TALLINN UNIVERSITY OF TECHNOLOGY
SCHOOL OF ENGINEERING
Department of Mechanical and Industrial Engineering

CONTROL AND ETHICS IN DIGITAL IDENTITIES

New opportunities through inclusive personal data management

DIGITAALSETE IDENTITEETIDE KONTROLL JA EETIKA

Uute võimaluste loomine inimesi kaasava andmete haldamise kaudu

MASTER THESIS

Student: Taavi Aher

Student code: 182584MADM

Supervisor: Prof. Martin Pärn

Tallinn, 2020

AUTHOR'S DECLARATION

Hereby I declare, that I have written this thesis independently. No academic degree has been applied for based on this material. All works, major viewpoints and data of the other authors used in this thesis have been referenced.

"....." ..... 201…..

Author: .....
/signature /

Thesis is in accordance with terms and requirements

"....." ..... 201….

Supervisor: …….
/signature/

Accepted for defence

"....."..... 201… .

Chairman of theses defence commission: ……..
/name and signature/

Non-exclusive Licence for Publication and Reproduction of Graduation Thesis[1]

I, Taavi Aher (09.04.1991) hereby

1. grant Tallinn University of Technology (TalTech) a non-exclusive license for my thesis
CONTROL AND ETHICS IN DIGITAL IDENTITIES – New opportunities through inclusive personal data management

supervised by Professor Martin Pärn,

1.1 reproduced for the purposes of preservation and electronic publication, incl. to be entered in the digital collection of TalTech library until expiry of the term of copyright;

1.2 published via the web of TalTech, incl. to be entered in the digital collection of TalTech library until expiry of the term of copyright.

1.3 I am aware that the author also retains the rights specified in clause 1 of this license.

2. I confirm that granting the non-exclusive license does not infringe third persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

[1] Non-exclusive Licence for Publication and Reproduction of Graduation Thesis is not valid during the validity period of restriction on access, except the university`s right to reproduce the thesis only for preservation purposes.

Department of Mechanical and Industrial Engineering

THESIS TASK

Student: Taavi Aher, 182584MADM
Study programme: MADM10/18, Design and Technology Futures
Main speciality: Design
Supervisor: Professor, Martin Pärn, +372 513 8791

Thesis topic:

English CONTROL AND ETHICS IN DIGITAL IDENTITIES
New opportunities through inclusive personal data management

Estonian DIGITAALSETE IDENTITEETIDE KONTROLL JA EETIKA
Uute võimaluste loomine inimesi kaasava andmete haldamise kaudu

Thesis main objectives:

1. Understand the current issues in personal data management
2. Explore opportunities for change in this paradigm
3. Design concept that supports people and organizations in personal data management

Thesis tasks and time schedule:

No	Task description	Deadline
1.	User research	27.02.20
2.	Analysis and problem framing	26.03.20
3.	Design brief and concept development	14.04.20
4.	Concept finalization and validation	05.05.20
5.	Thesis writing finalization	22.05.20

Language: English **Deadline for submission of thesis:** 25.05.2020

Student: Taavi Aher …… "…." …… 2020

Supervisor: Martin Pärn …… "…." …… 2020

Head of study programme: Martin Pärn …… "…." …… 2020

ABSTRACT

Individuals create a wealth of personal data that is collected and processed by different organizations. This data is a powerful resource that, when used unethically, can influence behaviors for purposes not aligned with an individual's best interests. Efforts are being made through legislation and advocacy to enforce personal data rights, but people still lack ways to control their digital identity, as these efforts focus on organizations and exclude individuals. Organizations lack motivation and support to use data ethically, relying on design approaches that force their user into a passive role.

To bring meaningful change to the situation, individuals need to be empowered to act as the owners of their personal data, enabling them to take responsibility and understand its value. At the same time, organizations need to be supported in ethical handling of data, creating the opportunity to shift their mindset. This meaningful change requires both an ethical framework for data exchange and a design approach that elevates passive users into the role of actor.

I propose a design concept that empowers organizations and individuals to act as equals through a framework based on the X-Room architecture, enabling the safe and purposeful processing of personal data. Individuals control their digital identity with the help of a digital assistant within the framework, which analyses the use of their data, enforces their decisions regarding it, and keeps it accurate. For organizations, complying with ethical norms and regulations is simplified, creating opportunities for new business models that leverage the ethical use of high-quality personal data to emerge, providing benefit for both parties.

EESTIKEELNE KOKKUVÕTE

Inimeste digitaalne tegevus jätab suure jälje digitaalsete isikuandmete näol, mida erinevad ettevõtted enda tarbeks koguvad ja töötlevad. Isikuandmetes peitub võim, sest nende töötlemise kaudu on võimalik juhtida inimeste tähelepanu ja läbi selle teenida kasumit. Sellest tulenev tähelepanumajandus on teinud ühiskonnale kahju vähendades inimeste võimet iseseisvalt mõelda. Olukorda on püütud leevendada mitmete määruste kaudu, nagu näiteks GDPR, mis kaitseb isikuandmetega seotud õigusi. Mitmed organisatsioonid tegelevad küll nende õiguste jõustamisega, kuid nende tegevus keskendub eelkõige ettevõtete strateegilistele muutustele. Praeguses olukorras pole inimestel võimalik ise enda omanduses olevaid isikuandmeid hallata, mis loob jõuetuse tunnet. Ettevõtetel puudub samas motivatsioon ja ka võimekus isikuandmeid eetiliselt hallata ning jätkavad pakutavate toodete disainis lähenemisviiside kasutamist, mis suurendavad veelgi mainitud jõuetust kasutajas.

Probleemi uurimisel kasutasin metoodikat, mille eesmärgiks on võimaldada inimestel võtta aktiivse osaleja roll. Läbi intervjuude ja praeguse olukorra kaardistamise selgus, et sisulise muutuse saavutamiseks on oluline võimendada inimestes iseenda isikuandmete omamise tunnet ja luua võimutasakaal inimeste ja ettevõtete vahel. Ainult nii on võimalik inimestel käsitleda oma andmeid kui osa nende digitaalsest identiteedist ja võtta selle eest teadlikult vastutus. Ettevõtted vajavad isikuandmete eetilise haldamise ja töötlemise infrastruktuuri. Magistritöö käigus koostasin kasutajakogemuse disaini meetodite analüüsi. Analüüsi tulemusena koostasin uued põhimõtted, toetamaks kaasava disainlahenduste loomist kasutajakogemuse disainis.

Disainkontseptsiooni Instant eesmärk on võimaldada nii ettevõtetele kui ka inimestele isikuandmete turvaline, eetiline ja sihipärane kasutus läbi X-tee arhitektuurile ehitatud raamistiku. Inimesed saavad kontrollida oma digitaalset identiteeti läbi digitaalse assistendi, mis analüüsib andmete kasutust, jõustab nende otsuseid ja tagab andmete täpsuse. Instant'i raamistik lihtsustab ettevõtete jaoks eetikanormide järgimist ja määrustele vastamist luues samas võimalusi uute eetiliste ärimudelite elluviimiseks.

Kontseptsiooni eesmärk on pakkuda välja üks võimalikest viisidest, milline võiks välja näha üksikisikute andmehaldus, rajanedes juba olemasolevatele andmete privaatsuse tagamiseks loodud tehniliste infrastruktuuri kontseptsioonidele. Isikuandmete haldamisel on palju võimalikke tulevikke. Põhimõtteid, mis olid määratletud Instant kontseptsiooni suunamiseks, saab kasutada alternatiivsete võimestavate kontseptsioonide loomiseks.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AI - Artificial intelligence
DPO - Data Protection Officer
EU - European Union
GDPR - General Data Protection Regulation
SME - Small and medium-sized enterprises
UX - User experience

1 INTRODUCTION

The Internet is a technological framework that has changed the way we relate to information. This framework makes information accessible through devices connected to the network, and since its first launch in the 1980s has grown to become the primary way of sharing and consuming information. There is an overwhelming quantity of information shared within this network and it has enabled people to connect across the globe, as physical distance no longer prohibits communication.

However, there are growing anxieties that the Internet is actively changing the way people think, with the primary criticism being that the same nature of how information is delivered and the sheer quantity of it is sacrificing people's ability to read and think deeply. 58.8% of the world population uses the Internet[1] and the average person spends more and more time on their device, averaging around 145 daily minutes of device usage.[2]

Among these daily minutes, social media use makes up the most significant percentage, with 69% of 18 to 29-year-olds and 38% of those ages 30 to 49 getting their information mainly through this source.[3] These websites feed users with content at breakneck speed, depending on how the website is configured, there could be an update every second, leading to an overabundance of content to consume. This has a significant effect on people's attention spans, as it is split between many sources, making processing information shallow and fragmented.

The Internet is designed to be a free channel for storing and sharing information. With its commercialization and expansion, the upkeep costs of servers necessitated a consistent way to cover the expenses. Of the different business models in use, the most popular source of income is through advertisements. Users get to browse content and, in exchange, are advertised to.

The root of this free model goes back to the 1970s, when the Internet was being developed in the United States. The academia and hacker culture there were focusing on what the future of software was going to be. They believed that software should be

[1] World Internet Users Statistics and 2019 World Population Stats. (n.d.). Retrieved 14 January 2020, from https://www.Internetworldstats.com/stats.htm

[2] Winnick, M. (n.d.). Putting a Finger on Our Phone Obsession. Retrieved 14 January 2020, from https://blog.dscout.com/mobile-touches

[3] Sumida, N., Walker, M., & Mitchell, A. (2019, April 23). 3. The role of social media in news. Pew Research Center's Journalism Project. https://www.journalism.org/2019/04/23/the-role-of-social-media-in-news/

free to use and have its source code accessible as proprietary software slows progress. There is no reason to build the same thing over and over again, instead focus can be put on building upon what already exists.[4]

The same egalitarian ideas were applied to the creation of the Internet – all information should be free, and all data should be free to use. The belief was that there would not be any global control over this data. However, the new system had to be financially viable as the goal was to expand it to commercial use, eventually making it accessible to everyone. The model of free services with advertising was deemed as the best way to make the Internet sustainable.

The issues with this model began to show when the capability of gathering and analyzing data about people started to outpace the capacity for oversight. The question arose – how should the control and privacy of this data be handled? Should it be decentralized, handled by the government or privatized? Due to the political climate at the time, companies, who process personal data, were given the freedom to use it for their benefit. Who owns the data was left ambiguous.[5]

A shift in the balance of powers began. The gradual development of data gathering and storing capability has, over time, changed the advertising model. Digital services can track user behavior, personal information, and statistics, storing this information for later use. Advertisers use this data to target their advertisements more accurately. The aim is to generate as much income as possible, so optimizing this targeting is critical for success. User engagement, or the amount of attention garnered from users, has become the primary metric through which this optimization is measured. Thus, if advertisers are looking to optimize for profit, they focus on gaining and keeping the users' attention.

Attention is one of the most valuable resources in the economy of the free Internet[6]. It is the currency with which users pay for the content they consume. This framework is referred to as the attention economy. In this dynamic, people and their personal data are the product being sold not the customer.

The human capacity for paying attention is limited, influenced by how long they have been awake, stress levels, how tired they are, and if their attention is split between

[4] Lanier, J. (2018). *Ten Arguments for Deleting Your Social Media Accounts Right Now*. Henry Holt and Co.

[5] ibid.

[6] Experience, W. L. in R.-B. U. (n.d.). *The Attention Economy*. Nielsen Norman Group. Retrieved 14 January 2020, from https://www.nngroup.com/articles/attention-economy/

different things. The cycle of gathering data to make advertising more effective and gain more attention from users paradoxically has an adverse effect on the amount of attention users can give.

The effectiveness of advertising through the use of data has a converse effect on the potential for user engagement, making the attention economy unsustainable in the long run.[7] This effectiveness erodes the agency people have to make their own conscious decisions, as they are consistently fed content that lowers their mental capacity and capability to exercise free will. Humans are being manipulated to act in a certain way because targeted content activates the brain's dopamine pathways.[8]

People are becoming technologically dependent, as seen through social media and smartphone addiction, to fulfill human needs such as validation, belonging, growth, and significance, which are vital in producing dopamine. In the brain, dopamine functions as a neurotransmitter and plays the primary role in motivating reward-seeking behavior, inspiring us to take action to meet our needs. The attention-seeking systems influence these pathways by offering an efficient way to release dopamine, creating addictive behaviors.

Societally these new behaviors have been correlated with a rise in depression, isolation, and anxiety, lowering conscious decision-making. The societal effects have political consequences, as illustrated by the Facebook–Cambridge Analytica data scandal. Unbeknownst to the users, their data was leveraged to micro-target them with precisely designed content meant to manipulate voting behavior, affecting the results of the 2016 United States presidential election.[9] Using data to manipulate users is creating rifts in society, as people lack control over their personal data and are vulnerable to being exploited by the companies that know how to gather and utilize it. The power of personal data stems from it being a representation of the person's behavior and identity, thus forming the basis of their digital identity. This new form of identity offers a completely new access to the psyche of the person, as it allows automated profiling. Data moves fast and is gathered in an invisible way, offering people little they can do about the situation. The overwhelming nature of the amount of data being processed about them and the lack of transparency leaves people in a

[7] Odell, J. (2019). *How to Do Nothing: Resisting the Attention Economy*. Melville House.

[8] Lewis, P. (2017, October 6). 'Our minds can be hijacked': The tech insiders who fear a smartphone dystopia. *The Guardian*. https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia

[9] Berghel, H. (2018). Malice Domestic: The Cambridge Analytica Dystopia. *Computer*, *51*(5), 84–89. https://doi.org/10.1109/MC.2018.2381135

disempowered state and vulnerable to manipulation. People have lost control over their digital identities.

Algorithms are used to process this personal data as they are extremely efficient in achieving goals and lack moral inhibitions. If they need to get a user's attention as fast as possible and keep it for as long as possible, they will find the fastest way to do this. The human brain is wired to generate negative emotions more quickly and hold on to them for longer[10]. This is something the algorithms quickly figured out and utilized.

Divisions between people create more engagement as it feeds the feeling of belonging and negative emotions at the same time. People are conditioned to relate to groups. Content that consolidates people's beliefs and worldview keeps them more engaged, giving a consistent source of dopamine. Even if the trigger for it is negative, people seek out more of this content, which teaches algorithms to provide more of it. This is how Internet bubbles are formed and become a part of the person's digital identity.

The analysis done by the algorithm may be based on very superficial, sometimes even incorrect data, meaning that some people's digital identity is forced to fit into a certain group. As people consume the content fed to them, the thoughts and behaviors start to change due to the neuroplasticity of the brain. Their content feed is tailor-made for that person, so they do not see things outside their already accepted perspective. This does not allow understanding the perspective of others, thus lowering the capacity for empathy.

This is exacerbated by the fact that reportedly less than 60% of the users on the Internet are real, so the group that people are made a part of might not be composed of real people. As the attention economy needs clicks, views, and engagement to function, people have developed automated scripts to drive up these metrics. This developed to the point where employees of YouTube feared that YouTube's systems for detecting fraudulent traffic would begin to regard these automated scripts as real and human users as fake.[11]

[10] Montalan, B., Boitout, A., Veujoz, M., Leleu, A., Germain, R., Personnaz, B., Lalonde, R., & Rebaï, M. (2011). Social identity-based motivation modulates attention bias toward negative information: An event-related brain potential study. *Socioaffective Neuroscience & Psychology*, *1*. https://doi.org/10.3402/snp.v1i0.5892

[11] Read, M. (2018, December 26). *How Much of the Internet Is Fake?* Intelligencer. http://nymag.com/intelligencer/2018/12/how-much-of-the-Internet-is-fake.html

There is a belief that the Internet as a medium is what enables these negative phenomena. There is evidence to counter this hypothesis. Through analyzing human development and particularly the development of language and writing, it has been argued that reading and comprehension are not instinctive skills for human beings. Nicholas Carr argues in his book "The Shallows" that as humans learn to translate symbols, their brains are rewired to tie certain symbols to a specific logic in order to speak a language. Human thought is shaped by the tools they use to make sense of their surroundings, such as the alphabet, maps, the printing press, and the clock.[12] The first texts ever written had no spaces between the words, just a stream of letters, as they were written exactly how they were read.

The way we think is malleable as our neuroplasticity allows our brain to change the way it functions continually. The goal of this process is to optimize neural networks to function more efficiently when being exposed consistently to new stimuli or coping with an injury. As such, the Internet as a framework can also be used to incite positive phenomenon and behaviors. With the right approach, it could support people in controlling their digital identity, making them less vulnerable to being manipulated with.

The lack of control over personal data and, through this, digital identities affects all Internet users. Algorithms that gather data about people's behavior categorize them into groups, feeding personalized content to keep them engaged for as long as possible. This has led to increases in social isolation, depression, and a lack of willful decision-making and empathy towards others, as people's identities are fragmented, making them vulnerable to manipulation.

The issue lies in how personal data is used. In Europe, according to the General Data Protection Regulation, people own their personal data, but organizations are the ones who process it as they see fit. Data processing is fundamental to making a profitable digital service, but the personal data is not handled ethically and with respect to its owner. People are distanced from their personal data and do not have power over their digital identity, becoming passive subjects. Even if there is concern about this data, there are few ways to influence the situation. People end up being the product sold, not the customer of a service.

A shift in this dynamic is needed. Establishing a fair and ethical model of data management could open up possibilities for a healthier relationship to exists between

[12] Carr, N. (2011). *The Shallows: What the Internet Is Doing to Our Brains*. W. W. Norton & Company.

people, their personal data, and organizations that provides benefit for all. As the current model is unsustainable because it reduces the capacity for attention while simultaneously requiring more of it to function, alternatives need to be proposed. These alternatives need guidelines for the people creating the digital services and a framework that supports ethical operation that is relatable to both the people and the organizations to have an impact.

2 METHODOLOGY

The issues people face in the digital world are strongly connected to their sense of free will, the ability to make conscious decisions, and opportunities to exercise their rights as they are treated as a passive subject. To enable more agency in people, the design methodology I chose approaches the issues from the perspective of empowering people from a passive role into an active one.

This required a multi-perspective view on how people perceive the issues related to data handling and their rights, as well as the role that organizations and governmental bodies play. Thus, the research was conducted using a combination of different methods. This included studying books related to the issues, reading research papers, and articles on key aspects related to the problem and qualitative interviews with people involved with the topic.

In the design and research process, I relied on the constructive design research model described in the conference paper "The Role of Hypothesis in Constructive Design Research" by Bang, Krogh, Ludvigsen, and Markussen[13] as a structure to guide the different activities. The constant loop of experimentation and evaluation allows for a flexible design process, where new knowledge or insight can quickly influence the direction of the work. The experiments were done using an expansive typology, as the topic itself is complex and requires a broader perspective to understand how the different aspects of the topic influence each other.

2.1 Motivation

2.1.1 Personal, societal and professional motivation

My interest in this topic stems from being a long-time Internet user, who has seen the development of different models of behavioral modification and been affected by them. Unethically designed social media products have influenced my behavior and attitudes towards others, only realizing in hindsight that I was being manipulated with. Working as a digital product designer, the question of how to create ethical products that do not cause adverse effects for their users is of great importance to me. As I design these products to also fill a business need, the issue of creating digital products

[13] Bang, A. L., Krogh, P. G., Ludvigsen, M., & Markussen, T. (2012). *The Role of Hypothesis in Constructive Design Research*.

that are profitable but do not leverage personal data in manipulative ways is a difficult goal to achieve, as from the business perspective anything that increases profit is considered, regardless of ethics. Thus exploring this topic and seeking ways to diversify the perspectives from which digital design is approached is something I would greatly benefit from on both a personal and professional level.

Studying the effects, causes and possible solutions to digital human downgrading through personal data manipulation is something the field of digital product design would benefit from. The current direction of digital design is ever more focused on metrics and measurable results, thus making the process also reliant on gathering and analyzing data, making it harder to empathize with the real human perspective. The business need for experiences optimized to keep users engaged as long as possible has led to the creation of "dark patterns" of UX design. These patterns are designed to influence people's behavior to serve the business goals of the service, regardless of what would benefit the user. These are deliberately designed and tested for efficient manipulation and are a symptom of design that focuses on creating business value first and foremost, instead of being a meaningful and balanced part of users' lives.

In a way, this is also a symptom of the growing ambivalence of digital product designers in a field that is increasingly focusing on metrics. The designers role is becoming more passive, as they rely on preset design patterns to create new products, therefore compounding the problem inherent in the existing model. Digital product design needs to enable the creation of new meanings and ways of interaction, that are intentionally made to benefit people using the products.

The distractions created by digital products are affecting people's physical health as well. For example, 3477 people died due to distractions from handheld devices from traffic-related accidents in 2015 in the US alone. Digital design patterns such as "infinite scrolling", which provides people with never-ending content feeds, keeps people distracted from their surroundings for longer periods. This can lead to an increased danger of accidents happening in traffic, meaning that decisions made for the digital world can have grave implications in the physical world.

The question this situation raises is how many of the methods and patterns used by user experience designers benefit people? The "dark patterns" created by designers are an issue and are becoming more prevalent, but currently, this is seen as something that has independently developed as a result of factors outside of user experience design itself. This separation does not consider the idea that there might

be a deeper issue with the mindset and the way of working within UX design itself and I aim to take a critical look at this.

2.1.2 Ethical motivation

Related to digital product design and user experience design in the field of design ethics that has been slowly growing in popularity. Some designers like Mike Monteiro are putting a lot of emphasis on the responsibility that designers have for the products they create and how they should acknowledge the impact of the products they create and the decisions that shape them[14]. He makes the point that the negative effects that digital products and services can have are not accidental or the result of something breaking, but the direct result of the design work done. Whether the negative effect is intentional or not, the impact comes from the attitude the designer has towards their work and their mindset while carrying it out. The importance of design ethics is not dismissed by designers, but few dedicate meaningful time to working on it because of the complexities involved.

Design ethics is something that is currently an ongoing discussion within user experience design, as there has now been time to see how digital products and the design that carries them impact people's lives in the long term. Tech companies like Google, where user experience design is applied in a widespread way, have been directly noted as having a strong societal impact through how their users interface with their products. Through analyzing how user experience design is related to digital human downgrading, the ethical implications of this relation will also become better understood.

2.2 Design process and methods

As currently there are few ways for people to make a meaningful impact on the digital world they see and there is a lack of control over digital identities because of the way data gathering is done, I formulated the following research question:

How to empower people to have an active role in the shaping of the digital world and their identities within it?

[14] Monteiro, M. (2019). *Ruined by design: How designers destroyed the world, and what we can do to fix it*. Independently published.

2.2.1 Understanding the current day context

The goals were to gain an understanding of the causes of the current disempowerment of people and what motivates businesses and governments to either keep the current system functioning as it does or bring about change. An analysis of the influencing factors had to be conducted. This was done through qualitative semi-structured interviews with people who have experience in different parts of the issue, such as technology law, data ethics avocation, e-governance, fair-data economy, and development of new data-based solutions. The analysis included looking into the activity of different organizations, related to data rights and the legislative efforts of the EU. Also, different case studies, research papers, and articles were analyzed to give a larger global context to the interviews, as the issue is global in scale and effect.

It was important to explore the technological limitations and opportunities as well, as this in large part dictates how people are able to communicate and interact with the systems handling their data.

2.2.2 Understanding the data management experience

In addition to the current day context, I aimed to understand what the practical experience of managing digital personal data is currently like, as this gives an idea of the hurdles that disempower people and the main pain points, which could be addressed through design intervention. For this, I attempted to understand and manage my data through interfacing with various services, tools, and sources. To compound this information, I also interviewed people who are regular Internet users or work in fields related to creating current-day digital experiences.

I also analyzed what kind of solutions are currently offered or have been proposed to help people with managing their data. This was done by attempting to use various tools and reading research papers.

Stemming from my motivation, I analyzed the role user experience design plays in the current situation. User experience design is an integral part of the digital product creation process. It required a critical analysis to be conducted on the impact designers can have on people using their products. This allowed for a better understanding of the ethical implications and motivations behind the business and design decisions.

2.2.3 Analysis through different viewpoints

It was important to understand the topic not just in its original context, but also analyze it through different contexts, as it is complex to the point of becoming convoluted at times. The aim of this was to create new connections between different aspects, to understand how a seemingly unimportant part of one side of the issue can have huge consequences in others and to provide a scenario for the design brief that would have a basis in reality.

Ethics within the context of design and business was one frame I looked at the topic through. As the digital world evolves quickly, the clear definition of ethics is something that often lags behind. The "move fast and break things" mentality that startups have cultivated has contributed a lot to the development of new technologies, but at the same time has reduced the conscious consideration of the possible consequences. Because of the success that this mindset has brought forth, it has heavily influenced governments, businesses, and designers with not very well understood consequences, thus it was important to apply this framing.

Another frame I studied the issues through was the idea of ownership. In the EU, the GDPR has clearly defined that people are the owners of their data, regardless of where it is stored or how it was collected. As the amount of data collected about a single person is too large to be feasibly stored and managed by the person, it has brought on a new concept of what ownership is. A person can own a lot of data about them, but essentially be unable to use it, while a company can store terabytes of data about somebody, use it for their benefit, but not own it. This new dynamic has a lot of implications on how people relate to their data and thus is worth investigating.

The idea of data being a human right was also a frame I used, as it recontextualized a lot of the issues and created new ideas about what the intended behavior and attitude in regard to personal data could be. This was important to understand what sort of change in mindset should be brought forth.

2.2.4 Experimenting and validating

Based on the research I compiled a design brief that covered the key aspects that the solutions should take into account. This included guiding principles for the work, which were more philosophical in nature, but relevant to the project as many issues in the topic stemmed from not enough thought being put into why something should function the way it does.

The design brief changed over time and thus the process of experimentation was heavily also iterative. The process did not rely on a linear way of working, but a combination of prototypes, maps, and concept descriptions was developed over time and aspects of the concept were validated with experts in the field during different iterations.

The work included creating low-fidelity prototypes to test basic concepts, high-fidelity prototypes to illustrate both function and philosophical ideas, system maps to show the different functions, which included system maps that showcased the solutions through different usage scenarios and written descriptions of how the concept works. The goal of this work was to show how the scenario, the framework of the system, and the user side of the solution function together and show the value of the new system.

2.3 Limitations

Because the topic is wide and includes many different aspects, it was important to apply limitations to the project, to ensure that a concept could be finalized. For this, I focused my attention mainly on what could be done in the context of Estonia. Because of the COVID-19 quarantine of spring 2020, I had little face to face contact with people, relying on digital channels to communicate, thus the majority of interviews and all validation happened through these channels.

3. ANALYSIS OF THE CURRENT DAY CONTEXT

Data rights is a fast-evolving field, with legislation to support and options to manage personal data constantly being advanced, while at the same time new, unregulated ways of collecting and utilizing personal data being developed. This is a push and pull situation and much of it happens on a level that is never explained or understood by most people it concerns. Because of this dynamic, it is important to understand what the current situation is regarding personal data rights, what is being done, and by whom.

3.1 New rights mandated by the GDPR

In the European Union, the General Data Protection Regulation (GDPR) was adopted on the 14th of April 2016. This regulation requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory. It applies even if the company using the data is outside the EU if they're processing EU citizen data. The penalty for not complying is a fine which maxes out at €20 million or 4% of global revenue, making breaking these regulations very expensive.[15]

The regulation itself defines some key terminology[16], which is required to understand how it works and what it affects:

- **Personal data**
  Any information that relates to an individual which can be directly or indirectly used to identify them. Examples are names and email addresses, but also include information such as location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions.
- **Data processing**
  Any automated or manual action performed on data. Specific examples are collecting, recording, organizing, structuring, storing, using, and erasing, although any action performed on data applies in general.
- **Data subject**
  The person whose data is processed. This is anybody who visits a website or uses a digital service that performs any sort of data processing on them.

[15] *General Data Protection Regulation (GDPR) – Official Legal Text*. (n.d.). General Data Protection Regulation (GDPR). Retrieved May 9, 2020, from https://gdpr-info.eu/

[16] *What is GDPR, the EU's new data protection law?* (2018, November 7). GDPR.Eu. https://gdpr.eu/what-is-gdpr/

- **Data controller**
  The person who decides why and how personal data will be processed in a company or institution.
- **Data processor**
  A third party that processes personal data on behalf of a data controller. Data processors have special rules that apply to them.

3.1.1 The 7 key principles of the GDPR[17]

Lawful, fair and transparent processing
Personal data should be processed lawfully, fairly, and transparently. All data processing activities must meet the requirements described in the GDPR. Fairness means that a data controller or processor must only use data for the purposes and duration described. Transparency means that the data subject must stay informed regarding the purposes and duration of the data processing.

Purpose limitation
Personal data should be collected for specific, and legitimate purposes and not further processed in a manner outside those purposes. Companies, and institutions have to be specific in this. Personal data can only be collected and used for the stated purposes the data subject has consented to.

Data minimization
Data collection should be adequate, relevant, and limited to what is the necessary minimum in relation to the purpose. The amount of data collected has to be justified.

Accuracy
Personal data should be accurate and kept up to date. Personal data that is inaccurate regarding the purposes for which they are processed, should be erased or corrected as fast as possible.

Storage limitation
Personal data is not stored in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which it is processed. The retention period for personal data has to be specifically set and justified.

[17] *The principles*. (2020, April 30). ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Integrity and confidentiality

Personal data is processed in a manner that ensures its security, including protection against unauthorized or unlawful processing and accidental loss, destruction or damage. It also means implementing an anonymization system to people's identities.

Accountability

The data controller is responsible for complying with the previous principles and has to be able to demonstrate this compliance. This means thorough documentation of all the policies that govern the collection and processing of data. If a company or institution thinks they're GDPR compliant, but do not have the documentation to back it up, then they are not considered compliant.

3.1.2 Important aspects to note

An important aspect described in Article 25 of the GDPR is that everything done in an organization must, "by design and by default," consider data protection.[18] While this article is directed more towards the design of technical solutions, it also has strong implications for how the design process for the user experience should function. It is the task of UX designers to communicate the purpose of personal data processing to the data subject, if unsuccessful, the product is not GDPR compliant. Thus, the GDPR should also drive meaningful change in the design process as well.

In Chapter 3 the data subject's rights are listed as[19]:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

Most of these are covered by the 7 principles, but are written from the data subject's point of view. The right to data portability is a key aspect defined here, which has far reaching implications, but very low awareness. Data portability is defined as the right of a person to receive their personal data in a structured and machine-readable format

[18] *Art. 25 GDPR - Data protection by design and by default*. (2018, November 14). GDPR.Eu. https://gdpr.eu/article-25-data-protection-by-design/

[19] *Chapter 3 (Art. 12-23) Archives*. (n.d.). GDPR.Eu. Retrieved May 9, 2020, from https://gdpr.eu/tag/chapter-3/

and to move that data to another controller without being hindered. This sets two far reaching precedents, one for technical compatibility between databases, where personal data should be stored in an universal way and the other is that people should have an option or interface to actually access and manage all their personal data between all the different databases.

The right of data portability brings to attention the concept of data ownership. On a basic level the GDPR sees personal data being owned by the data subject, this is illustrated by the rights defined for them. But data subjects are not the ones who are storing or processing this data, it is stored by the data controller or data processor, which is usually an organization. This creates a new paradigm for ownership as data subjects have the right to be informed about, access, erase, restrict, object to the use of their personal data, but they are not the storers or processors themselves. Traditionally ownership is defined as possessing an asset or property and having full control over it. The owner of any property also owns the economic benefits of that property. Under GDPR people have the right to decide over their personal data, but they cannot act upon it as their property in a traditional sense.

Data portability is the closest approach to data as property that currently exists. The aim of data portability is seen as enhancing an individual's control over their personal data to make sure that they can play an active role in the data ecosystem. This theoretically enables actions such as selling, trading or exchanging data, which bring it more into the realm of being an individual's property. This is, in a sense, the key to balancing the relationship between organizations and individuals, as it would enable all parties, from data controllers and processors to data subjects to act upon the personal data in the same way.

3.1.3 Impact of the GDPR

The GDPR has led to many organizations overhauling how they manage personal data and created a need for new services that assist with becoming GDPR compliant. The GDPR has affected organizations the most. While it does define the rights of people, since data is used by the data processors and controllers, they are the ones who have to comply with and be accountable for being GDPR compliant. Individuals have no control over the GDPR compliance of the services that wish to process their personal data, rather they have a right to decide if they wish to give access to a data controller or processor. The GDPR focuses on how organizations should act and change in order to guarantee this right to decide for the data subjects.

Fines and penalties

One of the main drivers for GDPR compliance is the danger of being fined. Many organizations have been fined for breaking the GDPR regulations, as of May 2020 the total sum of fines is €467,476,268.[20] The dangers of being fined for not being compliant has led to some organizations stopping providing their service in the EU.

When looking up information about the impact of the GDPR, the information mostly centers around breaches, fines and penalties. The conversations in mainstream media portray it as a set of strict limitations that can have financial consequences for organizations. The positive aspects and opportunities are mostly not covered, making it seem like legislation that is only meant to punish organizations.

Complying with the GDPR

Because of the requirements and strictness of the regulations, fully complying with the GDPR is not an easy task. It means creating new technical and organizational solutions. For example, data portability requires data to be portable without hindrance, while the appropriate security measures are quite obstructive by nature,[21] making the creation of an appropriate technical framework quite difficult. There is no set path or logic to becoming GDPR compliant, the current situation is that most organizations invent their own.

The enablers for complying are considered to be[22]:

- Designing an implementation roadmap
- Performing GDPR analysis
- Identifying risks
- Documenting processing operations
- Applying a robust data management system
- Implementing appropriate privacy security measures
- Carrying training sessions
- Designating a DPO

For most organizations, this means extensive monetary and human resource investments in building technical frameworks, training staff, documentation, changing the organizational mindset, and implementing secure data management systems.

[20] *GDPR Enforcement Tracker—List of GDPR fines*. (n.d.). Retrieved May 10, 2020, from http://www.enforcementtracker.com

[21] Bozdag, E. (2018). *Data Portability Under GDPR: Technical Challenges* (SSRN Scholarly Paper ID 3111866). Social Science Research Network. https://doi.org/10.2139/ssrn.3111866

[22] Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). The critical success factors of GDPR implementation: A systematic literature review. *Digital Policy, Regulation and Governance*, *21*(4), 402–418. https://doi.org/10.1108/DPRG-01-2019-0007

While this is feasible to some degree for big and medium-sized organizations, for small organizations, being in full accordance with the GDPR becomes nearly impossible, because of the restrictions in budget and manpower.

Most organizations with a digital service collect some form of data. An online store, operated by one or two people, can collect large amounts of personal data in the checkout process. Personal communication with people in Estonia, who took the responsibility for compliance said that the regulations were hard to fully understand. What was understood required more than just technical solutions, but a shift in the mindset of the organization. This was difficult to achieve for many, as other employees did not perceive the issue as important. Moreover, shifts in organizational mindset can take years and require constant attention.

During this personal communication the benefits of GDPR were not brought up. The conversation focused on the restrictions and limitations. Currently, it seems that ensuring people's rights regarding their personal data is seen as a hindrance to the daily operations of an organization.

3.2 Initiatives focused on the topic

Other than the GDPR, there are other initiatives to support digital rights. Since the advent of social media along with widespread data processing, many individuals and groups have started advocating for taking steps to tackle personal data rights. While the conversations started from privacy and protecting personal data, now the issues are also subject to human-rights-based analysis, as the problems stemming from unethical misuse of personal data is having societal and political effects.[23]

Since the issue is complex, these organizations have different approaches to tackling it, including lobbying tech companies to be more ethical, supplying people with ways to minimize the negative effects of digital products, creating solutions for processing personal data and developing technical frameworks to support data exchange. I analyzed their activities to get an understanding of what the current ideas and best practices are, and what offerings exist both for organizations and individuals. The goal was to find which ideas and practices empower people, and the areas that are currently lacking in attention.

[23] Harris, T. L., & Wyndham, J. M. (2015). Data Rights and Responsibilities: A Human Rights Perspective on Data Sharing. *Journal of Empirical Research on Human Research Ethics*, *10*(3), 334–337. https://doi.org/10.1177/1556264615591558

3.2.1 The IHAN initiative

The IHAN initiative is funded by the Finnish Innovation Fund. It focuses on developing a fair data economy that is based on trust and creating value for all parties.[24]

The fair data economy

The fair data economy is an initiative for supporting trust-based use of personal data, intending to create more market competitiveness, personalized services, and better public services. It should enable people to be in control of how their data is used and shared, while businesses get access to larger pools of data. This decentralizes control of data processing from large organizations by enabling smaller ones to have access to the same data.[25] Individuals would have the ability to share their personal data through consent and portability enabling a wide circulation of data between individuals and service providers, and between service providers themselves.

Understanding of the issues and focus of work

The people running the IHAN initiative understand that there are currently many obstacles that prevent the fair data economy from existing. Among these are the lack of technical interoperability, quality of data available, difficulties in understanding the benefits of data sharing, risks related to losing control of data and trade secrets, inability to coordinate data ecosystems, inability to define success and show value to others and create a common vision, mission, purpose, and values.

Their approach to the issue is focused on supporting businesses in shifting their mindset. They highlight that people are getting accustomed to different digital business models, such as paid subscriptions, where data enables new value through personalized services. The IHAN initiative posits that the public is increasingly aware of its data footprint and is beginning to take advantage of its data rights. New technologies make it possible for individuals to control and build entirely new data ecosystems at a reasonable cost.

[24] Fair data economy. (n.d.). *Sitra*. Retrieved May 12, 2020, from https://www.sitra.fi/en/topics/fair-data-economy/

[25] Sitra, T. F. I. F. (n.d.). *What is Fair Data Economy?* Retrieved May 12, 2020, from https://data-economy.sitra.fi

The roadmap they provide for establishing the fair data economy consists of[26]:

- Building on the already existing EU legal foundation to make the framework more powerful and effective
- Set an example with the way governments themselves use data
- Build business ecosystems to take better advantage of data
- Develop the infrastructure to break through sectoral silos
- Spread broader public awareness to create consumer demand and drive change

The IHAN initiative does have many articles meant to inform people on how their personal data is used and the opportunities that it presents if used well. The practical aspects of building the fair data economy focuses almost exclusively on businesses.

While they are funding multiple proof-of-concept pilot projects in many fields that apply data analysis, such as medicine and sports, to demonstrate new opportunities on how to use data, these projects are mostly technical[27]. A representative of the foundation said that user experience is only described from a theoretical standpoint[28], making the role and practical opportunities of individuals unknown as of yet.

Most of the work done is technical and includes building capabilities for sharing data. This includes the IHAN Rulebook, the data network forums, IHAN SME companies training program, IHAN Blueprint, the technical pilot projects, and the IHAN Testbed. Other work is focused on changing mindsets, which includes producing materials for decision-makers such as roadmaps, studies, digital profile tests, campaigns, and helping develop business models for companies. This leaves the full image of how the fair data economy operates on all levels unclear at the moment.

3.2.2 MyData

MyData Global is an international non-profit with the purpose of empowering individuals by improving their right to self-determination regarding their personal data.[29] Their declaration outlines their principles, the core of which is that it is of utmost importance that individuals are in a position to have knowledge about and control their personal data, as well as benefiting from it. The principles aim at

[26] Halenius, L., Hofheinz, P., Kalliola, M., Lepczynski, S., Mitta, C., Moise, C., Sinipuro, J., & Suokas, J. (n.d.). *A Roadmap for a Fair Data Economy*. 58.

[27] IHAN – proof of concept pilots. (n.d.). Sitra. Retrieved January 14, 2020, from https://www.sitra.fi/en/projects/ihan-proof-concept-pilots/

[28] Luoma-Kyyny, J. (2020, March 10). [Email interview].

[29] *MyData.org – Make it happen, make it right!* (n.d.). Retrieved May 12, 2020, from https://mydata.org/

restoring balance between organizations and individuals by moving towards a human-centric vision of personal data. This future is founded on trust and confidence, self-determination and maximising the collective benefits of personal data.[30]

MyData approach

MyData seeks to transform the current organization centric system of personal data management to focus on humans, as it should be a resource that the individual can access and control. Individuals should be empowered with rights and practical means, beyond their minimum legal requirements to do so.

To this end, they see it essential that personal data is technically easy to access and use, meaning it complies with the GDPR data portability standards of being accessible in a machine readable format through a safe network. As the current data is kept in closed silos, to create new services and produce value for individuals, society and support economic growth, it has to become a reusable resource.

They posit the need for an infrastructure that enables decentralized management of personal data. This improves interoperability and makes it easier for companies to comply with tightening data protection regulations, while allowing individuals to change service providers without proprietary data lock-ins.[31] While efforts in decentralized data management are being made in individual sectors such as health and finance, cooperation between sectors would yield better results.

MyData operators

Supporting the idea of centralized management of personal data is the concept of MyData operators, described in the paper "Understanding MyData Operators".[32] Operators are actors that provide infrastructure for human-centric personal data management and governance who operate the infrastructure set the limits on what kind of activity is possible or allowed.

One of the central ideas in this model is that data management will be a service provided by many different entities, as such they should be interoperable and technologically compatible.[33] Operators provide individuals an overview of their personal data, allow them to control consent, and inform of past data use. They

[30] *Declaration – MyData.org*. (n.d.). Retrieved May 13, 2020, from https://mydata.org/declaration/

[31] Poikola, A., Kuikkaniemi, K., & Honko, H. (n.d.). *A Nordic Model for human-centered personal data management and processing*. 12.

[32] Langford, J. (n.d.). *Understanding MyData Operators*. 40.

[33] ibid.

connect organizations to an ecosystem of data sources, other services and potential users in an easy and legally compliant way. The benefits for organizations would be access to high-quality data in real-time and tools for complying with legal needs such as audit trails of permissions.

An interesting aspect of this paper is the analysis of the high-level scenarios for data management architecture. In it two scenarios are highlighted:

Fully decentralized infrastructure: Technical infrastructure is standardized and protocols enable data connections without any operators. Individuals manage data flows from the services directly or through personal cloud-based applications.

Competition-based interoperable operator network: A model that functions similarly to how telecom operators, energy providers, or banks work currently. The competing providers are interoperable and together provide global-level connectivity.

Both scenarios posit advantages and disadvantages. A fully decentralized infrastructure provides the most flexibility to create software that does not depend on trusting a third-party and in this scenario individuals or organizations would have the sole ownership over the ability to control their accounts and personal data peer-to-peer cloud storage. While the most control could be maintained, this scenario could overly burden individuals with responsibility as well as making safeguards and regulatory oversight difficult to establish, thus leaving many people vulnerable as well as potentially fragmenting the system.

The competition-based interoperable operator network scenario would enable global connectivity through shared standards and arrangements, with operators making connections with individuals, data sources, and services accessible to a common ecosystem. Operators would provide value to each other through this ecosystem of interoperable operators, lowering costs through collaboration, risk-sharing, and standardization, this in addition to their value propositions to individuals and organizations, while also enabling regulation, oversight, and enforcement of human-centric rules. In the MyData community, there is strong support for this scenario, although the two scenarios could also co-exist.[34]

[34] Langford, J. (n.d.). *Understanding MyData Operators*. 40.

Implications

The vision posited by the MyData organization is one of the most comprehensive and human-centric currently available. Their declaration outlines the principles which support the existence of a human-centric data ecosystem and they have set the clear goal that data should empower individuals, organizations, and society. While they do have research that informs the technical infrastructure that would support this new paradigm, their vision lacks the aspect of how people would interface with this new system, what would change their mindset, what the practical experience would be. As such, the ideas are interesting to the people heavily involved in these topics but remain unrelatable for most people as of yet.

3.2.3 Center For Humane Technology

The Center For Humane Technology, run by former Google design ethicist Tristan Harris, works to establish technology that supports people's shared well-being, sense-making, democracy, and ability to tackle complex global challenges.[35]

Their goal is to bring about a better future through humane technologies designed with human vulnerabilities and capabilities in mind, that protect our minds and replenish society. This requires understanding the most vulnerable human instincts so they can be compassionately designed for, protecting them from abuse. Their work mostly focuses on lobbying tech companies to operate in a more ethical way, prompting them to change the way they apply technology to reach their goals. This includes working with a few product leadership teams to integrate the principles of humane technology into their culture.

They provide a design guide in the form of a worksheet which is intended to help product teams take meaningful steps towards identifying where they could take action to better consider human vulnerabilities.

[35] *Center for Humane Technology: Realigning Technology with Humanity*. (n.d.). Center for Humane Technology. Retrieved 14 January 2020, from https://humanetech.com/

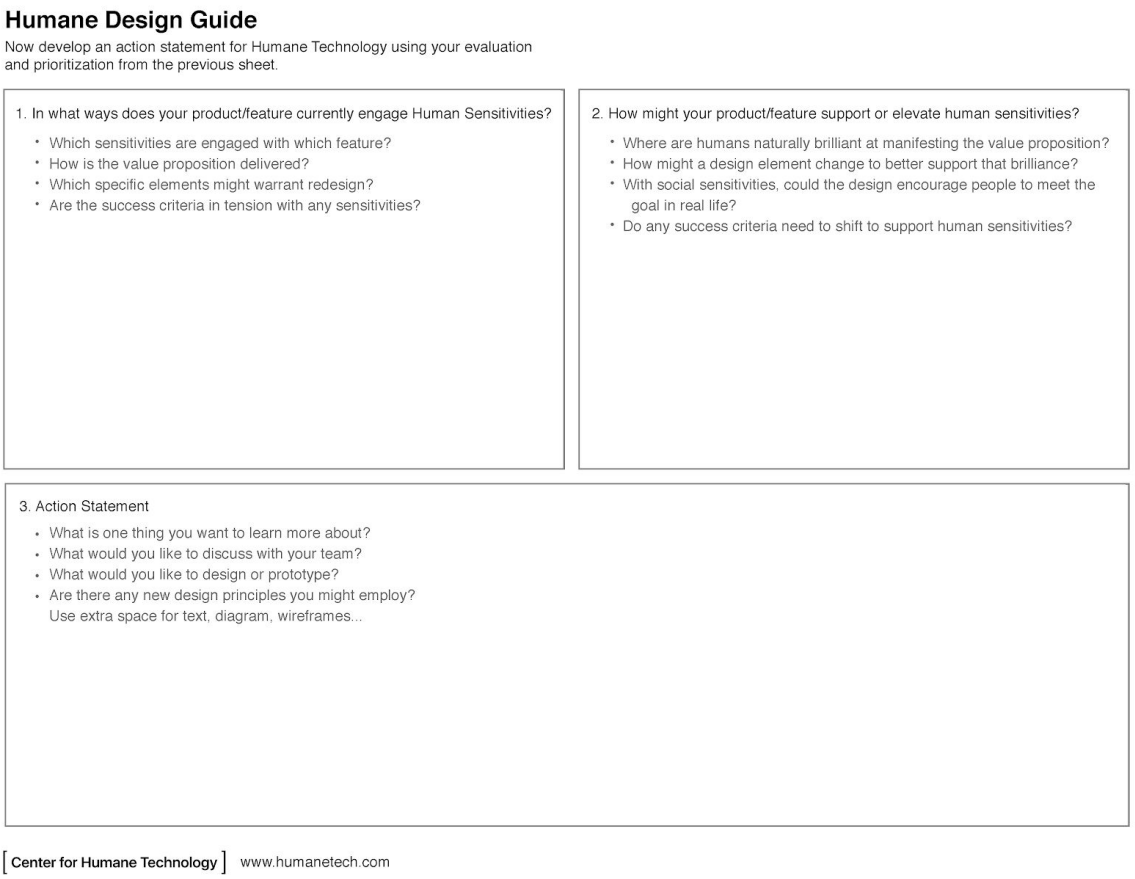


Figure 3.1 Humane Design Guide by the Center For Humane Technology

The worksheet is an assessment of six human sensitivities in the context of the current state of the product and ideation. The usefulness of this tool is questionable, as it is focused on assessing and creating statements, but provides no functional framework for changing the design process

The center works on informing people of the different negative impacts social media and mobile services can have on them through the Ledger of Harms[36]. They guide people in configuring their devices, adopting new behaviors and using supporting applications to avoid digital addiction. They do not offer a solution to people's issues, the offered methods help people avoid the current situation by not taking part in it. This approach further pushes people to be passive, as the expectation is that organizations have to change the way they function before people can have any say.

[36] *Ledger of Harms*. (n.d.). Retrieved May 13, 2020, from https://ledger.humanetech.com/

3.2.4 Calm technology

Calm technology is a philosophical approach to designing the communication and interfaces of products, moving the interaction between technology and its user out of the center of attention. The idea was first published in the article "Designing Calm Technology"[37]. As the abundance of information often works against calming by overwhelming people, it is important to consider how this information can reach us in a non disruptive way.

This idea has become especially important in the current day as the attention economy has made products constantly fight for our attention through notifications, endless streams of content and recommendation algorithms. The question of "what is necessary to show and what is not?" has been replaced with "what keeps the user engaged?". Digital technologies are built on speed, as the amount of information processed in many ways dictates the value of a solution. The digital world is technology-driven and fast-developing, so it is natural that it pushes people towards immediacy and speed.

The principles of calm technology

The book "Calm Technology: Principles and Patterns for Non-Intrusive Design" describes the following principles of calm technology, which can be applied to the product or service creation process.[38]

1. **Technology should require the smallest possible amount of attention.**
   Technology should be able to rely on ambient awareness through different senses. Communication should happen without taking the user out of their environment or task.

2. **Technology should inform and create calm.**
   A person's primary task should not be to compute but to be human. Technology should give them what they need to solve their problem, nothing more, thus serving the person in the way that they require.

3. **Technology should make use of the periphery**
   Technology should easily move from the periphery of our attention to the

[37] Weiser, M., & Brown, J. S. (n.d.). *Designing Calm Technology*. 5.

[38] Case, A. (2016). Calm Technology: Principles and Patterns for Non-Intrusive Design (1 edition). O'Reilly Media.

center and back. The periphery means that the technology maintains contact with the user and informs them, but does so without overburdening. It also relates this to the idea of an on-demand service, as that service reacts to people's needs whenever they express it, changing the dynamic to make the user the one who decides when to engage.

4. **Technology should amplify the best of technology and the best of humanity.**
   Things should not be designed to make machines act as humans or humans act like machines. The design process should consider people first.

5. **Technology can communicate but does not need to speak.**
   It's important to consider if the product relies on voice and if it can use a different communication method, as there are many ways to communicate its status.

6. **Technology should work even when it fails.**
   Failure and fallibility should be considered as parts of a technology or product. In the event of a failure, there should be a designed process. This principle also raises the idea of how people relate to machines and digital products. If people considered digital products to be imperfect and practiced healthy skepticism towards algorithms, it could provide a basis for taking more responsibility themselves and engaging with the digital world with a different mindset.

7. **The right amount of technology is the minimum needed to solve the problem.**
   The feature set of a product should be kept to a necessary minimum, so it only does what it needs to do and not burden people. Solving a problem should not necessitate more technology as the first step.

8. **Technology should respect social norms.**
   The digital products communicating with us are as much a part of society as we are and thus should conform to social norms. It should be thought through which social norms the product might violate or put stress on. Often digital products do not abide by social norms, such as valuing the time of others, by bombarding them with notifications or information the minute it becomes available. All the boundaries for this have to be set by the user as the product does not consider the necessity of these.

An example of calm technology is the tea kettle, which can be ignored most of the time. It only tells us when it is ready, and is off or quiet otherwise, not drawing constant attention to itself.

These principles establish a unique way of thinking about technology and digital products. They would be especially useful when applied to the design process of data-driven services, which by default focus more on how to process and use the data, rather than how to communicate with its users respectfully. The most important points that many products, such as social media platforms, fail to integrate are not having to exist in the center of attention to be effective or useful and conforming to social norms. Social media is useful by itself, as it allows connection with people, communication and sharing, the value proposition is substantial, but having it be the center of attention turns it into a negative factor in people's lives. A digital product should not act in a way that a respectful human would not, otherwise it forces the immediacy of the digital world upon people and disrupts their natural way of being.

3.2.5 Conclusion

Many approaches are being taken to deal with the issues regarding personal data rights and processing, most put organizations and the creators of a product at the center of their attention. Not that they do not take a human-centric approach, all of them have human needs and rights at the core of their philosophy and goals, but the change they are working on bringing about is top down. The human-centric approach has also been criticised for not bringing about radical innovation, but rather enabling incremental innovation, as it focuses on creating solutions considering the current framework in place and the attitudes people hold. There is no meaningful shift in people's lives or attitudes as the process restricts potential solutions to focus on things people already know about, thus it is not reasonable to expect people to start caring about their personal data when using this approach.[39]

Expecting organizations that create technologies and digital products to bring about radical change by slowly refocusing their design process will result in more incremental innovation, while the issue at hand does require a drastic shift in mindset and meanings.

[39] Norman, D., & Verganti, R. (2014). Incremental and Radical Innovation: Design Research vs. Technology and Meaning Change. *Design Issues*, *30*, 78–96. https://doi.org/10.1162/DESI_a_00250

For people, the most common offering is alleviation methods, which entail taking control through removing oneself from the situation or setting boundaries. This control is essentially based on opting out but does not allow people to exert any pressure or control on the situation meaningfully. These methods empower people to survive the wait for organizations to change things for the better and lack a way for them to be proactive.

Another issue is that, while there is a lot of material that touches on the personal data rights of the average Internet user, the content and values described remain tech-focused and abstract, remaining unrelatable to most people. Ideas such as being in full control of one's digital identity and personal data seem great on an abstract level, but for people to connect with it, the actual experience of doing so should be conveyed. As personal data and its value is abstract in itself already, philosophical principles and theoretical frameworks do not make the actual value and benefit of it clearer. A different approach to empowerment is needed.

There are many ideas to apply from the work of organizations discussed. The principles of calm technology serve to bring a different perspective into the design process, which can inform the way digital products communicate with people and change the current dynamic to favor human capability and social norms. The infrastructure ideas posited by the MyData organization are essential to establishing a scenario for which to design. Without a proper infrastructure, the way people share and control their data can only remain on an abstract level, prohibiting the creation of any practical concept. It is also important to understand the value this infrastructure and design process would give to organizations, as it is immense and opens up many new opportunities for ethical business models to emerge while leveraging high-quality data. To exit the current advertising based model, an alternative is needed to replace it. Building a new system considering these values has the potential to provide a sustainable alternative to a model that is destroying itself through its own efficiency. This has to be considered when designing a concept.

3.3 The value of personal data

The transformational potential of data and analytics is extensive, as it is tied to many of the current megatrends such as digitalization, the prevalence of AI, tribalization through societal bubbles, technology becoming embedded in everything, etc. This has triggered a process of digital platforms beginning to dominate key industries, because

of the need for information goods.[40] The competitive advantage offered by big data is alluring as it gives insight that is not obtainable through human analysis, helping optimize operations and business focus in a semi-automated way. Data is also the key element for developing new services and products as it helps ensure the success of said service or product.

Data has definite value for the organizations processing it, as it allows for new value propositions and undermining the competition. This digital transformation is still in its infancy in many ways, as companies focus on gathering all data possible, intending to do something with it in the future. In theory, the value of data rises exponentially with quantity, so storing unused data is not an issue as of yet. In this, the ambiguous nature of the value of personal data is exploited. For the average Internet user, it is hard to understand the value they give to companies in agreeing to have data collected about them, thus nothing prompts them to consider the situation.

The value of having huge quantities of data is illustrated by the increasing power and success of data brokers – businesses that aggregate information from a variety of sources, process or analyze it and license it to other organizations for use.[41] These are businesses that even companies like Facebook, who are currently in no danger of losing market share, buy data from as it helps consolidate their market position.

While traditionally personal data has leveraged for profit through personalized advertisements, this model has taken a hit in recent years with people using bypassing techniques such as ad-blocking software and preferring to pay to not see them entirely. The adoption of the GDPR has also influenced the situation, as websites now have to all ask for consent to process personal data. This new situation has led to the rise of the subscription-based business model and while this has proven successful, the need for more alternative models is becoming greater.

This rapid transition to the data based economy has made organizations value gathering data, but at the same time created new problems as the way the value of data is defined currently is through quantity. There are many aspects of the value of data that need to be explored to understand how to bring this value forward as well while maintaining the human-centric approach.

---

[40] Nuccio, M., & Guerzoni, M. (2019). Big data: Hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change*, *23*(3), 312–328. https://doi.org/10.1177/1024529418816525

[41] *Data Broker*. (n.d.). Gartner. Retrieved May 14, 2020, from https://www.gartner.com/en/information-technology/glossary/data-broker

3.3.1 The quality of data

The capability of gathering data has grown immensely and is being utilized by many organizations, but systems and frameworks to ensure the quality of the data are not as widely applied. The value of data is strongly tied to its quality, as inaccurate data leads to low quality analysis, which in turn can inform wrong decisions. At best, low quality data is inconsequential, but still has to be stored, consuming energy resources.

Machine learning algorithms, which decide what is shown on most dynamic, personalized content feeds such as Facebook or Youtube, requires large volumes of accurate data. The better the data, the better and faster the results. Low quality data on the other hand creates experiences which can distance and distress users.

There are a few key parameters to measure the quality of data by[42]:

1. **Accuracy**
   How correctly the data describes the "real-world" conditions it aims to describe. Inaccuracies have a direct effect on the conclusions derived from data.
2. **Completeness**
   The lack of gaps in the data based on what was supposed to be collected. If a user only partly fills out a survey then the data gathered is incomplete.
3. **Uniqueness**
   The duplication of data items within a data set or compared to another data set. Nothing should be recorded more than once, otherwise the risk of outdated information being stored increases. A database could have two entries for the same person, with one their middle name, but only one has the most up-to-date information.
4. **Validity**
   How the data is collected, not the content of it. Data is valid if it is in the right format and of the right type. Importing time data in the AM/PM format into a database that uses the 24h format will make the former invalid.
5. **Timeliness**
   The degree to which the data represents reality from the set point in time. Data should be recorded as soon after the real-world event as possible, as it becomes less accurate over time.
6. **Consistency**
   Data items lack differences across different databases, in both content and

[42] Askham, N., Cook, D., Doyle, M., Fereday, H., Gibson, M., Landbeck, U., Lee, R., Maynard, C., Palmer, G., & Schwarzenbach, J. (2013). *The Six Primary Dimensions for Data Quality Assessment*. 17.

format. If consistency is not established, different parties aiming to use the same data will have varying ideas of what is true.

The quality of data in different organizations often does not match up with these parameters. A study that analyzed the results of 75 data quality assessments collected over 2 years from a wide range of organizations revealed that on average, 47% of recently created data records have at least one critical error.[43] The total amount of data stored globally was estimated to be 33 zettabytes or 33 trillion gigabytes in 2018 and this is estimated to reach 175 zettabytes in 2025.[44] Not all of this is personal data, but it does illustrate a wider issue with data processing that affects it.

Maintaining quality in line with all of these parameters is not an easy task for organizations. It is influenced by factors like information coming from multiple sources and systems, data being in diverse formats, and inconsistencies in the data provided, which are all tied to the lack of supporting infrastructure for data portability. The approach that many companies take, with preferring quantity over quality also exacerbates the issue, because if the organization is lacking proper and effective data management systems, then the amount of bad quality data will become too much to handle over time.

But it is necessary to have structures in place to assure data quality, at least in Europe, because it is mandated by the GDPR that personal data should be processed purposefully and should be as accurate as possible. This means all low-quality data has to be removed, which is a very expensive process if the data is poorly managed and it is harder to demonstrate compliance if the data is disorganized or poorly maintained.

The issue of data quality directly affects the owners of the personal data as well. The article "The Data Brokers So Powerful Even Facebook Bought Their Data - But They Got Me Wildly Wrong"[45] by Kalev Leetaru details how he was profiled as being 65 years old when he was in his mid 30's, which led him to request his personal data from a large data broker. He found that 78% of the data held about him bore no resemblance

[43] Nagle, T., Redman, T., & Sammon, D. (2020). Assessing data quality: A managerial call to action. *Business Horizons*, *63*(3), 325–337. https://doi.org/10.1016/j.bushor.2020.01.006

[44] Reinsel, D., Gantz, J., & Rydning, J. (2018). *The Digitization of the World from Edge to Core*. 28.

[45] Leetaru, K. (n.d.). *The Data Brokers So Powerful Even Facebook Bought Their Data—But They Got Me Wildly Wrong*. Forbes. Retrieved May 16, 2020, from https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/

to his real identity. These data brokers amass data without directly interacting with the people, keeping their operations a secret. Oracle, an organization that owns and works with more than 80 data brokers, has claimed to have data on more than 300 million people, with 30,000 data attributes per individual.[46] The total amount of people whose data these companies hold is unknown, but different analyses set under question the validity of the quality of their data.

This erosion of data quality affects the digital identities of the people who it belongs to, thus not just affecting not organizations and their business goals. There is an opportunity here to offer an alternative model to the current mass gathering and analysis. This new model could be based on the ideas outlined in the GDPR, motivating businesses to be ethical and operate with consent by enabling them to purposefully gather high-quality data, which saves them a lot of time and effort by ensuring that high-quality analysis can be conducted. Having an infrastructure that supports them in their processing activities is paramount, but this is a place where people could also be empowered to be involved with their own digital identities. Having the means to control and keep their personal data accurate would not only benefit organizations with high-quality data but also enable people to exercise their data rights.

3.3.2 The role of unused data

Another issue stemming from the quantity over quality approach is data that is gathered but not utilized for analysis. This data is called "dark data" and is divided into two subcategories: data that has been captured but there is a lack of knowledge on how to use it and data which existence is not even known with complete certainty.[47] It is reported that between 60-73% of data gathered by an organization goes unused and becomes dark data.[48] Data has to be utilized for it to create value, otherwise it just takes up storage space, which requires energy for upkeep, having an effect on the environment as well. It also produces security risks as if a database that holds the dark data is hacked and it, unbeknownst to the data processor, contains sensitive personal data, this can have severe implications on people's lives.

[46] Murgia, M., & Ram, A. (2019, January 8). *Data brokers: Regulators try to rein in the 'privacy deathstars.'* https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521

[47] Hasan, A. (2018). Dark Data for Analytics. In M. Ahmed & A.-S. K. Pathan (Eds.), *Data Analytics* (1st ed., pp. 275–293). CRC Press. https://doi.org/10.1201/9780429446177-11

[48] Hadoop Is Data's Darling For A Reason. (2016, January 22). *Forrester*. https://go.forrester.com/blogs/hadoop-is-datas-darling-for-a-reason/

Currently, similar to the data quality problem, organizations have no reason to shift their mindset from monopolizing data by gathering and holding on to it as many of them operate on legacy systems, which do not support the modern requirements for data management and they also lack the infrastructure for proper data management.

The dark data of one organization could benefit another in their work, especially if it is of high quality as it can be used to add new value to a product. Thus, as outlined before, an infrastructure that enables the ethical processing of data is needed, but it is important to also consider data sharing and querying between organizations. The existence of this dynamic within a safe infrastructure provides many opportunities for new business models and services.

3.3.3 Value through selling personal data

Many people have proposed the idea of data subjects being able to sell personal data to data processors. For some, it is seen as the logical step in giving people control of their personal data as currently, organizations are the ones who benefit and profit from it. A new type of startup called "data exchanges" promises to build platforms where people can collect, store, and sell their personal data, including everything from Instagram posts to bank statements. There are multiple models created for selling data. One, proposed by a company called UBDI[49] (Universal Basic Data Income), is based on analyzing the user's data in house and only selling the insights gained from it. Another company Streamr[50] wants to sell user data in real-time by adding all recorded data into aggregated data sets, which it offers to organizations for a subscription fee.

More startups are working on these solutions, but a commonality between them is that they do not pay users directly in the currency of their choice. Instead, they offer rewards if the forms of points or proprietary cryptocurrency. Essentially this means that the value gained for the user is locked within a specific system, and the use of this currency is limited. This means these new solutions do not disrupt the existing systems, but work as an added layer on top of them.

To get a better understanding of this situation, I consulted with a lawyer specializing in IT and technology[51], which introduced a more ethically complicated outlook. The right

[49] *UBDI - Universal Basic Data Income*. (n.d.). Retrieved May 19, 2020, from https://www.ubdi.com/

[50] *Streamr*. (n.d.). Retrieved May 19, 2020, from https://streamr.network/

[51] Kala, K. (2020, March 20). [Digital personal interview].

to privacy is a human right, meaning data protection laws are an extension of that right as they pertain to digital privacy. This essentially means that the rights defined by the GDPR are also strongly connected to our fundamental human rights. The European Union is against bargaining or conducting any trade with human rights as it undermines the sanctity of these and can lead to these being compromised. This also includes data. Data is not just a person's property, it is a piece of who they are, and thus it is not ethical to be able to sell away pieces of it.

Conducting further analysis on monetizing personal data led me to conclude that a system that assigns a monetary value on data is not only legally complicated but also ethically complicated as this value is influenceable. In a free data market, the goal would still be to buy low and sell high, getting the most for the least, so organizations would be inclined to find ways to lower the price of data. In a system reliant on direct monetary value, respectful and ethical use of data that conforms to privacy standards would be hard to establish.

People with a higher standard of living would fare better in this system, as they are not reliant on the profits from the personal data to survive. On the other hand, people of lower-income are very easily influenced in this regard, as they are in a more vulnerable position. This could be exploited by organizations to make these people agree to unfavorable terms and conditions because they have fewer options.

The value of data is also directly correlated with its quantity and quality. A single piece of high-quality data is not valuable on its own. The value comes from processing and analyzing vast quantities of it, as that is how insight can be generated. Thus it can be argued that putting a monetary value on single pieces of personal data would not empower people to sell it as the sums would be meager and would also make it hard to measure and transparently communicate where this value is coming from, as the privacy of others can not be compromised. A monetary exchange also does not promote using data for societally beneficial projects such as optimizing bus routes or public services.

Sharing personal data should give value to its owner, but based on the analysis, the more sustainable way to do this would be a system focused on subjective value. People share their data and get to use a service or have more features on a particular service. Access to high-quality insight from their personal data or behavior could be given to them, or they could willingly contribute to something that has value for

society. This way, the ethical and respectful use of data is easier to maintain, as subjective value is more open to personal interpretation than direct monetary value.

3.4 The Estonian government

Estonia is known for being a digital and connected country, as most of the public services are available online, many of which have been automated. According to the 2018 E-Government Development Index created by the United Nations, Estonia is not the highest-ranking country in terms of e-government solutions. However, the Estonian government is very willing to explore innovative ideas even if they do not fully succeed. In an interview with Marten Kaevats[52], a national digital advisor for The Government Office of Estonia, and Ott Velsberg[53], the Government Chief Data Officer of Estonia, many of these developments were discussed.

Estonia already has many aspects that support the fair and safe sharing and processing of data, such as a single state-issued digital identity, the main form of identification in Estonia. The X-Road framework enables interoperability between different organizations and information systems, allowing various public and private sector e-service information systems to connect. The security of this system is supported by a scalable blockchain technology that protects from intrusions and ensures data integrity. Besides this, many developments are moving the country further towards ethical and safe personnel data management.

3.4.1 The role of X-Road

The state collects and stores the personal data of Estonian citizens in a decentralized way. It is kept in different data banks managed by specific state organizations, not a single server. For example, healthcare data is kept in its data bank and is accessible by institutions that have been given authorization. Distributing data over a network guarantees that the whole system cannot be compromised all at once. It also means that the data is more easily managed, as it is already sorted into databases assuring higher quality data.

Different state organizations can access each other's databases through the X-road framework, enabling interoperability between them, enabling data portability,

[52] Kaevats, M. (2020, March 10). [Personal interview].

[53] Velsberg, O. (2020, April 6). [Digital personal interview].

something which is a key aspect of the GDPR. All data is digitally signed and encrypted, thus ensuring its safety.

Ott Velsberg shared that this infrastructure is not just usable by state systems but private organizations can also connect as well by meeting certain requirements[54]. Organizations have to be compliant with specific security rules and regulations and prepare their own systems for connection, after which they already meet specific high standards for data processing. If they wish to use state data, they have to request specific data and state the purpose of using it. This sets a good precedent for the best practices of processing data, with the core ideas of the GDPR being applied at a fundamental level.

3.4.2 National consent service

The government is, as of 2020, developing and preparing to launch a consent service meant to allow data subjects to give consent to a third party to use their personal data.[55] This service enables:

- Citizens to give and revoke consent to government services.
- Citizens to review services that have consent to use their data.
- Enable the automated checking of consent when sharing data with a data processor.

The ideological goals of this solution match with the GDPR and data rights organizations in giving people more control over their personal data. The focus, however, is narrow in scope, as it mainly aims to enable organizations to get access to data held by the government. The technical framework for this solution is being developed along with a user interface through which citizens can manage their consent settings. A prototype exists of this solution, but the user experience is not ideal. The solution itself is still very technical and functionally looks like it is meant to manage bureaucracy, not empower people in regard to their personal data.

However, the existence of this framework can be utilized in the creation of a more comprehensive concept, which puts empowering people at the core of not just its ideology, but the practical user experience as well.

[54] Velsberg, O. (2020, April 6). [Digital personal interview].

[55] Kaevats, M. (2020, March 10). [Personal interview].

3.4.3 Bürokratt initiative

An exciting ongoing development is the Bürokratt initiative, which is a vision of how public services could digitally work by utilizing artificial intelligence. The idea is to create an AI-based virtual assistant, which could be interacted with through a voice-based interface. It would be an interoperable network of public and private sector AI applications, which, from the user's perspective, would work as a single channel for accessing public direct and informational services. The solution would be based on the same decentralized architecture that Estonia's other digital services operate on, as this allows for the safe transfer of information and reduces the risk of system downtime.[56]

The vision paper of the initiative states that people want public services to work in a way that they would not have to make an effort to use the services – they want to get things done as efficiently as possible via simple user interfaces. Everything should be automated as possible, but within reason, without the user having to know where to turn or remember deadlines. The state should be proactive in offering its services and help, and a voice-based interface is the most intuitive way of delivering on this goal. Everyone would have their own personal assistant.

This initiative is an important step, as AI applications are already in use by the government with plans to develop more, but the interoperability of these systems has to be guaranteed. Otherwise silos between government agencies and systems may be created or extended, making the experience for people using the system a burden.

The initiative does set up technical requirements, which are currently being worked to fulfill. The first is a microservice-based set-up of information systems, and the second is a data exchange based on a messaging room set-up, which is meant to complement the X-Road, essentially turning it into X-Room. The X-Road's synchronous connections may not sufficiently support many AI applications working in parallel so that these technical solutions would enable greater scalability of the system. This would also greatly benefit large scale data management infrastructure.

3.4.4 Opportunities from the Estonian example

The X-Road and future X-Room extension of it, along with the consent service capabilities and digital assistant framework, gives Estonia the necessary systems to

[56] Ideepaber. (n.d.). Krattide veebileht. Retrieved May 19, 2020, from https://www.kratid.ee/ideepaber

create an ethical, safe, and fair data management infrastructure. This infrastructure could support data management on a vast scale. The support for many simultaneous AI applications creates the opportunity to perform real-time analysis on ethical data processing activities, compliance with the GDPR, and translating complex data activities into something that could be understood by the average person. There is potential to create an empowering, inclusive, and accessible system that, at its core, works to enable people to take more control and responsibility for their personal data. At the same time, services could use this data with the person's consent to create new value — a controlled environment for sharing and managing large volumes of high-quality data in an ethical way.

4 THE HUMAN EXPERIENCE OF MANAGING PERSONAL DATA

4.1 The concept of ownership of personal data

The GDPR defines people as the owners of their personal data. It is their property to use and manage as they wish. In concept, this is very valid, but practically the GDPR has introduced a whole new idea of ownership. Personal data is something that, on its own, has very little use for the average person. Most people do not have any capability to analyze and create insights from it, profit from it, or utilize it in any way. Personal data is personal property whose value is defined by how it is used and who uses it. It has no inherent value for its owner. It is also inaccessible, existing as a line of incomprehensible code in a database, which provides little immediate value even if accessed.

Personal data does not fit into the traditional idea of ownership, and thus people have a hard time relating to it. Getting to choose who uses some abstract piece of information about a person or gathers a log of where they click on a website does not create the feeling of ownership. People can be told that databases with thousands of data items about them are used to profile and influence them, but this only creates ambivalence. On the one hand, there is anxiety and repulsion because people are being influenced, as the real-world impact of manipulation through data can be felt. On the other hand, the machinations creating this impact and how a person's data plays into it is too complex to comprehend.

Even the GDPR states that the responsibility for ensuring people's right to their own personal data is on the data controller. The situation is paradoxical as the organizations that do not own the data but have gained consent to use it are the ones who ensure the rights of the people who are the owners. Thus, it is too much to assume people take responsibility and care for this data, when the impact it has on their lives is entirely abstract and from which they are distanced by the very systems and regulations meant to empower them. In discussing these topics with Tanel Mällo, lead for digital literacy at University of Tartu, he emphasized that a balance of responsibility has to be achieved to empower people in this regard, people cannot be expected to know everything.[57] The concept of having a single digital identity cannot exist if it lacks a connection with personal data and ownership of it for most people.

[57] Mällo, T. (2020, March 20). [Digital personal interview].

However, digital services are trying to give people ways to exercise these new rights and return control to the rightful owners, whether it is just to comply with the GDPR, to create a new business model or to provide benefit to society.

4.2 The user experience of the GDPR

The implementation of the GDPR did have a practical effect on people's experience on the Internet. The requirements of the GDPR have created new best practices in terms of UX design, with the main differences being the consent prompts on websites, that are necessary to comply with the requirements. All users must give informed consent to the service requesting their data. The purpose of this processing has to be clearly understood, the personal data kept safe, and consent revocable at any time.

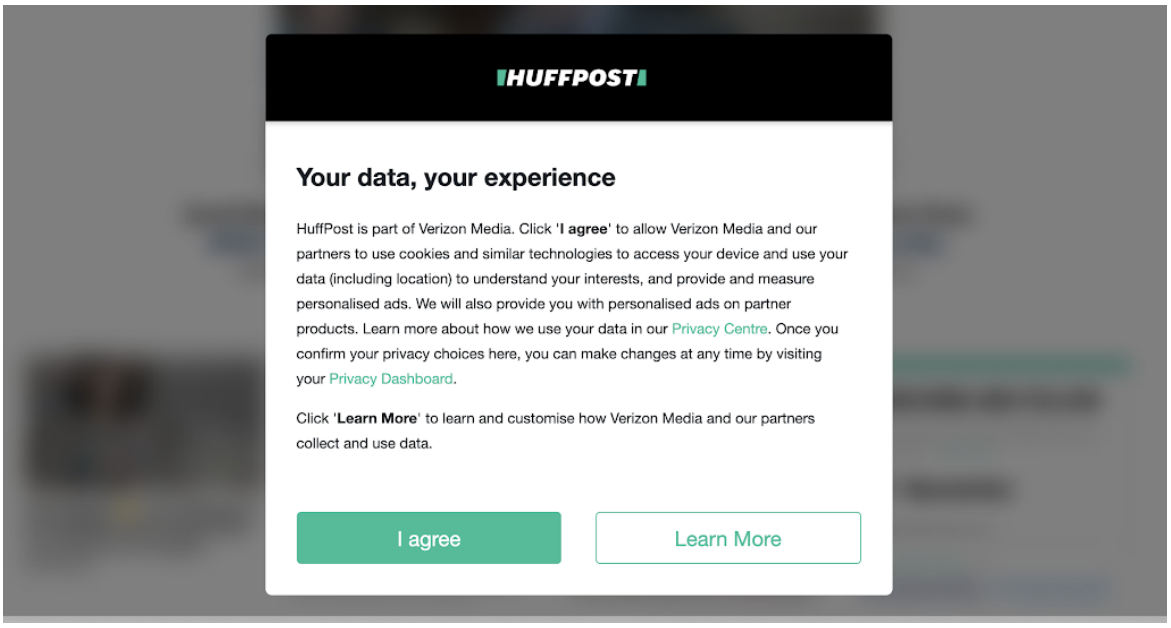


Figure 4.1 Example of GDPR consent prompt. Retrieved from http://www.huffpost.com

These principles sound empowering, but the reality of this experience is a binary choice of accepting or rejecting. These consent prompts are different on most websites, as there is no unified logic to them, thus it all feels disconnected from each other. Most users accept without reading, as it currently is an extra step to get to the content that the user wishes to see. There is no clear indication of what changes compared to saying yes or no. These prompts require the user to be already actively interested in how their data, but the language to describe the purpose and why it is collected is presented in technical lingo. In a way, the GDPR requirements are responsible for this situation, as they require these prompts to be very comprehensive and transparent and, at the same time, inform people clearly and concisely.

The way these requirements are implemented rely on existing user experience design logic. There is no fundamental shift in the presentation logic because the goal is to comply with new standards without disrupting the current experience. If users were to start going through the consent forms of all websites, the time to actually reach the content would be drastically increased based on the current implementation.

The fact that these prompts are perceived as an obstacle means that UX designers focus on making the experience as convenient and fast as possible. Users are nudged towards giving consent as it is the simplest way to continue, enabling them to be passive subjects, who do not know what they have agreed to. This works against the goals of the GDPR. Another issue is that it enables exploitation through dark pattern design. By making blind consent the most straightforward option, organizations can hide their intentions, so users never find out exactly what their data is going to be used for and by whom. This is done to support an already unethical business model.

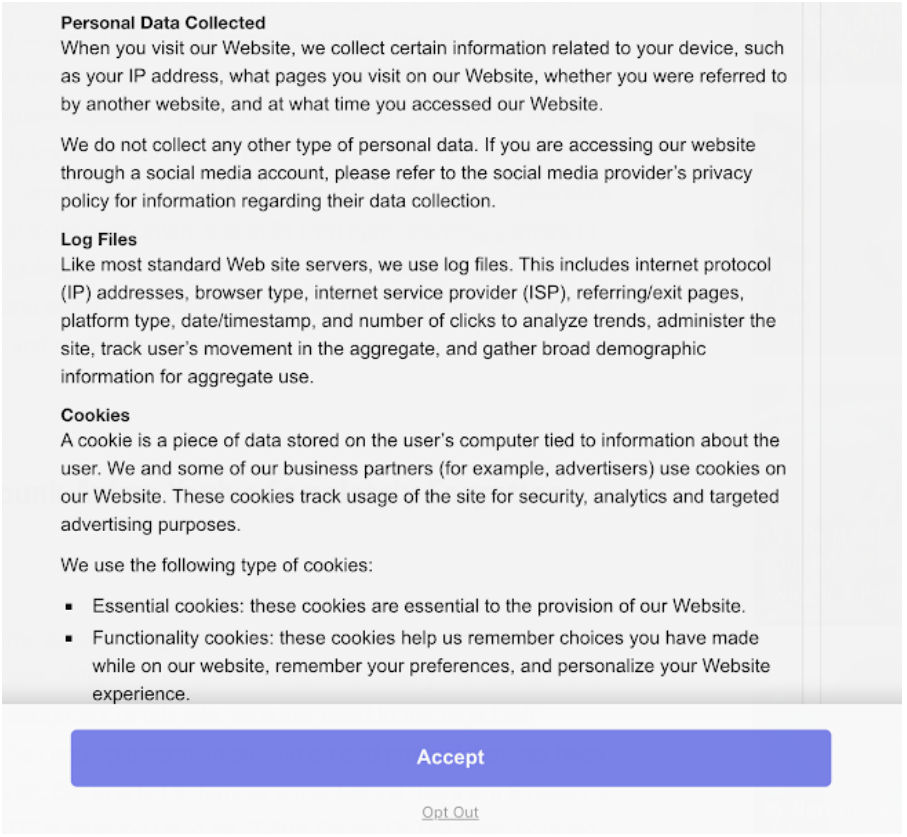
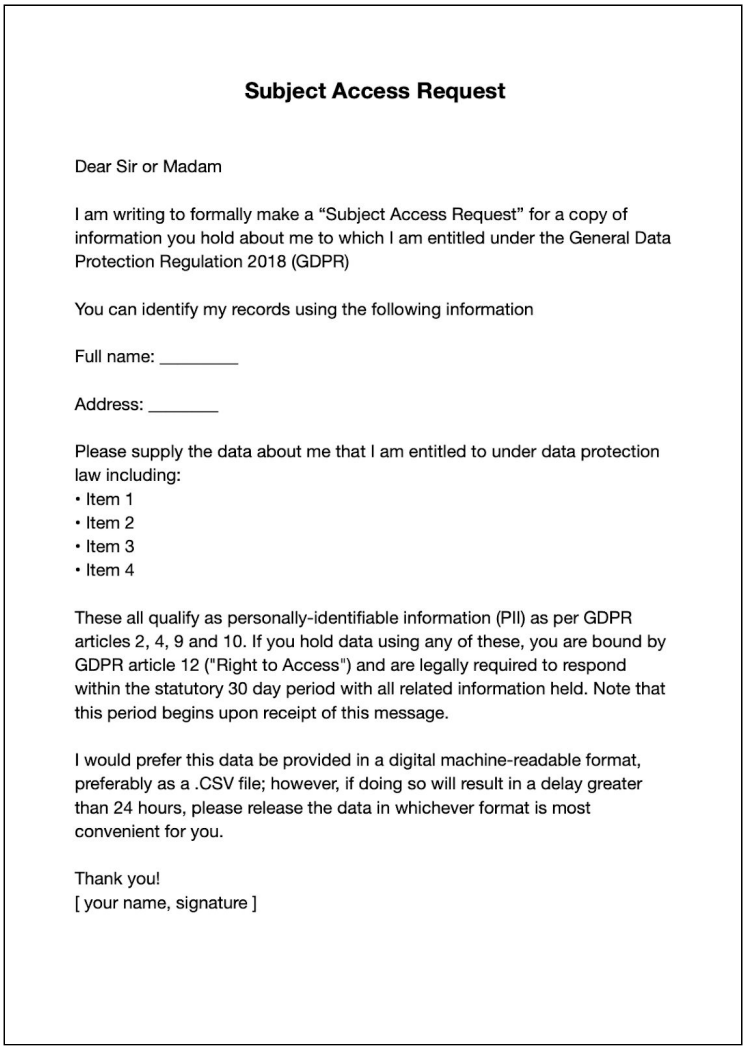


Figure 4.2 Example of GDPR consent prompt. Retrieved from: http://www.cbr.com

The complexity that people have to analyze and understand to give meaningful and informed consent is too much to handle at the moment. People do not have the capability or time to analyze all of the information given meaningfully, and the services are struggling to make the information as simple as possible, while still staying compliant with the GDPR.

The current, clearest way to exercise rights like erasure and rectification is through different GDPR forms. Most of these are either online forms or physical forms that people have to fill out with their personal information. The type of information requested has to be specified on the form, so people have to know exactly what they are seeking. There are services which help people compile these forms, but they request a fee. For individuals, there is no simple way exercising the rights defined by the GDPR in a meaningful way.



Subject Access Request

Dear Sir or Madam

I am writing to formally make a “Subject Access Request” for a copy of information you hold about me to which I am entitled under the General Data Protection Regulation 2018 (GDPR)

You can identify my records using the following information

Full name: _____

Address: _____

Please supply the data about me that I am entitled to under data protection law including:
• Item 1
• Item 2
• Item 3
• Item 4

These all qualify as personally-identifiable information (PII) as per GDPR articles 2, 4, 9 and 10. If you hold data using any of these, you are bound by GDPR article 12 ("Right to Access") and are legally required to respond within the statutory 30 day period with all related information held. Note that this period begins upon receipt of this message.

I would prefer this data be provided in a digital machine-readable format, preferably as a .CSV file; however, if doing so will result in a delay greater than 24 hours, please release the data in whichever format is most convenient for you.

Thank you!
[your name, signature]

Figure 4.3 Subject Access Request form

In a study conducted by the Finnish Innovation Fund about the effects of the GDPR on people, more than a third of the respondents (36%) indicated that its introduction did not affect their behavior in any way. 29% indicate that they had accepted new terms of use from service providers without reading them in detail. This indicates that a more substantial shift in behavior has yet to happen, requiring a rethought approach to how the GDPR is applied to the current user experience provided by different services.

4.3 Exercising rights on different services

People have many rights regarding their data according to the GDPR, like the right to access, rectification, object, and erasure. Many digital services, including data processing giants like Facebook and Google, provide options for exercising these rights. This is done to show people that these services are ethical, compliant, and can be trusted. The way these rights are implemented, however, speak of different intentions.

Accessing the personal data Facebook has about a person is a multi-step process. It requires going four layers deep into settings, where there is an option called "Access your information". This opens a view with many categories to browse about the information Facebook has collected, including location history, advertising interests, advertisers that have been interacted with, posts, comments, and others. My experience exploring this information was that while direct information like search history and posts were accurate, my advertising interests were inaccurate with no indication of what they are based on. This interface is comprehensive in displaying information but offers nothing in terms of rectifying or removing data.

09:30:00.000Z	09:45:00.000Z	43.791327265437644	338.37278413772583		59.4208245	24.7925337	59.4209234	24.7929112	0.6931686253032818	1.2945696115493774	0.36373046040534973	529
09:45:00.000Z	10:00:00.000Z	36.351373026057566	280.86513471603394		59.4211016	24.7931117	59.4219994	24.7942721	0.9008509701312135	1.7482550144195557	0.16955938935279846	357
10:00:00.000Z	10:15:00.000Z	24.773758791697226	89.56584119796753		59.4219329	24.7928506	59.4224069	24.7935964	0.7463252353714189	1.0531197786331177	0.2754066288471222	335
10:15:00.000Z	10:30:00.000Z	32.07292050673689	101.83425831794739		59.421475	24.7932615	59.4223563	24.793424	0.8724892960531831	1.0059661865234375	0.7369232773780823	305
10:30:00.000Z	10:45:00.000Z	22.082791995686154	17.165626049041748		59.4216928	24.7933932	59.4216928	24.7933932	1.0052627325057983	1.0052627325057983	1.0052627325057983	97
10:45:00.000Z	11:00:00.000Z	31.52542121166795	134.6431748867035						0.4123647993772287	1.1577273607254028	0.2551811933517456	305
11:00:00.000Z	11:15:00.000Z	23.68018368681452	43.918917655944824						0.9745903647514927	1.06290602684021	0.7793243527412415	161
11:15:00.000Z	11:30:00.000Z	20.365328790322046	83.07178641652828						1.233969807624817	1.233969807624817	1.233969807624817	149
11:30:00.000Z	11:45:00.000Z	20.19896095772633	23.691986071112105						0.3180752396583557	0.3180752396583557	0.3180752396583557	17
11:45:00.000Z	12:00:00.000Z	20.56790266965519	8.804691314697266		59.4216309	24.79499	59.4216309	24.79499	0.26607733964920044	0.26607733964920044	0.26607733964920044	48
12:00:00.000Z	12:15:00.000Z	29.91651540935565	114.8180685043335		59.4212433	24.7940819	59.4216417	24.7948219	0.7941391875953059	1.249548077583313	0.33041518926620483	169
12:15:00.000Z	12:30:00.000Z	58.9761080130089	413.25179904699326		59.420897	24.7923788	59.4213134	24.7939133	0.7551644831303816	1.2990698814392090	0.3386419117450714	674
12:30:00.000Z	12:45:00.000Z	20.44671691633127	27.26744150340465		59.4212854	24.7935927	59.4216	24.7943971	0.8950772285461426	0.8950772285461426	0.8950772285461426	116
12:45:00.000Z	13:00:00.000Z	28.511165584915553	97.35280443012806		59.421254	24.7938787	59.421254	24.7938787	0.4789505537706045	0.8935503363609314	0.3386419415473938	353
13:00:00.000Z	13:15:00.000Z	39.27690443552983	280.60036943751265		59.4209928	24.7930192	59.4213393	24.7939539	0.6957862690638582	0.9277862310409546	0.47760841250419617	453
13:15:00.000Z	13:30:00.000Z	52.32244779142077	330.5501846234233		59.4218748	24.7903036	59.4241856	24.7928632	0.6899627978286577	1.29251229763031	0.4057803452014923	497
13:30:00.000Z	13:45:00.000Z	16.6354150261057										4
13:45:00.000Z	14:00:00.000Z	24.86469449079292	48.36565351486206		59.426622	24.6512194	59.4266797	24.651506	1.0940113067626953	1.2522019147872925	0.9358206987380981	119
14:00:00.000Z	14:15:00.000Z	38.251104092243274	139.101129531860351		59.4265942	24.6512311	59.4271502	24.6523247	0.7978454426389892	1.312013030052185	0.16560623049736023	243
14:15:00.000Z	14:30:00.000Z	39.40768465940785	111.13833332061768		59.4266207	24.6512388	59.4272719	24.6525753	0.9315151758051264	1.1750189065933228	0.4501977860927582	431
14:30:00.000Z	14:45:00.000Z	28.492992522892077	78.43154621124268		59.4265734	24.6510957	59.4266985	24.6514683	0.7807555349788944	1.234364628791809	0.3176773190498352	170
14:45:00.000Z	15:00:00.000Z	32.92975373708178	310.29040813446045						1.1675391207368626	3.685580253601074	0.6937450766563416	317

Figure 4.4 Excerpt from personal data file provided by Google

Many services offer the option to download a copy of all the personal data stored. I used this option with my Google account, generating a 20-gigabyte archive containing many plain text files with raw data in them and extremely long activity logs with abstract information. This data is mostly incomprehensible and offers no value, as there is nothing an average person can do with it. The same applies to downloading personal data from Facebook. These options mostly provide what they promise, but the intention is not to empower people to exercise their rights. Instead, the goal

seems to be to provide the bare minimum required to be able to claim to upload ethical standards.

Removing or objecting to the collection of certain data is where this is most evident. This is something that can be accessed by going six layers deep into user settings in Facebook. There is a list of options, of which the last one opens a form that has to be filled out with the specific information which data processing activities are being objected to. The average person is unable to describe what a data processing activity is. This option is only usable by people who would not let Facebook mishandle their data in the first place. The other options in the list lead to articles, most of which explain in detail how to do a specific task on Facebook. The fact that this information is hidden so deep in Facebook's system indicates that they prefer not to do these things.

The simplest option given to users to remove personal data from Facebook is to delete their account. The option first tries to convince users to deactivate their account and emphasizes that the user will lose all access to everything they had on Facebook. Even after confirming the deletion, there is a 30 day grace period before the account is genuinely deleted, during which it is possible the data is still being analyzed and shared (there is no information available about this). After the deletion is done, there is no guarantee that all the personal data is now gone, as it has most likely been shared with third-party organizations. As there is no infrastructure to track and document the use of data, there can never be any absolute confirmation that the deleted data is completely gone.

Exercising personal data rights is something that many services that gather large quantities of data enable at first glance, but do so in a way that nudges users away from those options. The interfaces are designed so that these options are hidden away and require much effort to utilize them fully. The personal data is presented in a way that is useless to the average person, giving no reason to care about this data. This approach does not empower users, instead, it seems to be designed to preserve the status quo while presenting the image of being ethical. As these services all work as separate silos, because they lack a shared infrastructure, the data cannot be moved from one service to another very easily, and users can never be sure if the data they deleted was removed. There are many reasons to care how these companies use personal data, but the experience steers people towards apathy and blind acceptance, rather than ownership and responsibility.

4.4 Empowering active participants

A person's data is their digital identity, nobody except themselves can own their identity. The systems and solutions meant for people to manage their data do not empower them to think of it in this way. While people do own the personal data processed by different services, the way they get to express this ownership does not put them in charge of anything. The GDPR consent prompts are the most primary way of expressing their will, but it actively detracts from their experience and achieving their goals. The consequences of consent are not fully visible without reading difficult to understand terms and conditions. Currently, to be an active owner of one's personal data, one has to be very knowledgeable in technology, have a high capacity for analysis, and enough free time and tenacity to use the scattered options and forms that exist. As in the binary choices offered by many services in terms of control (delete or keep everything as is), people also have a seemingly binary choice – full responsibility on all levels or no responsibility at all.

Not exercising responsibility does not mean that people trust the systems that handle their data. For example, a study found that 60% of people in the United States do not trust Facebook with their data,[58] yet it has 221 million users.[59] This distrust of data processing services does not translate into people taking action as they are inhibited from doing so by those services and lack other tools and frameworks to support them. There is also a lack of clear understanding of the consequences for giving consent to their personal data and thus cannot be empowered to be active participants if they do not even understand what they are responsible for.

Moreso, for the individual, their personal data holds no value in its raw form. The archives that can be downloaded off websites are not usable in any way by the average person. Sometimes, not giving consent means that a service is inaccessible, making the data even less valuable. It offers nothing of interest and does not relate to the idea of a digital identity, but at the same time there is still fear regarding it, as the fact that it is used to manipulate is becoming common knowledge.

These issues are not something that can be fixed by giving people more access to their data or more tools, because, in the current ecosystem, they have assumed a passive role. While many steps are being taken towards solving the technical aspects

[58] *Poll: Americans give social media a clear thumbs-down*. (n.d.). NBC News. Retrieved May 22, 2020, from https://www.nbcnews.com/politics/meet-the-press/poll-americans-give-social-media-clear-thumbs-down-n991086

[59] *Facebook users in U.S.* (n.d.). Statista. Retrieved May 22, 2020, from https://www.statista.com/statistics/408971/number-of-us-facebook-users/

of creating an ethical data management ecosystem, for anything to change fundamentally, there have to be steps taken towards making the digital world more understandable for humans and the value of personal data clear.

5 A CRITICAL ANALYSIS OF USER EXPERIENCE DESIGN

While analyzing the current experience of managing personal data, I began with ideation and prototyping for a system to empower people in this regard. While I did apply all my knowledge of how to create a good user experience, the design process proved difficult. It did not produce any results that were markedly better from what already exists in the form of GDPR consent prompts. Instead, the improvements were incremental, and testing with users did not indicate that the solutions would bring about any significant behavioral change.

I had knowledge of the weak points of current solutions, analyzed the user needs, and set clear goals, but the way I was designing just led down the same path. This turned my focus towards the ideas and methods of user experience design. I hypothesized that aspects of the philosophy driving user experience design were only focusing on user needs from a specific, simplified perspective that is being influenced not only by the designer's mindset but also by organizational goals. To empower users, a holistic understanding of their needs is necessary, so I set out to analyze what is currently preventing this understanding from being reached.

5.1 Mindset driving user experience design

User experience design is, at its core, meant to guide products and services to serve the needs of humans using them. The Nielsen Norman Group defines "user experience" as something that encompasses all aspects of the end-user's interaction with the company, its services, and its products. [60]

When delving into the conversations happening in UX design through articles and discussions, serving user needs is touted as the core of the field. The best experience for users cannot be created without focusing on what the users want. This means that extensive research into user behaviors needs to be conducted, interviews and observations carried out, and all of it has to be empathically analyzed. As the field has developed, the rules that guide the creation of user experiences have also become more well defined. For example, the website "Laws of UX"[61] lays out 20 guidelines that inform designers about different aspects of human psychology and how they relate to how people use interfaces. The Nielsen Norman Group has also contributed a lot to the

[60] Experience, W. L. in R.-B. U. (n.d.). *The Definition of User Experience (UX)*. Nielsen Norman Group. Retrieved April 19, 2020, from https://www.nngroup.com/articles/definition-user-experience/

[61] Yablonski, J. (n.d.). *Home | Laws of UX*. Retrieved April 19, 2020, from https://lawsofux.com

field in the form of best practices. Many articles detail the best approach to provide a good experience and how to best use different user interface components.

The best user experience is defined as one that meets the user's needs without burdening them with too much information, complexities, or obstacles. Using a product or service should give users joy while providing value through simplicity and convenience. Designers are only there to make sure the users have what they need, and every study and analysis should lead them closer to serving user needs. This is something that is repeated in many articles and sources that talk about UX design.

In concept, designing while taking the best practices into account should ensure that the field produces products and services that enrich people's lives, but this is not always the case. While many products have a sub-par user experience, which burden users with overly complex interactions and bad methods of conveying information, these products usually do not develop large user bases and are limited in the negative effect they can have. On the other hand, user experiences offered by services such as Facebook and Instagram are, in essence, high quality – they provide a comfortable service that serves the user's needs quickly without burdening them with too many complexities. Thus, these also have large user bases and long-term user retention.

At the same time, these two services are commonly brought up in conversations about how digital products can harm their user's mental health. These products do adhere to UX design's best practices but are still having a negative effect on their users. This effect has been correlated with the use of "dark patterns," which are persuasive and manipulative techniques used to influence users into behaving in a certain way, which may be against their best interest.[62] These patterns are treated as something outside the norm of UX design's best practices, as they no longer serve user needs. They are seen as something which can be combated by applying the proper UX mindset and best practices, immoral use contracted by proper use. This type of thinking does not consider that the mindset, methods, and best practices of UX design might be flawed and that the "dark patterns" are not a phenomenon born from somewhere else entirely.

Core concepts such as "serving user needs" use language that portrays people in a passive role, as the recipients of something they need, not active participants in fulfilling their own needs. While the goal of serving these needs is noble, the way the

[62] Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 1–14. https://doi.org/10.1145/3173574.3174108

designer sees the people they are designing also defines what they create and the paradigm it supports. The universal truths of user experience design that see value in simplicity hiding complexities, convenience, and comfort, so users do not have to think too much and thus have a more satisfactory experience, start to persuade people into taking on the passive roles of the "user." The designer assumes that people prefer to have no friction in any of their digital experiences. These truths are not all born from human-centric design thinking. This is heavily tied to the business goals driving the design as well, as designers can end up in a role where they work on how to make the experience smooth, but are disconnected from the actual goals and have no say in these. In this situation, the user gets what they seemingly want but does not know that through this, they are giving the business something they would not willingly give otherwise.

5.2 The influence of business-centric thinking

The core aspects of UX design are influenced both by human-centric thinking and achieving business goals. The methods used by user experience designers are focused on humans and their thinking, but the goals are generally based on creating business value. Looking at the core aspects through the lens of business thinking gives new insight into the processes driving UX design. For example, having a convenient and simple service, in theory, provides users with a more smooth, joyful experience. At the same time, from the business perspective, it also enables users to more quickly complete tasks that create business value, such as 1-click-ordering on e-commerce websites like Amazon. The experience itself is smooth and convenient, but at the same time, it removes many opportunities for reflection for the person using the service to assess if they need what they are ordering.

In this, UX design starts to serve two goals at once, ones that stem from what is best for humans and ones that are defined by what enables the best growth for a business. How data privacy is handled on services like Facebook is a good example of how this duality can be expressed. As mentioned before, users are given an option to download or delete their data from the service as a showing of good faith and ethical conduct. However, reviewing this personal data is not proactively offered, and doing anything with it through Facebook is cumbersome. This creates a paradox of responsibility, as the user is given the option to download, delete, rectify, and so on, it implies that they can and are responsible for how their data is used. At the same time, nothing on the service prompts users to think in ways not beneficial to Facebook, who process their personal data for their profit.

The convenient and frictionless experience offered by Instagram also illustrates this dual nature. The service is designed to load content very fast, and the "infinite scrolling" pattern used in the content feed essentially keeps loading new content for as long as users are willing to scroll. On the one hand, this does serve user needs and wants by giving them more and more content to look at and pass the time, resulting in a satisfying user experience. However, as there are no limits set and no prompts to stop, this can result in unhealthy amounts of time spent on the service, doing tasks that do not provide the user much value outside short-term gratification. On the other hand, having users scroll endlessly through content also creates endless possibilities for advertising and creating business value, along with high user retention metrics, which attract advertisers.

The reason why UX is strongly tied to business value may come from the nature of digital products and services themselves. These products enable the collection and tracking of different metrics that can inform how successful the product is. It is much easier to generate and track metrics tied to a business value such as user retention and conversion, than more abstract values such as responsibility and meaning added to a person's life. This is also one of the reasons why UX designers push frictionless experiences, as they remove barriers for users completing tasks that create business value and thus drive growth. The metrics then reflect a successful product.

This is not to say that business goals corrupt or disrupt UX design, rather the idea is that when designing these experiences, all friction and convenience should not be treated as equal. Careful consideration should be made when applying the best practices of UX design of how they play into the balance between human-centric goals and business goals. Beyond this, it shows a need for structures that support ethical digital services beyond the user experience. Ethical operation and transparency is something that many brands tout as core to their thinking and is something that people respond to as well. Digital services that use a lot of data do have obstacles in being ethical because, as stated before, complying with the GDPR is difficult. Huge corporations like Facebook can create these structures as they have the technical know-how and budget, but they lack the incentive to do so, as it would affect their profits. Medium-sized and small organizations could benefit from the creation of proper infrastructure that enables the ethical handling of data, as new business models could emerge. With that, designers could establish new rules and focus on different behaviors to create experiences that do not influence people to fulfill goals that do not benefit them. New market niches would be created that empower people

to use their data ethically, creating a new situation where both the people and organizations benefit.

5.3 Data-driven design

The data-driven nature of digital products influences the methods used for UX design. As these products enable the definition and tracking of different metrics, it is logical that designers would take advantage of these to support their work and gather data for analysis. This can be beneficial for analyzing and optimizing a website's information architecture, as it gives quantitative information about how users move from one page to another. However, these metrics are also applied to other aspects of the experience to the extent of trying to quantify qualitative data into attitudinal UX metrics.[63]

This quantification means taking human aspects like loyalty, trust, and appearance and using combinations of metrics to assign scores to them, which then can be used to make design decisions. One example of this effort is the HEART framework, developed by Google with the goal of using quantitative data to rate the quality of a user experience.[64]The focus points set by this framework are as follows:

Happiness – Used to measure user attitudes, often collected via survey. The metrics used here are customer satisfaction (CSAT) and net-promoter score (NPS). Both of these metrics rely on simple surveys that ask users a specific question and rate it on a scale of 1-5 or 1-10.

Engagement – The level of user involvement is typically measured through the number of visits by a user in a week, the number of photos uploaded, and amount of times shared. The goal is to quantify behavioral proxies such as frequency, intensity, or depth of interaction over a specific period.

Adoption – How many new users the product or feature has, such as the number of accounts created in the last seven days, subscription numbers, or purchases made by new users.

---

[63] What metrics and KPIs do the experts use to measure UX effectiveness? (2019, May 28). *UserZoom*. https://www.userzoom.com/blog/what-metrics-do-the-experts-use-to-measure-ux-effectiveness/

[64] *How to Choose the Right UX Metrics for Your Product*. (n.d.). Retrieved April 22, 2020, from https://www.dtelepathy.com/ux-metrics/

Retention – The rate at which existing users are returning. Examples are renewal rate or failure to renew, otherwise known as "churn" or repeat purchases by users.

Task success – Traditional behavioral metrics of user experience, such as efficiency (e.g., time to complete a task), effectiveness (e.g., percent of tasks completed), and error rate.

These metrics can produce useful insight into user behavior from large data-sets, that cover behaviors on a macroscale and give a basis for making and explaining decisions, something which is often hard in fields focused on soft, user-centered values. They offer a safe fallback for designers by giving the feeling of certainty to their decisions, and through this also a way to have business and technical-minded people relate to those decisions. Metrics can be seen as a way to support and reframe the decisions and insight of designers to make them understandable to others. On the other hand, there is a danger of adopting the business and technical way of thinking to make the process easier and more manageable.

The wealth of data and the importance that it holds in current-day digital products influences the design process as well, but it is subject to the same shortcomings, like relying on high volumes of low-quality data, which can lead to insights that do not reflect actual human behaviors. Furthermore, it can influence designers to rely on the performance of key metrics, such as conversions or user retention, to rate the quality of their product and focus on increasing this performance, losing sight of the humans using the product.

What quantification removes from the design process is the aspect of reflection. When designers reflect, they reconsider an idea or experience. This process puts under question the work done, its validity, and its relevance to the situation. Questioning whether the metrics used can be trusted and are saying something of value and questioning their judgment as a designer gives way to put aside biases and goal-focused thinking to see the situation as a human on the same level as the humans that are being designed for. Metrics cannot answer questions such as "Am I making the world a worse place?" or "What sort of meaning does this solution have in the lives of the people it is meant for?".

Furthermore, products and services designed without reflecting do not enable their users to reflect as well. A product designed with efficiency and convenience in mind will expect efficiency and convenient thinking from its users. The solution primes and

nudges the thinking of the people using it. By making a product that focuses on convenience and simplified thinking that is continuously re-engineered to bring users back, the users start to lose their ability to think in more complex ways. They do not have a chance to reflect on how their behavior is impacting their lives.

5.4 The role of dark patterns

Dark patterns are usually blamed for services and products being harmful or addictive, reducing the quality of life of their users. This conversation is centered around how layouts, components, buttons, and interface logic is applied in a negative way. They are treated as a subversion of the general UX patterns, which should benefit users, and the goal is to shame companies and designers using these patterns. However, what this conversation does not address is the mindset that enables the creation and usage of these patterns.

The absence of reflection in the design process is something that enables interfaces to become focused on the "what?" and leaves the "why?" by the wayside. The image of the malevolent designer, looking to manipulate users into behaviors that intentionally negatively impact them, is commonly associated with dark pattern design. The aspect of intentionality underpins the conversation, but the aspect of where the patterns are born is not addressed. There is a lack of reflection in the UX design field itself when it comes to these patterns. The question is, what makes designers act in unethical ways?

The easy answer might point to the lack of character of a specific designer, which hinders them from making ethical choices. Another framing of the issue is that the companies the designers work for pressure them into these decisions. However, designers can and have unwillingly created experiences that have had adverse effects. The people who first designed Facebook did not have influencing elections in mind when creating it. Here, the missing process of reflection enables designers to see the larger picture and critically look at where the metrics and data are moving the product or service to is of paramount importance.

The user-centric mindset of UX design, based on the gathering and analysis of metrics and large-scale data, contributes as much to creating dark patterns as the lack of ethics of a specific person or company. When UX designers treat user-centric thinking as a best practice and do not put its different aspects into question, it is natural that focus is lost from the real humans who are being designed for. The questioning of so-called "common knowledge" is what produces new knowledge, meaning that

putting under question the assumption that user-centric thinking is a best practice that should guide all UX design is something that would also generate new knowledge. By critically looking at the core of user experience design, which is serving user needs and wants, questions such as "What is a user?", "Do users want to be served?" "Are all needs and wants equal?" and "Can I decide what is best?" can start to be asked.

Rather than trying to define user-centricity and best practices through the most beneficial use components and interface logic, the definition could start from a layer above. A best practice of regularly reconsidering what user-centricity is in the context of a product or service would serve to stem unethical ways of thinking from appearing. Humans are not static objects and serve many roles in their daily lives, with ever-changing motivations for doing something. Thus user-centricity is not something that can also be defined clearly but is ever-changing. This creates a much more ambiguous and complex picture of who the user is and what they need, which hinders designers from thinking reductively about them.

Dark patterns can be born from a lack of ethical thinking, but from the attitude, the designer has towards their user. If ideas behind user-centric thinking are not questioned, the "common knowledge" approach moves the designer into a position above the user, inadvertently making the user a subject of their design, not their design driver. This imbalance unconsciously makes designers rely more on metrics and data, which are presented as empathetic thinking, but in reality, they are closer to business analytics. The human at the core of the process becomes an object and is expected to adopt the behaviors and mindset of an object as well.

5.5 Empowering users into actors

Understandably, the word "user" is a core piece of the language used by user experience designers, but the word itself carries within it a connotation of passivity in the context of this design field. Understanding and serving user needs is what UX designers are supposed to do, but this is done in the framework of defining these needs through the lens of what makes the experience as positive and comfortable as possible. The needs are strongly tied to aspects of simplicity, convenience, and reducing cognitive load, which considerably narrow the possible outcomes of the design process. Not all needs and wants are created equal. Understanding this requires reflecting on the role of a user in a system.

A user of a social media platform prefers their content to load instantly and to have easy access to different types of stimulation, thus to have a user-centric social media platform that serves these needs, this is where the focus should be. This is also supported by the business side of a social media platform, as more content scrolled through means more ad revenue. Nevertheless, analysis has shown that what drives this need for easy access to more content are addictive patterns of behavior. Serving this need only further drives users into a passive role, removing the option for critical thought. This experience might delight and bring joy to users, but it does not consider the fact that the human experience does not just revolve around fulfilling every need there is. People need to have a chance to consider what is right and wrong for them, not have a digital product assume this based on data analysis. To remove this passive connotation and reconsider what it is to be a user, reflection also needs to be enabled from the user's side.

5.5.1 Two modes of thinking

The values we have define the way we interact with things and what we expect from them. In this sense, being a "user" can be defined as a mode of thought, where the main values are speed, comfort, and convenience. It is an operational way of thinking, concerned with achieving a specific goal in a fast and automated way. Because of this, it lacks mindfulness in decision-making and analysis. However, people also have other values that are existential, such as respect, autonomy, and trust. Thus, a second mode of thought of being an "actor" can also be defined, where conscious reflection and mindful decision-making based on these values is done. Both of these are important for balanced cognitive functioning, but currently, the user experience design focuses mostly on the "user" mode of thinking. However, if both are engaged, the user experience becomes a rich experience instead, as it incorporates human functions holistically and respectfully. There is an opportunity to enable this through deliberate design choices and a reflective process.

The immediate jumping to user-centric modes of designing is symptomatic of a solution-led process. The assumptions about the person's values have been pre-made to fit the role of the "user", thus fast-tracking the definition of what the problem is and removing the uncertainty of what the solution should be. To incorporate the values of the "actor", these assumptions must be set aside, and the ill-defined nature of the design task must be embraced. This means that in practice, designers must spend some time in a process called "problem formulation", whereby some initial assumptions are made about requirements and constraints. Even in the case of a

well-defined problem, the process of problem formulation is necessary to be able to consider the full extent of a person's values. This process is invariably incomplete, fluid, and time-limited, but enables us to see the context and the values tied to it better.

A core value of being an actor is having your boundaries respected and being empowered to understand, think independently, and be responsible. Understanding this within the context of the experience being designed allows the relationship between the person and the solution to be defined. Here, designers also hold a lot of power as, in some cases, people's habits lend to them not acting in ways that support their existential values, but through conscious design choices, new behaviors and habits can be encouraged. The "actor" mode of thinking is not always the most instantly gratifying, but there are ways to create experiences that incorporate this without burdening people, but rather by embracing their complexity.

5.5.2 Designing for friction

Design friction is a term used in many articles about user experience design and refers to points of difficulty occurring during interaction with technology. As stated before, friction is treated as something that should be actively removed from an experience to reduce the risk of frustration and disengagement. However, friction actually plays a vital role in design. For example, it is essential in safety-critical design, which stops people from performing actions that have severe consequences without them being fully aware of them. While safety-critical design usually applies to systems related to infrastructure, transport, or medicine, it is used in more widely accessible digital systems as well. One example is that the deletion process in many interfaces includes a prompt to confirm this decision. This prompt gives people a moment to consider what the effect of deletion will be.

We can expand this idea of friction for safety to friction for values. By using friction to interrupt automatic interactions, slow people down, and give an option for reflection, people can be empowered to use the actor mode of thinking. Frictions designed with intention, and introduced with care, have the potential to elicit interactions that are reflective, informed, and safe. This friction does not need to bring the experience to a halt but can be integrated carefully. A concept called a microboundary[65] provides a small obstacle prior to an interaction, acting as an intervention that slows people down

[65] Cox, A., Gould, S., Cecchinato, M., Iacovides, I., & Renfree, I. (2016). Design Frictions for Mindful Interactions: The Case for Microboundaries. *In: CHI EA '16 Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. (Pp. Pp. 1389-1397). ACM: New York*. http://discovery.ucl.ac.uk/1475258/1/Design%20Frictions_CHI2016LBW_v18.camera.ready.pdf

before acting or moving from one context to another. It creates a brief moment in which people can reflect on what they are doing.

UX design often also focuses on creating pleasant experiences, but negative emotions can also elicit people to behave in ways beneficial to them. The paper "Ten Ways to Design for Disgust, Sadness, and Other Enjoyments: A Design Approach to Enrich Product Experiences with Negative Emotions"[66] by Fokkinga & Desmet describes an approach where by combining a negative emotion with a protective frame a rich experience can be created. Emotions can become rich if they include a paradox and a temporary discomfort is a strong motivator.[67] In the case of empowering people to be actors, creating negative emotions through demonstrating that their existential values have been violated or even forgone by the person themselves can be used to incite people to action. This requires giving the person actionable steps to take at the moment of negative emotion, so there is an outlet for them to create a positive experience for themselves, to take control essentially.

5.5.3 Value based design

Designers need to understand the values of the people they are designing for. Values are regularly considered in design work, but usually not explicitly moral or political ones. The article "Values and Ethics in Human-Computer Interaction"[68] by Shilton expands on a concept called "value levers", which are factors that encourage values discussions in design. (citation) Examples of these factors are working in interdisciplinary teams, which encourage team members to explain their decision-making to others and reflect on those decisions. Questions asked by outsiders can invoke concerns about values or ethical issues. Self-testing the design can incite a reflective form of critical thinking, experiencing the value related possibilities and problems first hand. Designing around technical and policy constraints can encourage conversations about why these constraints exist and the values they are meant to support (especially relevant in the case of the GDPR).

Here it is also essential to consider the designer's own values as their work is also knowingly or unknowingly a reflection of them. The methods chosen and the path

[66] Fokkinga, S., & Desmet, P. M. A. (2013). *Ten ways to design for disgust, sadness, and other enjoyments: A design approach to enrich product experiences with negative emotions*. https://www.semanticscholar.org/paper/Ten-ways-to-design-for-disgust%2C-sadness%2C-and-other-Fokkinga-Desmet/44811ef0e051e937440801dee6c3f099aa389d34

[67] Benford, S., Greenhalgh, C., Giannachi, G., Walker, B., Marshall, J., & Rodden, T. (2012). Uncomfortable interactions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2005–2014. https://doi.org/10.1145/2207676.2208347

[68] Shilton, K. (2018). Values and Ethics in Human-Computer Interaction. *Foundations and Trends® in Human–Computer Interaction*, *12*(2), 107–171. https://doi.org/10.1561/1100000073

taken towards a solution are shaped by their individual hopes and aspirations, along with their fears and doubts. These are also shaped by the context in which design happens. The Silicon Valley model of user-centric design, encapsulated by Facebook's former motto of "move fast and break things", has defined for many UX designers the way they should operate. Silicon Valley has demonstrated numerous highly successful and popular digital products, and this is something many designers wish to emulate. The products also have been demonstrated to have unintended consequences for people as behind the prestige, the focus is on profits. The methods Silicon Valley enforces, nudge the people in its periphery toward the standardizations needed for the mobility of capital rather than supporting ethical design practices.[69] Grand visions of a technologically powered and globally-aligned future are presented that may not ultimately support the very workforce it is supposed to help. Designers must consider the influence of these examples on their work.

5.5.3 Undesign

Harold Nelson and Erik Stolterman characterize design as "the ability to imagine that-which-does-not-yet-exist, to make it appear in concrete form as a new, purposeful addition to the real world."[70] Undesign is a conceptual inversion of design as the ability to understand that-which-currently-exists, to make it disappear in concrete form as a new, purposeful subtraction from the real world. It is not a black or white proposition, but there are gradations to it. Utilizing it offers a view that otherwise is left unexplored, or how things we consider good or useful might be even better when restricted or in a lesser form.[71]

For example, digital systems are highly connected and instant in communication, meaning they reach out to people in the same way, often disrupting other activities through notifications and other means. Looking at this from the undesign perspective, we can think about inhibiting technology at the level of individual interactions, displacing it at the level of routine social practices, and utterly erasing or foreclosing it at the societal or existential level. Creating a digital system designed for self-inhibition in the way it communicates and operates can also open a way to make room for people's under articulated needs. A system that is open about its weaknesses and capacity for failure can be the basis for a richer experience and empower people to take more responsibility for themselves.

---

[69] Avle, S., Lindtner, S., & Williams, K. (2017). How Methods Make Designers. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 472–483. https://doi.org/10.1145/3025453.3025864

[70] Nelson, H. G., & Stolterman, E. (2012). *The Design Way: Intentional Change in an Unpredictable World*. The MIT Press.

[71] Pierce, J. (2014). *Undesigning interaction*. Association for Computing Machinery. https://doi.org/10.1145/2626373

Undesign is also good to explore potential futures. While the focus in design is usually on the best possible outcomes, descriptions for what should not happen, what should not exist, and how things should not function can also be considered a design solution. Even if it is clear to the designer why something should not exist, describing these solutions through text and examples articulate the reasoning for this and can inform the creation of a better alternative. If the goal is to create a utopian scenario, a strong understanding of the dystopian scenario is needed. Otherwise, there is a risk of the values of the two blending together.

6 DESIGN BRIEF AND PRINCIPLES

Since the topic of personal data management is complex, for successful conceptualization, a more specific framing is required. Based on the analysis conducted, key issues related to control over digital identities and personal data relating both to individuals and organizations were identified. These findings are the basis for defining the goals and needs of the concept.

6.1 Key findings

- **The GDPR is hard to comply with**
  While the GDPR does set a necessary precedent for how personal data should be handled, the requirements to do so are steep, and the motivation for doing so is tied to avoiding fines, not respecting people's privacy.

- **Lack of infrastructure to support ethical data handling**
  Organizations do not have the necessary infrastructure to support data management in a scalable way. As it is required to document and log the use and purpose of personal data processed, many organizations lack the human resources and knowledge to do so in a sustainable way. Different organizations also lack a common infrastructure to ensure data portability, making the ethical and safe sharing of data difficult.

- **Organizations use rely on large amounts of low quality data**
  Organizations gather vast amounts of low-quality data, leading to low-quality insights that do not benefit the business and harm the digital identities of the individuals involved.

- **There are large quantities of data gathered that remains unused**
  Organizations gather data that they do not use and, in some cases, lack knowledge of even storing some data. Unused data produces no value, lacks oversight and purpose, and is a security risk.

- **People have no sense of ownership over their personal data**
  The intangible nature and current lack of control over personal data leave people feeling ambivalent about it. On the one hand, people do see privacy as an issue, but on the other hand, not many take responsibility for by actively working towards it. Personal data is not seen as comprising their digital

identity, and even the GDPR states that the data controllers are the ones who have to ensure people their rights.

- **There is a lack of ways to exercise our data rights in an impactful way**
  The existing solutions for exercising these rights are either ineffectual (GDPR consent prompts) or cumbersome (data request forms, managing data through service features). This leaves people feeling powerless, and managing one's digital identity remains a topic for discussion for enthusiasts only.

- **People do not sense the importance of these rights and the value and impact of their personal data**
  Raw personal data is unusable by most people, thus it lacks any practical value for them when storing and managing it by themselves. At the same time, this data is valuable to organizations because they can generate insights from it, but individuals do not feel this impact. The consequences of the misuse of their data are unknown to them, even though they may be severe.

- **The design approach behind current digital experiences do not empower people to be responsible**
  UX design currently focuses on creating smooth, simple and comfortable experiences for people. This approach however, does not enable people to reflect on their actions and their consequences. These user experiences treat people as passive users, thus they are unable to actively participate, decide, and be responsible.

6.2 The needs of individuals and organizations

Based on these findings, the core needs for supporting control over digital identities were identified:

An infrastructure that enables the ethical sharing and transfer of data between services and data banks.
As the main issue for GDPR compliance is the lack of infrastructure to support organizations in all the activities required by it, providing this would already be of great benefit to organizations. This is especially true for small and medium-sized organizations, as they do not have as many human resources or a large budget. This infrastructure is also crucial for enabling data portability, creating many new business opportunities related to data processing. This infrastructure can automate many

processes relating to the documentation of data use and gathering purpose, acting as an oversight organ as well. Joining this infrastructure already means that organizations have to comply with specific privacy and compatibility standards.

A way for people to analyze and understand their data, how it is used, and to make decisions regarding it.

The gathering and use of personal data are near impossible for people to analyze and understand on their own (within a reasonable amount of time). People need assistance in understanding all the terms and conditions and implications of giving consent, as well as the value of their personal data. This analytical support should not decide for them, but rather give more information on-demand and support them in being empowered and active participants who make decisions based on their values.

A design approach that elevates the user to the role of actor, by focusing on creating experiences that do not seek to eliminate friction, but to provide space for it.

The user-centric approach is not enough to design an empowering digital identity management system. The design has to empower users into being actors, thus both the design process and the solution need to have space for reflection. Beneficial friction needs to be incorporated in a mindful way to incite people into behaving as actors. The designers need to be aware of not just the operational values of a person (speed, simplicity) but their existential values as well and design to support those.

6.3 The guiding principles

The goal of this thesis is not to fully define what the single best answer to these issues and opportunities is, but rather to define a way of looking at these issues that comply with the goal of empowering people to assume control of their digital identities. There are many possible futures in this regard that are dependent on the infrastructure used, regulations and restrictions in place, and the development of business models. I aimed to define principles independent of these factors, that ensure that whichever scenario is being designed for the focus remains on the human experience in the center of it. This topic's underlying issue is the violation of people's values and dignity through manipulation, unethical behavior, and careless regard, which may even be unknowing. Giving people who wish to tackle this topic (or related topics) principles to follow helps ensure the respectful treatment of the humans at the core of it.

- **Users can become actors**

  People should not be forced to only take the passive role of a user, but have the opportunity to actively participate as an actor. This has to be proactively initiated by the solution.

- **Following social norms**

  The solution is also a part of society as it interacts with people, thus it has to follow social norms. This means knowing and respecting the person's values.

- **Ethics on all levels**

  The solution cannot uphold an ethical standard if all parts do not comply with this. All the potential for failure should be considered here by analyzing both the utopian and dystopian outcomes of each scenario or idea.

- **Freedom from estimations**

  The solution should not overly estimate what people wish to see and offer limited options in this regard. People have to have the option to estimate for themselves and express this to the solution.

- **The context and consent of communication**

  Because the solution has to respect social norms, it also has to respect the value of people's time. The relationship between the solution and person includes within it the agreement of when to communicate. Instead of the solution having access to the person's life at any time through notifications and prompts, the person has on-demand access to the solution and decides the context of the communication.

- **Augmenting and enhancing human capability**

  Humans have a high capacity for analysis and understanding which should not be underestimated. The solution has to enhance and augment this capability, to support people in decision-making and taking responsibility. This means making difficult to comprehend things such as terms and conditions understandable and giving options to naturally delve deeper.

- **Balance between automatization and responsibility**

  While fully manually managing personal data in a sustainable way is not possible and automatization processes such as giving consent can help people, there should be a careful balance between automatization and responsibility. Personal data privacy is strongly tied to human rights, meaning people also have to take responsibility for maintaining them. Something which they should be prompted to do.

- **The fallibility of a "black box"**

  If using narrow AI algorithms, their nature as a "black box" has to be considered. As we cannot fully understand how it reaches its conclusions it cannot be used to decide for the person. It should always be possible to override the "black box" and the solution should push people to decide independently. The solution should be open to criticism and should make people aware of its own weaknesses.

- **Promoting the use of data**

  The solution should highlight ways to use personal data and demonstrate its benefits. Just hoarding data will not generate any value to the person or benefit society in any way. The goal is to reach an ethical and symbiotic relationship between people and organizations.

7 CONCEPT: INSTANT FRAMEWORK AND ASSISTANT

The goal of the concept is to provide an example of a possible future for ethical data management. This is done following the principles defined beforehand and considering the current day developments. Currently, there are many theoretical proposals for how people could manage their personal data, but here the idea is to create a visual example of what personal data management could actually look like for people in a practical sense. As the idea of data management is abstract for many, this design proposal seeks to make the topic more relatable.

At a base level, conceptualization required a specific scenario to design for, where the framework for supporting data rights was established in some way. As there are many possible futures in this topic that are strongly tied to the infrastructure of data management, it was logical to establish a scenario by defining this infrastructure. Before describing the nature of how Instant works, some key points have to be defined.

7.1 X-Room: The foundation for ethical data management

The infrastructure to share data securely and privately already exists in Estonia in the form of X-Road. It allows the nation's public and private sector e-service information systems to connect and share data. With the current process of upgrading it to the more scalable X-Room, it has all the necessary functions that allow for the ethical and secure management of data:

A distributed network

It is a distributed network, meaning that data is kept in separate databases specific to an organization. When a service wishes to use another one's data, it is not moved out of that database, but accessed through X-Road. This ensures that personal data does not get duplicated or modified, and in the case of a security or ethical concern, this access can be revoked immediately. A distributed system cannot be easily hacked or its functioning disrupted.

Data portability through interoperability

Connecting to X-Room, means that an organization has to comply with specific format and security standards for storing and processing data. This enables a key element of

the GDPR: data portability. The access of data and its compatibility is not hindered by technical issues.

A digital trail

All data is digitally signed and encrypted, meaning it is trackable and documented. Since all the information systems within this infrastructure is compatible, it allows for automated oversight over the purpose and use of data.

A layered, scalable system

The architecture of this infrastructure enables the creation of a multitude of systems, such as AI assistants, working in parallel. The scalable nature of the system means its capacity for these systems is very high.

This system is currently implemented in many countries, mostly on a governmental level. This expansion continues as well, so extrapolating a situation from this where many countries have implemented X-Road as a central infrastructure for sharing data across the country not just for the government but private businesses as well, creates a scenario where the concept of ethical digital identity management can be explored. In this scenario the personal data is all owned by the data subject and it is kept in separate databases, but as the interoperability enables access and movement of this data, a new level of control can be given to people. Organizations outside this infrastructure have no access to the information within it.

Instant is a concept that aims to utilize this infrastructure to provide organizations with the necessary framework and assistance to handle personal data ethically and build new business models, and individuals with assistance and empowerment in controlling their digital identity and gaining value from their data. The concept consists of two parts, the Instant framework, meant to help businesses stay ethical and handle data and the Instant digital assistant, meant to assist people in controlling their digital identity.

To better explain how the system and its parts work the persona Toomas is used. He represents the regular person using the system. Toomas is primarily a mobile user. He has knowledge of personal data but usually agrees to all of the GDPR consent prompts, because it is too much to read and understand. Toomas uses a lot of digital services so his data footprint is quite vast. He values his digital privacy at a theoretical level, but has never been active in managing it. Before using instant, he did not consider personal data to be his digital identity.

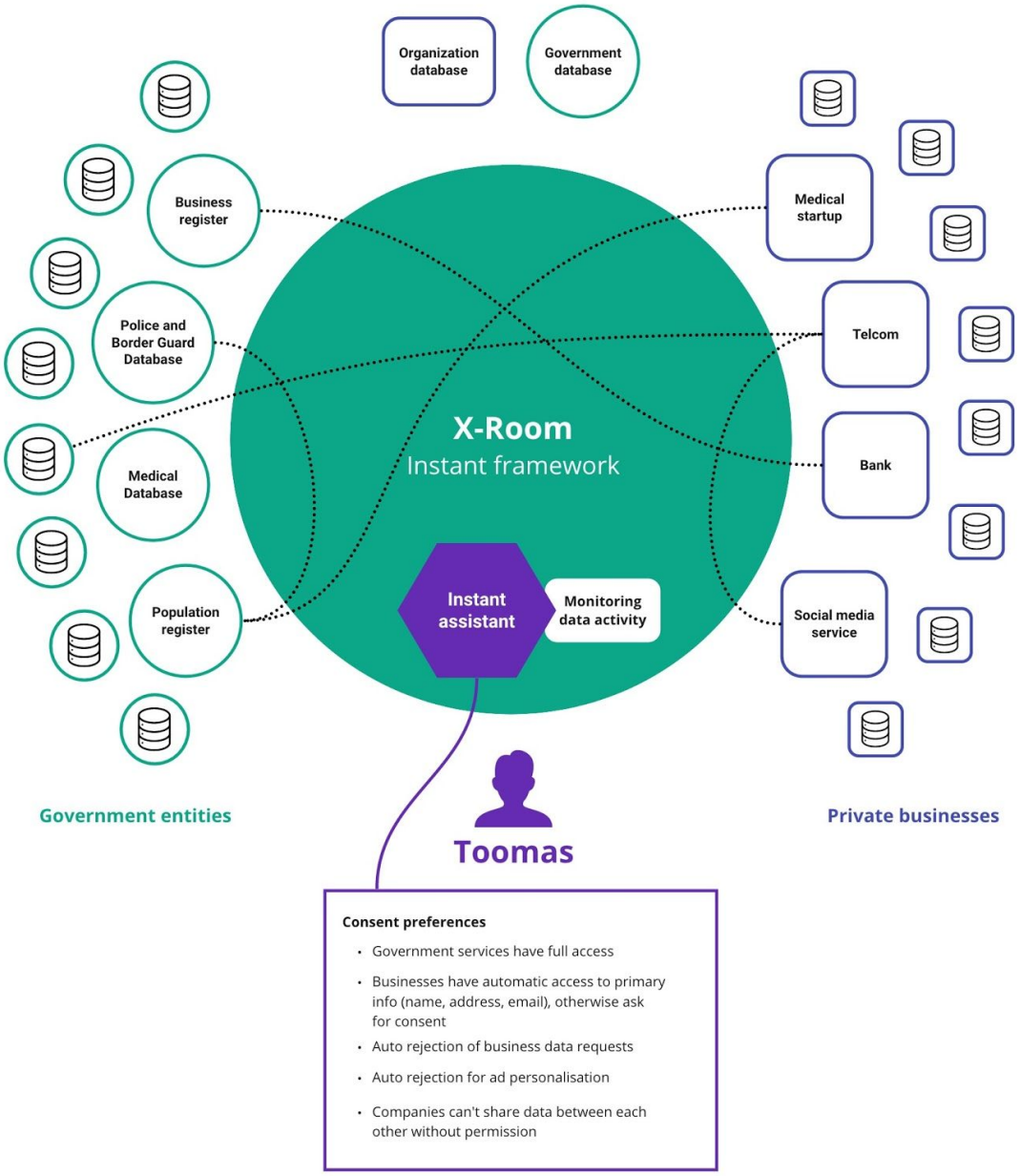


Figure 7.1 Instant framework scheme

To illustrate how this system works a system scheme was created that shows how the relationships and interactions between the key stakeholders in the system. In the middle is the X-Room, where the communication between organizations and individuals happens. For the sake of simplicity, the public sector databases are represented on the left and private sector databases on the right. The red square marks organizations or databases not connected to the infrastructure. At the bottom is an example of an individual connected to the system, in the form of Toomas. His consent preferences are listed as well. Within this infrastructure, the data handling is managed by Instant, which is represented as a framework for organizations and a personal assistant for individuals.

7.2 The Instant framework

Connecting to the infrastructure not only makes organizations comply with interoperability and security standards, but offers a host of benefits through the Instant framework. As organizations need motivation to operate at a high ethical standard, this has to be enabled and automated for them to make being part of the infrastructure worthwhile.

Complying with GDPR standards

On a base level, the framework automates the documentation and logging processes required by the GDPR. Whenever the organization accesses or processes data, Instant automatically creates a footprint of this that stores the purpose and use of the data. This ensures that there is always clear knowledge of that activity around personal data. This footprint is useful for the organization, but it also allows for automated oversight of data processing. If the data is accessed in a way that goes against the stated purpose, the framework is alerted and it notifies the data subject and other data controllers involved. Fast and action can be taken to protect the personal data involved.

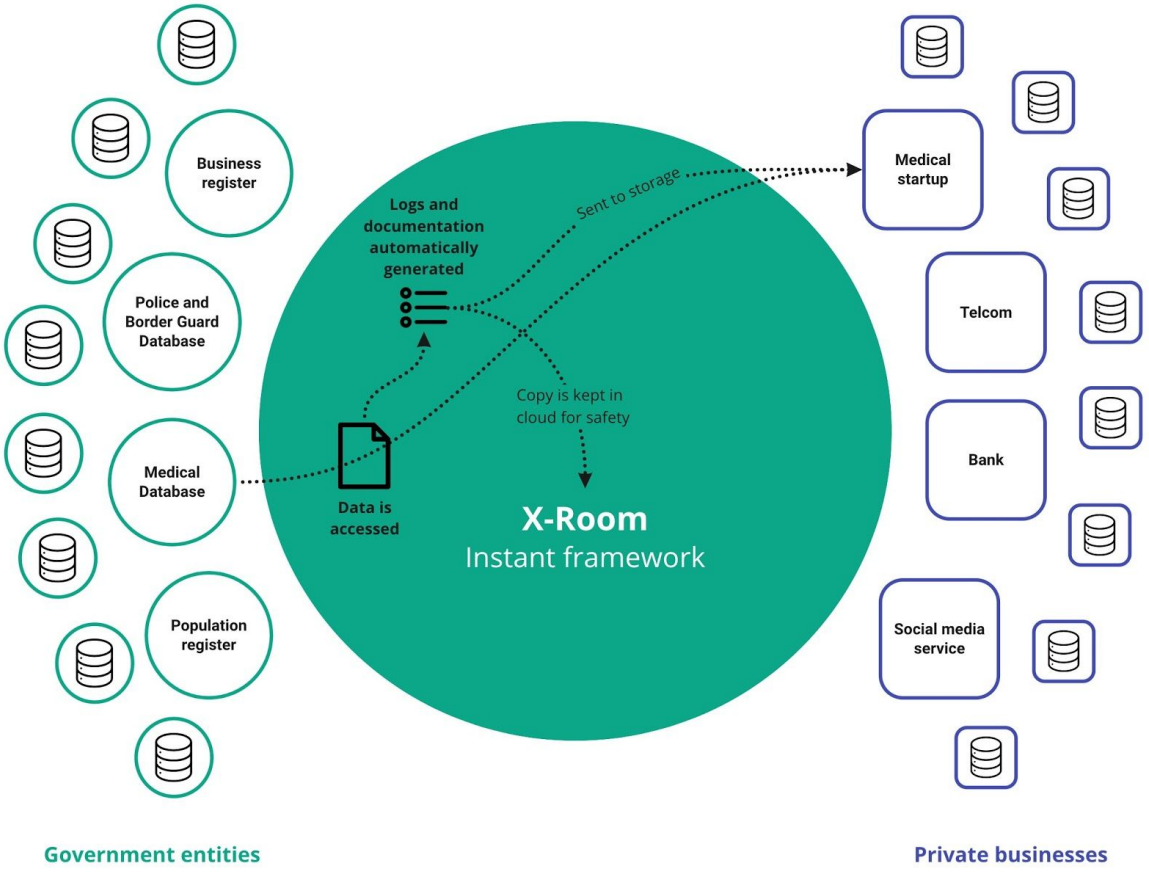


Figure 7.2 Instant framework automatic documentation scheme

High-quality data and freedom from storage

The standards enforced by the infrastructure and the help afforded by the Instant framework help keep data at a high-quality. For one, Instant helps remove old and irrelevant data from databases. Collaborating with the data subject, the accuracy of the data is kept in check, ensuring that databases only hold high-quality relevant data and there are no breaches of the GDPR by storing unnecessary personal data. Instant automates many of these processes, so the people running the organization do not have to dedicate human resources to this end.

Instant works to help organizations comply with the six parameters of data quality: accuracy, completeness, uniqueness, validity, timeliness and consistency. High-quality data is highly beneficial for organizations, as analyzing it ensures insights that are relevant to the real-world situation and represent the data subject in an accurate way.

This distributed and decentralized network also helps keep all the separate databases in order. Organizations do not have to worry about keeping all data up-to-date, only specific items stored in their database. This also means savings on the cost of storage and a more sustainable model of databases. Storing high-volumes of data requires many servers either physically or cloud-based. Removing this need, frees up financial resources that can be directed elsewhere. These factors motivate organizations to comply with ethical standards, as it becomes more financially viable for them.

Access to large amounts of data

The instant framework does not just ensure the quality of the organization's own data, but enables access to the data of other organizations and the government as well. This data sharing economy is a stark departure from the monopolizing of data that is happening currently. By giving the option to organizations to securely access and share their data and insights generated (with the permission of the data subject), the quality of new analyses and the depth of insights increases. Access to public sector data, means that high-quality medical data can be used to create beneficial services for people. Basic details about a person such as their name, birthday and email are accessible and always up-to-date, reducing the misrepresentation of people by organizations.

This access gives organizations a new data based model of cooperation as well, that is hard to have without the infrastructure or framework. Giving organizations (and governmental bodies as well) the tools to work together and produce value leads to less unethical handling of personal data, which is often tied to keeping a tight hold on

market share. If sharing and collaborating with others produces more value than hoarding and secrecy, then there is no reason to risk data breaches and paying upkeep for endless amounts of storage.

Equal opportunity for smaller companies

While still being beneficial for large corporations, the framework helps equalize the market power between large and small companies. Currently, large corporations have the most capability for gathering and processing large amounts of personal data, thus they have an advantage in this regard. They also have the budget and human resources to be GDPR compliant (for the most part) on their own, something which is not easy for small companies.

In the Instant framework, small businesses now have access to as much high-quality data as large corporations and can leverage their more agile nature to create new beneficial services for people. Trustworthy, high-value services, offered by relatable small businesses can compete with large corporations in this infrastructure and they can leverage their knowledge and expertise to even form ethical partnerships with the corporations.

7.3 New opportunities for business models

As the infrastructure and Instant framework enable new ethical ways of using data and collaborating, I devised some examples of possible new business models and partnerships and illustrated these through the system scheme.

7.3.1 Financial data helper

Analysis and insight is what gives data its value. Often this is used to optimize the processes and business of organizations, but the new framework offers an opportunity to provide this service to individuals. One example is a business that would help people utilize their financial data to get the best deal or conditions for a loan or other financial transaction. Taking out a loan and getting good terms is not simple. The current situation is that an individual's bank has all their transaction information, credit history and other relevant information, but access to this personal data does not guarantee good terms or that the individual does not have to do manual work, by producing paperwork and working through layers of bureaucracy. If a person wishes to take out a loan from a different bank, this requires even more manual work, taking up valuable time.

In the scenario described in Appendix 1, the actor, Toomas, wishes to take out a loan, but does not want to deal with all the paperwork. He contacts a data helper business, which offers to help him if he gives them access to his relevant data. In this situation, Toomas forms a partnership with the business and gives them volition to access his data and act on his behalf. The business sets out to find the best deal for Toomas according to the needs he has expressed. The benefit for Toomas is that the data helper business has a high capacity for analysis specifically configured for this field. They have tools to understand what the best deal in the current financial situation could be and what is needed to get it. The same powerful algorithms used to optimize systems to work as efficiently as possible can be used to benefit individuals through the same type of hyper-optimization.

The business anonymizes Toomas' analyzed data and compiles requests that are sent to different banks. After receiving the offers from the banks, the business analyzes these as well to figure out which is the most optimal to take, or if needed, negotiate more with the bank. The anonymous approach enables people to do hypothetical checks from different banks, without leaving a trail that this specific person was looking for a loan.

The business sends Toomas the best loan offers and gives him suggestions on how to proceed. After their partnership is concluded, Toomas revokes access to his personal data from the data helper business. None of Toomas' personal data is left in the hands of the business, only the analysis, which he can also move out of their storage to somewhere else if he wishes.

7.3.2 Collaborative model

Data and analysis based collaboration is enabled by the Instant framework. The COVID-19 pandemic of spring 2020 has presented a host of new challenges for society as people have to consciously keep away from each other to avoid the spread of the virus. The Instant framework offers an opportunity here to track the spread of the virus and the most dangerous areas through collaboration and data sharing between multiple organizations and the use of a large quality of location specific personal data.

The model is described visually in Appendix 2.

A organization that deals in predictive analytics sends out a request for data through the Instant framework including: location data, home and workplace, age, specific illnesses and confirmed cases. All of these are located in different databases, with location data being stored by telecommunications companies, demographic info stored by the government and medical data, personal and general, stored by the medical system. Without the framework, getting access to all of this data would be extremely difficult, but the Instant framework enables sending requests for all of these and the interoperability ensures that it is usable.

Toomas is approached with requests for his data. The government supports this endeavor so it officially endorses the request, making the decision to consent simple for Toomas. The organization commences building a prediction model of the virus' spread. As more people give consent for processing their data, the model becomes more accurate. This model is handed to a developer, who makes a visualization of said model, which can be seen by people and the Instant assistant can use it to inform Toomas of risks. By selling access to this model, different businesses such as supermarkets, banks, social services and so on, can predict how it is going to affect them as well, potentially building new layers of services on top of it.

7.3.3 Other opportunities

There are other opportunities as well, for example, cooperation between institutions, where institutions can build upon each other's work and analysis, using each other's data to optimize and research further. Data visualizations are growing ever more critical as the complexity of the data grows. Businesses based on building visualizations using other's analyses would provide benefits to organizations in the form of more presentable and easily understood analytics. The process of visualization could generate new insights, as well.

Access to high-quality personal data means that researchers and organizations can work together with people that have highly specific profiles. This can make research faster and more accurate while allowing organizations to create many small micro-targeted services meant for specific niches.

Many societal opportunities are also available as high-quality data from specific regions or cities can be used to predict public transport needs.

7.4 Instant Digital Assistant

The infrastructure is designed to empower people to take control of their digital identities and have ways to make sure that the way their data is used is in line with their values. As huge quantities of data are hard to analyze for people themselves, the Instant framework provides a digital assistant service that helps them with managing their data. The assistant works in line with the principles stated before and is designed to respect the autonomy and capabilities of the human it serves.

The digital assistant works on two levels: it exists within the X-Room as an entity that keeps watch over all the processing of a particular individual's personal data and also works as a layer in all of the devices the person uses to communicate and assist the individual on-demand.

It is designed to proactively communicate with people, but only at a time that both parties have agreed to. It does not interrupt the person's life with notifications at all times, respecting social norms. Instant is designed to be highly capable of analysis and works to understand the online behavior of the person it assists, to help them set better rules in regard to their personal data use. As the quality of data is important both to the functioning of the infrastructure and the digital identity of the person, Instant assists in conducting digital hygiene, keeping the individual's personal data free of errors. It automates the process of giving and revoking consent by analysing the content of the data request from the organization and providing the actor with relevant information. Instant does not present its analysis as the absolute truth, it is always emphasized that the final responsibility lies with the person. Since the assistant monitors all processing of an individual's personal data, it acts as its guardian and immediately informs in case of misuse or suspicious circumstances. It is what guarantees the ethical use of their data to the individual.

Instant is contextual and thus can be accessed through all devices as a layer running on top of the other applications or through a dashboard for more detailed data management.

The goal of the Instant digital assistant is to also highlight the value of personal data and how using it can benefit the individual or society. Data should be kept in use in an ethical way and this requires people to be aware of the benefits and opportunities they have.

7.4.1 Introducing the system

A big issue regarding control over digital identities is that people lack interest in it and do not feel as if they are the owners of their personal data. Some may feel that their privacy is at risk or that they are being manipulated, but remain ambivalent, as they do not know how to interface with the abstract complexity of data. It is unreasonable to expect people to start caring about it and taking responsibility overnight when introducing an assistant to help them. A shift in mindset needs to be brought about deliberately.

The onboarding process of Instant is designed to push people into action. It does so in a controlled environment by creating negative emotions, but also providing immediate ways to take action to improve the situation. Showing people that they do have a way to exercise their will and autonomy creates a positive connection with the digital assistant and the idea of managing personal data.

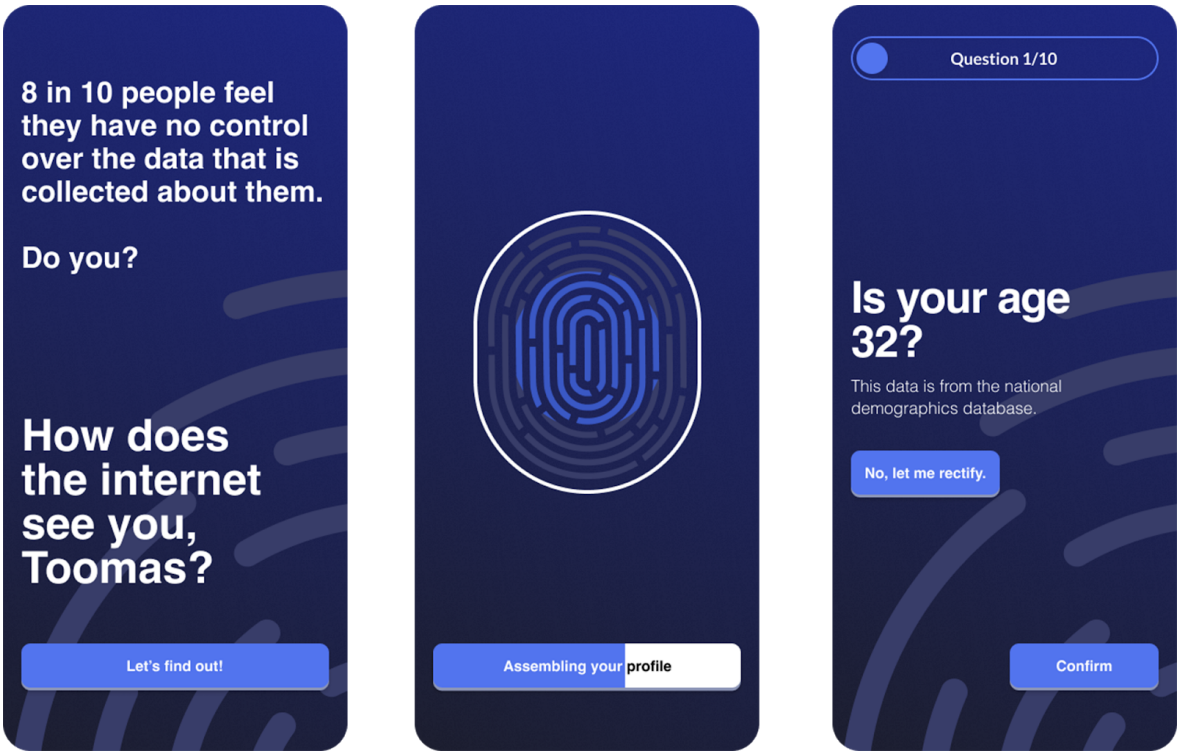


Figure 7.3 Instant assistant onboarding

The service is accessed through using a valid ID as the system has to confirm the identity before giving access to personal data. The first time when logging in, the assistant provokes the person by offering an analysis of the quality of their digital identity. Upon agreeing, it creates a presentation of the person's data, in this example, Toomas. Before continuing, if there are some data items Instant is unsure of, it asks to confirm the validity of those.

It then presents the person with their analysis. In Toomas' case, many aspects of his digital identity are plagued by inaccurate data. The system shows that many services perceive him to be 62 years old, even though he is 32. Per every inaccuracy, the possible consequences of it are also shown. For example, with the inaccuracy of the age, the consequence is wildly off-target advertisements online. Other examples, such as being misrepresented as having type 2 diabetes, have resulted in him being denied life insurance. Other facts brought to attention are the number of accounts on different services, the amount of organizations using the personal data currently, the number of mailing lists subscribed to, or marketing databases with the personal data.

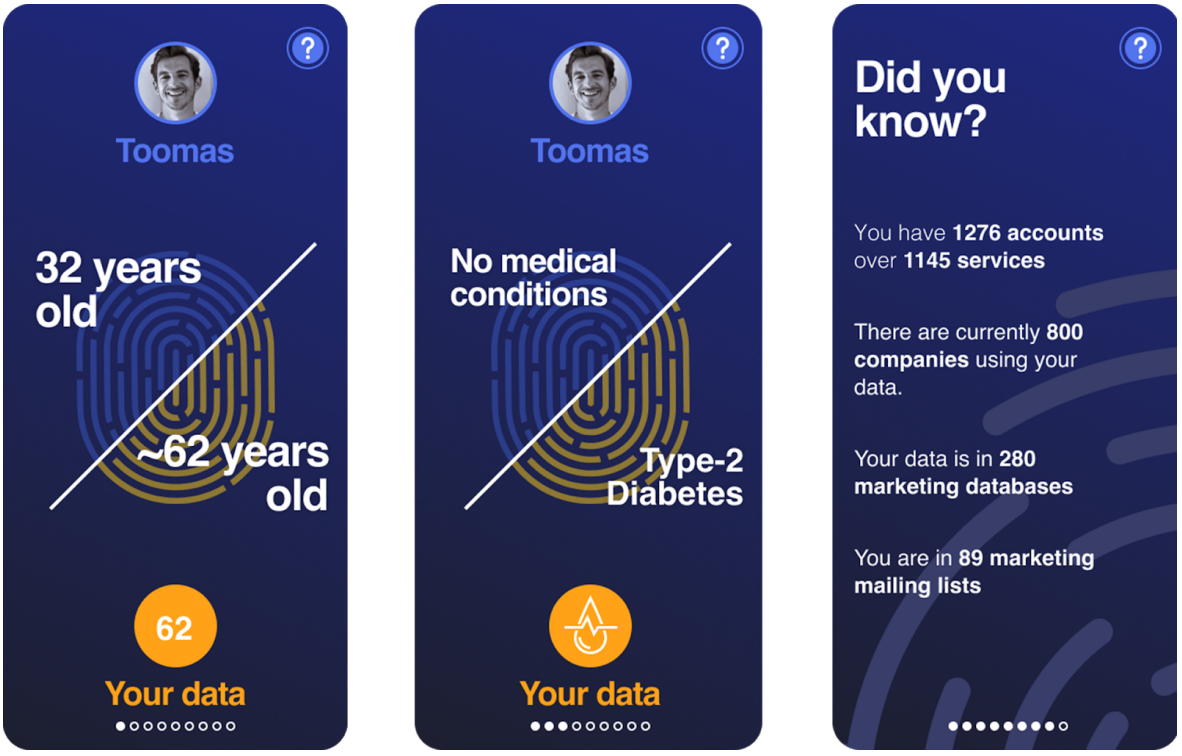
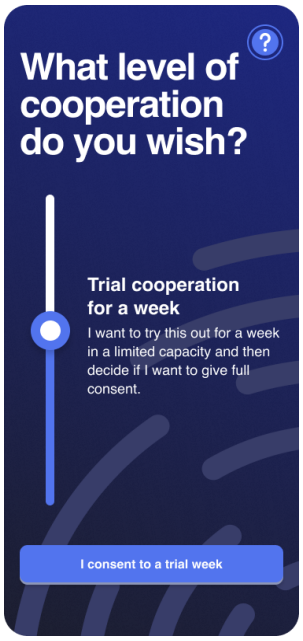


Figure 7.4 Instant assistant personal data analysis

Figure 7.5 Instant assistant data score

The goal here is to create moments of disturbance and reflection as to how the digital identity has been breached and used for things outside of the person's values. At the end of the demonstration, a score is given for the accuracy of the digital identity. This gives people a metric to understand the state of the digital identity better. It is based on the number of inaccuracies in the data and how regularly it is maintained. Near the end, Instant introduces what rights there are regarding data, and articulates how it can help maintain these rights and consistent digital identity.



Instant operates on the idea of respect for individuals and social norms. Thus it aims to match the person's expectations and needs in collaboration and communication. It prompts Toomas for what level of cooperation he wishes for. The choice in the level of cooperation is granular and also leaves people with the option to opt-out and seek alternatives to Instant as well. When it comes to communication, the assistant follows the principle of respecting people's time and seeks an agreement with the person on when to communicate, offering them some options to start. The full onboarding flow is available in Appendix 4.

Figure 7.6 Instant assistant cooperation view

7.4.2 Management of consent

Consent management is a vital part of Instant. The GDPR requires people to be fully aware of how their data is processed and for what purpose. The consent has to be unambiguous, freely given, and informed. The difficulty currently is that the terms and conditions and other explanatory texts are hard to comprehend. Furthermore, the varying designs of the consent prompts require too much effort from people to understand and leave people open to being manipulated, as the design can nudge them towards a specific decision. Revoking consent and removing personal data is, in many cases, challenging, sometimes needing a form to be sent via e-mail. The often-used binary choice of accepting or disagreeing does not leave much room for people to act autonomously.

Instant works to consolidate the consent related actions into a single point of contact, with a consistent design and logic. It also offers people a host of tools that they can use to understand and lessen the burden of managing their data.

Consent automation
The Instant assistant provides a way to automate consent through setting rules and thresholds. Managing consent for every digital service is too much to handle for people, as seen by the ineffectiveness of the current GDPR prompt.

The rules are set based on the type of personal data and the nature of the processing. For example, advertising is something that websites commonly gather data for, but many people do not appreciate the personalized advertisements they are shown as they tend to be either too accurate or irrelevant. In this case, people can set rules that say that news websites can only gather the most basic necessary info, but have no collection rights outside this.

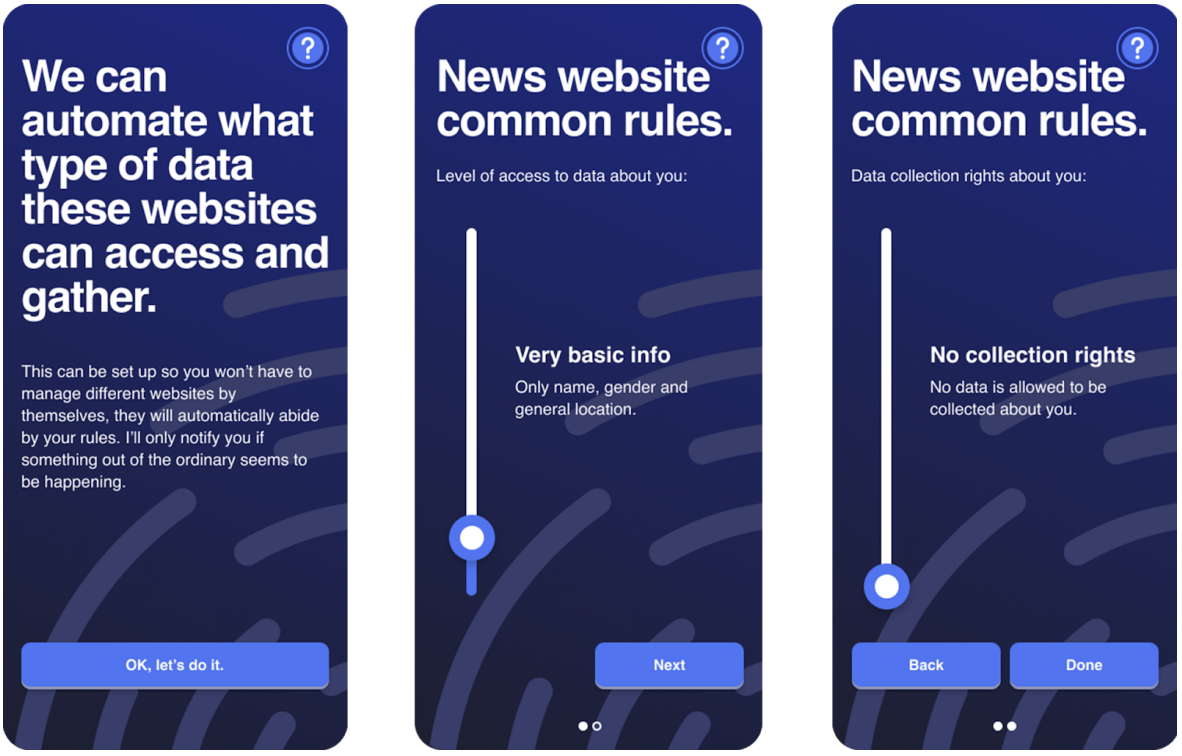


Figure 7.7 Instant assistant setting rules

Since Instant sees how the person's data is used, it can give suggestions based on this. Instant knows from Toomas' activity that he tends to agree to all GDPR notices on news websites, setting his digital identity at risk, thus it proactively offers to set some basic rules for these websites so that Toomas' data is protected. Furthermore, as now the rules for news websites are set, Instant revokes access from all the news websites that had access before and removes personal data from them they should not have, automating this process as well.

Levels of consent

Instant provides a more granular way of giving consent. Instead of the all or nothing approach most services use in the current day, using checkboxes, binary buttons, or toggle elements, Instant works by providing control over thresholds. At a lower threshold, only primary information is given out. The system only notifies the person if giving more access would provide them a benefit or if the current threshold would

potentially compromise the privacy and ethical use of the personal data. Consent is fluid, giving people more nuanced decision-making capability.

In this example, per the agreement between Toomas and Instant, the assistant prompts him at their agreed time with a data request from a medical startup, which wishes to use Toomas' cardiovascular data. Instant provides Toomas with an analysis of the request, which Toomas can study and prompts him to make a decision. There is also always the option to dismiss a request. In the decision view, Toomas can choose on a scale of how much he wishes to cooperate, in this case, deciding for a trial cooperation for two weeks. In this case, he can see what sort of practical value they will provide and will decide further once the trial is done.

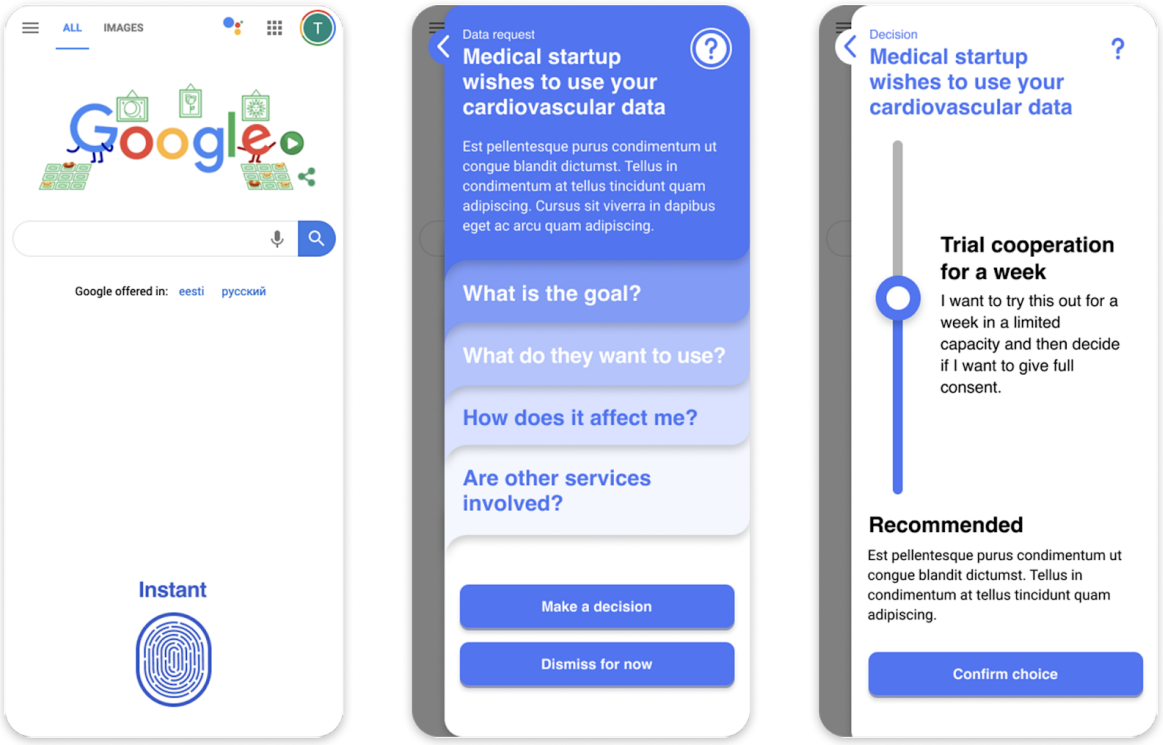


Figure 7.8 Instant assistant proactive prompt

The assistant would provide suggestions on how to decide when presenting a choice, as many people might have a hard time making a judgment call on what is most beneficial to them and their values in a data-related situation. The goal is not to decide for the person, but to give them some indication of the most beneficial outcome and the potential other outcomes. The system view of this can be seen in Appendix 3 and the full user interface flow can be seen in Appendix 6.

Contextual analysis and query interaction

The digital assistant can contextually and dynamically analyze content on-demand. This is necessary to give people a way to get information without searching through pre-made documents, in the hopes of finding an answer. Instant does not offer users binary choices in what people can know more about, but procedural and contextual analysis provides relevant information about anything the person asks about. This gives the person as much information as they need. It also enables interacting with elements on services that use personal data, for example, personalized advertisements. This feature is especially important because the digital assistant is not presented as an all-knowing entity, but rather something that should be questioned. The responsibility for making the final decisions lies with the owner of the data.

The querying works using a new type of interaction where all parts of the interface can be queried through a draggable element. This element either sits in the corner of the screen or can be summoned using a gesture, then dragged on the element or text the person wishes to have analyzed. Querying has no limits on how deep it can go, as the point is to give people as much flexibility as they wish.

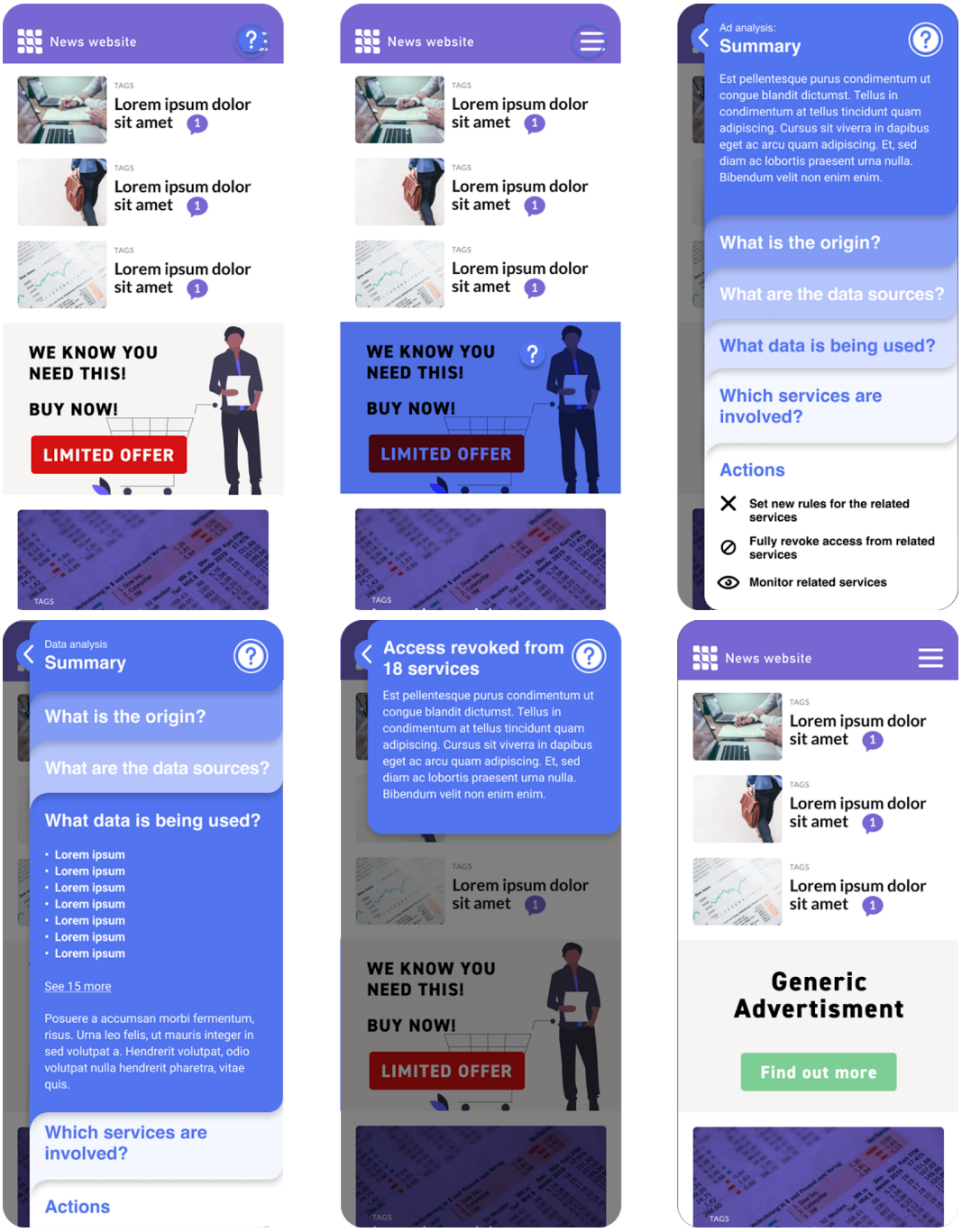


Figure 7.9 Using the Instant assistant proactively

For example, Toomas sees an oddly specific advertisement and wishes to know where this information is from and stop seeing advertisements like this. For this, he uses the query interaction on it, and Instant gathers up all the data that is informing the advertisement, its source and content, analyses it, and presents it to Toomas. As this data is deemed by Toomas to be too personal and dangerous in the hands of these services, he decides to entirely revoke access from all 18 services who are using it. The personalized advertisement, as a result, becomes generic. The full interface flow can be seen in Appendix 5.

Contextual prediction of benefits

The system would give contextual predictions on how the experience would change to give people a better understanding of how giving access to their data changes their experience or benefits them. A simple example is agreeing to share data with a news website would enable them to provide personalized advertisements. The system could predict, based on the providers, which kinds of advertisements the person would get from the website. It would also warn about how the data would be analyzed and highlight potential unethical use.

7.4.3 Enabling proactive creation of value

Managing consent and how services can use personal data is a vital part of the value of Instant. However, for people to feel like they are the owners of their data, they need to be able to generate value from it themselves proactively. This can be done in many ways.

Benefiting from data

The digital assistant enables people to exercise their right to data portability. This means actors can easily move their data between services. For example, if a person wishes to change their bank, they can move all of their financial and personal data to that bank. People can also actively offer their data to different services, in exchange for benefits or a better experience. An important factor is creating societal value from data as well. As data is more valuable in larger quantities, people can give access to their data to services like public transport for optimizing routes. Genetic data can be used to predict which types of conditions the hospitals should equip themselves to handle.

Keeping data up to date

Part of proactively keeping personal data valuable is dealing with its quality, meaning it is up-to-date and accurate. The digital assistant monitors changes or discrepancies in data and confirms these with the owner. In this scenario, the government and organizations benefit from having up-to-date data to use, and people benefit by having the personalization of their experience be accurate and tied to who they actually are because their digital identity reflects them accurately. This quality is reflected in the personal data score that helps people understand the state of their data in this regard and benefits organizations, as they can specifically reach out to people who keep their data at a high-quality. With high-quality data, people have more opportunities to benefit from it, thus offering an incentive to manage it.

7.5 Validation

The concept was tested and validated in many stages of its development, starting from the first ideas. This was a complicated process, as the COVID-19 quarantine of spring 2020 meant that most of it had to be done online, at a distance. The validation happened in many forms, from conversations about concepts and ideas to showing prototypes and content. As the issue is complex, there were many questions around this concept, particularly about the technical aspects and how it would promote ethics. This prompted further development of the ethical aspects, although some of the technical questions were difficult to incorporate as they would have required developing specific system architecture schemes, something outside the scope of this thesis.

The assistant was adjusted multiple times as its design was not engaging enough and in the early stages unclear in its operation. The underlying issue was relying on standard UX practices to design it, thus reaching a similar output to other interfaces. This feedback was also one of the reasons that the critical analysis of UX design was conducted as this allowed for new principles to be created for the design process. In the conversations, an understanding of how disconnected people are from the ownership of their data was also apparent, giving structure to the final concept in this aspect.

A desire for a way to sell data was expressed, but this is something that was not incorporated into the concept, because of ethical concerns that could not be resolved in a reasonable amount of time.

An alternative validation approach was also used in the form of undesign, where the most utopian and most dystopian outcomes of the concept were explored to understand what would influence the concept to develop in either direction.

Utopian scenario

In the utopian future, all organizations and governments have their own national X-Room infrastructure, which is connected to the other countries' X-Room infrastructures. Concrete ethical standards for processing personal data exist, and organizations fully comply with these. Their business models are focused on providing solutions that ethically benefit people and society. The high-quality data and lessened costs from bureaucracy and upkeep of servers and management software allow them to be more financially successful. The people feel ownership of their data and actively

participate in managing and generating value from it by keeping their data high-quality and carefully choosing how to use it.

Dystopian scenario

In the dystopian future, the X-Room infrastructure becomes a data marketplace that is eventually bought out and privatized by an enormous technology corporation. The assistant is focused on the full automatization of giving consent, going back to the "simple, comfortable, and fast" rules of UX design. Users are given money in exchange for sharing their data, and the entire system is geared to have people agree to this. People have been further distanced from their personal data, focusing only on the monetary benefit of sharing it but losing their values in the process. Its use is unknown to them, and they lack interest as they are making money (even if it is a fraction of what it actually is worth). The attention economy has taken a new shape.

7.6 Opportunities for further research

In some respects, this topic of personal data management has been extensively researched, but not at all in others. Much has been written about the technical aspects of the topic and the organizational and business impact, but the human aspects of it, like the idea of ownership, are less explored. In this thesis, I analyzed many aspects of the idea of ownership and the psychological aspects of data management, including the feeling of empowerment, but further research into these aspects is required. As I approached this topic from the perspective of a designer, the work led me to study it through that framing as well. Looking at these issues with different framing would produce new knowledge necessary to bring about a better future.

The idea of a dashboard for data management was mentioned, but was not fully prototyped or tested, as the idea was complex to execute and other aspects of the concept needed development. There is definite value in exploring this idea further, as it is an essential access point for people to their personal data, but it requires extensive analysis before any practical design work can be done.

Selling personal data was also mentioned, and there is definite value in it because it is instantly relatable for people, and it does deserve further analysis. Currently, there are many ethical problems to solve, many of which are tied to the infrastructure and how to keep organizations within it operating ethically. There is also the question of the monetary value of personal data and how to define it.

Beyond this, the concept is not meant to be a complete solution to the entire issue of the attention economy and societal problems stemming from the digital world. The idea was to propose a specific way to make sure that digital identities are controlled by their owners. While providing alleviation, this does not solve the issue of social media and digital service addiction. The platforms may have less access to personal data, but the need for social validation and dopamine remains and keeps people vulnerable. These issues cannot be solved with tools or interfaces alone and require a societally conscious solution or broader strategy.

8 CONCLUSION

Currently, people are not in control of their digital identities. This is not for lack of rights as the GDPR has defined people as the owners of their personal data, which is what their digital identity consists of. Due to the abstract nature of the data and the lack of ways to express their rights, they do not feel ownership over it. The GDPR, while defining the people's rights, also states that the responsibility for ensuring these rights is on data controllers, the organizations that store the data. Understanding these aspects is critical to empowering people to be in control of their data, as they have to be given a way to feel responsible without overwhelming them. People have to be included in the process to feel like they are an equal part of the system.

Organizations currently do not handle data in an ethical and empowering way for individuals. This is due to a focus on amassing high volumes of data of varying quality and the difficulty in complying with GDPR standards. Organizations require an infrastructure for gathering and processing data that ensures interoperability and data portability. This is the foundation for an ethical framework, which gives businesses new opportunities to use data while enabling the automation of oversight tasks, such as documentation and logging.

Designing a tool or interface that empowers people to take control of their digital identity cannot be done by following user-centric UX design practices. This process focuses on making everything as smooth and simple as possible for the user. The result focuses more on the operational aspects of the experience (how does it work?) and fulfilling surface-level user needs than the meaning it is supposed to have in people's lives (what are we trying to create and why?) and their actual needs. I had to reevaluate the methods that I was using to design concepts and critically analyze the common UX design approach. I grew a lot in the process as I defined a new approach to UX design to empower users into actors and incorporated many methods that enable reflection and inversion of the common ways of working in UX.

The result of this work is a set of principles that work as a guide for people who wish to design an empowering data management or digital solution for people. The focus is on treating the person being designed for with respect, by making solutions that follow social norms, augment human capability, and do not promote blind trust.

The design concept Instant that was born from these principles is one example of the possible future of data management. Instant aims to include both individuals and

organizations as equals in data management and is based on the X-Room infrastructure that is in development in Estonia. It provides organizations with an ethical framework that allows them to use data in ways not possible before and automates oversight processes, while also ensuring they adhere to best practices and ethical standards. Organizations have access to high-quality data not just from individuals but also from other organizations, which creates opportunities for new business models to emerge.

Individuals are empowered by a digital assistant that helps them understand how their personal data is being used, its value, and how they can benefit from it. The assistant automates tedious tasks such as low consequence consent but gives people the tools they need to engage with their personal data through contextual query and analysis, prediction of the effect on their experience, and enabling proactive use of data. Through this, it includes people in controlling their personal data, giving them tools to exercise their rights, and act as the owners of it, thus enabling them to have a digital identity that reflects them as a person.

The work and the analysis contained within is one of the first visual concepts for how personal data management could look like from the individual's perspective. I hope the principles and ideas presented will inspire others to develop these ideas further and move towards a world where people and their identities are respected both in the physical and digital world.

9 SUMMARY

Individuals create a wealth of personal data that is collected and processed by different organizations. This data is a powerful resource that is currently being exploited to control people's attention. This attention economy has led to many adverse societal effects and thus requires active intervention. Efforts are being made through legislation and advocacy to enforce personal data rights, including the GDPR and initiatives by different organizations, but these focus on organizations and leave people feeling like they have no power and are not the true owners of their data. At the same time, organizations lack motivation and support to use data ethically, relying on design approaches that force their user into a passive role.

This issue was researched using a methodology based on empowering people to become active participants. Through interviews and studying the current situation, it was found that to bring meaningful change to the situation, individuals need to have a way to feel equal to organizations and to act as the owners of their personal data. This enables them to take responsibility and see its value, thus assuming control of their digital identity. At the same time, organizations need to be supported in the ethical handling of data, requiring an infrastructure that enables an ethical framework for data exchange to exist. Through conducting a critical analysis of UX design, principles for empowering people into active participants were defined, and they became the basis for the design concept.

The design concept Instant empowers organizations and individuals through a framework based on the X-Road architecture, enabling the safe and purposeful processing of personal data. Individuals control their digital identity with the help of a digital assistant within the framework, which analyses the use of their data, enforces their decisions regarding it, and keeps it accurate. For organizations, complying with ethical norms and regulations is simplified, creating opportunities for new business models that leverage the ethical use of high-quality personal data to emerge, providing benefits for both parties.

The goal of the concept was to provide an idea of what data management could look like for individuals, as there are already many technical infrastructure concepts to ensure data privacy. This concept is one possible solution to the issues of control over digital identities, as there are many possible futures for personal data management and the principals that were defined to guide it can be used to create alternative concepts that empower people.

10 TABLE OF FIGURES

11 LIST OF REFERENCES

1. Almeida Teixeira, G., Mira da Silva, M., & Pereira, R. (2019). The critical success factors of GDPR implementation: A systematic literature review. *Digital Policy, Regulation and Governance*, *21*(4), 402–418. https://doi.org/10.1108/DPRG-01-2019-0007

2. *Art. 25 GDPR - Data protection by design and by default*. (2018, November 14). GDPR.Eu. https://gdpr.eu/article-25-data-protection-by-design/

3. Askham, N., Cook, D., Doyle, M., Fereday, H., Gibson, M., Landbeck, U., Lee, R., Maynard, C., Palmer, G., & Schwarzenbach, J. (2013). *The Six Primary Dimensions for Data Quality Assessment*. 17.

4. Avle, S., Lindtner, S., & Williams, K. (2017). How Methods Make Designers. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, 472–483. https://doi.org/10.1145/3025453.3025864

5. Bang, A. L., Krogh, P. G., Ludvigsen, M., & Markussen, T. (2012). *The Role of Hypothesis in Constructive Design Research*.

6. Benford, S., Greenhalgh, C., Giannachi, G., Walker, B., Marshall, J., & Rodden, T. (2012). Uncomfortable interactions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2005–2014. https://doi.org/10.1145/2207676.2208347

7. Berghel, H. (2018). Malice Domestic: The Cambridge Analytica Dystopia. *Computer*, *51*(5), 84–89. https://doi.org/10.1109/MC.2018.2381135

8. Bozdag, E. (2018). *Data Portability Under GDPR: Technical Challenges* (SSRN Scholarly Paper ID 3111866). Social Science Research Network. https://doi.org/10.2139/ssrn.3111866

9. Carr, N. (2011). *The Shallows: What the Internet Is Doing to Our Brains*. W. W. Norton & Company.

10. Case, A. (2016). *Calm Technology: Principles and Patterns for Non-Intrusive Design* (1 edition). O'Reilly Media.

11. *Center for Humane Technology: Realigning Technology with Humanity*. (n.d.). Center for Humane Technology. Retrieved January 14, 2020, from https://humanetech.com/

12. *Chapter 3 (Art. 12-23) Archives*. (n.d.). GDPR.Eu. Retrieved May 9, 2020, from https://gdpr.eu/tag/chapter-3/

13. Cox, A., Gould, S., Cecchinato, M., Iacovides, I., & Renfree, I. (2016). Design Frictions for Mindful Interactions: The Case for Microboundaries. *In: CHI EA '16 Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems. (Pp. Pp. 1389-1397). ACM: New York*. http://discovery.ucl.ac.uk/1475258/1/Design%20Frictions_CHI2016LBW_v18.camera.ready.pdf

14. *Data Broker*. (n.d.). Gartner. Retrieved May 14, 2020, from https://www.gartner.com/en/information-technology/glossary/data-broker

15. *Declaration – MyData.org*. (n.d.). Retrieved May 13, 2020, from https://mydata.org/declaration/

16. Experience, W. L. in R.-B. U. (n.d.-a). *The Attention Economy*. Nielsen Norman Group. Retrieved January 14, 2020, from https://www.nngroup.com/articles/attention-economy/

17. Experience, W. L. in R.-B. U. (n.d.-b). *The Definition of User Experience (UX)*. Nielsen Norman Group. Retrieved April 19, 2020, from https://www.nngroup.com/articles/definition-user-experience/

18. *Facebook users in U.S.* (n.d.). Statista. Retrieved May 22, 2020, from https://www.statista.com/statistics/408971/number-of-us-facebook-users/

19. Fair data economy. (n.d.). *Sitra*. Retrieved May 12, 2020, from https://www.sitra.fi/en/topics/fair-data-economy/

20. Fokkinga, S., & Desmet, P. M. A. (2013). *Ten ways to design for disgust, sadness, and other enjoyments: A design approach to enrich product experiences with negative emotions*. https://www.semanticscholar.org/paper/Ten-ways-to-design-for-disgust%2C-sadness%2C-and-other-Fokkinga-Desmet/44811ef0e051e937440801dee6c3f099aa389d34

21. *GDPR Enforcement Tracker—List of GDPR fines*. (n.d.). Retrieved May 10, 2020, from http://www.enforcementtracker.com

22. *General Data Protection Regulation (GDPR) – Official Legal Text*. (n.d.). General Data Protection Regulation (GDPR). Retrieved May 9, 2020, from https://gdpr-info.eu/

23. Gray, C. M., Kou, Y., Battles, B., Hoggatt, J., & Toombs, A. L. (2018). The Dark (Patterns) Side of UX Design. *Proceedings of the 2018 CHI Conference on*

Human Factors in Computing Systems - CHI '18, 1–14. https://doi.org/10.1145/3173574.3174108

24. Hadoop Is Data's Darling For A Reason. (2016, January 22). *Forrester*. https://go.forrester.com/blogs/hadoop-is-datas-darling-for-a-reason/

25. Halenius, L., Hofheinz, P., Kalliola, M., Lepczynski, S., Mitta, C., Moise, C., Sinipuro, J., & Suokas, J. (n.d.). *A Roadmap for a Fair Data Economy*. 58.

26. Harris, T. L., & Wyndham, J. M. (2015). Data Rights and Responsibilities: A Human Rights Perspective on Data Sharing. *Journal of Empirical Research on Human Research Ethics*, *10*(3), 334–337. https://doi.org/10.1177/1556264615591558

27. Hasan, A. (2018). Dark Data for Analytics. In M. Ahmed & A.-S. K. Pathan (Eds.), *Data Analytics* (1st ed., pp. 275–293). CRC Press. https://doi.org/10.1201/9780429446177-11

28. *How to Choose the Right UX Metrics for Your Product*. (n.d.). Retrieved April 22, 2020, from https://www.dtelepathy.com/ux-metrics/#happiness

29. *Ideepaber*. (n.d.). Krattide veebileht. Retrieved May 19, 2020, from https://www.kratid.ee/ideepaber

30. IHAN – proof of concept pilots. (n.d.). *Sitra*. Retrieved January 14, 2020, from https://www.sitra.fi/en/projects/ihan-proof-concept-pilots/

31. Kaevats, M. (2020, March 10). [Personal interview].

32. Kala, K. (2020, March 20). [Digital personal interview].

33. Langford, J. (n.d.). *Understanding MyData Operators*. 40.

34. Lanier, J. (2018). *Ten Arguments for Deleting Your Social Media Accounts Right Now*. Henry Holt and Co.

35. *Ledger of Harms*. (n.d.). Retrieved May 13, 2020, from https://ledger.humanetech.com/

36. Leetaru, K. (n.d.). *The Data Brokers So Powerful Even Facebook Bought Their Data—But They Got Me Wildly Wrong*. Forbes. Retrieved April 3, 2020, from https://www.forbes.com/sites/kalevleetaru/2018/04/05/the-data-brokers-so-powerful-even-facebook-bought-their-data-but-they-got-me-wildly-wrong/

37. Lewis, P. (2017, October 6). "Our minds can be hijacked": The tech insiders who fear a smartphone dystopia. *The Guardian*.

https://www.theguardian.com/technology/2017/oct/05/smartphone-addiction-silicon-valley-dystopia

38. Luoma-Kyyny, J. (2020, March 10). [Email interview].

39. Mällo, T. (2020, March 20). [Digital personal interview].

40. Montalan, B., Boitout, A., Veujoz, M., Leleu, A., Germain, R., Personnaz, B., Lalonde, R., & Rebaï, M. (2011). Social identity-based motivation modulates attention bias toward negative information: An event-related brain potential study. *Socioaffective Neuroscience & Psychology*, *1*. https://doi.org/10.3402/snp.v1i0.5892

41. Monteiro, M. (2019). *Ruined by design: How designers destroyed the world, andwhat we can do to fix it*. Independently published.

42. Murgia, M., & Ram, A. (2019, January 8). *Data brokers: Regulators try to rein in the 'privacy deathstars.'* https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521

43. *MyData.org – Make it happen, make it right!* (n.d.). Retrieved May 12, 2020, from https://mydata.org/

44. Nagle, T., Redman, T., & Sammon, D. (2020). Assessing data quality: A managerial call to action. *Business Horizons*, *63*(3), 325–337. https://doi.org/10.1016/j.bushor.2020.01.006

45. Nelson, H. G., & Stolterman, E. (2012). *The Design Way: Intentional Change in an Unpredictable World*. The MIT Press.

46. Norman, D., & Verganti, R. (2014). Incremental and Radical Innovation: Design Research vs. Technology and Meaning Change. *Design Issues*, *30*, 78–96. https://doi.org/10.1162/DESI_a_00250

47. Nuccio, M., & Guerzoni, M. (2019). Big data: Hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change*, *23*(3), 312–328. https://doi.org/10.1177/1024529418816525

48. Odell, J. (2019). *How to Do Nothing: Resisting the Attention Economy*. Melville House.

49. Pierce, J. (2014). *Undesigning interaction*. Association for Computing Machinery. https://doi.org/10.1145/2626373

50. Poikola, A., Kuikkaniemi, K., & Honko, H. (n.d.). *A Nordic Model for human-centered*. 12.

51. *Poll: Americans give social media a clear thumbs-down*. (n.d.). NBC News. Retrieved May 22, 2020, from https://www.nbcnews.com/politics/meet-the-press/poll-americans-give-social-media-clear-thumbs-down-n991086

52. Read, M. (2018, December 26). *How Much of the Internet Is Fake?* Intelligencer. http://nymag.com/intelligencer/2018/12/how-much-of-the-internet-is-fake.html

53. Reinsel, D., Gantz, J., & Rydning, J. (2018). *The Digitization of the World from Edge to Core*. 28.

54. Shilton, K. (2018). Values and Ethics in Human-Computer Interaction. *Foundations and Trends® in Human–Computer Interaction*, *12*(2), 107–171. https://doi.org/10.1561/1100000073

55. Sitra, T. F. I. F. (n.d.). *What is Fair Data Economy?* Retrieved May 12, 2020, from https://data-economy.sitra.fi

56. *Streamr*. (n.d.). Retrieved May 19, 2020, from https://streamr.network/

57. Sumida, N., Walker, M., & Mitchell, A. (2019, April 23). 3. The role of social media in news. *Pew Research Center's Journalism Project*. https://www.journalism.org/2019/04/23/the-role-of-social-media-in-news/

58. *The principles*. (2020, April 30). ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

59. *UBDI - Universal Basic Data Income*. (n.d.). Retrieved May 19, 2020, from https://www.ubdi.com/

60. Velsberg, O. (2020, April 6). [Digital personal interview].

61. Weiser, M., & Brown, J. S. (n.d.). *Designing Calm Technology*. 5.

62. *What is GDPR, the EU's new data protection law?* (2018, November 7). GDPR.Eu. https://gdpr.eu/what-is-gdpr/

63. What metrics and KPIs do the experts use to measure UX effectiveness? (2019, May 28). *UserZoom*. https://www.userzoom.com/blog/what-metrics-do-the-experts-use-to-measure-ux-effectiveness/

64. Winnick, M. (n.d.). *Putting a Finger on Our Phone Obsession*. Retrieved January 14, 2020, from https://blog.dscout.com/mobile-touches

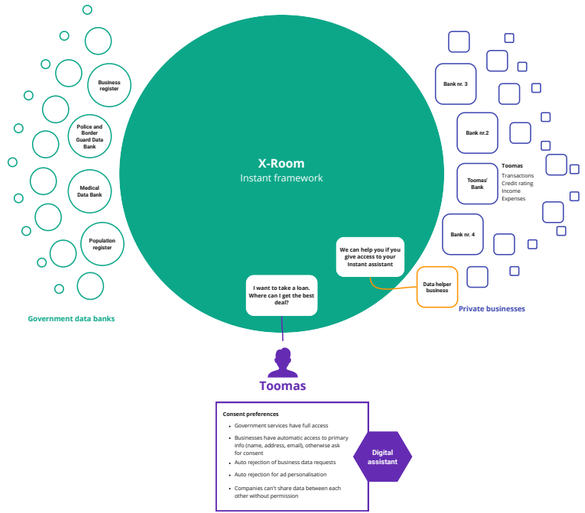
65. *World Internet Users Statistics and 2019 World Population Stats*. (n.d.). Retrieved January 14, 2020, from https://www.internetworldstats.com/stats.htm

66. Yablonski, J. (n.d.). *Home | Laws of UX*. Retrieved April 19, 2020, from https://lawsofux.com

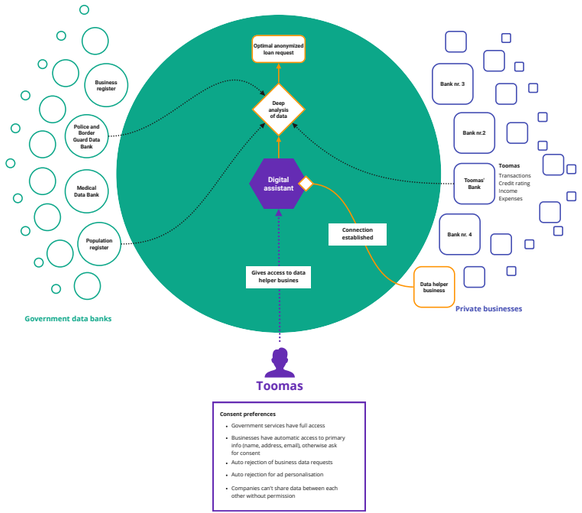
12 APPENDICES

Appendix 1: Data helper business model

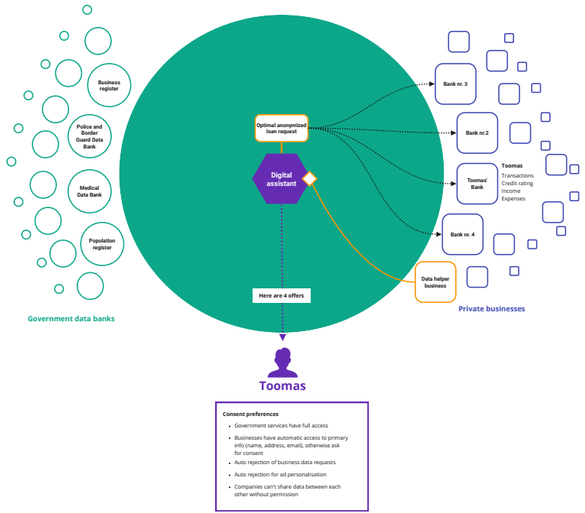
1.



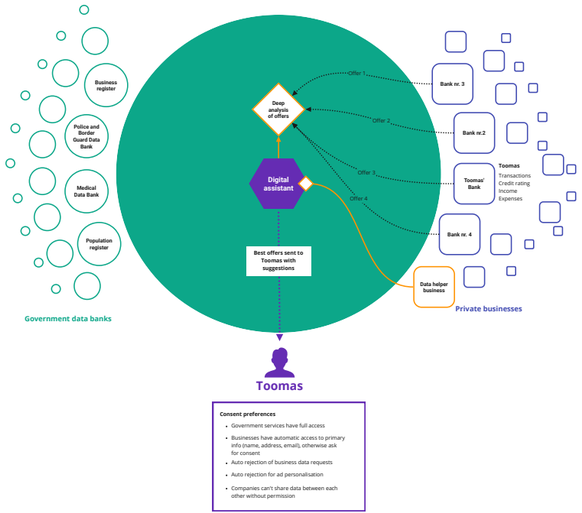
2.



3.

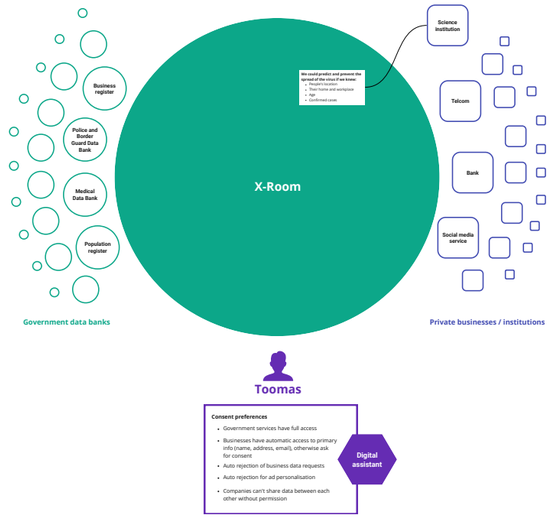


4.

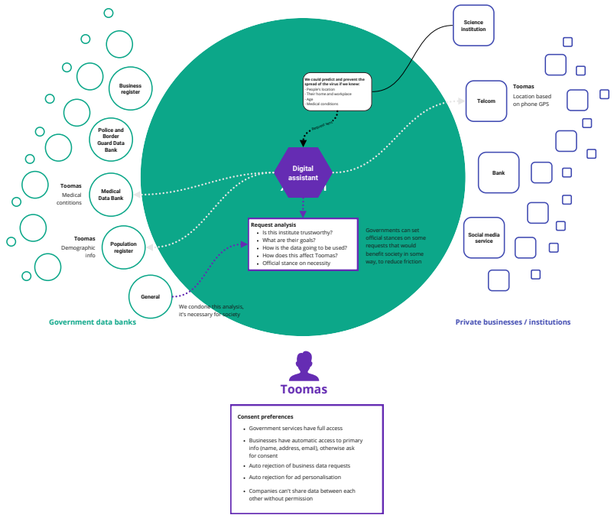


Appendix 2: Collaborative data business model

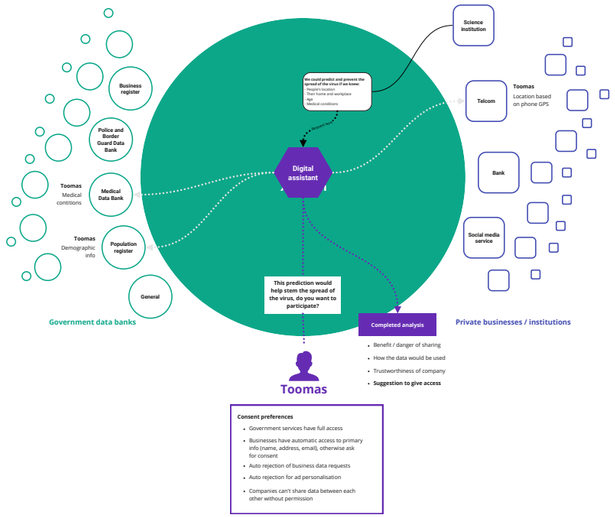
5.



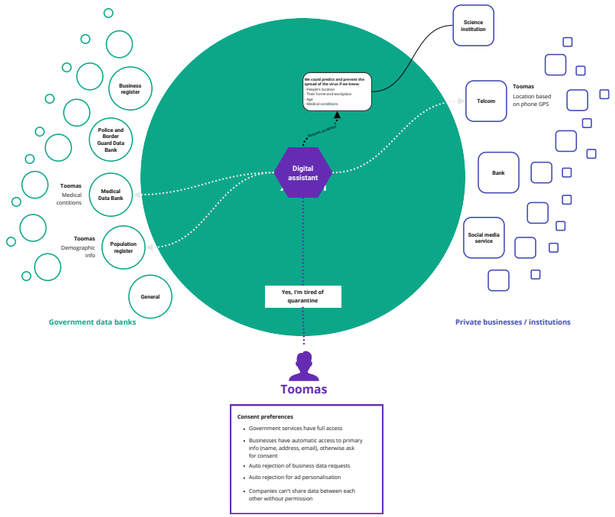
6.



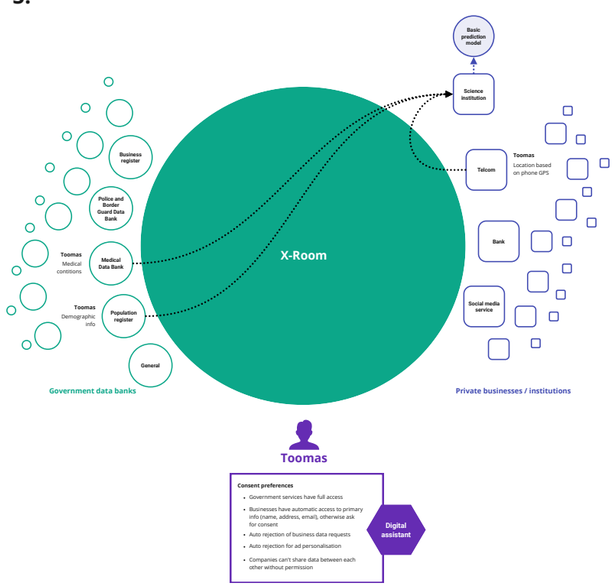
7.



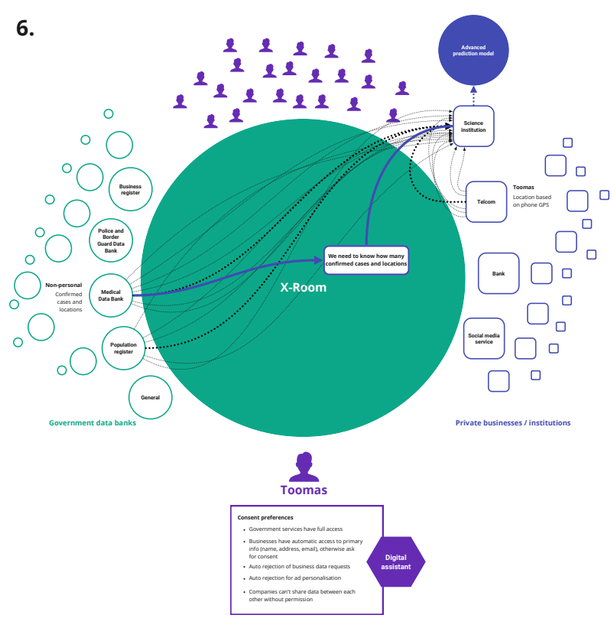
8.



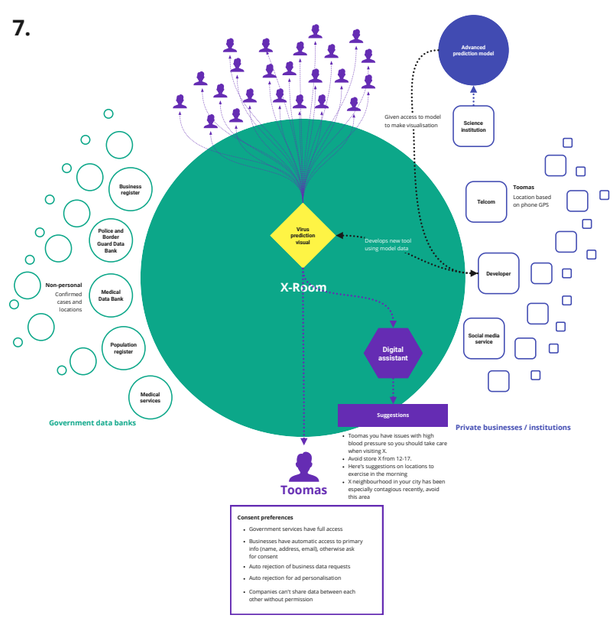
5.



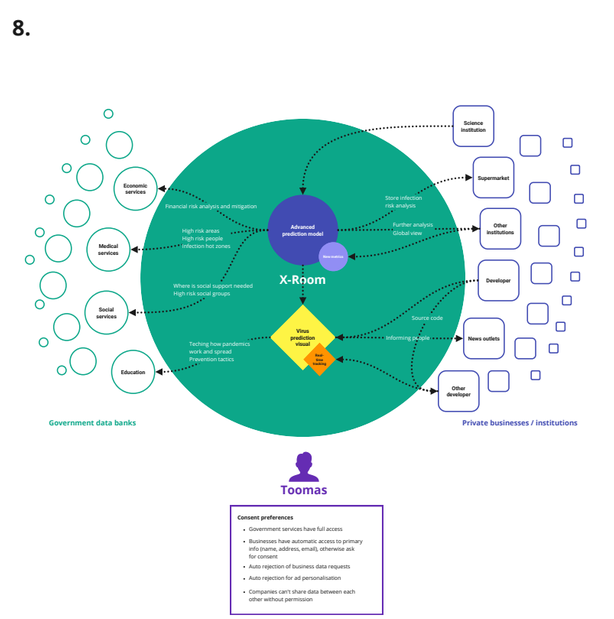
6.



7.

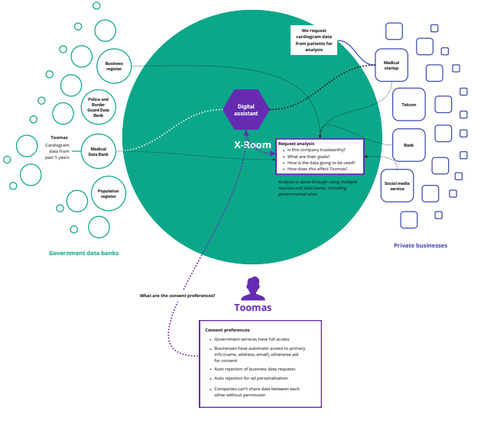


8.

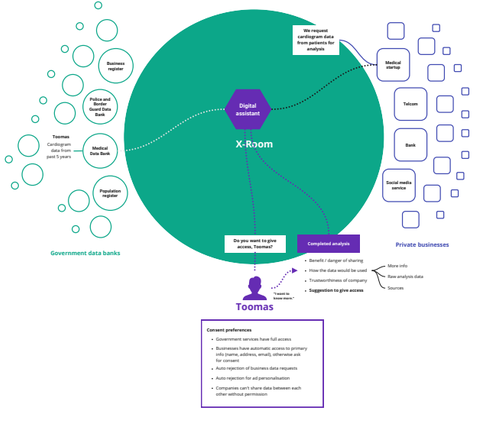


Appendix 3: Medical startup request

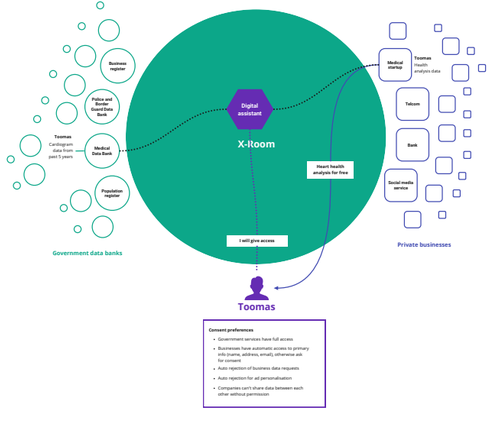
1.



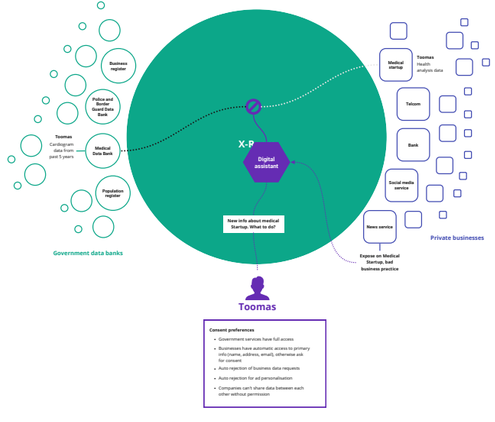
2.



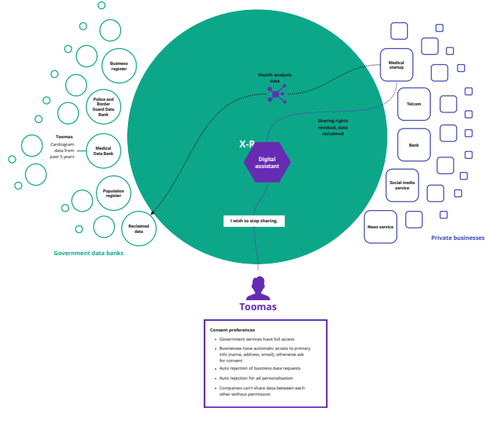
3.



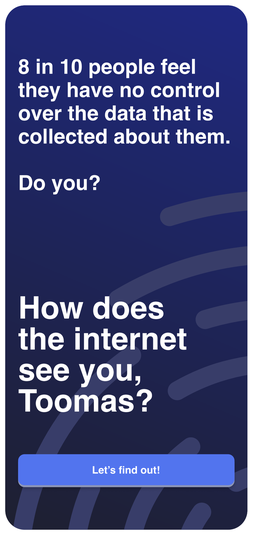
4.

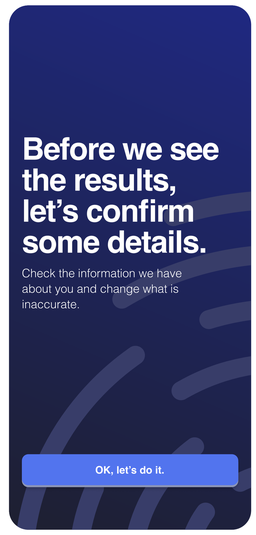


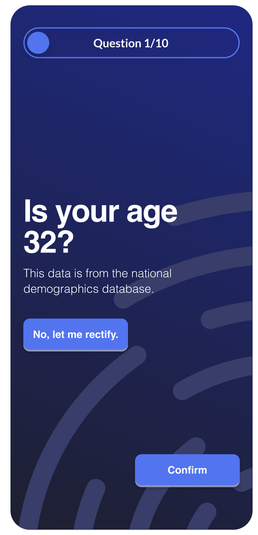
5.

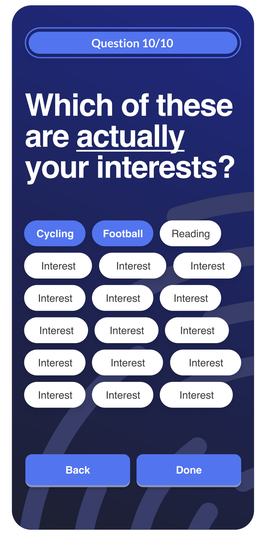


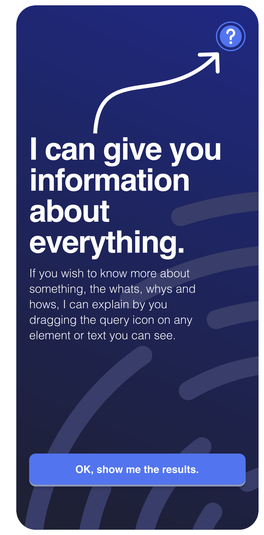
Appendix 4: Instant onboarding flow UI views

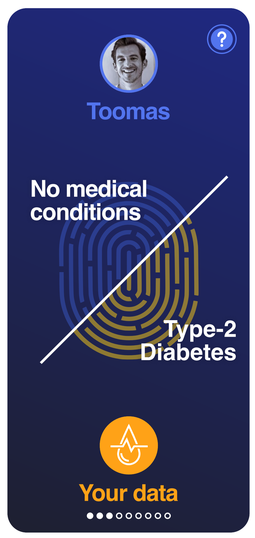


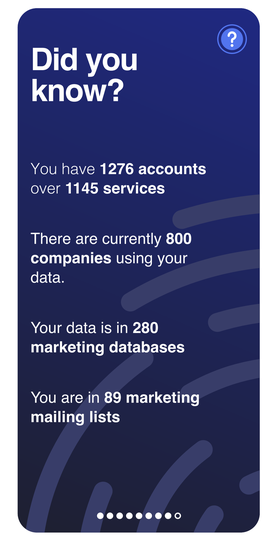


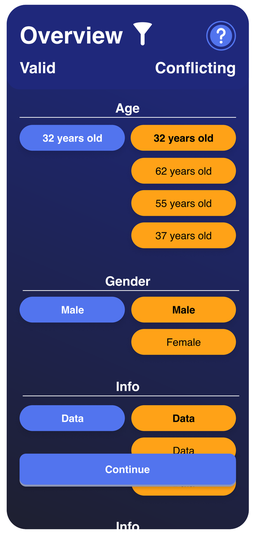


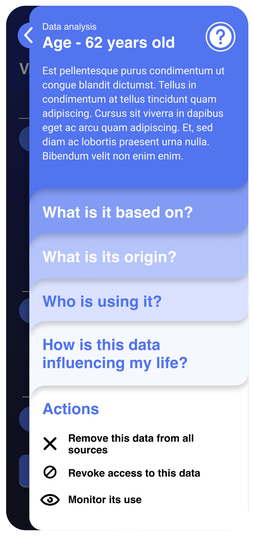


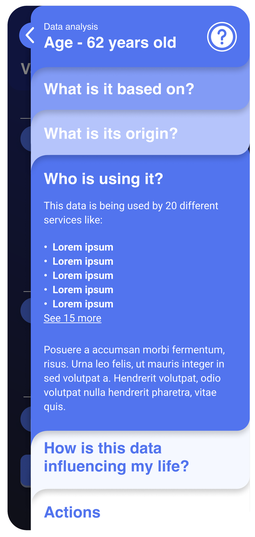


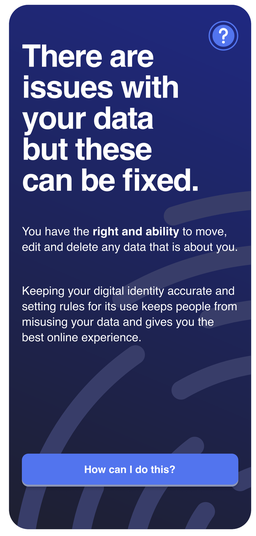


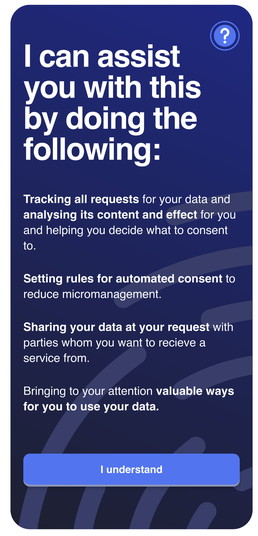


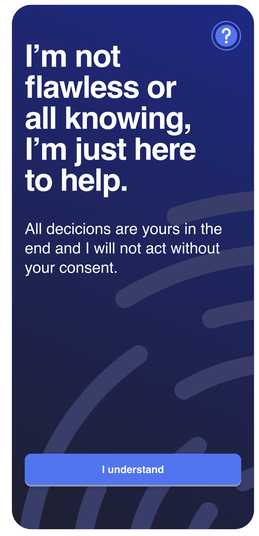


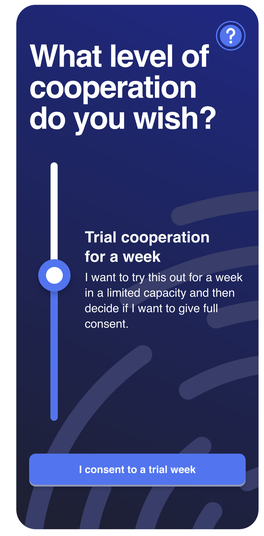


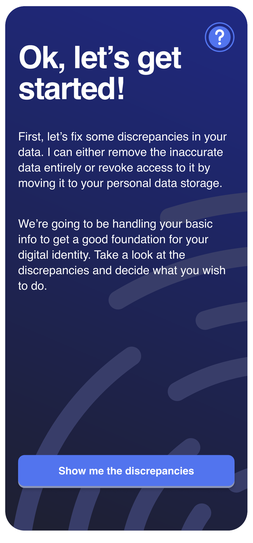


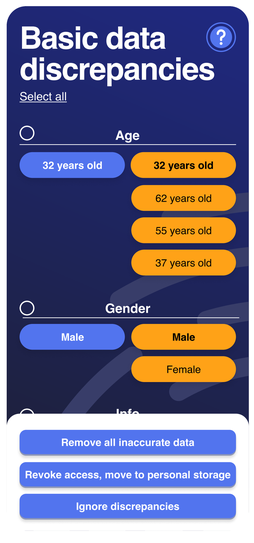


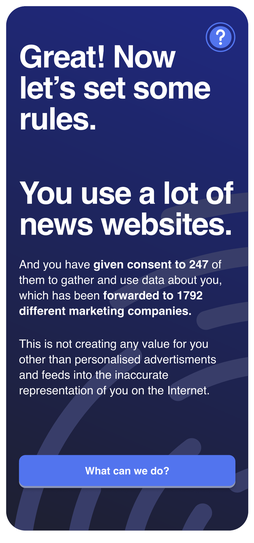


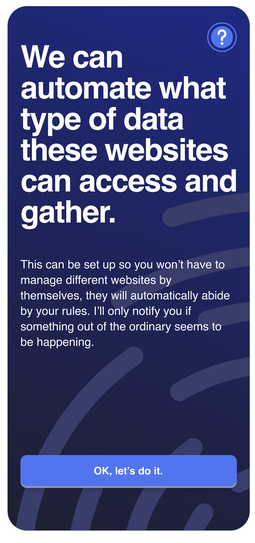


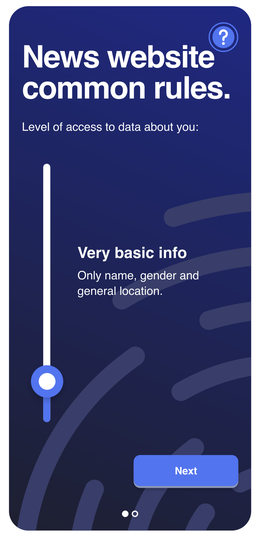


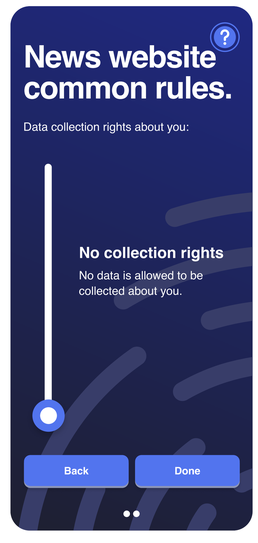


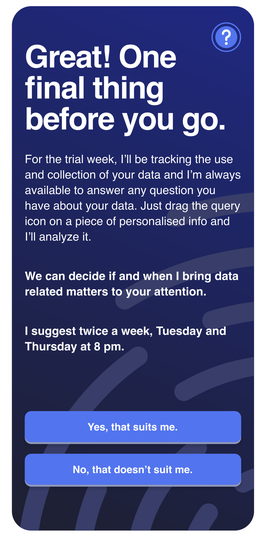




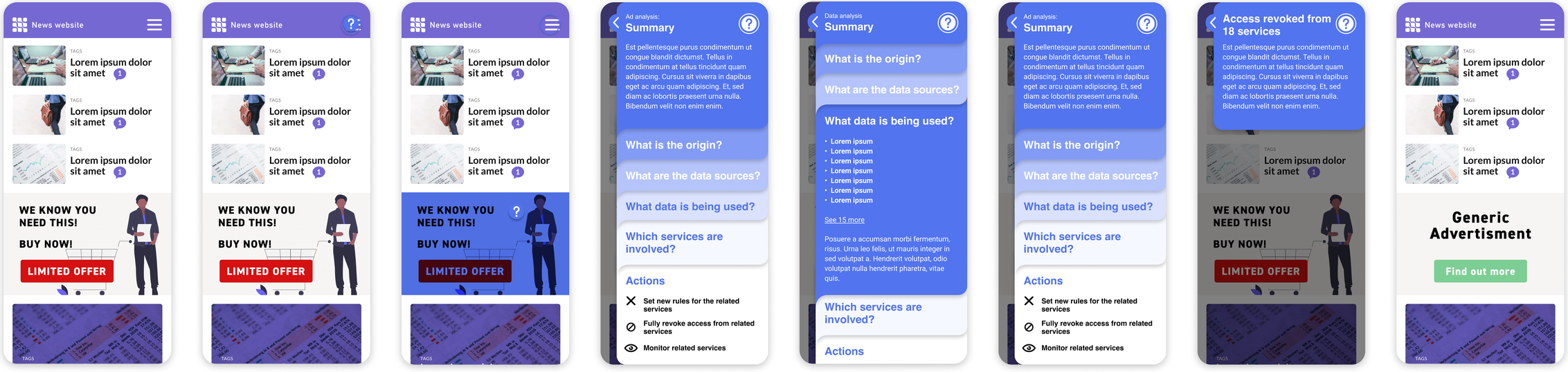








Appendix 5: Instant advertisement query flow



Appendix 6: Instant proactive prompt flow