it"
G2-P7	"What will happen if I carry my data everywhere"	"I don't want it to happen to me. But it's interesting "	"It could help but not that much"
G2-P8	"after a while, I might be tired of like turning it on and off all the time.. "	"I hope to get something happen next"	"It could be annoying."
Summary	The first speculative artifact sparked rich discussions on such as **"control over technology"**, **"the link between digital data and physical actions"**, **"data granularity"**, **"wearable data device"**, and **"data privacy education"**. Participants expressed predominantly positive emotions, including **"anticipation", "playful", "hope", and "self- control".** The responses indicated enthusiasm and interest. The emotion icon most frequently mentioned:	The second speculative artifact led to discussions about the **"relationships between data providers and data reviewers"**, **"the value of privacy"** on both personal and societal levels, and the **"understanding of data processing"**. The emotions triggered were complex, with participants finding the artifact both **"interesting"** and **"frightening"**. The most commonly mentioned feelings included excitement and fear, reflecting an awareness of the uncertainties and possibilities that future might bring. The emotion icon most frequently mentioned:	The third speculative artifact elicited the most negative reactions, prompting concerns about data privacy and **trust in the current system**, and individuals' **ability to protect their rights**. Participants expressed emotions such as **"sadness"**, **"confused"**, and **"fatigue"**. The discussions also focused on the **responsibilities** in digital systems. The overall sentiment suggested **skepticism** and concern about the long-term privacy protection. The emotion icon most frequently mentioned:

Figure 4.9: Reaction and emotion analysis

Limitation

- One limitation of this workshop was that all participants came from a design background. This homogeneity may have influenced the discussions, as designers often approach privacy expectations through a particular lens, prioritizing conceptual and system exploration over representing a broader range of perspectives from different fields or everyday users.
- Another limitation is that only eight participants were involved in the workshop. The findings cannot be generalized to a broader population and should be viewed as exploratory rather than conclusive. This also means that the findings can be expanded and further explored in the next round of research.

Conclusion

In this chapter, we introduce a follow-up workshop featuring three speculative artifacts to raise people's awareness of privacy and gather collective insights.

In this workshop, we identified nine different privacy concerns that reflect a wide range of issues within the broader topic of privacy. These concerns emerged from group discussions with the artifacts, revealing the diverse values people hold and their varying experiences of privacy in the online environment. We did not look at these concerns as separate problems.

We tried to explore privacy issues using three artifacts as probes, which represent the privacy in each phrase. However, during the workshop, it became clear that this rigid taxonomy was not always perceived as separate by individuals. Participants felt that privacy issues often overlap, connect, and depend on the specific situation.

This revealed an important limitation of fixed privacy models: even though each privacy issue seemed distinct on its own, in practice, they were often interconnected, forming a web of related issues rather than fitting neatly into separate categories.

One of the key lessons from the workshop is the need for more flexible approaches to thinking about and designing for privacy. We should accept that privacy concerns often depend on the context and can change over time. Design methods should be able to adapt to these changes, rather than forcing everything into set categories.

05

Reframe the Design Direction

In this chapter, we wrap up the collective findings from previous stages and reframe the design direction. From the “preposterous future”, we shifted our direction towards a **more meaningful and valuable future: “plausible future design”.**

Findings

Privacy concern map

In the previous chapters, we gathered collective insights on privacy concerns from the auto-ethnography study and the speculative workshop. To make the findings more transparent and more accessible, we use a single word to represent each theme from the previous findings and interpret them for further exploration.

The following figure shows that nine privacy concerns represent what people value and care about for future online privacy.To clarify, we also map the key items in the relational map to identify concerns at individual, interaction, and social levels, as well as system levels, within the domains.

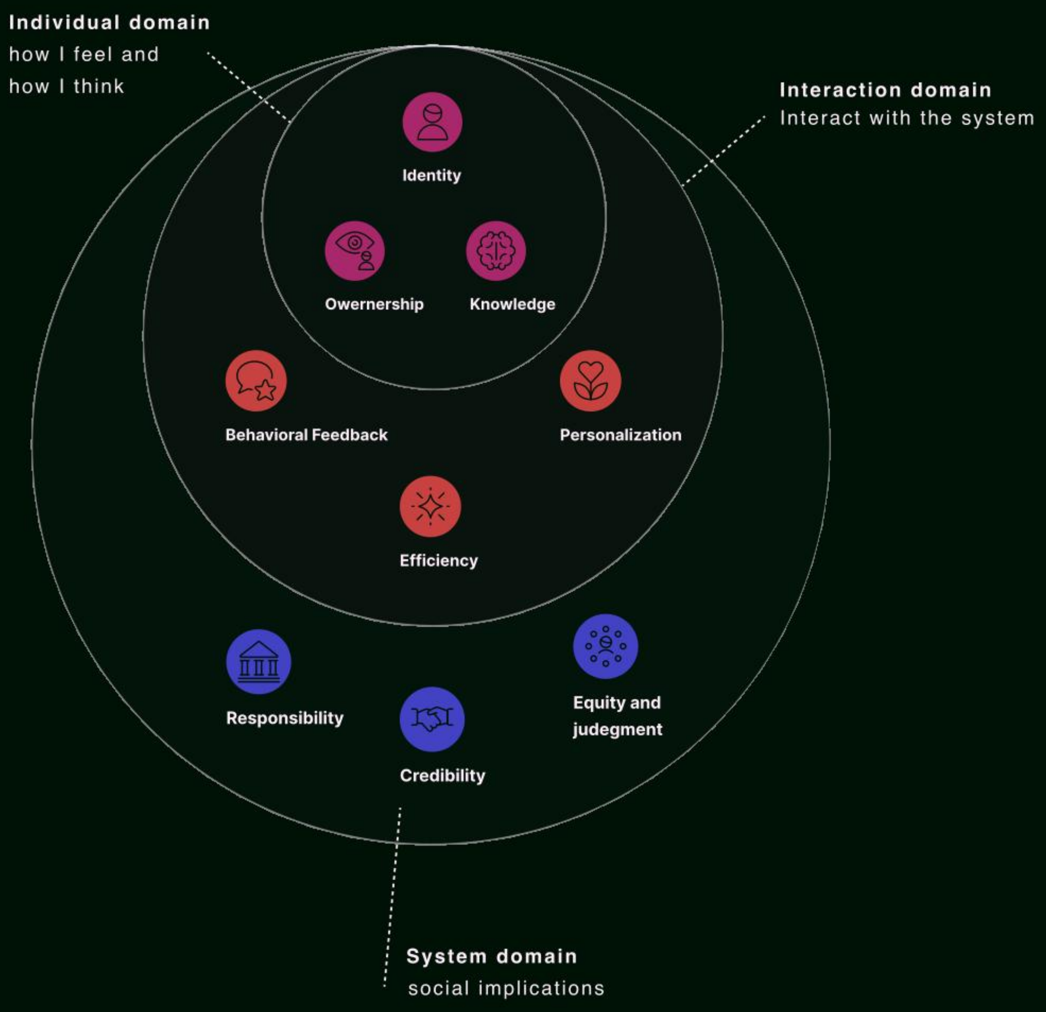


Figure5.1: Privacy concerns map

domain	Identified concerns	Open to Future Interpretation	Source
Individual Domain of that how I feel and how I think	**Knowledge**	How do I know what is happening to my data?	"Previously I knew that my data was collected..."
	Identity	How can I control how I am represented online?	"I am concerned that fake data could spread rumors and discredit me
	Ownership	Do I have control over how my personal data is used?	Auto-ethnography study: Lack of connection of my data
Interaction individual and experience domain	**Efficiency**	How can I receive effective protection without friction?	"I also don't want to be constantly interrupted with reminders..."
	Personalization	How can I get a privacy experience tailored to my needs?	"what types of data I care more about and what I'm less concerned about?"
	Behavioral Feedback	How can I learn from the system how my behaviors affect my privacy?	"I don't know which websites I need to turn off."
System social implication domain	**Responsibility**	How to define that who is accountable to protection and risks?	"Less and less our responsibility in the future..."
	Credibility	How can build trust for individuals when trust the systems that collect and process the data?	"Does this approach actually guarantee privacy protection?"
	Equity and judgement	Are privacy protections fair and inclusive for all groups? Am individual at risk of being unfairly judged based on my digital traces?	"If someone is a web developer, will they be able to block their own data from these websites?"

Figure 5.2: Privacy concerns

Reframe direction

What is the limitations from the previous study?

Alignment with user experience

In the previous research, we initially used the privacy taxonomy as a literature-based framework to guide the construction of speculative artifacts across three key phases of the data lifecycle: collection, processing, and storage. This structured approach helped organize our exploration and ensured theoretical grounding during the artifact-building process.

However, a key limitation of this classification is that in real-world contexts, these privacy risks are intertwined when people are aware of them, which is far more complex than just the three key phrases. As a result, the framework may not fully capture the nuanced and interconnected aspects of the lived experience of privacy. In the following phrase, we should consider the coherence experience and make it tangible for individuals.

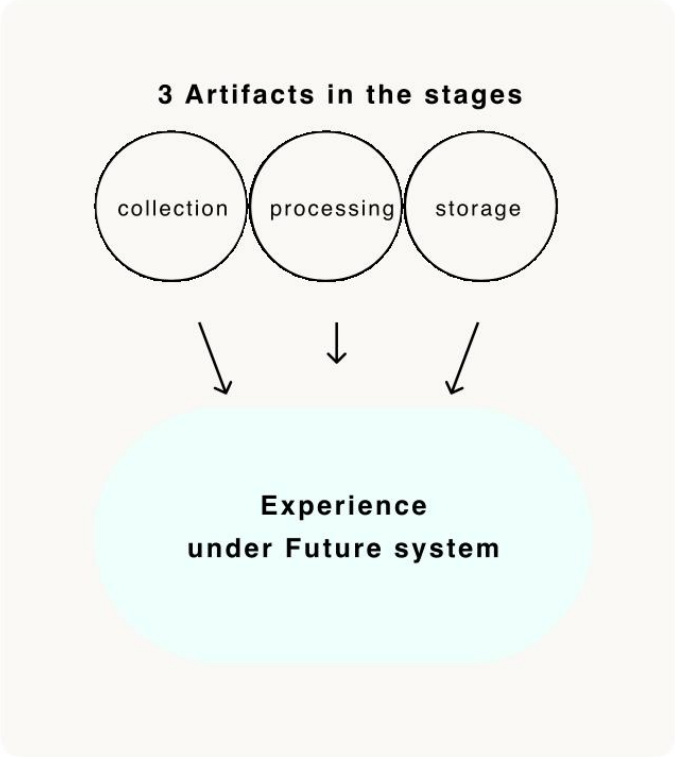


Figure 5.3 : experience under future system

Event-Based privacy awareness

Another limitation of the study lies in its predominant focus on generalized, risk-based interpretations of privacy concerns. Much of the workshop dialogue centered around abstract threats and conceptual risks, rather than grounding the analysis in concrete, event-based scenarios drawn from everyday life. In the following phrases, we should put more thought into the privacy risks in the event and empower individuals in Event-Based future awareness.

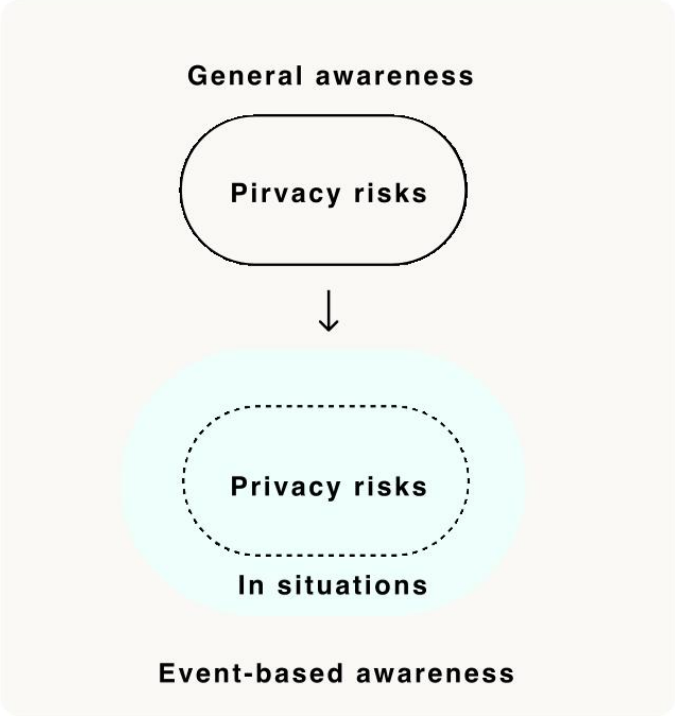


Figure 5.4: Towards event-based awareness

What is more valuable direction towards society transformation?

In speculative design, “preposterous” futures have long been valued as a means to provoke reflection and challenge dominant paradigms, enabling us to view the present from new perspectives (Dunne & Raby, 2013). However, when such futures are not connected to potential transitions or the implications they might have, the ability of these preposterous futures to guide meaningful change can be limited.

In this project, we propose a shift: from purely “preposterous” futures to plausible and meaningful futures. This approach, increasingly supported by scholars and practitioners (Dunne & Raby, 2013), not only imagines what the future could look like but also highlights the critical role of designers in actively shaping that future.

> Iwabuchi (2022) emphasized that speculation is not always a linear process: “I thought it was essential to repeat this process of ‘imagination through design.”

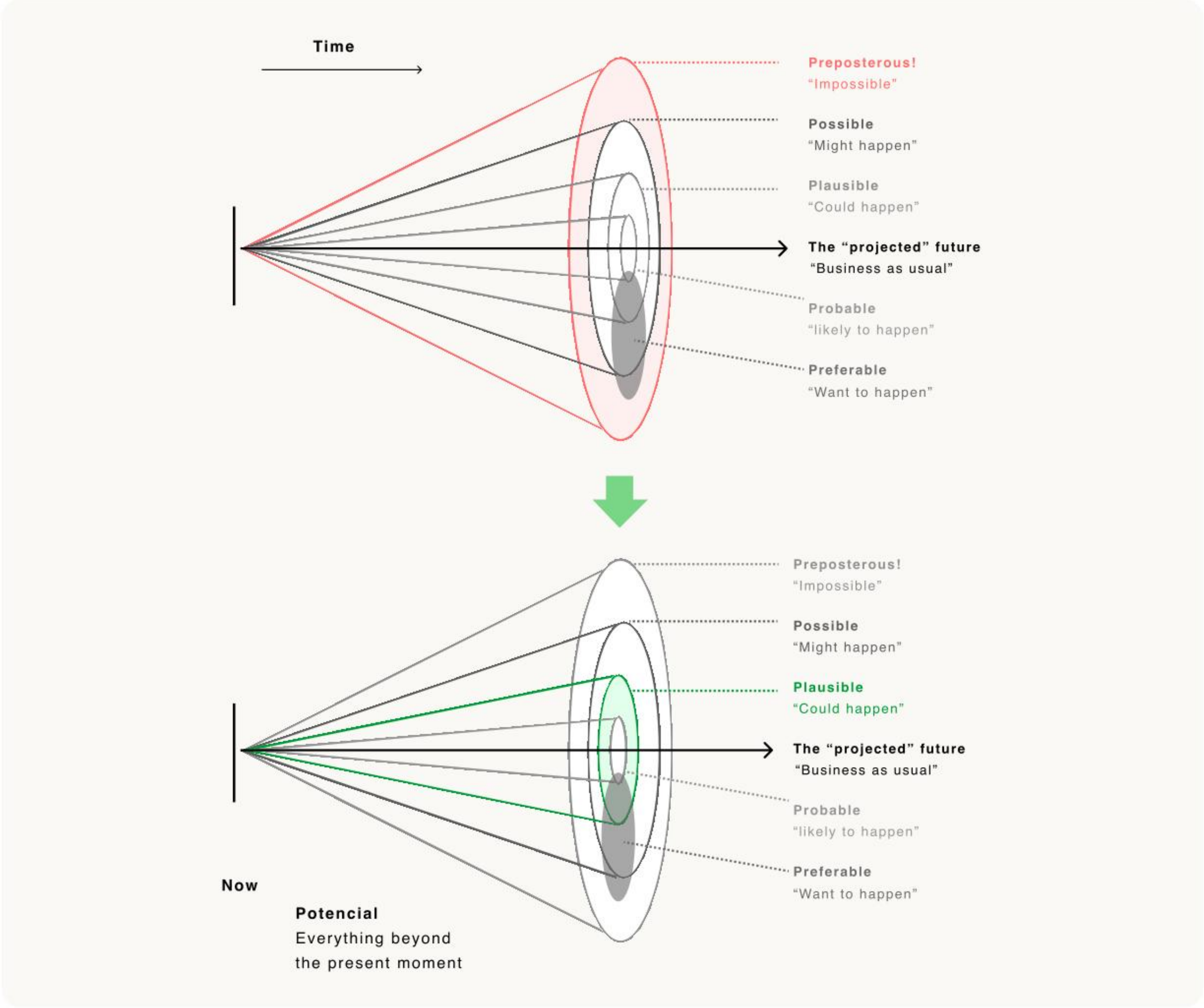
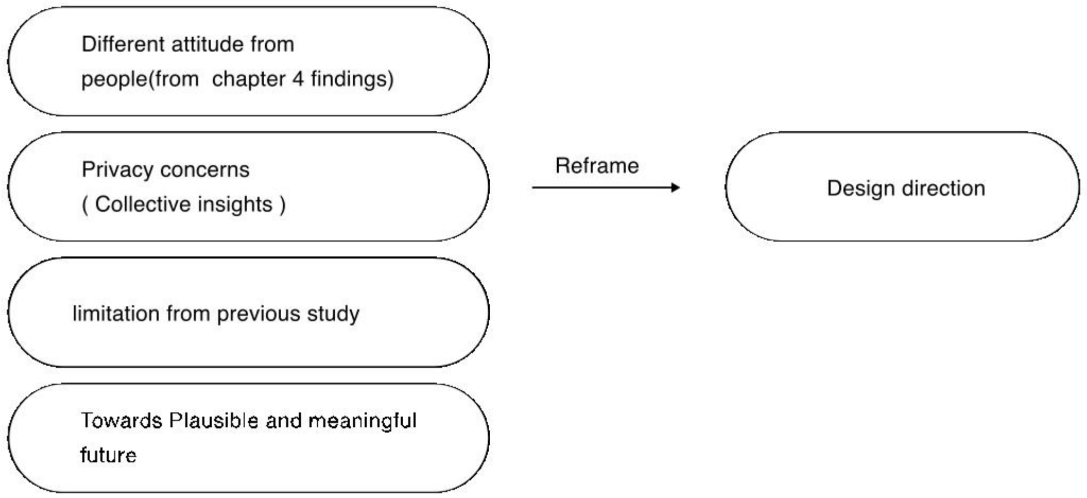


Figure 5.5: From “preposterous future” towards “plausible” futures(Dunne & Raby, 2013)

Design direction

To clarify the direction of “plausible and meaningful futures” meaning, we explain that them is the five dimensions related to the project goal.

1. **Potentially towards potential desirable futures:** Oriented toward improved conditions for individuals, communities, and the environment
2. **Under coherence future system:** Logically structured and internally consistent within the individual experience and the imagined context
3. **Awareness in situations:** Informed by event-based online data privacy risks or signals that the user can be aware of
4. **Spark individual’s reflection:** The system is designed to foster critical individual awareness rather than passive acceptance.
5. **Actionable futuristic prototypes:** Offering plausible pathways for individuals to experience future-oriented design interventions and imagine the future transitions



Different attitude from people(from chapter 4 findings)

Privacy concerns (Collective insights)

limitation from previous study

Towards Plausible and meaningful future

Reframe

Design direction

Figure 5.6: How to reframe the design direction

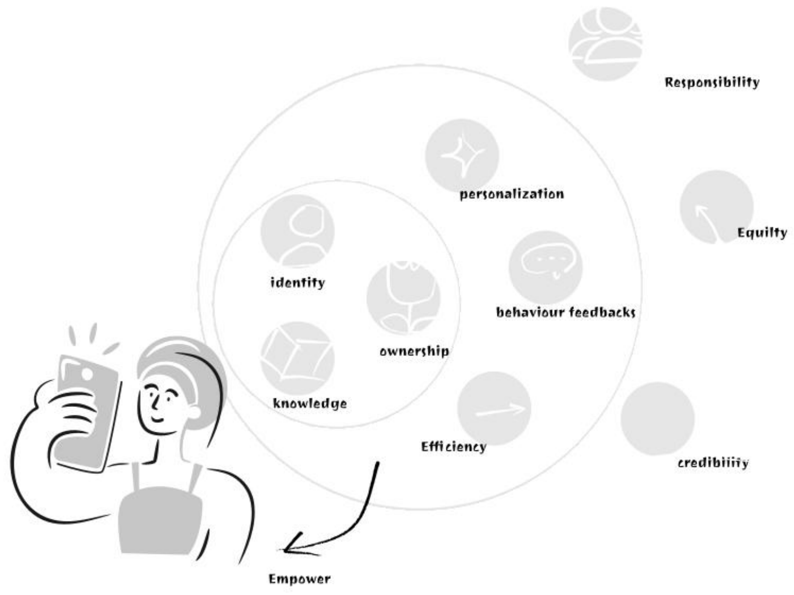
Combining the findings on personal different attitude towards privacy, privacy concerns, of the limitations of the current approach, and considering the opportunities for future value design, our design direction has evolved into the following:

Propose an **alternative intervention** set in a **plausible future experience** for **online users, leveraging levels of privacy concerns (knowledge, identity, ownership, efficiency, personalization, feedback, responsibility, credibility, and equity)** that could **empowers** them to be **aware of and reflect** on their online **privacy, in a meaningful way.**

This reframed direction aims to facilitate intervention and promote discussions on the implementation of inferences about the future.

More specifically, this alternative future intervention includes:

- The future service blueprint for future intervention.
- An actionable prototype to show the tangible future of the service and gather people's opinions on the future service implementation



Future 5.6 : Direction illustration

06

Plausible future exploration

How might leverage the collective insights towards plausible futures?

In this chapter, we examine what could be a plausible future for online data privacy.
The futurist’s co-creation session was conducted. The goal of the workshop is to envision plausible future ideas that might help people become aware of their online privacy.
After the workshop, we cluster the findings into **12 plausible future proposals**, which represent potential transformation towards the plausible future.

Future Trend analysis

Plausible Future trend analysis

Based on the previous case study and the workshop findings, this part answers the question: What might happen to future online privacy? In this section, we explore the privacy within the plausible future setting. The PESTLE analysis was employed to gather the plausible future signals in a broader landscape. As a strategic foresight tool, the PESTLE analysis encompasses six key factors: political, economic, **society**, technological, legal, and environmental, all of which are related to online privacy. This helps set a foundation for a plausible future privacy vision.

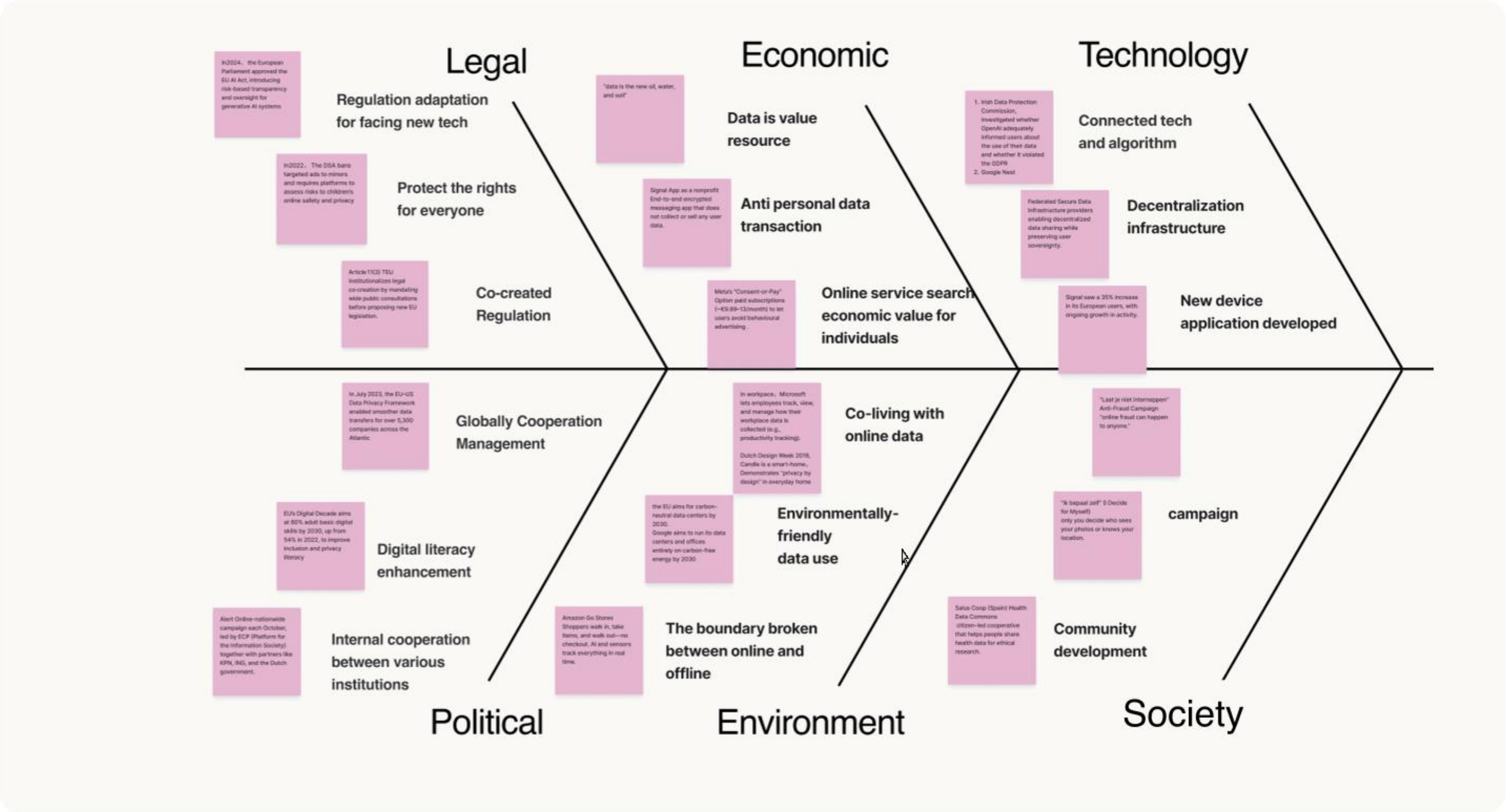

Legal
In2024, the European Parliament approved the EU AI Act, introducing risk-based transparency and oversight for generative AI systems
Regulation adaptation for facing new tech
In2022, The DSA bans targeted ads to minors and requires platforms to assess risks to children's online safety and privacy
Protect the rights for everyone
Article 11(3) TEU institutionalizes legal co-creation by mandating wide public consultations before proposing new EU legislation.
Co-created Regulation
Economic
"data is the new oil, water, and soil"
Data is value resource
Signal App as a nonprofit End-to-end encrypted messaging app that does not collect or sell any user data.
Anti personal data transaction
Meta's "Consent-or-Pay" Option paid subscriptions (~€9.99–13/month) to let users avoid behavioural advertising
Online service search economic value for individuals
Technology
1. Irish Data Protection Commission, investigated whether OpenAI adequately informed users about the use of their data and whether it violated the GDPR
2. Google Nest
Connected tech and algorithm
Federated Secure Data Infrastructure providers enabling decentralized data sharing while preserving user sovereignty.
Decentralization infrastructure
Signal saw a 35% increase in its European users, with ongoing growth in activity.
New device application developed
In July 2023, the EU-US Data Privacy Framework enabled smoother data transfers for over 5,300 companies across the Atlantic
Globally Cooperation Management
EU's Digital Decade aims at 80% adult basic digital skills by 2030, up from 54% in 2022, to improve inclusion and privacy literacy
Digital literacy enhancement
Alert Online-nationwide campaign each October, led by ECP (Platform for the Information Society) together with partners like KPN, ING, and the Dutch government.
Internal cooperation between various institutions
Political
In workspace, Microsoft lets employees track, view, and manage how their workplace data is collected (e.g., productivity tracking).
Dutch Design Week 2019, Candle is a smart-home, Demonstrates "privacy by design" in everyday home
Co-living with online data
the EU aims for carbon-neutral data centers by 2030.
Google aims to run its data centers and offices entirely on carbon-free energy by 2030
Environmentally-friendly data use
Amazon Go Stores Shoppers walk in, take items, and walk out—no checkout. AI and sensors track everything in real time.
The boundary broken between online and offline
Environment
"Laat je niet interneppen" Anti-Fraud Campaign "online fraud can happen to anyone."
"Ik bepaal zelf" (I Decide for Myself) only you decide who sees your photos or knows your location.
campaign
Salus Coop (Spain) Health Data Commons citizen-led cooperative that helps people share health data for ethical research.
Community development
Society

Figure 6.1: plausible future trend analysis map with cases

Trends

Legal

Rights-focused framework that emphasizes adaptive regulation and collective accountability

With the development of technology, regulations could become more adaptive to these new technologies. (Lescrauwaet et al., 2022)

Legal protection ensures everyone's rights in the online environment, aiming to promote social equality and justice (Müller, 2025)

Legal institutions collaborate with individuals, online services, and data protection organizations to develop regulations that protect human-centered rights (European Commission, n.d.).

Political

Globalization future where privacy is democracy with more understanding and cooperation.

With the globalization of privacy issues, cooperation between countries could become closer. (Vistra Group Holdings S.A., 2023)

Data feminism is going deeper and challenging structural issues, which could have an impact on everyone (D'Ignazio & Klein, 2023)

Digital literacy enhancement requires people to gain more access and protect their privacy.(Phan, Do, & Le, 2025)

Governments have stronger cooperation with various internal institutions to call for the right to protect privacy. (KPN, 2024)

Economic

Data-driven economy of the future, where information is the core analytical asset for value creation and decision-making.

Personal data is a valuable resource that is being treated more cautiously by online services and institutions. (Mandel, 2017)

With restrictions on personal data transactions, online services are seeking alternative forms of economic value from individuals, such as maintaining regular services and offering users more personalized experiences. (CMSWire, 2024)

Environmental

Sustainable paradigm in which privacy is designed in harmony with ecological responsibility.

With the blurring of online and offline boundaries, people are increasingly co-living with their data, and the risks are no longer confined to specific spaces. (Kumar, 2024)

There is a strong call for environmentally friendly data use, which means data handling that reduces harm. (Banerjee, 2025)

Surveillance could become increasingly invisible (Project SHERPA, 2019).

Technology

Highly connected ecosystem where digital systems are seamlessly integrated into everyday life.

Connected technologies, such as IoT and algorithmic systems, provide more abundant data sources that everyone can access. (Pinsent Masons, 2024)

Decentralized infrastructure, such as blockchain, is being developed to protect the security of personal data (Caprolu et al., 2024).

With the development of new devices and applications, data is being transferred more frequently across connected devices and applications.

Privacy-first technology empowers individuals to take control of their privacy.

society

Resilient social environment where communities actively shape privacy norms and expectations

Numerous digital communities are being established, and collaboration within these communities is utilized to facilitate the sharing of data.(Kavaliauskienė & Juknaitė, 2021)

Campaigns on privacy risks are being developed, calling for more ethical and friendly personal data collection and analysis.(Rijksoverheid, 2023)

There are also campaigns to raise people's awareness and educate them about privacy risks that happen in real life. (Dans, 2024)

People are anti-discriminatory and try to protect everyone in society.(Van der Meer, 2023)

“Futurist” Session

To explore how we leverage the collective concerns that could lead to plausible futures, we conducted this futurist session. This session aimed to build a shared understanding of the findings from the previous phase and explore possible, plausible solutions with the participants together.

In response, we organized two rounds of futurist sessions designed to generate and synthesize ideas based on privacy-related experiences.

Prior process

Prior to the workshop, several ideas (N ≈ 30) were gathered from feedback on earlier speculative probes and an informal pilot co-creation process.

However, these insights were fragmented and rendered them insufficient to draw support and strategy. Thus, in the two sessions, we use these ideas as a prompt to expand the exploration in the two rounds of the futurist session. We selected nine representative ideas to represent each of the privacy concerns. To stimulate imagination and facilitate more grounded ideation during the workshop sessions, we provided the images to support the ideas. The images are generated and visually translated using OpenAI’s ChatGPT image-generation with these text prompts.

Approach

The futurist session’s guidelines for generating ideas follow the Model of Creative Diamond 2.0 (Heine & Van der Meer, 2019). The approach helps us organize these ideas, utilizing convergence, divergence, and reversal, ultimately grouping them into future categories.

Participants

The participants were all IDE students. Two rounds of sessions were conducted, with 6 participants and the researcher serving as the facilitator. The first session lasted approximately 1.5 hours, and the second session lasted 2.5 hours.

Process

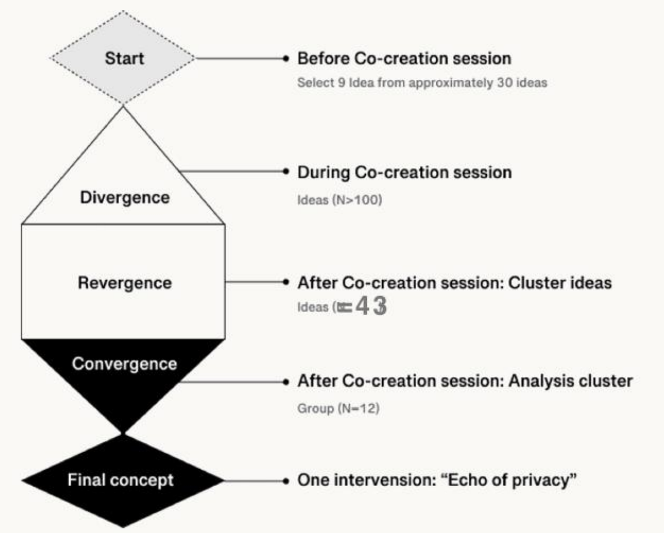
1. Introduction: The session began with a concise presentation outlining the research objectives and workshop structure. Emphasis was placed on the exploratory and future-oriented nature of the activity. Firstly, we used a PowerPoint slide to present the project’s purpose and goals. Then we gave each participant a future trend map to make them aware of the To anchor participants within the conceptual space of privacy systems, each was provided with a printed A3 diagram representing the overarching privacy framework. Clarifying questions were addressed before proceeding to the ideation phase.

2. Rounds of brainstorming and group discussion: Participants received A3 sheets featuring a timeline towards the future and were encouraged to envision how privacy might evolve independently. This timeline served as a cognitive scaffold to support structured foresight. The pre-identified tensions were grouped into three thematic clusters, each allocated 10 minutes for individual reflection. Participants were invited to engage with speculative artifacts as optional sources of inspiration.

Following each brainstorming session, participants engaged in small-group discussions designed to cross ideas. These collaborative exchanges enriched both the quality and diversity of the concepts produced.

3. Mapping ideas together: After all rounds of brainstorming in each session. All generated ideas were gathered and visually re-mapped onto an extensive A3 timeline that spanned. This collective mapping exercise allowed participants to reflect on how each idea might evolve and contribute to future privacy experiences.

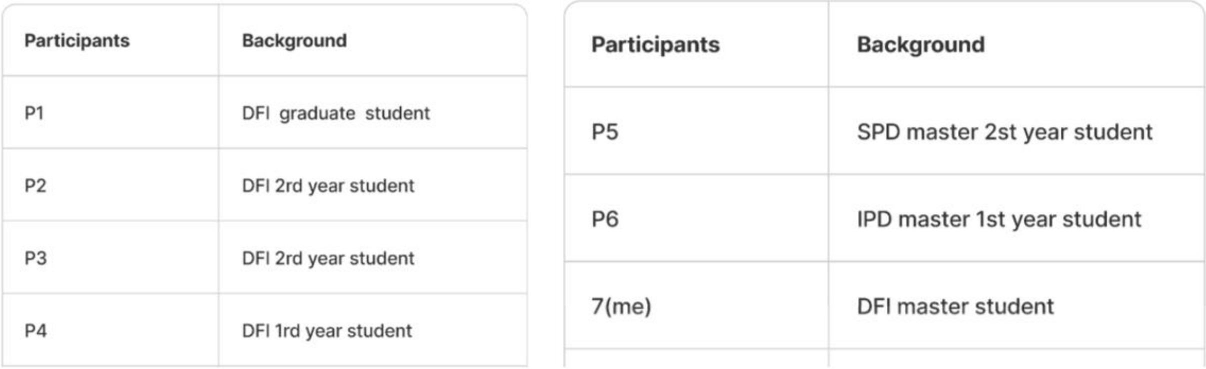
At the final stage of this activity, participants used star stickers to mark their favorite ideas, those they found most compelling or impactful. This simple yet effective method enabled a shared prioritization process and surfaced concepts with the strongest group resonance.



Start
Before Co-creation session
Select 9 Idea from approximately 30 ideas
Divergence
During Co-creation session
Ideas (N>100)
Revergence
After Co-creation session: Cluster ideas
Ideas (N=43
Convergence
After Co-creation session: Analysis cluster
Group (N=12)
Final concept
One intervension: “Echo of privacy”

Figure 6.1: idea development

Figure 6.2: Participants involved in the Futurist sessions



Participants	Background
P1	DFI graduate student
P2	DFI 2rd year student
P3	DFI 2rd year student
P4	DFI 1rd year student

Participants	Background
P5	SPD master 2st year student
P6	IPD master 1st year student
7(me)	DFI master student

Figure6.3 : Participants involved in the Futurist sessions

Results analysis

The analysis is divided into four steps, which help us develop overarching future possibilities.

- Translate ideas into a digital format: After the co-creation workshop, we initiated data analysis. To preserve the accessibility of the content generated during the session, all physical sticky notes were carefully digitized and imported into FigJam. This digital format allows for easier review and organization. During digitization, each idea was reformatted using a standardized “Title + Explanation” structure. This consistent format improved clarity and interpretability across the dataset.

- Cluster ideas: To identify alternative design concepts that are both socially meaningful and strategically promising within the theme of online data privacy, we applied four criteria derived from relevant literature and the objectives of this chapter:

    - From “Favourite ideas” (Heine & Van der Meer, 2019): We began by examining the ideas that participants identified as their “favorite futures” during the workshop. These concepts resonated emotionally and contextually, representing desirable directions for development.
    - Align with fundamental ethical values of privacy, which can be grounded in both technical and social principles.
    - Align with plausible future trends: We emphasized proposals that could bridge current realities with plausible future conditions, ensuring their relevance within future-oriented strategic contexts.

- Conceptual distinctiveness: We ensured that the final set of proposals represented a distinctive and compelling range of directions. Each proposal reflects meaningful ideas about the future of privacy.

- Develop future proposals: During this process, we clustered the ideas into 12 groups based on their distinct features and developed each group into a unique future scenario. Finally, we generated 12 potential future proposals that integrate various aspects of privacy concerns and leverage their combined potential.

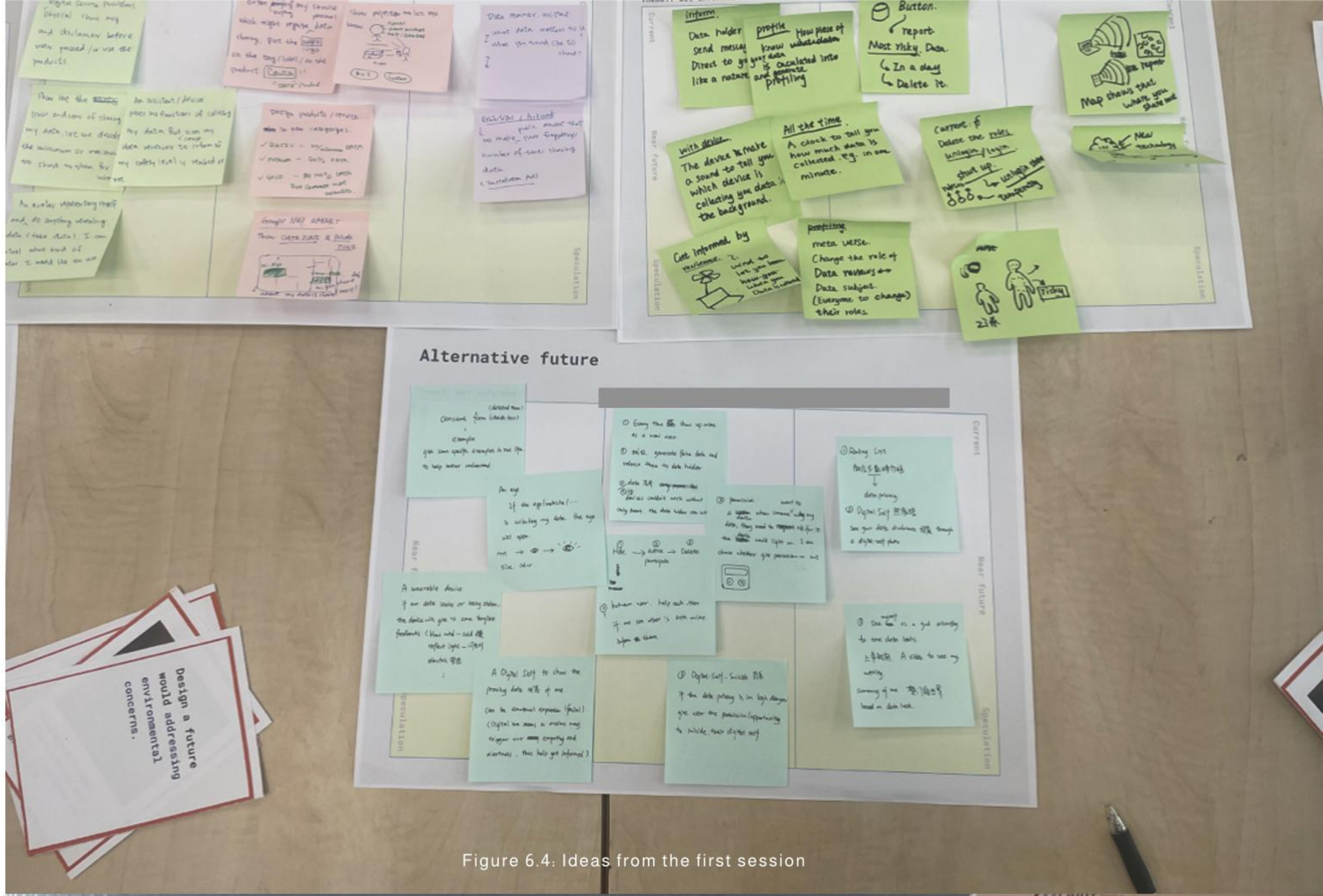


Figure 6.4: Ideas from the first session

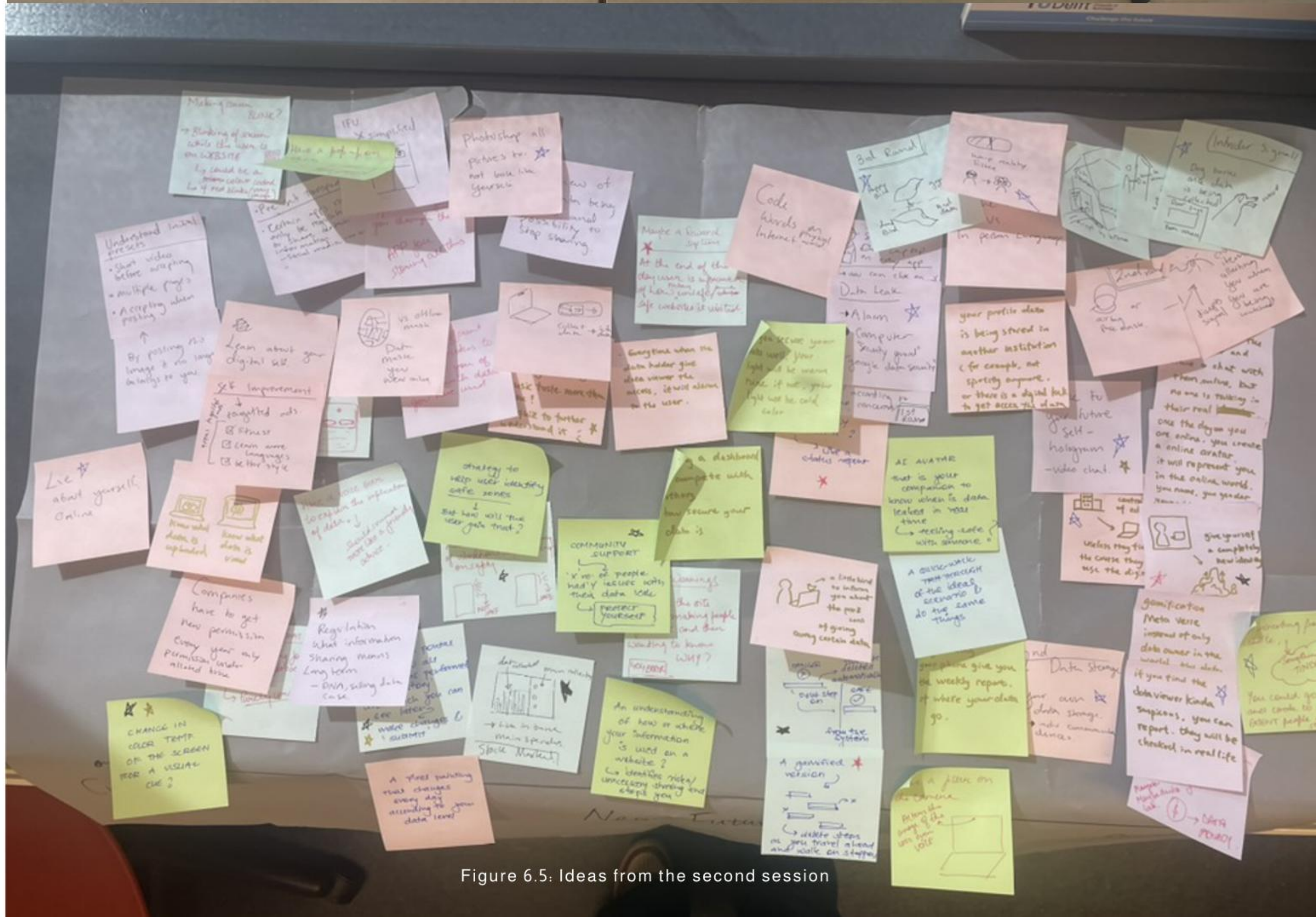
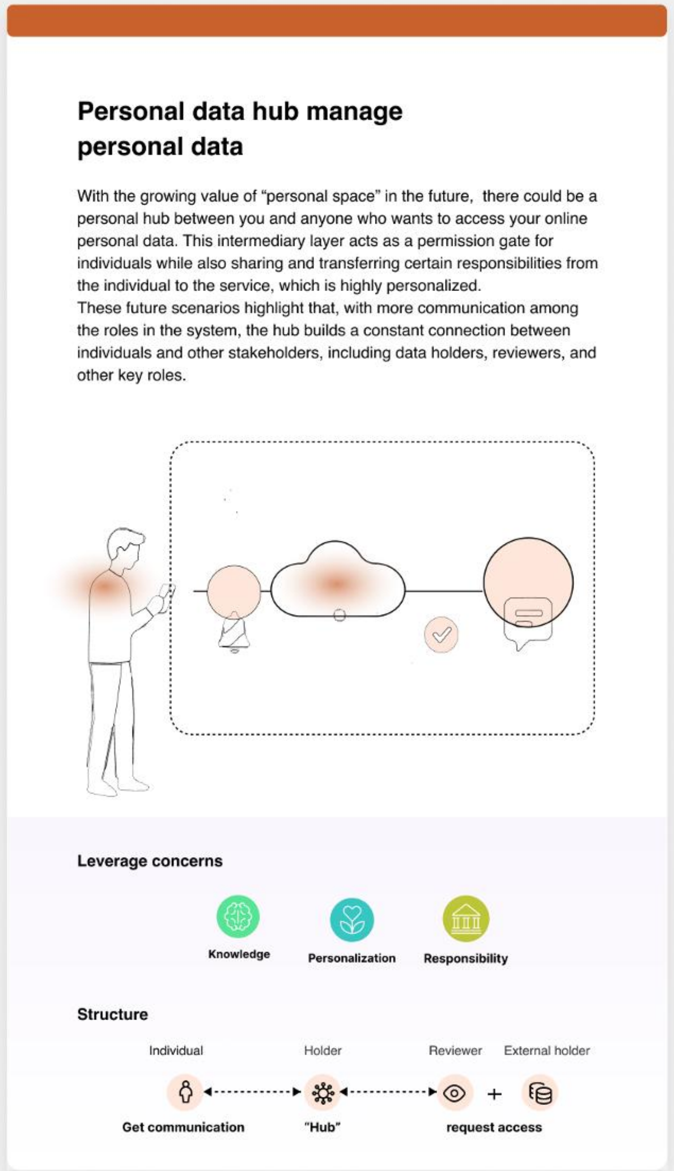


Figure 6.5: Ideas from the second session

Future proposals

To better present the future ideas to readers, we analyzed them in detail. These posters for future proposals included explaining the future strategies title, what each idea could be, how it could leverage privacy concerns, and how it might balance individual awareness with structural support in the future. By doing so, we generated 12 posters for these ideas, which could represent plausible future strategies.



Personal data hub manage personal data

With the growing value of “personal space” in the future, there could be a personal hub between you and anyone who wants to access your online personal data. This intermediary layer acts as a permission gate for individuals while also sharing and transferring certain responsibilities from the individual to the service, which is highly personalized.
These future scenarios highlight that, with more communication among the roles in the system, the hub builds a constant connection between individuals and other stakeholders, including data holders, reviewers, and other key roles.

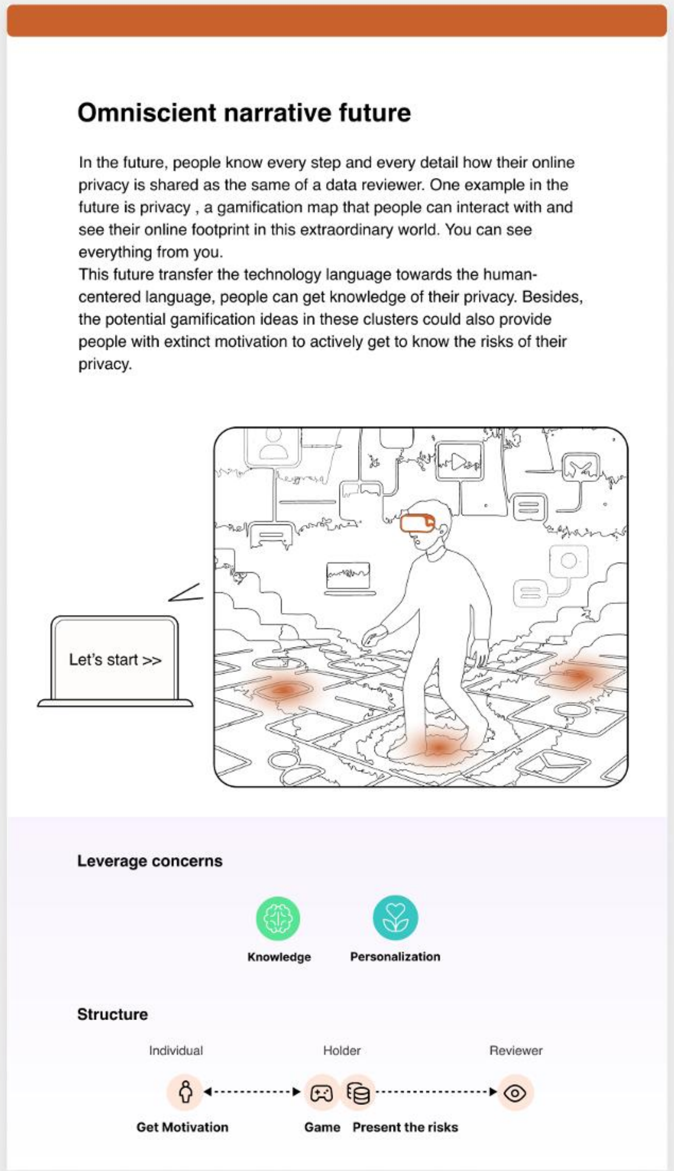
Leverage concerns

Knowledge
Personalization
Responsibility

Structure

Individual ◂·····▸ Holder ◂·····▸ Reviewer + External holder

Get communication · "Hub" · request access



Omniscient narrative future

In the future, people know every step and every detail how their online privacy is shared as the same of a data reviewer. One example in the future is privacy , a gamification map that people can interact with and see their online footprint in this extraordinary world. You can see everything from you.
This future transfer the technology language towards the human-centered language, people can get knowledge of their privacy. Besides, the potential gamification ideas in these clusters could also provide people with extinct motivation to actively get to know the risks of their privacy.

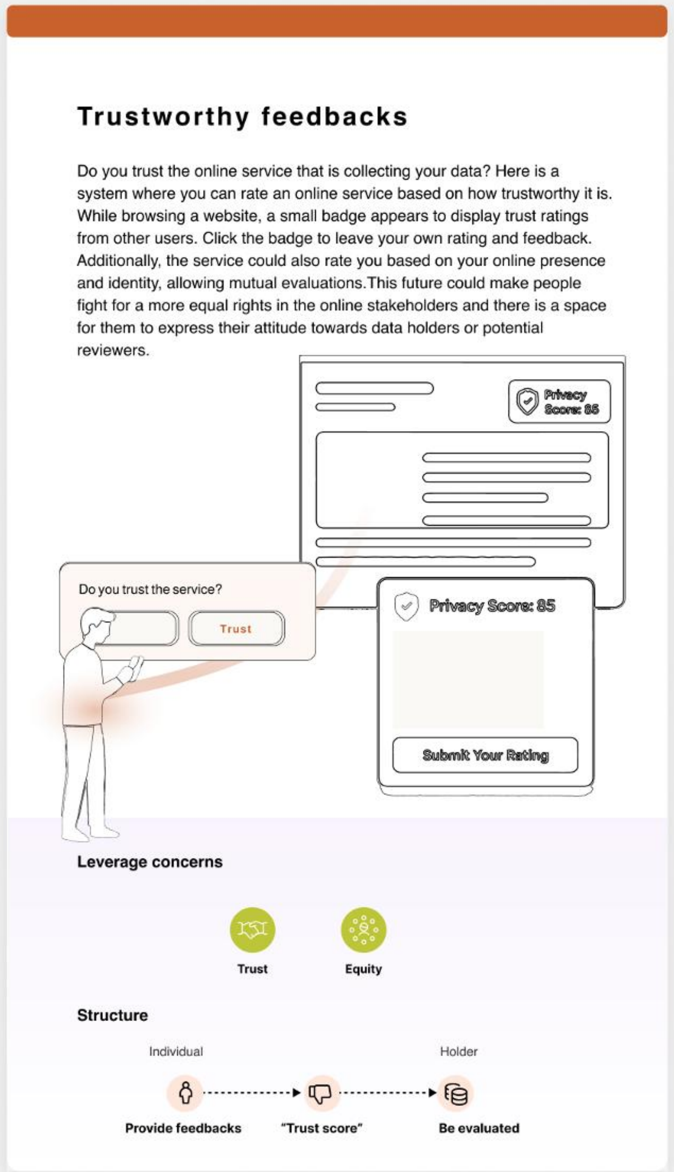
Leverage concerns

Knowledge
Personalization

Structure

Individual ◂·····▸ Holder ·····▸ Reviewer

Get Motivation · Game · Present the risks



Trustworthy feedbacks

Do you trust the online service that is collecting your data? Here is a system where you can rate an online service based on how trustworthy it is. While browsing a website, a small badge appears to display trust ratings from other users. Click the badge to leave your own rating and feedback. Additionally, the service could also rate you based on your online presence and identity, allowing mutual evaluations.This future could make people fight for a more equal rights in the online stakeholders and there is a space for them to express their attitude towards data holders or potential reviewers.

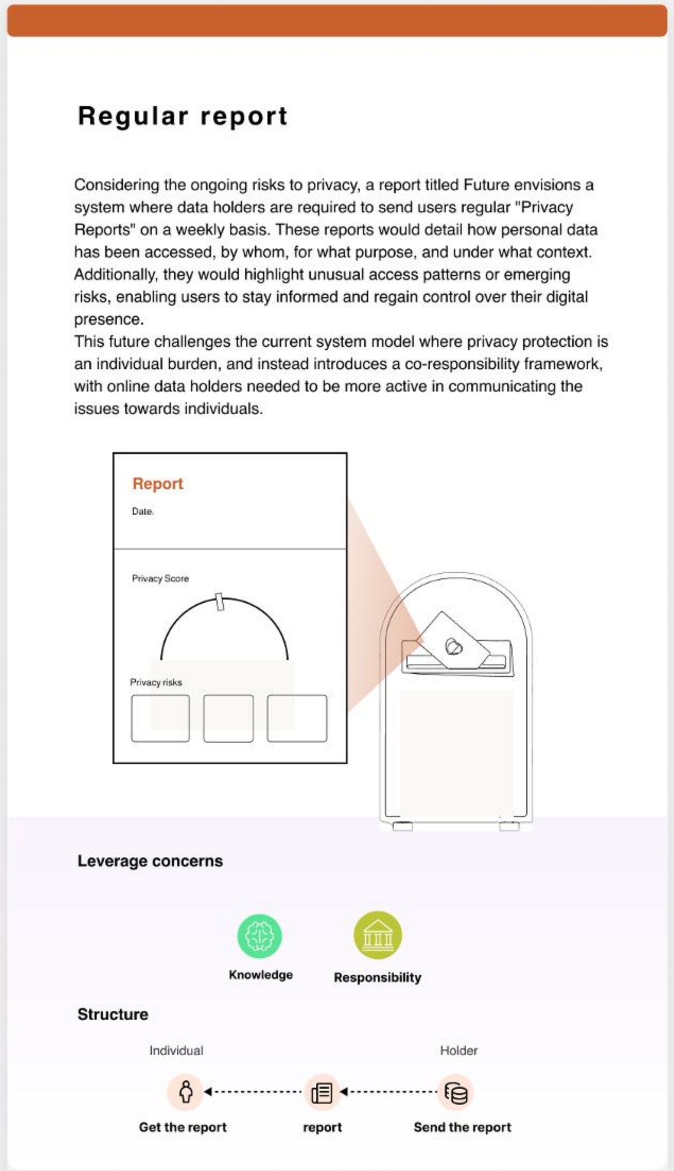
Leverage concerns

Trust
Equity

Structure

Individual ·····▸ ·····▸ Holder

Provide feedbacks · “Trust score” · Be evaluated



Regular report

Considering the ongoing risks to privacy, a report titled Future envisions a system where data holders are required to send users regular "Privacy Reports" on a weekly basis. These reports would detail how personal data has been accessed, by whom, for what purpose, and under what context. Additionally, they would highlight unusual access patterns or emerging risks, enabling users to stay informed and regain control over their digital presence.
This future challenges the current system model where privacy protection is an individual burden, and instead introduces a co-responsibility framework, with online data holders needed to be more active in communicating the issues towards individuals.

Leverage concerns

Knowledge
Responsibility

Structure

Individual ◂····· ◂····· Holder

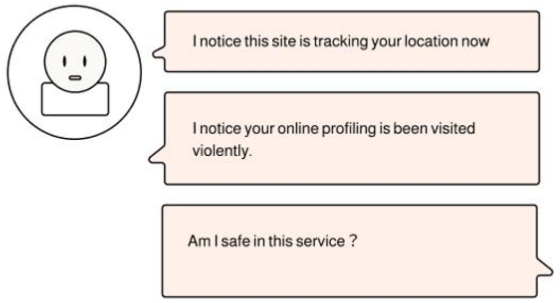
Get the report · report · Send the report

Figure 6.6: 12 future proposal

Future proposals

Adaptive agent consulting

With advances in algorithms in the future, adaptive agents will empower individuals to understand and navigate risks. People can actively communicate with the agent to consult about potential risks. Meanwhile, when a risk is detected, the agent initiates a dialogue, explaining what is happening and advising on what actions can be taken. The agent belongs to users and tailors its feedback entirely to their preferences.
Responsibility for privacy will extend beyond individuals to encompass the agent itself.
This shift will transform how individuals communicate with data viewers and holders. Information flow will become more flexible, and access will become easier for individuals.



I notice this site is tracking your location now

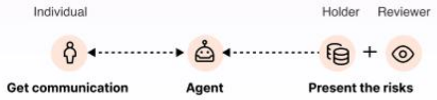
I notice your online profiling is been visited violently.

Am I safe in this service ?

Leverage concerns

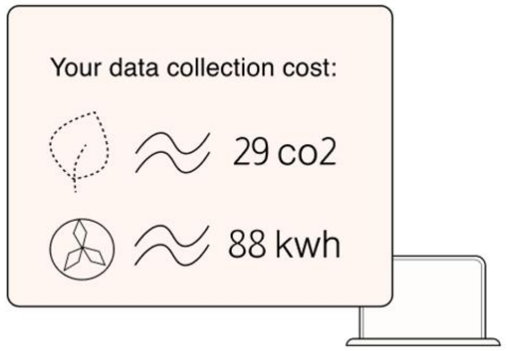
Knowledge · Personalization · Behavioral Feedback · Responsibility

Structure



Sustainble aware and dashboard

With the calling for minimize the personal data usage in the future, there is a sustainable system which shows how much your data is accessed by online services each day. The figure reflect the environmental impact of your data use, it can kind of reflect the status of your privacy. The future shows the paradox of connection data and the real privacy you feel in the world. Through empathic visualization, these data practices and inferred privacy become accessible and emotionally resonant.



Your data collection cost:

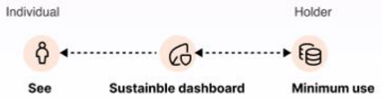
29 co2

88 kwh

Leverage concerns

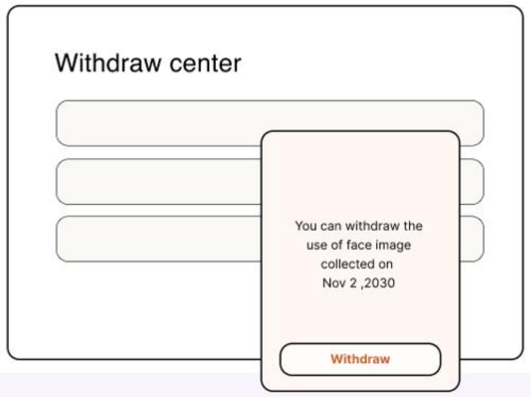
Knowledge · Responsibility

Structure



Treating the privacy in the data's afterlife

To support participants in the system, it allows people to actively withdraw their data at any time, even after it has been shared with a platform, app, or institution. With just one click, users can immediately retract their consent and remove their data. This future prioritizes user agency in data storage and dissemination, enabling individuals to reclaim control over the data that has been collected.



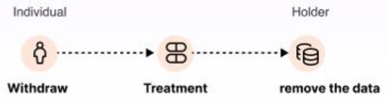
Withdraw center

You can withdraw the use of face image collected on Nov 2 ,2030

Leverage concerns

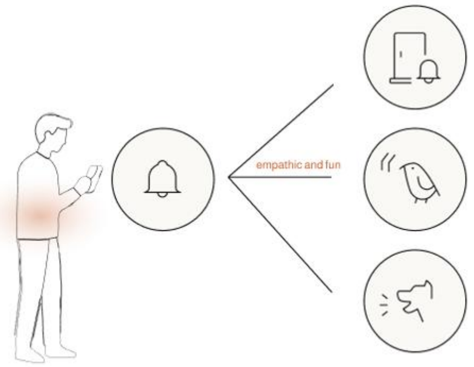
Knowledge · Efficiency · Responsibility

Structure



Strong, empathic and fun notifying the intension

The future involves informing individuals about real-world risks within context, designing an empathic informing system that encourages active engagement. For instance, when a suspicious service attempts to collect your data, a knocking sound begins, signaling that someone is trying to knock on your door. The sound of an urgent, heavy knock indicates the potential for more severe consequences. By employing empathic informing methods, this system helps individuals recognize and respond to privacy risks.



Leverage concerns

Knowledge · Behavioral Feedback

Structure

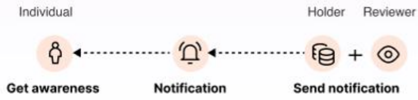
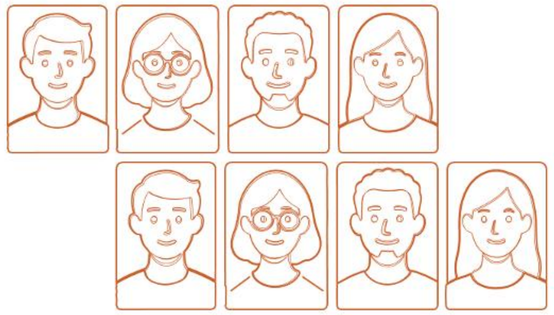


Figure 6.6: 12 future proposal

Future proposals

Seperated Online Identify

All of our online data is all connected, and profiling based on that data creates serious privacy risks. In the future here is a system where people can organize different parts of their identity into separate, unconnected "identity boxes." Each box would hold specific information, like career, health, or social life, and they would not be linked to each other. This means people could switch between identities depending on the situation. For example, someone could share only their career-related information on a job recruitment app, while keeping their other identities private and separate.



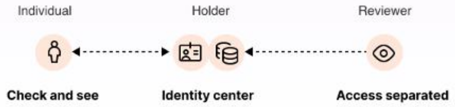
Leverage concerns

Identity

Personalization

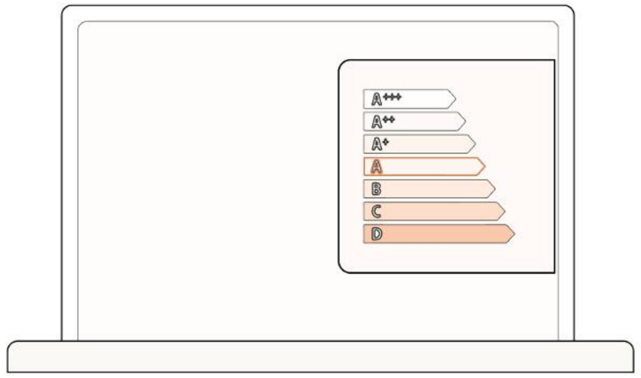
Equity

Structure



Grade the privacy risks in layers

The risks are personalized and should be informed with users in layers, eg, what is more highly risky and what is lower risks. Here we propose a privacy label system, integrated into online interaction flows for users. For example when people see a shopping website , they can also see the labels. It empowers people with the right to know and the ability to and initiates a shift in language from the individual the holders.



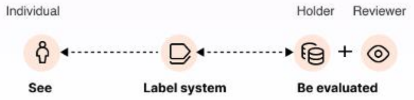
Leverage concerns

Knowledge

Efficiency

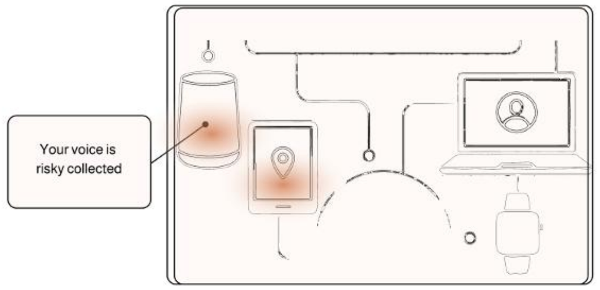
Responsibility

Structure



Visualization collection

Data collected through devices will serve as the first touchpoint for individual privacy.This future system envisions a platform that provides individuals with a clear overview of who is collecting their data. It will allow users to see not only which organizations or services are accessing their information, but also which specific devices are involved in the data exchange.

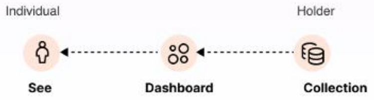


Leverage concerns

Knowledge

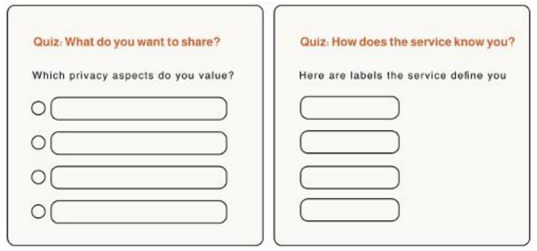
Efficiency

Structure



Building mutual understanding

what do I want to share and how to the services know me ? Design a quiz that helps build a common knowledge understanding between the data users knowingly share and the data inferred without their awareness. prompts like "Did you know that Spotify might understand your music taste better than you do?" encourage users to compare their self-perception with what happened in real life.


Quiz: What do you want to share?
Which privacy aspects do you value?
Quiz: How does the service know you?
Here are labels the service define you

Leverage concerns

Knowledge

Equity

Structure

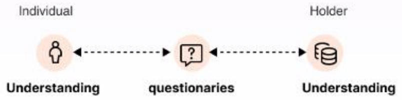


Figure 6.6: 12 future proposal

Reflection for Furturist session

- **From initial ideas to co-creation:** In this workshop, in addition to presenting the nine dimensions of privacy concerns through text-based slides, we also prepared a set of selected pictures of objects as tangible inspiration. This decision was made in consideration of the invisibility characteristic of privacy. These objects were intended to serve as prompts for reflection and creativity, and participants were free to choose whether or not to engage with them. Some participants responded positively, noting that the visual and physical materials helped stimulate their thoughts and expand their perspectives. However, others pointed out certain limitations. Specifically, that without sufficient contextual framing, the use of such objects could lead to misunderstandings or even constrain creativity. Additionally, the objects themselves might carry preconceived meanings or stereotypes, which could introduce bias and affect the diversity and openness of participants' expressions.

- **Scenarios providing:** At the beginning of the workshop, we introduced the plausible future via a presentation. A few specific scenarios were provided as starting points for reflection, such as "participating in a video conference in a work setting" or "using AI software at home." These scenarios were designed to offer concrete, relatable entry points. However, during the later exploration phase, we intentionally kept the structure open. We did not impose restrictions on the direction of participants' thinking in order to encourage diverse interpretations and creative outputs.

- **Openness and rationale in building an alternative future:** This open-ended approach led to a wide range of reflective directions. Some participants approached the topic from a macro or abstract perspective, for example, by designing a game to raise users' awareness of privacy issues. Others focused on specific, everyday situations, such as how privacy labels might be presented during online shopping.

- **Alignment with privacy concerns:** While each round of reflection was guided in a specific concern, these concerns as generative sources of future possibilities. While our ideation was not strictly limited by these themes. the creative exploration often moved beyond and as we can see the clustered ideas could leverage multiple parts of the privacy concerns .

Conclusion

This chapter presents a structured envisioning of a plausible alternative future generated throughout the ideation phases. Here, a bunch of ideas were developed into a map with links to the nine thematic privacy concerns. By clustering these ideas, 12 alternative design ideas were ultimately developed, serving as the building blocks for the future alternative design intervention.

In terms of the value of these ideas, these proposals not only inform the final concept development in this project but also have potential as future strategies leading the transformation of future privacy system development.

In the next chapter, we will demonstrate how these ideas are synthesized into a single alternative future intervention.

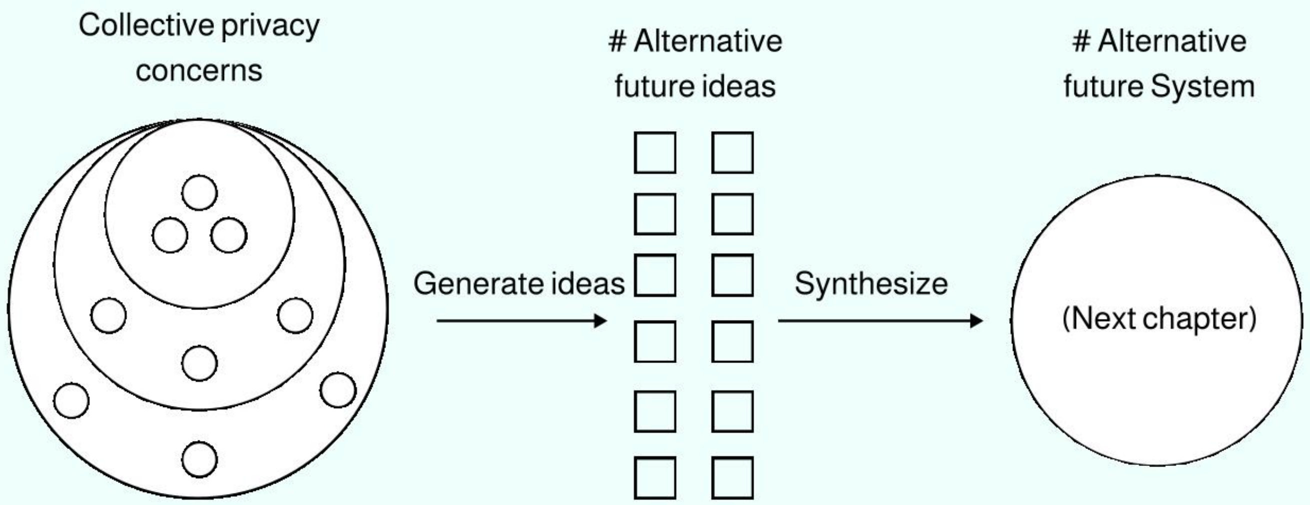

Collective privacy concerns
# Alternative future ideas
# Alternative future System
Generate ideas
Synthesize
(Next chapter)

Figure 6.7: Design process from privacy concerns to Alternative future intervention

07

Synthesis

From the 12 plausible future proposals, we synthesize them into a future intervention. This chapter demonstrates how we define the principles and prototype these ideas at various levels, aligning with the user experience. This chapter also shows some suggestions from iteration process on how to communicate the alternative future to individuals.

Synthesis

The goal for this chapter is to show how we synthesize 12 plausible futures into a coherent and integrated alternative future design proposal.

Principles

To achieve this future, we develop principles as the foundation. These discussions around these principles first emerged from the previous workshops and have been elaborated upon in the plausible workshop. The concepts of "coordination" and "sustainability" have been primarily discussed in previous workshops to raise awareness among the people. To clarify, we outline these principles in our future service, which we consider meaningful and empowering to individuals.

Encourage building good communication with individuals about their privacy risks.

Provide appropriate and meaningful information that allows them to understand those risks.

Encourage sustainable systems that support individuals in facing privacy issues.

Call for minimizing personal data usage by designing systems that are responsive to individual needs and resilient when privacy risks arise.

Future services should be accessible to everyone

Support equality and openness so that all individuals, regardless of their background, can benefit from equal access to privacy protections.

Appropriate structural support for individual awareness.

Envision the appropriate system structures to help individuals gain awareness, leverage the people's agency and structure ability

Future proposals in hierarchies

These 12 future proposals can be understood as existing across different hierarchies. To build a coherent future intervention, we organized the ideas according to these levels. In the following map, the purple ideas represent envisioned future models, the orange ideas represent interactions, and the yellow ideas focus on a more detailed level of visual communication. Within this coherent future, we will first prioritize the models and interaction strategies as the foundation for building the future service. The red dots in the number map for each idea represent the prioritization level.

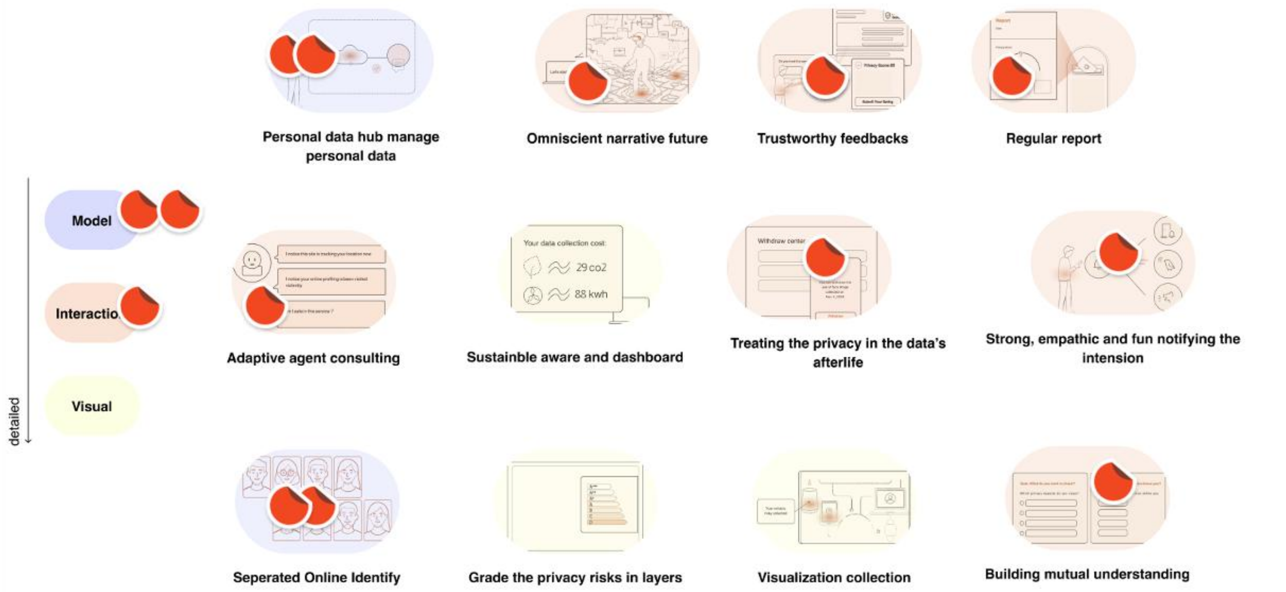
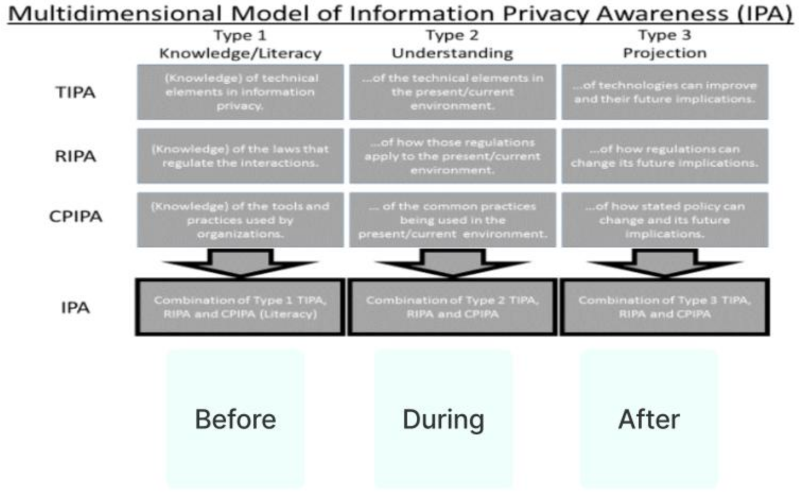

Personal data hub manage personal data
Omniscient narrative future
Trustworthy feedbacks
Regular report
Model
Interactio
Visual
detailed
Adaptive agent consulting
Your data collection cost:
29 co2
88 kwh
Sustainble aware and dashboard
Withdraw center
Treating the privacy in the data's afterlife
Strong, empathic and fun notifying the intension
Seperated Online Identify
Grade the privacy risks in layers
Visualization collection
Building mutual understanding

Figure 7.1: Prioritize ideas in hierarchies

Future proposals in experience

To make sense of this variety of future interventions and translate them into a speculative service, we organized the 12 selected future speculations along a timeline that reflects how individuals might experience them in real-life contexts.
Several insights from the literature informed the construction of this timeline. One key source of inspiration was the information privacy awareness literature (Correia & Compeau, 2017), which provided a basis for structuring future experiences according to their information privacy model.



Multidimensional Model of Information Privacy Awareness (IPA)

	Type 1 Knowledge/Literacy	Type 2 Understanding	Type 3 Projection
TIPA	(Knowledge) of technical elements in information privacy.	...of the technical elements in the present/current environment.	...of technologies can improve and their future implications.
RIPA	(Knowledge) of the laws that regulate the interactions.	...of how those regulations apply to the present/current environment.	...of how regulations can change its future implications.
CPIPA	(Knowledge) of the tools and practices used by organizations.	... of the common practices being used in the present/current environment.	...of how stated policy can change and its future implications.
IPA	Combination of Type 1 TIPA, RIPA and CPIPA (Literacy)	Combination of Type 2 TIPA, RIPA and CPIPA	Combination of Type 3 TIPA, RIPA and CPIPA

Figure 7.2: Model of information privacy awareness (Correia & Compeau, 2017)

In their work, Correia and Compeau (2017) distinguish between stages of privacy information awareness, each serving a distinct purpose, while acknowledging their interconnections in practice. Their model outlines three steps: (1) building users' privacy literacy, (2) surfacing and recognizing ongoing data practices in real-time contexts, and (3) helping users anticipate future consequences and engage in reflection.

Drawing from this awareness theory, we divided the future experience into three parts:

- **Initiation (before event-based risks):** Aimed at empowering individuals to build an initial understanding of privacy in online environments.
- **Awareness in events (during event-based risks):** Aimed at empowering individuals to recognize privacy risks in concrete situations.
- **Reflection (after event-based risks):** Aimed at empowering individuals to manage the afterlife of their data.

Following this timeline of experiences, we mapped the 12 ideas across the three parts. Considering the design direction, we prioritized ideas situated in the awareness in events stage, as they are most critical for supporting individuals in future interactions with privacy risks.

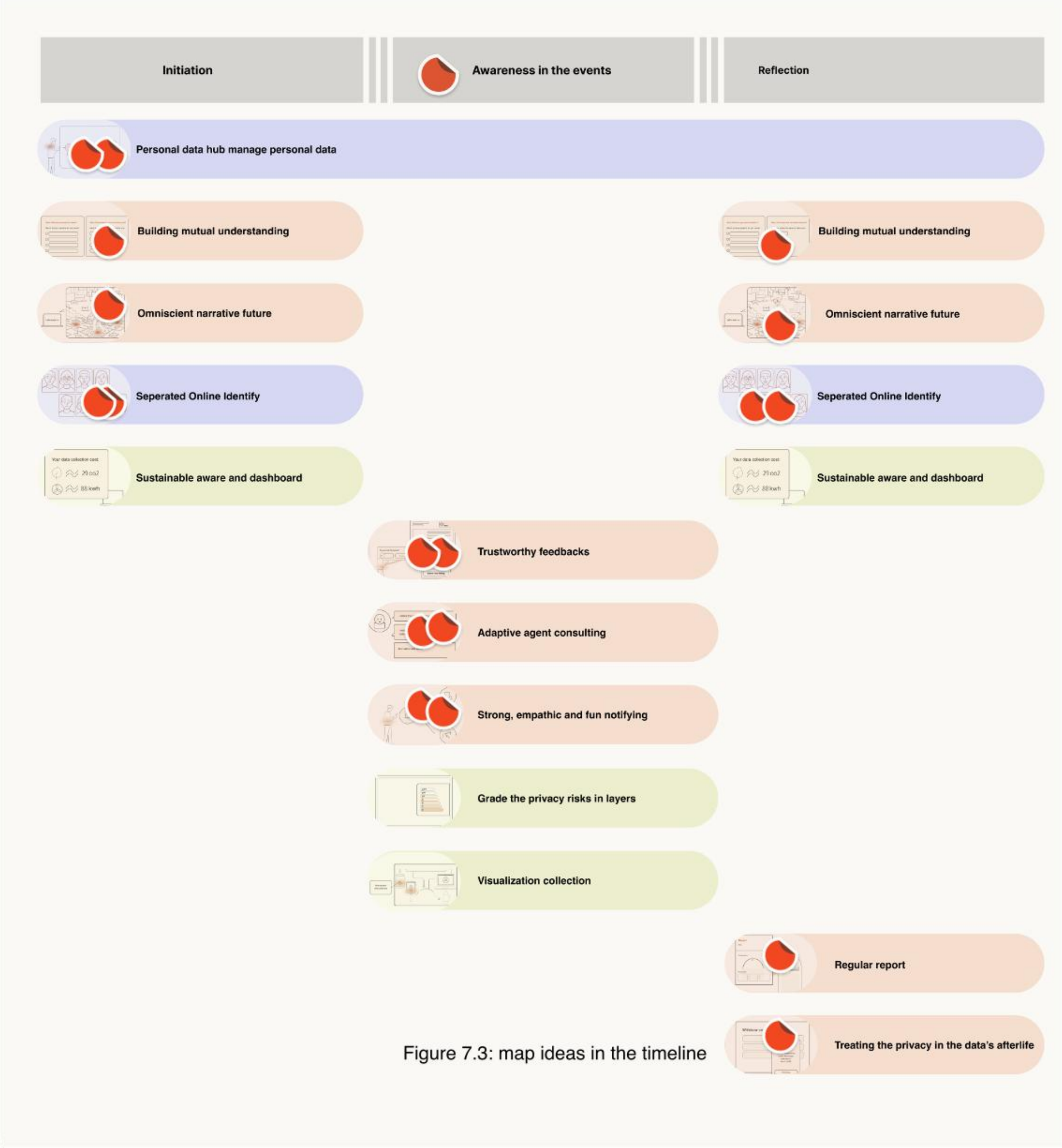

Initiation
Awareness in the events
Reflection
Personal data hub manage personal data
Building mutual understanding
Building mutual understanding
Omniscient narrative future
Omniscient narrative future
Seperated Online Identify
Seperated Online Identify
Sustainable aware and dashboard
Sustainable aware and dashboard
Trustworthy feedbacks
Adaptive agent consulting
Strong, empathic and fun notifying
Grade the privacy risks in layers
Visualization collection
Regular report
Treating the privacy in the data's afterlife

Figure 7.3: map ideas in the timeline

Developing alternative future intervention

To make the envisioned future more concrete and communicable, we created a representation of the potential future through rounds of discussion with designers. We went through the stages, mapped the links between ideas, and built them around the key flow of the service. The research presented a rapidly developed prototype, which was tested with design students in a quick review. This helped ensure that the ideas could be translated into a coherent future service experience. From these rounds of development, several key findings emerged. These suggestions illustrate **how we can communicate a tangible vision of the future to individuals.**

- **Present the future in layers**
  - To make the future intervention clear and accessible, we present it in three layers:
    - Background and roles introduction,
    - The future service aligned with the user journey
    - Actionable artifacts. These layers provide a comprehensive and tangible picture of possible privacy interventions.
- **Use an interactive App to support the future experience**
  - We decided to use an app as the carrier of the experience and service for two reasons:
    - It anchors the continuity of the future experience, providing a concrete interface through which to communicate with individuals about the future.
    - An app is easier to build, iterate on, and evaluate as a feasible prototyping medium, making the future service and system tangible.
- **Be flexible in approaching people**
  - Although we provided a timeline in experience, we designed the service to remain adaptable, allowing individuals to explore and tailor their experience.
- **Build a narrative**
  - In addition to visual elements, we incorporated a narrative component to illustrate how the service blueprint can be experienced in real-life scenarios. This narrative helps contextualize the touchpoint, making it easier for people to envision the future.

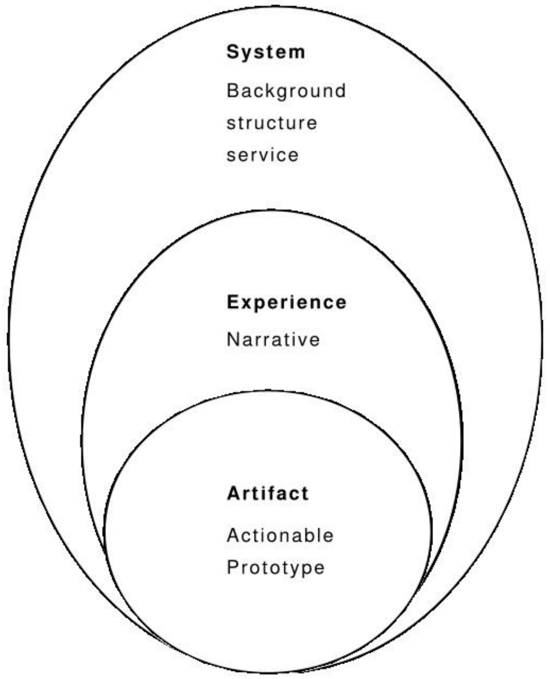


Figure 7.4: communicate the tangible future

- **Provide more text to guide an actionable prototype that supports engagement**
  - The initial synthesis showed that, without clear explanations, the prototypes felt too abstract. To address this, we added supporting text and simple guidelines to help users better understand and engage with the speculative future. This made the future experience more accessible.

- **Use metaphors in the stage of event-awareness**
  - Insights from the plausible futures workshop highlighted that metaphors are powerful tools for engaging people. We introduced metaphorical elements in the prototype to represent various privacy risks, making them more tangible.

- **Introduce question cards to prompt reflection**
  - To explore the broader implications of the future experience from an individual perspective, we developed a set of questions designed to generate deeper insights. These cards help users understand the future beyond their interactions with the actionable prototype, encouraging them to consider potential consequences and explore various use cases.

Conclusion

This chapter aims to transform the previously developed plausible future strategies into a coherent vision for the future.

First, we analyze the principles of developing an alternative future intervention, emphasizing the principles of “sustainability” and “coordination.”

Then we prioritized the ideas according to their hierarchy and the experience. In terms of the hierarchies, we place the 12 ideas related to models and interactions at the top, as they form the foundation for future experiences. We also prioritize ideas along a timeline of experience, focusing on awareness in events first.

Finally, we develop an initial, actionable prototype to gather feedback, which provides insights into how the tangible future could be effectively communicated.

08

Alternative Future Intervension

In this chapter, we propose an **alternative future intervention**, accompanied by a background service and a future narrative. The final system offers a comprehensive understanding of the entire research findings throughout this project.

You can find the evaluation of the future intervention, along with an actionable prototype, evaluation insights, and recommendations in this chapter.

Future background

In this proposal, we present the final intervention: a plausible and meaningful future that aims to empower people reflect on and aware privacy. This future intervention is an integrated outcome based on all plausible future analyses, offering a comprehensive understanding of the entire project. It envisions a future grounded in sustainable privacy, leveraging privacy concerns, striking a balance between structural support and individual awareness in online privacy.

System background

To illustrate this future proposal, we present the following systematic background. According to the future trend analysis in Chapter 6, the alternative system is positioned within the trend of sustainable privacy access for individuals in the near future.

The intervention is scheduled to take place in 2035. Several global developments will shape this new socio-technical landscape, which will be considered the future reality.

- Ethical privacy practices are increasingly promoted and valued, involving not only organizations and online services but also individuals. For example, the principle of minimum data use, collecting only what is necessary, has become a common standard.
- With the development of immersive and hyperconnected digital environments, privacy risks have become more complex. In these blended spaces, digital privacy violations can also lead to physical or emotional consequences for individuals.
- Shared responsibility for privacy is actively practiced by both online services and individual users.
- Algorithms are developing, with automated protocols coordinating access, roles, and responsibilities, calling for more flexible and user-centered control over personal data.

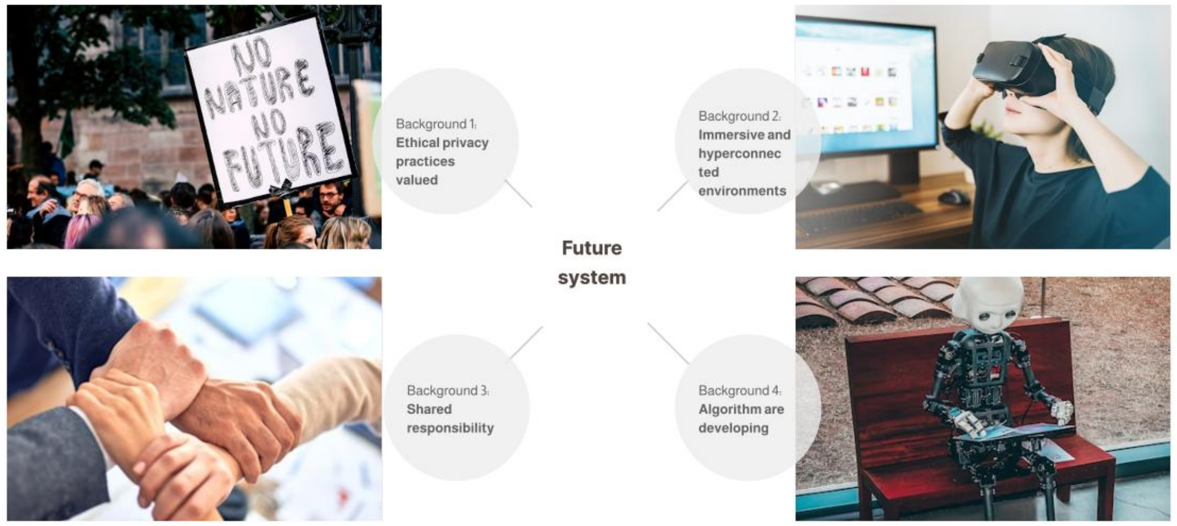

NO NATURE NO FUTURE
Background 1: Ethical privacy practices valued
Background 2: Immersive and hyperconnected environments
Future system
Background 3: Shared responsibility
Background 4: Algorithm are developing

Figure 8.1: Alternative system background

Roles

The alternative intervention, called PrivyDepot, reframes the roles of individuals, data holders, and data viewers. The diagram shows the position of the intervention within the relational diagram map.

In a future-oriented infrastructure, the intervention acts as a coordinator and agent within the system, with two layers of features: one for individuals and one for data holders and viewers.

- **Empowering individuals:** The intervention provides personalized services tailored to each individual, with their values and needs at the core of the system. It adjusts privacy strategies based on expressed privacy preferences. Specifically, PrivyDepot can represent the interests of individuals, act as a mediator, and provide necessary information about the risks associated with data collection and processing, as well as ongoing discussions of risks.
- **Coordinating in the backstage:** PrivyDepot also coordinates communication with both reviewers and holders. This collaboration happens in two parts. First, in collaboration with all data holders, PrivyDepot gathers all of an individual's online profiles from these holders. These separated identities represent the results of the data that has been collected and analyzed online. Second, it collaborates to identify and regulate risky data practices among holders and reviewers during events. Facilitating collaboration and interaction among these stakeholders helps cultivate a more sustainable and resilient privacy ecosystem.

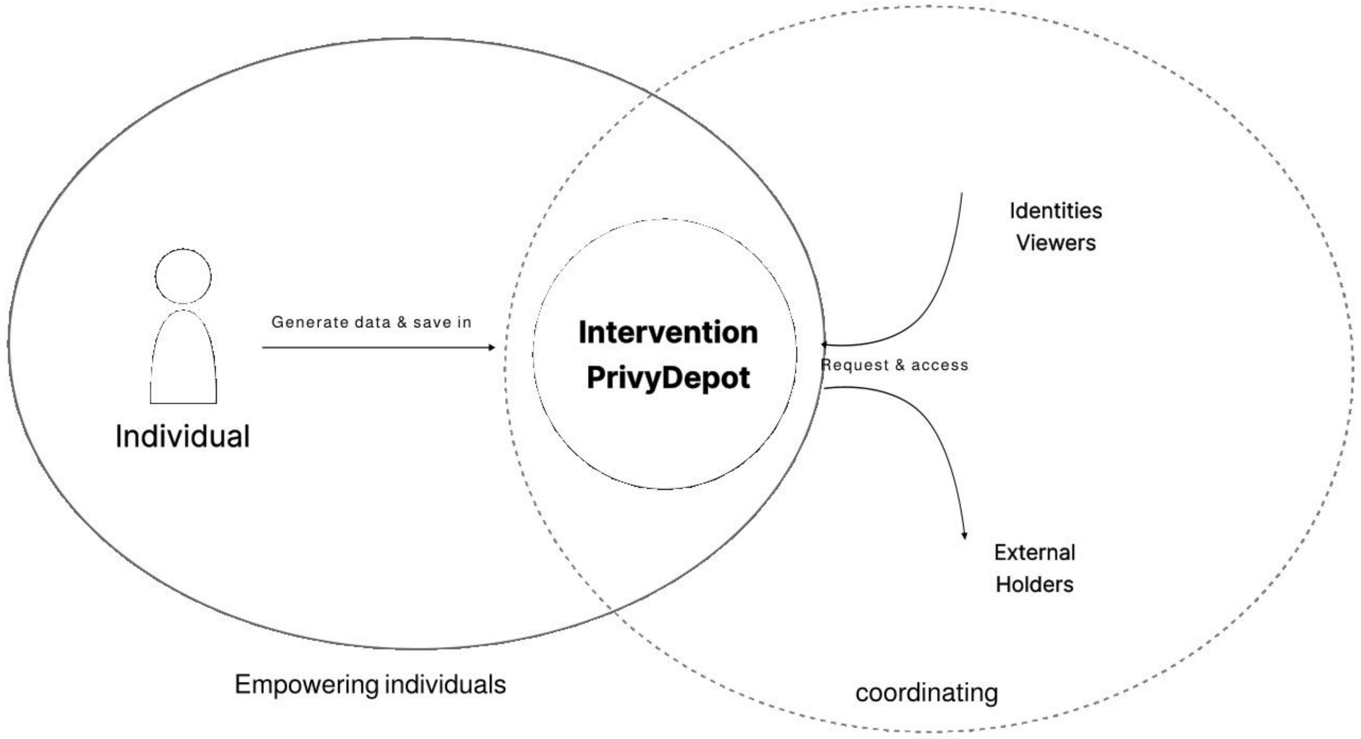


Figure 8.2: Alternative system roles map

Future Narrative

Since the alternative future service includes various touchpoints, the narrative aims to help people engage empathetically with concrete scenarios.

Within this narrative, we follow Emma, a digital freelancer living in the Netherlands in the year 2035, as she navigates a typical day. Through her eyes, we explore how privacy concerns manifest in subtle, emotional, and often invisible ways, and how thoughtful design interventions can support greater awareness.

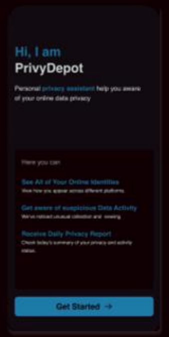
Initiation

Emma was installed and onboarded onto the Privacy Depot app. There were several **initial questions** to identify who she was and get her preference on being notified of the online data privacy.

After she answered a short set of questions, Emma **saw several cards that represented her online identities**, which are also her separate digital selves' personas, including social, health, financial, and career aspects, encompassing every part of her life.

She noticed something; for example, her health avatar includes sleep data from her wearable, while her professional avatar includes behavioral analytics from productivity tools. Her social identity has embedded emotional metadata extracted from message tone and emoji use.

"These parts of me are scattered across platforms," she thought.
"But luckily here these profiles are disconnected and stored from each other and cannot define a whole picture of me."



Hi, I am
PrivyDepot

Personal privacy assistant help you aware of your online data privacy

Here you can

See All of Your Online Identities
View how you appear across different platforms

Get aware of suspicious Data Activity
We've noticed unusual collection and viewing

Receive Daily Privacy Report
Check today's summary of your privacy and activity status

● **Hi, this is PrivyDepot**

The personal privacy assistant you can diagnose your privacy here

● **Identify who you are.**

To get your privacy preference and identified who you are.

● **Show who you are online**

Every part of me setting in the various domain.

Figure 8.3: Future narrative

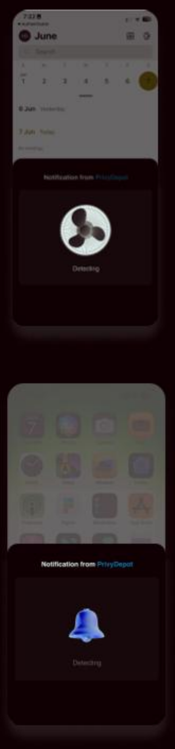
Aware with events

10:00 At the office workspace, Emma enters her shared office. Suddenly, she hears the soft whirring sound of a fan, which is coming from the app. The sound signals that "her voice data is being collected". Emma tags it as "Stop it," "Untrusted." The system records her reaction.

Noon, while grabbing lunch at a store, the same whirring sound plays through her earbuds. The APP informed her that "her location had been recorded". With hesitation, Emma taps "Stop it." This feedback will guide and adapt the system's future responses.

14:00 While Emma is working in the middle of the day, she hears a loud, urgent knock. "Her social avatar is being accessed". Emma quickly responds, "Stop it."

18:00 At the gym, while exercising, Emma hears a gentle and friendly knock sound: "Your social data is being accessed. " She taps, "Trust, continue."



● I am informing that

Suspicious Collection is happening

● I am informing that

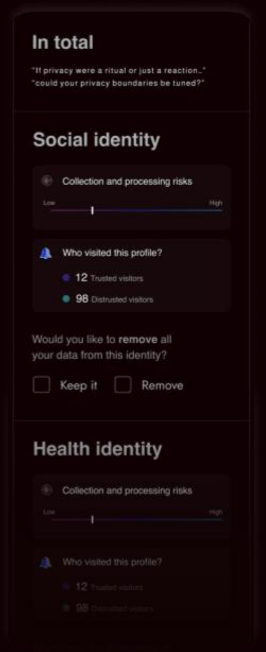
Suspicious visiting is happening

Reflection

Emma opened the app and received her Daily Privacy Report. It **summarizes the moments** that mattered, and she responded across various avatars.

At the end of the report, questions invite reflection:
"If privacy were a ritual or just a reaction…"
"Could your privacy boundaries be tuned?"
Emma does not take any further action. She does not revoke any data. She reads, pauses, and thinks.
Tomorrow begins again.

She is no longer a passive subject.
She is co-authoring her privacy together with Private Depot.



In total

"If privacy were a ritual or just a reaction…"
"could your privacy boundaries be tuned?"

Social identity

Collection and processing risks

Who visited this profile?

● 12 Trusted visitors
● 98 Distrusted visitors

Would you like to **remove** all your data from this identity?

□ Keep it □ Remove

Health identity

Collection and processing risks

Who visited this profile?

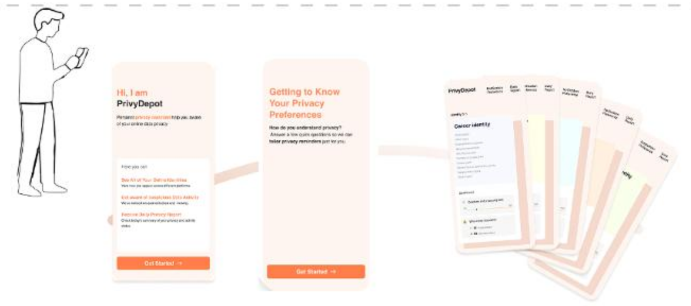
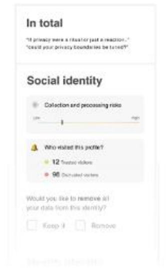
● 12 Trusted visitors
● 98 Distrusted visitors

● **Deliver the report to you**

Service blueprint

As with the system background and structure, we introduce the service blueprint. For this, we use a metaphor to describe the future service, known as the “Echo of Privacy.” This metaphor suggests that the service functions like a resonant chamber, generating echoes that raise awareness on multiple layers. These echoes are captured and amplified so that individuals can perceive, reflect upon, and respond to them.

In real-life settings, these stages are not strictly linear. Starting with initiation, continuous cycles of awareness triggered by events, and regular reflection can guide users over time. Within each stage, there are multiple moments and touchpoints designed to empower individuals.

		• build an initial understanding of online privacy	• Recognize privacy risks in concrete situations.	• Reflect the privacy in the afterlife of their personal data
Stage		Initiation	Aware with Events	Reflection
User Journey		Onboarding Answer questions View identities online	Aware of which risky data collection/ Aware of which risky identity view	Get the daily report.
Scenario				
Line of interaction				
Intervention Strategy	Frontstage	initial questions show risks in each indentity Sustainable dashboard	Strong, empathic and fun notifying Trustworthy feedbacks	Regular report Reflective questions
	Line of visibility			
	Backstage	Seperated Online Identify Building mutual understanding	Grade the privacy risks in layers Adaptive to individuals preference	Treating the privacy in the data's afterlife
		Personal data hub manage personal data		
Technology Capability		Processing individiuals privacy preferences Decentralized system keep all personal data	Processing the privacy risks Filtering the risks Adaption according to the feedbacks	Summarize the privacy risks Withdraw the data with feedbacks Develop and adapting the system
Support Coordination		External data holder Online platform Online community	External data holder Viewer Online platform Third parties	External data holder Viewer Online platform Online community Privacy insititution

Alternative future service

Future background

Hyper connected

Shared responsibility

Ethical practices

Algorithm developing

Principles

Build good communication

Sustainable systems

Accessible to everyone

Appropriate support

Statement

In the plausible future, a personalized intervention empowering people to awareness and reflect their privacy in online digital experiences, leveraging levels of privacy concerns of individual, interaction and social implication domain in a meaningful way.

Structure and roles

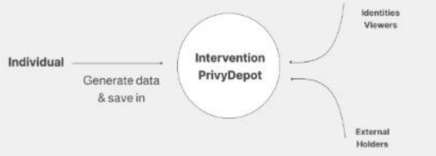


Figure 8.7: “Echo of privacy” service blueprint

Service detailing

Initiation

Stage aims to empower people to develop a basic understanding of privacy in the online environment. This stage involves the following parts.

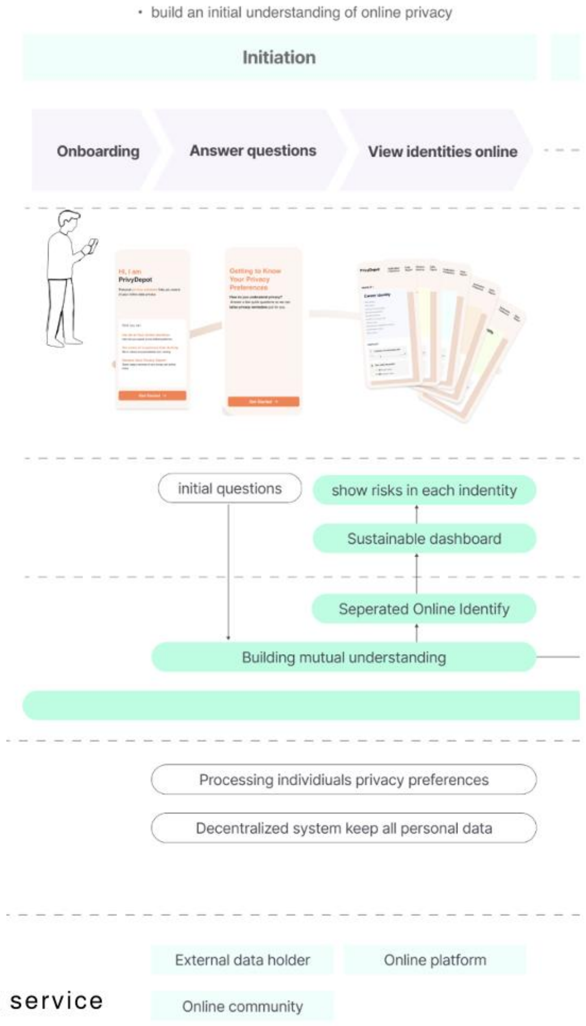
- **Mutual understanding**
- This is where individuals begin to answer questions about their privacy preferences, and the system begins to learn from them. The intervention starts by prompting individuals with a set of open-ended questions. These questions examine how they perceive privacy risks, which types of data they consider emotionally sensitive, and their attitudes toward data usage. The goal is not to create a rigid profile but to establish a baseline understanding that can adapt over time.

- **Online identities overview**
- After completing the initiation, individuals gain access to a dashboard that presents a comprehensive view of their online identities. The system gathers profiles from various data holders and visually reconstructs how the user's data is distributed across platforms. This visibility helps individuals begin to understand their digital presence.

It marks the first point of self-recognition, helping users see not just what is being collected but also how that data represents them in different contexts. It also aligns with earlier findings where users reported a lack of connection to or ownership of their data. By visualizing their identities, the intervention offers a tangible entry point into privacy empowerment.

Concern alignment:

- **Knowledge:** Provides individuals with an initial understanding of their online data.
- **Ownership:** People can develop a sense of ownership over their online privacy and generate more connections.
- **Identity:** Users can recognize their separate online identities and view their online presence.
- **Personalization:** As in our previous findings, individuals view privacy as highly personalized. People have different understandings of what counts as a "risky" situation. After initially downloading Privy Drop, the intervention presents a series of questions to understand personal attitudes toward online privacy.



• build an initial understanding of online privacy
Initiation
Onboarding
Answer questions
View identities online
initial questions
show risks in each indentity
Sustainable dashboard
Seperated Online Identify
Building mutual understanding
Processing individiuals privacy preferences
Decentralized system keep all personal data
External data holder
Online platform
Online community

Figure 8.4: Initiation service

Aware with events

Awareness in events aims to empower people to recognize privacy risks in concrete situations, especially key moments that matter to them during data collection and dissemination. The intervention is designed to activate awareness only when necessary, reducing the risk of fatigue or desensitization.
In the Chapter 6 workshop, participants expressed that they intuitively sense the intentions behind data usage when notifications are empathic and engaging. Therefore, we utilize metaphors to make data collection and online identity tracking more accessible, while also providing strong, empathetic, and engaging notifications.

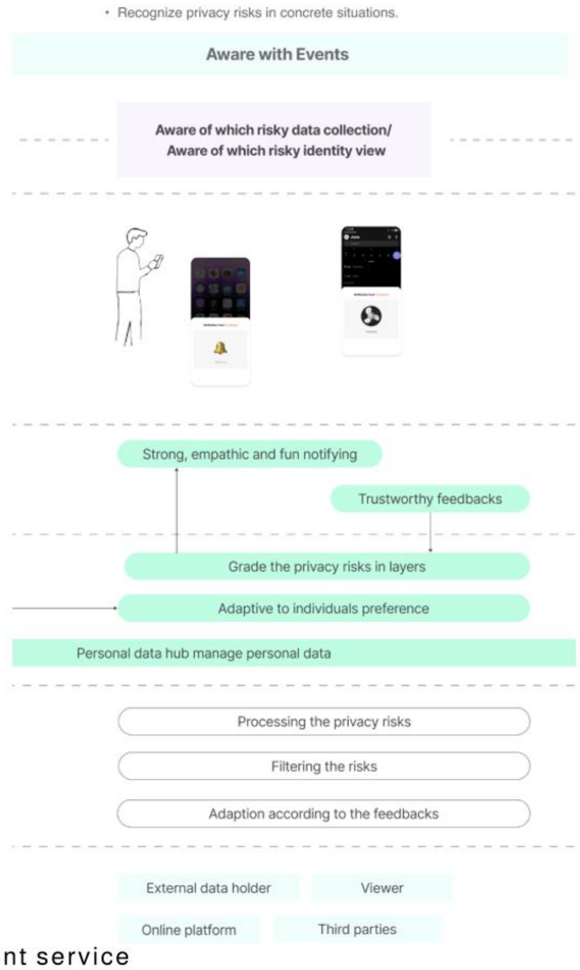
- **Notification of collection:** The intervention empowers individuals to recognize risky collection situations through tailored notifications. It clarifies what data is collected and the intentions behind it. PrivyDepot coordinates with data holders and empowers users to engage and pay attention at moments that truly matter.

- **Notification of dissemination:** The intervention empowers individuals to recognize and prevent the risky dissemination of their identities to viewers. It clarifies who is viewing the data and the intentions behind it. PrivyDepot coordinates with data reviewers and empowers users to engage and pay attention at moments that truly matter.

- **User feedback**: As part of the intervention, individuals can also provide feedback directly to data collectors and viewers. The aim is to build a sense of responsiveness and mutual negotiation, turning the system into a dialogic partner rather than a one-way information provider. This approach aligns with the idea of a more equitable privacy ecosystem, where individuals are not merely informed but can actively shape how their data is handled. This empowers users with the ability to act upon concrete risky events.

Concern alignment:

- **Knowledge:** Provides individuals with situational awareness about data collection and how their identities are perceived.
- **Efficiency:** Users can protect their data from being collected and viewed.
- **Personalization:** Users gain awareness tailored to their individual needs.
- **Behavior feedback:** Users can act on the behavioral feedback they receive.
- **Responsibility:** Users can understand the intentions behind data collection and viewing, enabling them to recognize the shared responsibility of both data collectors and viewers.
- **Credibility:** Through feedback provided to data viewers and data holders, the system can become more trustworthy.
- **Equality:** Users can push back and make judgments on online services, contributing to a more equitable system.



• Recognize privacy risks in concrete situations.
Aware with Events
Aware of which risky data collection/
Aware of which risky identity view
Strong, empathic and fun notifying
Trustworthy feedbacks
Grade the privacy risks in layers
Adaptive to individuals preference
Personal data hub manage personal data
Processing the privacy risks
Filtering the risks
Adaption according to the feedbacks
External data holder
Viewer
Online platform
Third parties

Figure 8.5: Aware with event service

Reflection

This stage aims to empower people in managing the afterlife of personal data. Considering online privacy risks is often seen as pointless and endless; this stage offers regular reflection, supporting individuals in revisiting their online privacy over time and allowing them to make adjustments.

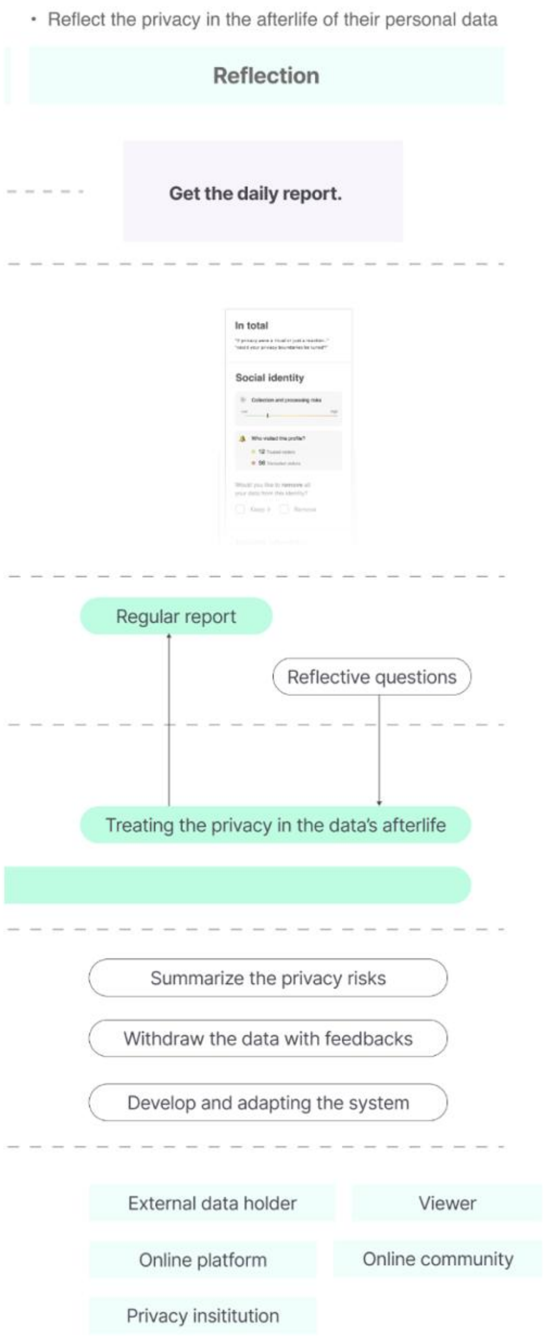
- **Report**
- The system prompts users to engage with these decisions by offering a Reflection Report, which shows how their data has been handled over time. The report outlines how data has been utilized, the feedback provided, and whether specific data flows have been modified. It is available in both online and offline formats:
  - Online: An interactive dashboard for those who prefer real-time insight.
  - Offline: A downloadable version for those who seek quiet, offline moments of contemplation.

- **Withdrawal**
- Through the Reflection Report, people can choose to keep or withdraw their data in each identity based on “risky” concerns, creating opportunities for individuals to have control over the afterlife of their online data.

Concern alignment:

- **Knowledge**: The system generates a regular Reflection Report to provide individuals with knowledge about how their data has been collected and its associated risk level.
- **Ownership**: Users can develop a connected sense of the afterlife of their data through the report.
- **Efficiency**: Users can be aware of the afterlife of their online privacy, and the system provides touchpoints for individuals to navigate the risks.
- **Responsibility**: Individuals share a responsibility for their data, supported by the system and self-awareness.

In conclusion, these stages form a continuous loop of interaction that supports long-term resilience in digital privacy awareness in the future. Initiation builds foundational trust, awareness creates contextual empowerment, and reflection sustains agency over time. Through this journey, individuals are not treated as passive recipients of their online privacy but as active participants in shaping how their data lives, flows, and remains online.



• Reflect the privacy in the afterlife of their personal data
Reflection
Get the daily report.
In total
Social identity
Collection and processing risks
Who visited this profile?
Regular report
Reflective questions
Treating the privacy in the data's afterlife
Summarize the privacy risks
Withdraw the data with feedbacks
Develop and adapting the system
External data holder
Viewer
Online platform
Online community
Privacy insititution

Figure 8.6: Reflection service

Evaluation

The **goal** of evaluation is two-fold:

- **To validate the understanding of the alternative service.** The actionable prototype needs to be effective in conveying an alternative service. The service needs to be understood by participants. Participants could express their opinions through the prototype.

- **To find the implication and use cases of the alternative future**. Through participants' understanding of the actionable prototype and narrative, they express their ideas about these specific futures, which could provide some recommendations and concrete use cases for the future potential transition of online data privacy.

Evaluation Session

Each session has been approximately 30 minutes. 5 participants are recruited. The test material includes a QR code to download and set up the prototype, we use the narrative to guide the people in the test and a question card that helps them express their ideas about this alternative future.

Process

1. Introduction about Future Context

The session began with an introduction that presented the future background, helping participants understand the speculative context of the prototype.

2. Experience the Actionable Prototype

Participants interacted with the actionable prototype, navigating through key moments that highlight critical aspects of the speculative service. To keep the experience cohesive, Participants were provided with a narrative story that further elaborated the future context.

3. **Respond to Question Cards**

To support the discussion and reflection, participants were given a set of open-ended question cards. These questions aimed to explore their understanding of the service and its broader implications in various use cases. Participants were free to select and answer the questions most relevant to them, offering personal reflections on the envisioned future.

4. **Discussion**

With the question cards supported, the researcher and the participants have a deep discussion on the concrete future. In this part, we encourage open discussion.

About future

1. **What do you think this app is used for?**

→ This question aims to understand how participants interpret the use case of the intervention.

2. Who do you think would create an app like this?

→ This explores participants' perceptions of the stakeholders or institutions behind such an intervention.

3. What story do you think this app tells about the future?

→ This question invites reflection on the broader societal or systemic future implied by the app.

4. What story do you think this APP tells about how people experience this future?

→ To understand which aspects of the future vision participants find desirable or meaningful.

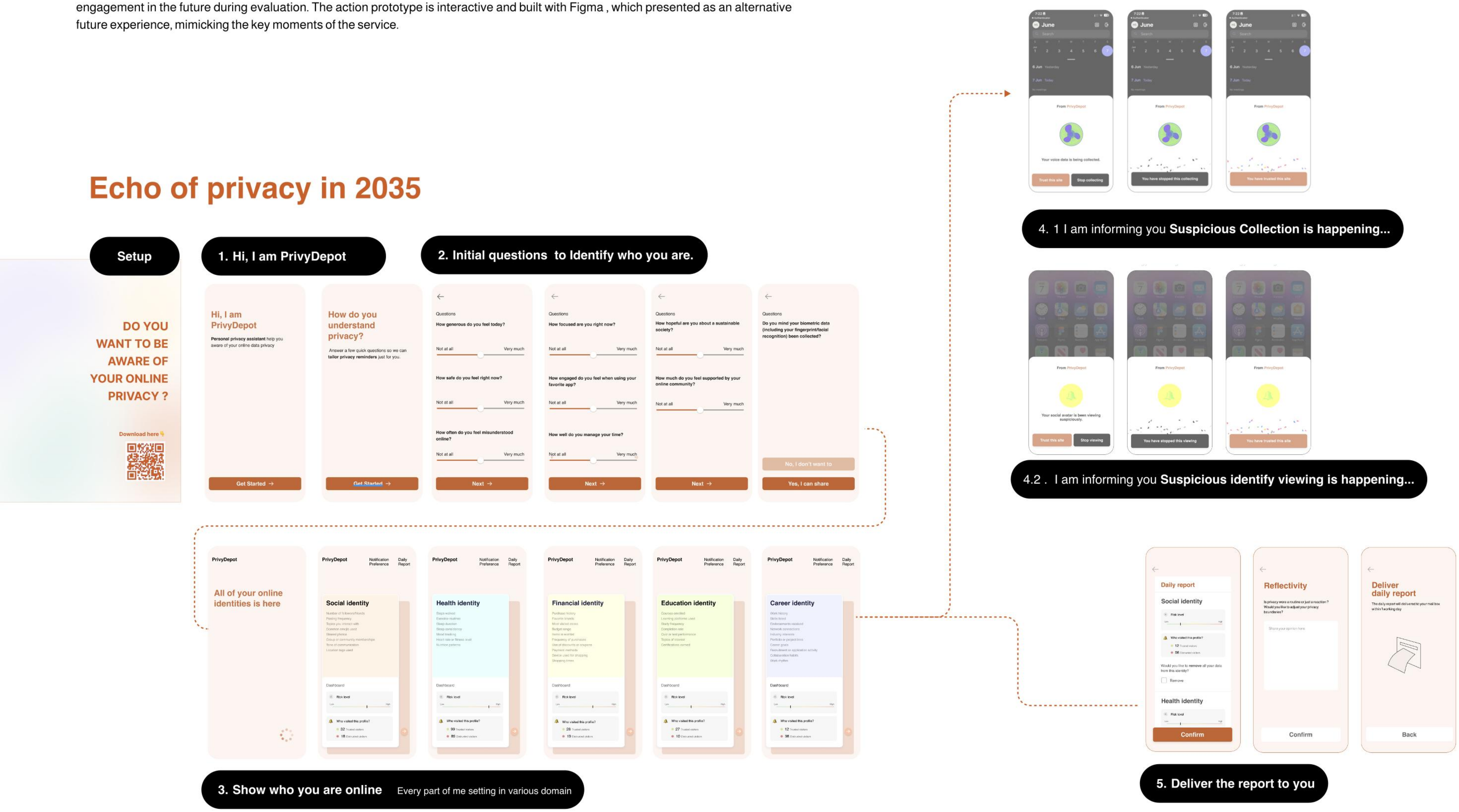
5. What will online data privacy look like in this future?

→ To explore participants' worries, doubts, or perceived risks about the envisioned future..

Figure 8.8: Questions card (with explanation)

Actionable prototype

To make the service blueprint tangible for people to grasp, we have developed an actionable prototype that can enhance user engagement in the future during evaluation. The action prototype is interactive and built with Figma , which presented as an alternative future experience, mimicking the key moments of the service.



Echo of privacy in 2035

Setup

DO YOU WANT TO BE AWARE OF YOUR ONLINE PRIVACY ?

Download here 👇

1. Hi, I am PrivyDepot

Hi, I am PrivyDepot

Personal privacy assistant help you aware of your online data privacy

Get Started →

How do you understand privacy?

Answer a few quick questions so we can **tailor privacy reminders** just for you.

Get Started →

2. Initial questions to Identify who you are.

Questions

How generous do you feel today?

Not at all — Very much

How safe do you feel right now?

Not at all — Very much

How often do you feel misunderstood online?

Not at all — Very much

Next →

Questions

How focused are you right now?

Not at all — Very much

How engaged do you feel when using your favorite app?

Not at all — Very much

How well do you manage your time?

Not at all — Very much

Next →

Questions

How hopeful are you about a sustainable society?

Not at all — Very much

How much do you feel supported by your online community?

Not at all — Very much

Next →

Questions

Do you mind your biometric data (including your fingerprint/facial recognition) been collected?

No, I don't want to

Yes, I can share

3. Show who you are online   Every part of me setting in various domain

PrivyDepot

All of your online identities is here

PrivyDepot   Notification Preference   Daily Report

Social identity

Health identity

Financial identity

Education identity

Career identity

Dashboard

Risk level

Who visited this profile?

4. 1 I am informing you **Suspicious Collection is happening...**

From PrivyDepot

Your voice data is being collected.

Trust this site   Stop collecting

You have stopped this collecting

You have trusted this site

4.2 . I am informing you **Suspicious identify viewing is happening...**

From PrivyDepot

Your social avatar is been viewing suspiciously.

Trust this site   Stop viewing

You have stopped this viewing

You have trusted this site

5. Deliver the report to you

Daily report

Social identity

Risk level

Who visited this profile?

12

58

Would you like to **remove** all your data from this identity?

□ Remove

Health identity

Risk level

Confirm

Reflectivity

Is privacy were a routine or just a reaction ? Would you like to adjust your privacy boundaries?

Share your opinion here

Confirm

Deliver daily report

The daily report will delivered to your mail box within 1 working day

Back

Figure 8.9: Actionable prototype

Key insights

Risks of alternative future

Motivation, incentives & engagement

Incentives

"I hope I can see much more benefit for me to use the app in the beginning, probably always show how much my privacy is promoted."

One key discussion was around what would motivate people to use such a system in the future. People acknowledged that the system could help individuals become more aware of online risks and better understand their boundaries and space. However, there is still a feeling that it might not be enough to engage with the alternative service. Participants expressed the need for clearer incentives or motivation strategies, something that would help people recognize the potential benefits early on and encourage them to start using the service. This highlights an important thing. Although privacy is often framed as a fundamental human right, in everyday life, people tend to approach it in more practical or even utilitarian terms. How to effectively motivate individuals with these interventions is a challenge that needs to be considered in the future.

Voluntary engagement

Another important point was that individuals' engagement should remain voluntary. Participants were concerned that if such systems became mandatory in the future, they would feel more like a chore than an empowerment service. If there is not enough flexibility, a meaningful privacy service might turn into just another type of "cookie", people feel forced to accept, rather than something they truly "value".

"If it is a mandatory use in the future, could it become something that replaces cookies?

Long-term engagement

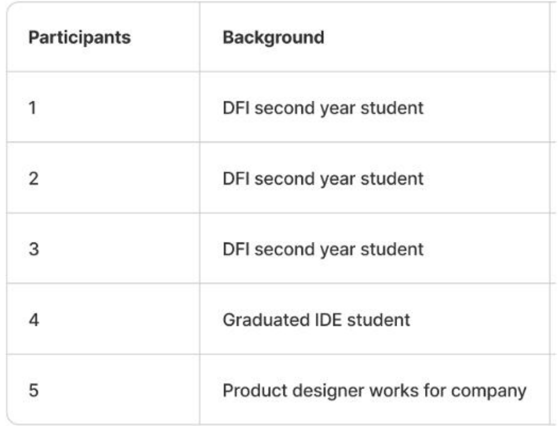
There are also raised concerns about how the system might evolve. When faced with frequent access requests from multiple services, users may become desensitized or indifferent to privacy notifications or these daily reports, regardless of the system's ethical design or adaptive capabilities. Building a long-term habit for individuals or establishing a trust-based relationship between individuals and the intervention is still something we should consider in the future.This also represent that their are different types of use attitude towards online privacy will influence the engagement for the system.

"I might not use it for long. I will not just look at this report, like a supermarket invoice, it only gives me"

Graded privacy risks

Some discussion centers on the privacy grading; some people mention that they can see the benefit of grading privacy for various stakeholders, provided sufficient information has been considered, which could benefit both self-management and data sharing. In this topic, a thorough discussion of this grading system was deemed beneficial for multiple stakeholders. For example, Individuals could better understand the consequences of sharing certain types of data and make more informed decisions. Organizations could tailor their requests and policies based on the sensitivity of the data they collect.

"I felt like the data you provide on the internet is going to be more and more layered. I think in the future there will be many libraries showing the risks of different data provided for different individuals."



Participants	Background
1	DFI second year student
2	DFI second year student
3	DFI second year student
4	Graduated IDE student
5	Product designer works for company

Figure 8.10 Participants involved in the evaluation sessions

There are discussions on how to rationalize these graded privacy settings and make them accessible in the future. In the alternative artifacts' notification, people express that the grading is a little "abstract"; they want to know what the risk level means to them. Making the grading risks clearer for individuals to interpret is something we should consider in the future.

"I can envision there might be a risk happening... I also want to know what the line is and what it stands for."

Quantified self risks

Another emerging topic in the discussion was the potential use of the service for self-tracking privacy, where individuals' digital privacy is measured and assigned scores. This aligns with the concept of the quantified self as discussed by Lupton (2016). One Participant discussed that this service could be a tool to monitor and reflect on various aspects of their lives. On the positive side, quantified privacy could empower users to understand their digital presence and make informed choices. On the other hand, there are concerns that such personal preferences obtained by the system cannot be properly kept, and their disclosure may cause more privacy crises. For example, the potential for malicious misuse to reveal someone's identity demonstrates that there is no "100% safe" protection in terms of complex privacy issues. However, we need to make an effort to improve the future.

"For self-measuring. My life can be recorded and measured. Everything is graded. The story could be that people become cautious about their behaviour because they can be monitored. I do not think this is the best future. I am afraid it may cause more resistance."

Trust vs Fun

Based on previous findings from the futurist session and development, the notifications employed playful metaphors, such as a fan animation representing data collection and a bell animation representing identity access, to foster empathy and connection regarding online privacy. Some participants responded positively, describing the animations as "cool" and enjoyable, suggesting that this approach can help humanize privacy communication.

However, others raised concerns about the potential trade-off between playfulness and trust. One participant noted that privacy is a serious issue, and if the metaphors appear too casual or playful, they might reduce the perceived trustworthiness of the intervention system.

This highlights the need for a balanced tone in communicating privacy to individuals. The messaging should be empathetic enough to raise awareness while also maintaining the credibility and trustworthiness of the system.

"I like the animation, I think it is something in working."

" I feel like it is untrustworthy . It look like shaky."

Value of alternative future

Personal space adjustment

"It feels like… My data is like my home, my personal space. And then there's someone constantly knocking on my door. My reaction is like: every day, someone comes to my house. Sometimes I open the door, and that's a reaction. Then, at the end of the day, I can check who the visitors were and who came. And if someone came and messed up my house, then I definitely wouldn't welcome them back."

The participant described their data as being closely tied to their personal space, using a metaphor to express their feelings: While the boundaries of space are dynamic, thus no "one-cut" strategies could fit the future, which also aligns with the personalization experience of privacy of Zhang & Sundar (2019). The participant reflects that the system allowed them to engage selectively at different times and make decisions on their terms.

Automatic Decision

"I hope this assistant can help me make more decisions. If the information is beneficial to me, I will not withdraw it. For example, if I need to find a job on LinkedIn, I need to share my information."

Participants welcomed the idea of an automated system to assist them in making informed privacy decisions, particularly when the system could assess risks and benefits and provide recommendations.
One implication is related to automated decisions concerning the use of personal data. Participants hoped the system could offer more value through automatic support. This could not only involve identifying risky uses of personal data, as we envisioned, but also helping individuals recognize which uses might be beneficial. There was also an argument that the future service and technology should be human-centered for the sake of individuals.

Human-centric mindset

In discussions with the participants, we emphasized that, rather than only knowing how much personal data is at risk or who is accessing their privacy, what matters most is that the system consistently prioritizes the individual's best interests in the future.
"Beyond showing these risks and the violations, I wonder how well this system would work for more in the future."

This aligns with our previous findings: individuals are experts in their own experiences, and future systems should place the individual at the center of their experience. The highlight of the future privacy service is that it should always prioritize individuals, not only in raising awareness, but also in presenting that awareness in a suitable way.

Usage cases infer

For the interference use case, participants expressed different views; the value is not only for individuals but also for building ethical use of data, and could provide value for other stakeholders. We elaborate on participants' answers in the following four parts:

- **Continuous privacy education for individuals**

The service could act as a daily companion that continuously educates individuals and their communities about protecting personal boundaries in the digital world. One envisioned outcome of the discussion is the government developing such an intervention to promote long-term public awareness of digital privacy.

- **Tailored privacy concerns in various scenarios**

The envisioned service allows individuals to manage their privacy across different environments and contexts. For example, a person who is particularly privacy-aware in the workplace and fears that companies may collect sensitive data could set stricter privacy controls in that context. In contrast, in more open or informal settings, they might choose more flexible sharing preferences.

- **Support for privacy-sensitive individuals**

The service could offer emotional support to those who are particularly sensitive about online privacy. For example, individuals who have experienced online harassment and feel anxious about personal data exposure. It helps create a more positive and controllable online environment.

- **Promoting ethical data use among companies**

There were also discussions about the possibility of companies being more tightly regulated in the future. The intervention could promote more ethical handling of personal data. One envisioned case featured a privacy-first company developing such an intervention to ensure responsible data practices.

"I think data security analysts working for a company may be more dedicated to the company for data Protection."

"People are becoming more and more concerned about their privacy and the risks of online abuse."

"Education. Governments or the privacy organizations can use this to educate the public "

"Advertisers may use it to enhance their strategies and more effectively monitor people's behaviour."

Discussion

Actionable Prototype's communicative power

The Prototype proved effective in envisioning a concrete future. Participants were largely able to infer the core intentions of the future service through interacting with the Prototype and its background explanation. Through their responses to the question cards, they articulated various interpretations and extrapolations of the future system. Participants expressed that they “enjoyed” (P3) and were “satisfied” (P2) with the opportunity to learn new things about online privacy through the app’s detailed information.

While there were limitations in testing, one notable issue was the inconsistencies in the connections between the questions in the initiation stage and the personalized awareness environment in the testing procedure. Participants expressed a desire for stronger links to understand this. As one participant noted, “I did not find much connection between these scenarios and the main app.”

In their reactions to the scenarios, participants also indicated that the information provided should be more concrete and specific. Some found it difficult to answer questions like “Trust or not trust” due to the lack of contextual details. **This suggests that providing more concrete situational background** could help participants engage more deeply and better understand the intended interactions within the future system.

Discuss about the future narrative

For the narrative, participants expressed a positive attitude and interest when reading the future scenario. We found it empathetic and helpful for evaluating the proposed future service. However, we also received feedback that the Emma persona included in the narrative could be described in greater detail to make it more engaging. In other words, the concrete scenarios could be more strongly connected to the persona, making the narrative more coherent and immersive.

During the discussion, the researcher also raised the question with the participants of whether the narrative influenced participants’ ability to imagine potential future use cases. Participants generally felt that they could envision possibilities beyond what was presented in the narrative. **We also recommended that including a greater diversity of personas in the narrative** could encourage them to think further beyond the original narrative and to interpret more potential use cases in the future.

Discuss the overarching experience in the alternative service

In the initial stage of understanding, when participants viewed their online profiles, most of them scrutinized them. They expressed a desire to learn more about the meaning of each label and its privacy implications.
One participant described feeling normal when answering the initial questions and seeing the identity overview.
In contrast, they felt “surprised” (P3) during the stage of becoming aware through events, as they had not realized such risks could occur in those scenarios. Others mentioned that they would prefer a more friendly and approachable form of awareness(P5). Overall, event-based awareness was perceived to bring more thinking and discussion. **Contextualized awareness has the potential to provide greater value for future systems.**

Limitation & Recommendation

Simplify interactions of the APP and focus on the future service

To provide a coherent experience, the current prototype includes detailed interactions and visual elements. However, these go beyond the scope of the intended service blueprint and may be considered a limitation. These details were initially designed to help users engage with the experience. However, during real testing, we found that they sometimes distracted participants, shifting their focus toward interface details rather than the core concept of the service. Therefore, it is necessary to simplify unnecessary interactions in the app, such as removing unnecessary animations and reducing complexity. This streamlining enables users to focus more effectively on envisioning and reflecting on alternative future scenarios.

Evaluate this alternative intervention in participants' daily lives.

During the testing phase, participants were invited to explore the future scenario through a combination of narrative and app within a project room. Since the concept involves long-term engagement with an alternative future, participants found it challenging to grasp the long-term implications of the system fully. Moreover, because the service envisions a highly personal and contextualized experience, simulating it in a static environment limited the reflection to some extent. The future studies could embed the intervention into participants' everyday lives, allowing them to encounter privacy-related moments naturally as part of their routine. Such real-life integration could provide more insights than narrative exploration alone.

Expand more concrete scenarios to maximize the value of the actionable prototype

During the narrative and app experience, we provided only four example scenarios to inform users about their data environment. For instance, receiving notifications about suspicious data collection or identifying unknown data viewers. Based on the feedback, we observed that people have different perceptions of privacy in these scenarios. Therefore, it is valuable to expand the app's contextual scenarios to include a broader range of concrete, everyday experiences, which would help gather more diverse user opinions and demonstrate the app's scalability and potential to evolve into a future tool that supports a more nuanced understanding of digital privacy..

Involve more diverse participants

In the evaluation phase, we mainly involved design students from TU Delft to test and provide feedback. These participants tended to have a more positive outlook toward such future systems, which could be a limitation. In future studies, it is essential to include participants from diverse backgrounds to gather a broader range of feedback and gain a deeper understanding of the implications of alternative futures.. For future, we can build different persona for people based on individuals attitude towards privacy and see their various opinion towards future.

Integrate more stakeholder

The current testing primarily involved discussions with individuals. However, since the future service also impacts parties beyond individual users, it is valuable to gather and incorporate feedback from other stakeholders, such as privacy experts, policymakers, and online service providers, in future development. Comparing their perspectives with those of individuals could form the basis for joint evaluation sessions involving a more diverse group of participants. This approach would offer more multi-perspective feedback and support the further transition of the system.

Maximize the value of the alternative future service

Although the service blueprint was developed with the background structure in mind, the service primarily targets individuals. In the validation sessions, we focused more on the user experience from the individual's perspective, while coordination with multiple data holders and data viewers was not within the scope of our testing. However, through the use-case interventions, we recognized the broader value of the service, including its potential for public education and promoting more ethical data usage among online companies. Therefore, the alternative service could be expanded to include more use cases with broader participant involvement, or as tools to investigate the opinions of more people about this future and develop the roadmap towards it. We can maximize the value of alternative services, enabling broader applications and facilitating future transitions.

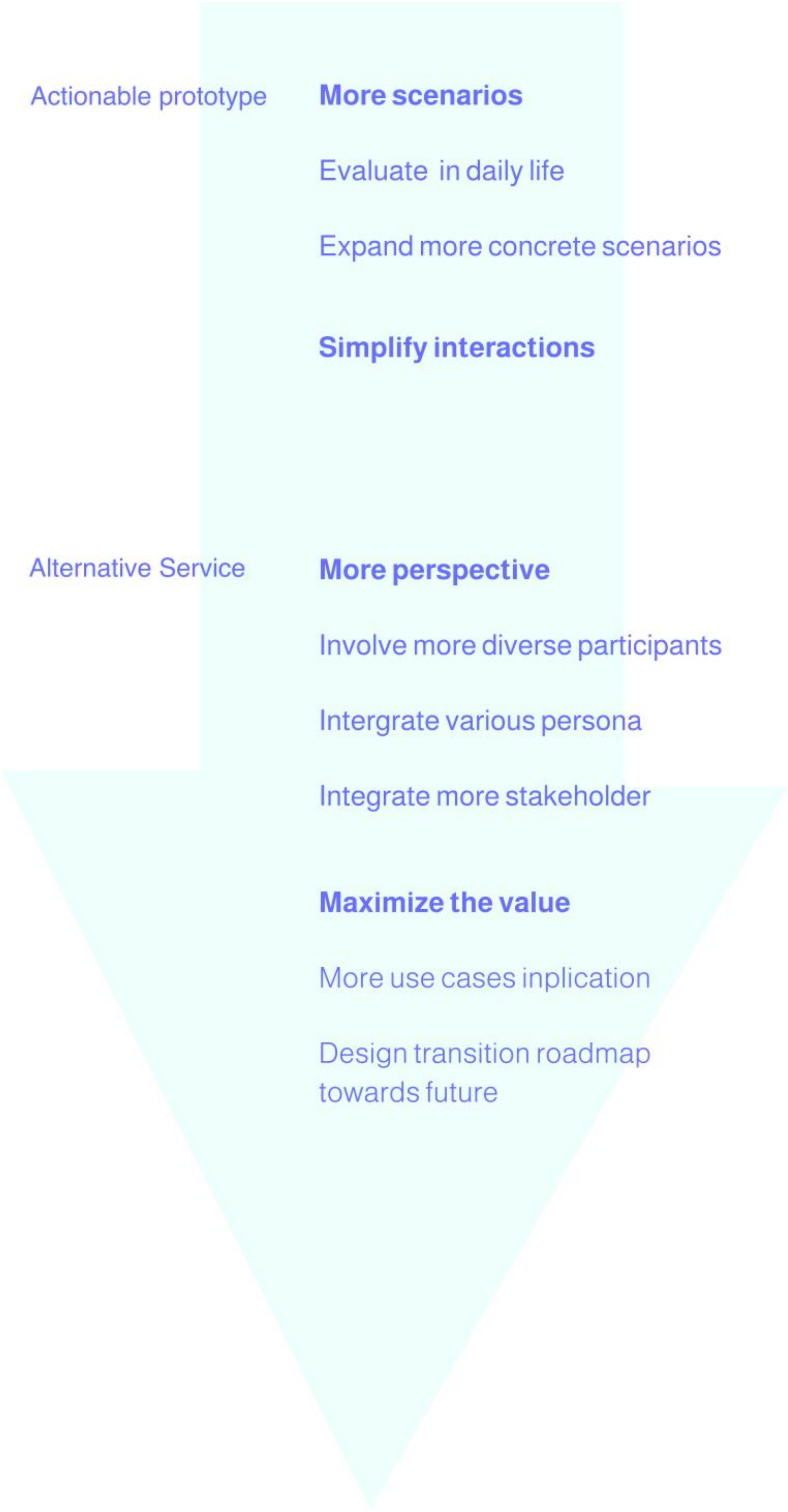

Actionable prototype
More scenarios
Evaluate in daily life
Expand more concrete scenarios
Simplify interactions
Alternative Service
More perspective
Involve more diverse participants
Intergrate various persona
Integrate more stakeholder
Maximize the value
More use cases inplication
Design transition roadmap towards future

Figure 8.11： Recommendation list

09

Conclusion

In this chapter, we present the conclusion of this project and a personal reflection on the entire project journey.

Conclusion

RQ 1:Raise awareness through “Preposterous Futures” How design could help provoke individual awareness of online data privacy?

To address the question, we first ground the current context. Since privacy risks are often invisible in everyday life, we employ three complementary methods here to capture the “invisibility” in the social-tech background.
To raise awareness and increase understanding of privacy among individuals, we developed three artifacts that envision the “preposterous future” based on our previous findings. Two follow-up workshops gathered participants’ concerns about online data privacy regarding these three artifacts, specifically in the areas of collection, processing, and storage.
The findings highlight the privacy concerns associated with layer of value for individuals. We map them across three levels, including personal, experiential, and social implication domains. Personal domain shows that how people think about their privacy in the personal domains, including” knowledge,” “identity,” and “ownership,” in the experience of how they interact with the system a“behavior feedbacks” “personalization” “efficiency” and the how they perceive the system and other social implications in the system domain including the “responsibility” “credibility” and “equity.” These insights expanded the understanding of privacy.

RQ 2: Explore “Plausible Futures” intervention: How can design leverage the collective opinions into meaningful and plausible futures?

From the collective privacy concerns identified, we move toward envisioning a plausible future. To build on these collective findings, we will conduct two additional rounds of workshops with designers. Each workshop theme will explore how future possibilities can be shaped based on the collective insights map. This process aims to expand our understanding of privacy concerns and to picture the future more concretely and practically. The outcomes from this phase include 12 plausible alternative ideas for the future.

After collecting these alternatives, we propose to the final alternative future intervention in the plausible future ,an integrated experience to everyday life in a future of sustainable privacy and awareness. We present this through a service blueprint structured in three stages: initiation, awareness with events, and reflection. To make the concept more tangible, we developed an actionable prototype. During the evaluation process, this future-oriented intervention functions as a tool for reflecting on values, risks, and potential use cases Ultimately, these finding help us seeks possibilities to empower people, and provide insights and give us inspiration of how online privacy practices could be strengthened for individuals in the future.

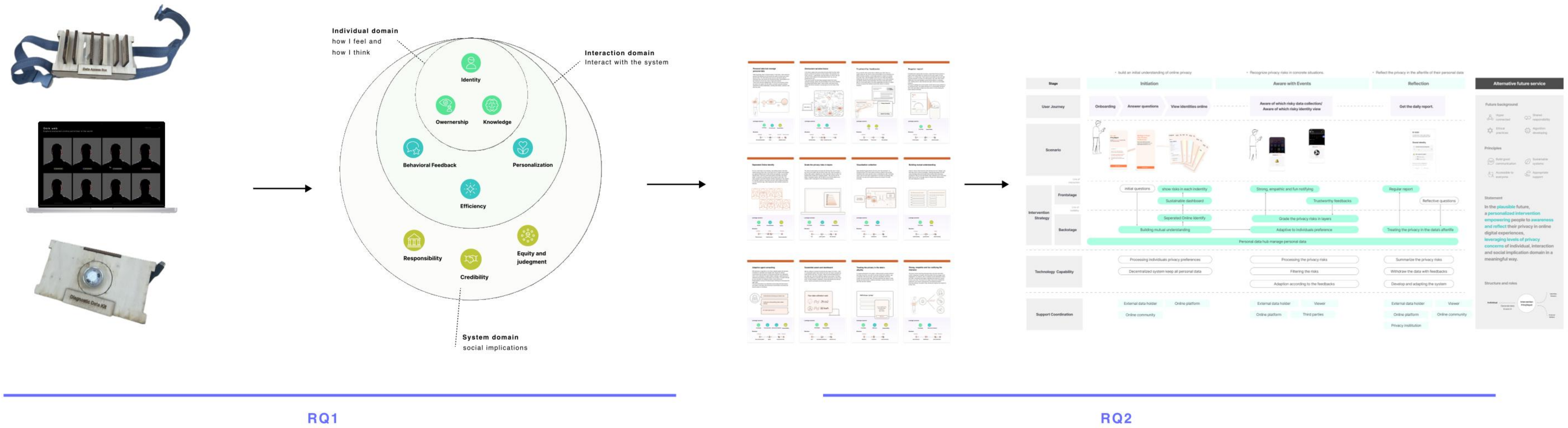

Data Autumn Box
Dark web
Diagnostic Data Kit
Individual domain
how I feel and how I think
Interaction domain
Interact with the system
Identity
Ownership
Knowledge
Behavioral Feedback
Personalization
Efficiency
Responsibility
Credibility
Equity and judgement
System domain
social implications
• build an initial understanding of online privacy
• Recognize privacy risks in concrete situations
• Reflect the privacy in the afterlife of their personal data
Stage
Initiation
Aware with Events
Reflection
User Journey
Onboarding
Answer questions
View identities online
Aware of which risky data collection/ Aware of which risky identity view
Get the daily report.
Scenario
Intervention Strategy
Frontstage
Backstage
initial questions
show risks in each indentity
Sustainable dashboard
Seperated Online identify
Building mutual understanding
Strong, empathic and fun notifying
Trustworthy feedbacks
Grade the privacy risks in layers
Adaptive to individuals preference
Regular report
Reflective questions
Treating the privacy in the data's afterlife
Personal data hub manage personal data
Technology Capability
Processing individuals privacy preferences
Decentralized system keep all personal data
Processing the privacy risks
Filtering the risks
Adaption according to the feedbacks
Summarize the privacy risks
Withdraw the data with feedbacks
Develop and adapting the system
Support Coordination
External data holder
Online platform
Online community
External data holder
Viewer
Online platform
Third parties
External data holder
Viewer
Online platform
Online community
Privacy institution
Alternative future service
Future background
Principles
Statement
In the plausible future, a personalized intervention empowering people to awareness and reflect their privacy in online digital experiences, leveraging levels of privacy concerns of individual, interaction and social implication domain in a meaningful way.
Structure and roles
RQ1
RQ2

Figure 9.1: conclusion of the project

Theory contribution

Using auto-ethnography as a valuable research method to generate insights

This study adopts auto-ethnographic methods to explore privacy as a subjective and situated experience. It generates first-hand insights and preliminary models to serve as the starting point for research and speculation. By combining auto-ethnographic methods with speculative design, the insights are transformed into actionable prototypes and expanded. This integration expands the scope and depth of the investigation into understanding privacy. This demonstrates that, in understanding abstract concepts, the designer can act as a user, already being sensitive and generating more value through design.

Applying privacy taxonomy theory as foundation

Another key application is linked to the theoretical privacy risks of taxonomy(Solve, 2010) towards speculation. While existing taxonomies may have some limitations, they still provide a practical structural framework for exploring future privacy risks and system interventions. The three key phrases can not only make people associate with their online experience, but also prompt them to question the future in a broader context.

From "preposterous future" to “plausible future” exploration

In futures studies and speculative design, alternative futures challenge the dominant narratives. These futures can be utopian, dystopian, or somewhere in between (Dunne & Raby, 2016). Instead of envisioning a plausible future direction, the research took a step back to explore the “preposterous” future. The findings also contribute to our understanding of the current context in which people perceive privacy. Overall, this study combines two dimensions to achieve two goals: raising awareness and envisioning future possibilities. The design process follows a progressive path, where insights from earlier stages inform and shape later design outcomes, allowing for a more grounded and layered exploration.

Practical contribution

3 speculative artifacts workshop
During two rounds of workshops, we got diverse results on privacy concerns. This practice has been proven to be a valuable tool for studying people’s views on privacy and generating ideas for the future.
The workshop can be conducted more times in the future to expand the understanding of privacy further.

Plausible future service envision
Another research outcome is a concrete envisioning of future systems for individuals. This result advances privacy research by speculating on plausible and potentially desirable futures, offering inspiration for more sustainable and ethical privacy practices. This service is designed for individuals, where validation questioning the use case prompts people to provide additional cases for further implication. The service blueprint can serve as a reference for individuals and related stakeholders to reflect on and envision the future.

Personal reflection

Over the past months, this project has been more than just an academic exploration; it has been a journey of self-discovery. This is the first time I have managed such a large future design project. I gradually realized that I had not fully grasped my strengths and limitations before. Through consistent reflection throughout the journey, I have begun to truly see and accept who I am and how I can work as a person.

Keep focused and own the project

One of the biggest challenges I faced was managing the project. The timeline was extended, partly because I struggled to ensure the new findings aligned with the original direction and scope I had defined. Although I started with my goal, I was often drawn to discoveries, which caused me to lose focus and doubt my precious direction. While this openness helped me explore uncertainty and test new ideas, it also led me down unnecessary paths, pulling me away from my core objectives.
I understand that exploration is essential to design, while I need clear boundaries for the scope. One of the most important lessons I learned was the importance of knowing when to move forward and when to pause. Setting priorities and maintaining focus became necessary for both my personal and professional growth.

Step by step

At times, I was too ambitious and too eager to find something new. That pressure caused me to rush in certain stages and overlook consistency in others. This project helped me realize that meaningful progress doesn’t come from bold leaps, but from thoughtful decisions made consistently over time.
I’ve learned to slow down the process, manage my energy more wisely, and embrace moments of uncertainty. Taking time to pause, recover, and reflect has proven far more valuable than simply striving for ambitious results.

Continue to grow several skills

- **Documentation & academic writing:** In the early stages, I often neglected to clearly document my process. I always told myself, “I can refine it later.” However, I realized that without coherent documentation, I lost track of the reasoning behind my decisions and couldn’t trace how my thinking evolved. Now, I make a conscious effort to capture my process, mainly how to document them academically.
- **Keep learning storytelling skills:** Another thing I learned and need to improve is how to do storytelling. As a designer, I need to improve my storytelling skills, particularly in conveying the broader perspective. I still need to improve my ability to present multi-layered findings and write clear reasons for them.

Overall, I value the journey of the entire project, which did not achieve my initial goal of understanding the privacy and criticism of the current online data privacy system, but also catalyzed my future self-development.

Reference

- Ackoff, R. L. (1989). From data to wisdom. Journal of Applied Systems Analysis, 16(1), 3–19.
- Acquisti, A., et al. (2017). Nudges for privacy and security. ACM Computing Surveys, 50(3), 1–41. https://doi.org/10.1145/3054926
- Angel, M. P., & Calo, R. (2024). Distinguishing privacy law: A critique of privacy as social taxonomy. Columbia Law Review, 124(3), 507–540. https://digitalcommons.law.uw.edu/faculty-articles/1070/
- Autoriteit Persoonsgegevens. (2024, April 10). Report data breaches 2023. https://www.autoriteitpersoonsgegevens.nl/en/documents/report-data-breaches-2023
- Banerjee, S. (2025). Sustainable data engineering: Building business success with eco-friendly innovations. In Driving business success through eco-friendly strategies (pp. 375–396). IGI Global.
- Barad, K. (2007). Meeting the universe halfway: Quantum physics and the entanglement of matter and meaning. Duke University Press.
- Barocas, S., & Nissenbaum, H. (2014). Big data's end run around anonymity and consent. In J. Lane, V. Stodden, S. Bender, & H. Nissenbaum (Eds.), Privacy, Big Data, and the Public Good: Frameworks for Engagement (pp. 44–75). Cambridge University Press.
- Bellinger, G., Castro, D., & Mills, A. (2004). Data, information, knowledge, and wisdom. Retrieved from https://homepages.dcc.ufmg.br/~amendes/SistemasInformacaoTP/TextosBasicos/Data-Information-Knowledge.pdf
- Bongard-Blanchy, K., Rossi, A., Rivas, S., & Lenzini, G. (2021). I am definitely manipulated, even when I am aware of it. It's ridiculous! — Dark patterns from the end-user perspective. Proceedings of the Designing Interactive Systems Conference 2021, 1–14. https://doi.org/10.1145/3461778.3462086
- Cadwalladr, C. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
- Caprolu, M., Raponi, S., & Di Pietro, R. (2024, November). Sharing is (s)caring: Security and privacy issues in decentralized physical infrastructure networks (DePIN). In International Conference on Network and System Security (pp. 301–318). Springer Nature Singapore. https://doi.org/10.1007/978-981-96-3531-3_15
- Chang, H. (2008). Autoethnography as method. Routledge. https://doi.org/10.4324/9781315433370
- Chen, M., Ebert, D., Hagen, H., Laramee, R. S., van Liere, R., Ma, K.-L., Ribarsky, W., Scheuermann, G., & Silver, D. (2009). Data, information, and knowledge in visualization. IEEE Computer Graphics and Applications, 29(1), 12–19.https://doi.org/10.1109/MCG.2009.6
- Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 81, 42-51. https://doi-org.tudelft.idm.oclc.org/10.1016/j.chb.2017.12.001
- CMSWire. (2024). Inside the privacy-first approach to the personalized customer experience. https://www.cmswire.com/customer-experience/inside-the-privacy-first-approach-to-the-personalized-customer-experience/
- Correia, J., & Compeau, D. (2017). Information privacy awareness (IPA): A review of the use, definition and measurement of IPA. In Proceedings of the 50th Hawaii International Conference on System Sciences (pp. 4856–4865). https://doi.org/10.24251/HICSS.2017.486
- Cradock, E., Stalla-Bourdillon, S., & Millard, D. (2017). Nobody puts data in a corner? Why a new approach to categorising personal data is required for the obligation to inform. Computer Law & Security Review, 33(2), 142–158.
- Dans, E. (2024, July 31). Apple has come up with a flocking good campaign to raise awareness about online privacy. Medium. https://medium.com/enrique-dans/apple-has-come-up-with-a-flocking-good-campaign-to-raise-awareness-about-online-privacy-cd1a93d4f862
- Desmet, P. M. A. (2017). PrEmo Card Set: Male Version. Delft University of Technology. diopd.org/premo/
- D'ignazio, C., & Klein, L. F. (2023). Data feminism. MIT Press.
- Dunne, A. (2013). Speculative design: Crafting the speculation. Digital Creativity, 24(1), 11–35. https://doi.org/10.1080/14626268.2013.767276
- Dunne, A., & Raby, F. (2013). Speculative everything: Design, fiction, and social dreaming. MIT Press.
- Electronic Privacy Information Center. (2024, December 17). EPIC comments to Dutch DPA on emotion recognition prohibition under EU AI Act. https://epic.org/documents/epic-comments-to-dutch-dpa-on-emotion-recognition-prohibition-under-eu-ai-act/
- Erfani, S., Abedin, B., & Blount, Y. (2015). Social support, social belongingness, and psychological well-being: Evidence for values of online healthcare community membership. Proceedings of the Pacific Asia Conference on Information Systems (PACIS) 2015, 1–13. https://opus.lib.uts.edu.au/bitstream/10453/46320/3/PACIS%2002.pdf
- European Commission. (n.d.). Law-making process. https://commission.europa.eu/law/law-making-process_en
- European Court of Human Rights. (2018). López Ribalda and Others v. Spain. https://hudoc.echr.coe.int/eng?i=002-11799
- Finck, M., & Pallas, F. (2020). They who must not be identified—Distinguishing personal from non-personal data under the GDPR. International Data Privacy Law, 10(1), 11–36. https://doi.org/10.1093/idpl/ipz026
- Floridi, L. (2005). The ontological interpretation of informational privacy. Ethics and Information Technology, 7(4), 185–200. https://doi.org/10.1007/s10676-006-0001-7
- Fowler, J. (2024, January 22). COVID test data breach: 1.3 million patient records exposed online. vpnMentor. https://www.vpnmentor.com/news/report-coronalab-breach/
- GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council. (2018). Official legal text. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- Goffman, E. (1959). The presentation of self in everyday life. Anchor.
- Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: Consumers' awareness and concerns. Journal of Consumer Marketing, 19(4), 302–318. https://doi.org/10.1108/07363760210433627
- Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law, 2(2), 68–92.
- Harris, S. (2019, September 18). Data privacy: Tracking our every move. The New York Times. https://www.nytimes.com/2019/09/18/opinion/data-privacy-tracking.html
- Helbing, D. (2023, March). Privacy, human rights, and Society 5.0. ResearchGate. https://www.researchgate.net/publication/369088659_Privacy_Human_Rights_and_Society_50
- Heijne, K., & Van der Meer, H. (2019). Road map for creative problem-solving techniques: Organizing and facilitating group sessions. Boom uitgevers.

- Hill, K. (2012, February 16). How Target figured out a teen girl was pregnant before her father did. Forbes. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

- Hoffmann, C. P., et al. (2016). Privacy cynicism: A new approach to the privacy paradox. Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 10(4). https://doi.org/10.5817/cp2016-4-7

- Inayatullah, S. (2013). Futures studies: Theories and methods. There's a future: Visions for a better world, 30(20240420203101485854387).

- Iwabuchi, M. (2022, January 23). Speculative design and designed realities: How to design futures in the 2020s. UX Planet. Retrieved March 20, 2025, from https://uxplanet.org/speculative-design-and-designed-realities-ade514cc3426

- Johannessen, L. K., Keitsch, M. M., & Pettersen, I. N. (2019). Speculative and critical design — Features, methods, and practices. Proceedings of the Design Society: International Conference on Engineering Design, 1(1), 1623–1632. https://doi.org/10.1017/dsi.2019.168

- Karwatzki, S., Trenz, M., & Veit, D. (2022). The multidimensional nature of privacy risks: Conceptualisation, measurement and implications for digital services. Information Systems Journal, 32(6), 1126–1157. https://doi.org/10.1111/isj.12386

- Kavaliauskienė, A., & Juknaitė, D. (2021). How to build sustainable online communities: Implications from Lithuania urban communities case study. Sustainability, 13(16), 9192. https://doi.org/10.3390/su13169192

- Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & Security, 64, 122–134.

- Kumar, D. (2024, April 17). An update on Amazon's plans for Just Walk Out and checkout-free technology. Amazon. Retrieved March 28, 2025, from https://www.aboutamazon.com/news/retail/amazon-just-walk-out-dash-cart-grocery-shopping-checkout-stores

- KPN. (2024, July 4). ING and KPN are committed to making consumers digitally resilient. KPN. Retrieved March 28, 2025, from https://www.overons.kpn/nieuws/en/ing-and-kpn-are-committed-to-making-consumers-digitally-resilient/

- Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Zittrain, J. L. (2018). The science of fake news. Science, 359(6380), 1094–1096. https://doi.org/10.1126/science.aao2998

- Lescrauwaet, L., Wagner, H., Yoon, C., & Shukla, S. (2022). Adaptive legal frameworks and economic dynamics in emerging technologies: Navigating the intersection for responsible innovation. Law and Economics, 16(3), 203–219. https://doi.org/10.2139/ssrn.3759886

- Li, Y. (2012). Theories in online information privacy research: A critical review and an integrated framework. Decision Support Systems, 54(1), 471–481.

- Liu, H. (2021). Who Is Surveilliant-a New Survillient Plan. RCA.ac.uk. https://2021.rca.ac.uk/students/hao-liu/

- Lupton, D. (2016). The quantified self. John Wiley & Sons.

- Lupton, D. (2016). Personal data practices in the age of lively data. In J. Daniels, K. Gregory, & T. McMillan Cottom (Eds.), Digital sociologies (pp. 335–350). Policy Press.

- Lupton, D. (2017). Feeling your data: Touch and making sense of personal digital data. New Media & Society, 19(10), 1599–1614. https://doi.org/10.1177/1461444817717515

- Malpass, M. (2017). Critical design in context: History, theory, and practice. Bloomsbury Academic. https://doi.org/10.5040/9781474293822

- Mandel, M. (2017, July). The economic impact of data: Why data is not like oil. Progressive Policy Institute. https://www.progressivepolicy.org/wp-content/uploads/2017/07/PowerofData-Report_2017.pdf

- Manjoo, F. (2019, September 18). The case for data privacy. The New York Times. https://www.nytimes.com/2019/09/18/opinion/data-privacy-tracking.html

- Mavroeidi, A.-G., Kitsiou, A., & Kalloniatis, C. (2019). The interrelation of game elements and privacy requirements for the design of a system: A metamodel. In S. Gritzalis, E. Weippl, S. K. Katsikas, G. Anderst-Kotsis, A. M. Tjoa, & I. Khalil (Eds.), Trust, Privacy and Security in Digital Business (pp. 110–125). Springer. https://doi.org/10.1007/978-3-030-27813-7_8

- McIntyre, L. (2016). Big data privacy: The datafication of personal information. The Information Society, 32(3), 192–199. https://doi.org/10.1080/01972243.2016.1153010

- Meuwese, A. (2020). Regulating algorithmic decision-making one case at a time: A note on the Dutch 'SyRI' judgment. European Review of Digital Administration & Law, 2020. https://research.tilburguniversity.edu/files/43647493/syri_case_note.pdf

- Miller, B. (2021). Is technology value-neutral? Science, Technology, & Human Values, 46(1), 53–80. https://doi.org/10.1177/0162243919900965

- Montgomery, E. (2020). Mapping speculative design. EPM*ID. https://epmid.com/projects/Mapping-Speculative-Design

- Müller, J. (2025). Rights in the digital age. International Institute for Democracy and Electoral Assistance (International IDEA). https://doi.org/10.31752/idea.2025.33

- Nelissen, L., & Funk, M. (2022). Rationalizing dark patterns: Examining the process of designing privacy UX through speculative enactments. International Journal of Design, 16(1), 77–94. https://doi.org/10.57698/v16i1.05

- New Yorker. (2017, December 4). The Gaydar of modern science. Retrieved from https://www.newyorker.com/magazine/2017/12/04/the-gaydar-of-modern-science

- Nissenbaum, H. (2009). Privacy in context: Technology, policy, and the integrity of social life. In Privacy in context. Stanford University Press.

- O'Byrne, I. (2025, March 25). Privacy fatigue: Managing digital burnout in a hyper-connected world. WIOByrne. https://wiobyrne.com/privacy-fatigue/

- Palen, L., & Dourish, P. (2003). Unpacking "privacy" for a networked world. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 129–136. https://doi.org/10.1145/642611.642635

- Phan, B. T., Do, P. H., & Le, D. Q. (2025). The impact of digital literacy on personal information security: Evidence from Vietnam. In D. Nguyen Van et al. (Eds.), *Proceedings of the International Conference on Emerging Challenges: Sustainable Strategies in the Data-Driven Economy (ICECH 2024)* (pp. 475–489). Atlantis Press. https://doi.org/10.2991/978-94-6463-694-9_32

- Pins, D., et al. (2022). Finding, getting and understanding: The user journey for the GDPR's right to access. Behaviour & Information Technology, 1–27. https://doi.org/10.1080/0144929x.2022.2074894

- Pinsent Masons. (2024, November 25). DPC inquiry serves reminder of artificial intelligence GDPR obligations. Pinsent Masons. Retrieved March 24, 2025, from https://www.pinsentmasons.com/out-law/news/dpc-inquiry-ai-gdpr-obligations
- Pitt, L. F., & Lunt, P. (2006). The privacy paradox: Personal information disclosure intentions versus behaviors. Journal of Consumer Affairs, 40(3), 383–406. https://doi.org/10.1111/j.1745-6606.2006.00070.x
- Pötzsch, S. (2009). Privacy awareness: A means to solve the privacy paradox? In The Future of Identity in the Information Society (pp. 226–236). Springer. https://doi.org/10.1007/978-3-642-03315-5_17 Computer Studies, 128*, 86–99.
- Privacy International. (2020). No body's business but mine: How menstruation apps are sharing your data. https://privacyinternational.org/long-read/3196/no-bodys-business-mine-how-menstruations-apps-are-sharing-your-data
- Project SHERPA. (2019, November 25). Candle makes waves at Dutch Design Week and on Reddit. SHERPA Project Blog.
- Pulitzer Center. (2024). How your data ends up in AI training sets. https://pulitzercenter.org/stories/how-your-data-ends-ai-training-sets
- Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299–1323. https://doi.org/10.1007/s11747-022-00845-y
- Rainie, L., & Anderson, J. (2014, December 18). The future of privacy. Pew Research Center. https://www.pewresearch.org/internet/2014/12/18/future-of-privacy/
- Regan, P. M. (2020, July 27). Putting our bodies online: The privacy risks of tech wearables. Centre for International Governance Innovation. https://www.cigionline.org/articles/putting-our-bodies-online-the-privacy-risks-of-tech-wearables/
- Rhydderch, A. (2017, June). Scenario building: The 2x2 matrix technique. The Prospective and Strategic Foresight Toolbox. https://www.researchgate.net/publication/331564544_Scenario_Building_The_2x2_Matrix_Technique
- Rijksoverheid. (2023, October 10). Start campagne tegen online criminaliteit: Laat je niet interneppen — online misleiding kan iedereen overkomen. https://www.rijksoverheid.nl/actueel/nieuws/2023/10/10/start-campagne-tegen-online-criminaliteit-laat-je-niet-interneppen---online-misleiding-kan-iedereen-overkomen
- Rossi, A., & Palmirani, M. (2019). DaPIS: An ontology-based data protection icon set. https://doi.org/10.3233/FAIA190020
- Rossi, A., Chatellier, R., Leucci, S., Ducato, R., & Hary, E. (2022). What if data protection embraced foresight and speculative design? In D. Lockton, S. Lenzi, P. Hekkert, A. Oak, J. Sádaba, & P. Lloyd (Eds.), DRS2022: Bilbao, 25 June – 3 July, Bilbao, Spain. https://doi.org/10.21606/drs.2022.681
- Sanders, E. B.-N., & Stappers, P. J. (2013). Convivial toolbox: Generative research for the front end of design. BIS Publishers. https://doi.org/10.1007/978-90-6369-284-1
- Sarigol, E., Garcia, D., & Schweitzer, F. (2014). Online privacy as a collective phenomenon. Proceedings of the 2014 ACM Conference on Online Social Networks (COSN), 37–46. https://doi.org/10.1145/2660460.2660470
- SC Staff. (2025). EU identity fraud up 88%, report finds. SC Media. https://www.scworld.com/brief/eu-identity-fraud-up-88-report-finds
- Schouwenberg, L., & Kaethler, M. (Eds.). (2021). The auto-ethnographic turn in design. Valiz.
- Sheahan, J., Chatting, D., Collins, R., Bley, J., Eriksson, A., Taylor, N., & Rozendaal, M. C. (2024, October). Designing with friction: inverting notions of seamless technology. In *Adjunct Proceedings of the 2024 Nordic Conference on Human-Computer Interaction* (pp. 1–4).
- Sinha, S. (2022). Data Aeternum [Interactive website]. https://data-aeternum.com/
- Smith, J., & Johnson, A. (2022). Still creepy after all these years: The normalization of affective privacy concerns in app use. In Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems (pp. 1–13). ACM. https://doi.org/10.1145/3491102.3502112
- Solove, D. J. (2008). Understanding privacy. Harvard University Press.
- Solove, D. J. (2023). Data is what data does: Regulating based on harm and risk instead of sensitive data. Nw. UL Rev., 118, 1081.
- Stappers, P. J., & Giaccardi, E. (2017). Research through design. In J. Frascara (Ed.), Design research: Methods and perspectives (pp. 142–163). Bloomsbury Academic.
- Stuart, A., et al. (2019). The psychology of privacy in the digital age. Social and Personality Psychology Compass, 13(11). https://doi.org/10.1111/spc3.12507
- Tang, J., Shoemaker, H., Teffera, L., Birrell, E., & Lerner, A. (2022, November 14). Buying privacy: User perceptions of privacy threats from mobile apps. arXiv. https://arxiv.org/abs/2211.07235
- u/CCPareNazies. (2013, September 14). Privacy action is better than isolation from modern technology. Here's why: [Reddit post]. Reddit. https://www.reddit.com/r/privacy/comments/1hmnjhh/privacy_action_is_better_than_isolation_from/
- Van der Meer, M. (2023). Ik bepaal zelf, dus ik ben: De invloed van leeftijd op de relatie tussen autonomie en identiteit [Master's thesis, Universiteit Leiden]. Leiden University Student Repository. https://studenttheses.universiteitleiden.nl/access/item%3A2660838/view
- Verbeek, P. P. C. C. (2008). Morality in design: Design ethics and the morality of technological artifacts. In P. Kroes, P. E. Vermaas, A. Light, & S. A. Moore (Eds.), Philosophy and design: From engineering to architecture (pp. 91–103). Springer. https://doi.org/10.1007/978-1-4020-6591-0_7
- Vistra Group Holdings S.A. (2023, October 4). Transferring personal data under the EU–US Data Privacy Framework. Vistra. Retrieved March 28, 2025, from https://www.vistra.com/insights/transferring-personal-data-under-eu-us-data-privacy-framework
- Voigt, P., & von dem Bussche, A. (2018). The EU General Data Protection Regulation (GDPR): A practical guide. Springer. https://doi.org/10.1007/978-3-319-57959-7
- Washington Post. (2022, January 13). German police used a tracing app to scout crime witnesses. Some say that's a problem. https://www.washingtonpost.com/world/2022/01/13/german-covid-contact-tracing-app-luca/
- Yanow, D., & Tsoukas, H. (2009). What is reflection-in-action? A phenomenological account. Journal of Management Studies, 46(8), 1339-1364. https://doi.org/10.1111/j.1467-6486.2009.00859.x
- Yu, S. (2016). Big Privacy: Challenges and opportunities of privacy study in the age of big data. IEEE Access, 4, 2751–2760. https://doi.org/10.1109/ACCESS.2016.2577036
- Zhang, B., & Sundar, S. S. (2019). Proactive vs. reactive personalization: Can customization of privacy enhance user experience?. *International Journal of Human-