MALMÖ UNIVERSITY

Play for the Black Box

Using Critical Play to raise awareness of data privacy issues

Anette Isabella Giesa

Anette Isabella Giesa
Interaction Design Master Programme (Two-year) ,K3, Malmö University
Interaction Design Master: Thesis Project II ,15 credits
Spring semester/2020
Supervisor: Clint Heyer
Examiner: Susan Kozel

Abstract

In the development of digitally connected solutions that require the use of personal data, the issue of data privacy is an important factor that must be taken into account. Simply informing users about how data is used and getting their consent with a simple click is not enough to create awareness of the issue of data privacy and let them make a conscious decision about the use of their personal data. Furthermore, there is a big gap in knowledge about what personal data is and what is considered sensitive data. Especially the knowledge about what biometric identifiers that they are used in a variety of everyday life applications and in which sense the handling can be problematic is unknown.

This thesis project explores how the use of critical play in form of an activist game can create awareness of the issue of data privacy, inform about the value of biometric data and foster self-reflection of handling one's own personal data. Through the simulation of dependencies between personal data, the motivation to share them and the aggregation of personal data in combination with real and prospective use cases, players are empowered to reflect on their behaviour and to critically deal with the topic of data privacy.

Acknowledgements

First of all, I would like to thank Yenika Castillo Muñoz and Chang Cai for being there all the time and supporting me during these hard times of work stress and additional social distancing. Further, I would like to thank all interviewees and playtest participants for spending some of their precious time and providing comprehensive feedback. I would also like to thank Mindlab Malmö and the Internet of things and people lab at Malmö University for lending me an Open BCI Kit and various biosensors.

Table of Contents

1. Introduction

Globalisation, datafication and digital networking are factors that are reshaping western modern society. Big Data and ubiquitous, automated data collection play a decisive role in that process. With increasing computational power and machine learning, the huge amounts of data that are collected can be processed, analyzed and recombined faster and more efficiently. These processes create a variety of new opportunities for new digital infrastructures, services, communication platforms and products that meet people's individual needs for information, self-expression, learning, participation, empowerment and social connection (Zuboff, 2015). In particular, personal and behavioural data are of great interest in order to enable user-adapted solutions that meet personal needs. Most of these solutions require a regular or permanent connection to the Internet and thus also affect our daily life. Customized services, apps and advertising are changing the way we work, how we interact with people and how, where and what we consume, to name but a few examples. The tracking and processing of the generated data basically serves to predict and modify human behaviour in order to increase revenue and improve market control. This new form of information capitalism is defined by Zuboff as "surveillance capitalism" (2015, 2016).

In a way, data is a kind of currency. In exchange for data that one knowingly and unknowingly provides, one receives a kind of benefit in return. Many people are willing to share their data if it increases security, provides new insights, makes their lives more convenient, improves their health and well-being, or simply provides entertainment and distraction (Castro & McLaughlin, 2019) ("Global Fraud Report 2019 | Experian", 2019) (Global Alliance of Data-Drive Marketing Association & UK DMA & Acxiom, 2018). Nevertheless, the endless amounts of data generated through everyday activities and the use of various products and systems, is extracted at no cost and monetized by firms.

Apart from the non-consensual extraction of data, users often do not know what kind of data is tracked and transmitted, when and in which way. Data extraction per se does not imply a risk, but storing, processing, and linking data, security leaks as well as sharing of data amongst companies, institutions and governments can cause serious damage in digital and real lives. Christl and Spiekermann are dividing these risks into six categories: Discrimination, Manipulation, Security Threats, societal changes, individual privacy and market imbalances (2016, p.81). Especially biometric data should be handled with care, as this type of data can uniquely identify a person without requiring a greater combination and interlinking of collected data sets.

Interaction Designers are playing a decisive role in the development and implementation of technological innovations and are more and more concerned with the usage of Big Data and Machine learning. Questions of personal data handling and data security are an increasingly important issue that must not only be considered during the development of digital products and systems, but should already be included in the initial conceptual considerations and follow the principles of "privacy by design" (Cavoukian, 2009). Besides data handling and privacy, possible ethical, social, and political implications should also be considered. Designers can make an important contribution to create transparency, inform the general public about the handling of data, create awareness for data privacy, offer levels of choice and thus contribute to democratization in surveillance capitalism. In addition, transparency and comprehensible information on the handling and types of private data used can make current behavioural patterns visible, thus enabling reflection and personal critical examination of the topic.

1.1. Research Focus & Question

Interaction designers are often concerned with identifying problems and finding the best and most innovative solution, which increasingly involves the use of personal data. This integration of personal data enables better personalization and adaptation to user needs but does not empower them. Storni (2014) describes design as de-sign or design as conjuring which is characterized by hiding and calls for greater empowerment of the user in terms of empowerment-in-use. Modern, appealing, and usable design solutions are often promoted with the ability to empower the user but are actually promoting “passive users whose access to the design is controlled and limited” (p.164). The black-boxing of infrastructures as well as access and control restrictions are necessary to some extent for protection and to guarantee of a certain level of quality and security, but that the black-boxing often goes beyond the security issue and various business models, licenses and encryption rather lead to disempowerment of the user (ibid.). Empowerment of the user in many ways, is possible through design. In participatory design, the user is involved in the design process and thus ought to be empowered through democratic voice and agency. Seamful design, OpenSource and DIY design approaches are providing empowerment-in-use (Storni,2014). Apart from user empowerment, which refers to the design object itself through participation in the development or possibility of manipulation and further development of the design object, design as such can contribute to user empowerment on a higher socio-political level. Asymmetries of power within surveillance capitalism are linked to asymmetries of knowledge. Increased transparency and didactic approaches in design can minimise these knowledge asymmetries between companies, institutions, and users, thus providing an opportunity for participation and a greater say for users in socio-economical terms. In addition, transparency and detailed and comprehensible information about the use and type of data can make current behavioural patterns visible, thus enabling reflection and personal critical examination of the topic of data privacy.

This thesis explores a playful way to inform people about how they are using their personal data in everyday life and in which context what type of personal data is required to receive a certain benefit. Thereby an awareness for the topic of data privacy and a critical examination of the question of data ownership should be created. Since the topic of data privacy is an extremely broad field, the focus lies on biometric data and biosignals. These types of data are perceived as highly private, as they relate directly to the human body. Especially biometric data are classified as particularly sensitive due to their characteristic as a unique identifier of an individuum (European Parliament, 2018). The use of biometric identifiers and biosignals and the resulting issue of data protection is omnipresent and cannot be limited to a specific context. Hence, the work does not focus on a specific target group but tries to address a broader spectrum of users. To achieve this, the exploration is located in the area of games using the theoretical frame of critical play. By using game as a medium, the users - who become players in this context - are allowed to explore the handling of their personal data on an abstracted level without drawing real consequences. As Crawford describes it, "a game is a safe way to experience reality" (1984,p.7). The theoretical framework that Flanagan calls "critical play" makes the game a tool for questioning reality and providing political and social criticism. In addition to raising awareness of the topic of data privacy through exploration and critical reflection regarding the handling of one's own personal data, the possibility of freedom of choice should be demonstrated.

The theoretical framework that Flanagan calls "critical play" makes the game a tool for questioning reality and providing political and social criticism. Since this project addresses a current, existing problem, critical play is applied in the form of an activist game. In addition to raising awareness of the topic of data protection through exploration and critical reflection regarding the handling of one's own personal data, the possibility of freedom of choice should be demonstrated. Besides the goal of creating awareness and critical reflection, the project aims to identify qualities that can be used by interaction designers outside of game design to educate and raise awareness on this topic. The research question can therefore be formulated as follows:

How can critical play in the form of an activist game raise awareness of the issue of data privacy and encourage critical reflection on one´s own behaviour with personal data?

2. Background & Theory

This chapter provides back ground information and theories to understand aspects and concepts relevant to the area this project is situated in.

2.1. Personal Data & Data protection

The definition of what constitutes personal data varies between different countries. By the European commission personal data is defined as “any information that relates to an identified or identifiable living individual. Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.” (What is personal data?, n.d.). Apart from different interpretations in various countries of the world, it is not possible to determine what constitutes personally identifiable information, as technological possibilities and limitations are constantly changing (Davis & Patterson, 2012).

The introduction of the General Data Protection Regulation (GDPR) in the European Union on 25 May 2018 brought a meaningful change to data regulations. That step does not only have an impact on European companies and citizens but worldwide. Although an essential benchmark for data handling, data privacy and identity protection was created by that, it is no worldwide standard. Nevertheless, in many areas, including design research and practice, a greater awareness has been created of what should be considered personal data that must be protected in order to respect a natural person's rights of freedom and the protection of personal information.

In the development of new technologies, services and products that are entailed with digital data, privacy-by-default and privacy-by-design are international frameworks that were already introduced before the introduction of the new GDPR to ensure a certain standard of data protection, mainly in the field of engineering. Privacy-by-default describes the compliance of basic data protection requirements by default settings, while Privacy-by-Design describes the proactive consideration of data protection requirements at the earliest possible stage of development (Kipker, 2015). In the new European GDPR "data protection by design" and "data protection by default" are included. Not only engineers and information and security architects are confronted with the handling of personal data in their work anymore. Interaction designers and researchers must also increasingly pay attention to these guidelines and regulations in the planning and development of digitally connected systems and implement them in their work processes.

Within the category of what can be classified as personal data, there is a special group that is considered as explicitly sensitive data (European Parliament, 2018). It is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person.

2.1.1. Biometrics and biometric data

The term biometrics refers to an automated method to measure and analyse a person's physical and behavioural characteristics. These measurable characteristics are what is referred to as biometric data or biometric identifiers. The number of what can be declared as biometric data is constantly growing with technological progress. In general, biometric identifiers can be categorised in physical and behavioural characteristics. What biometric data can be measured to date is shown below in Table 1

Biometric identifiers	
Physical	**Behavioural**
• DNA	• Voice/speech
• Facial characteristics	• Brain Waves
• Retina	• Heartbeat/wave
• Iris	• Muscle movement
• Fingerprint	• Gait
• Finger geometry	• Typing / keystroke pattern
• Hand geometry	• Signature
• Vein pattern (Palm, Finger, Eye)	• Handwriting characteristics
• Ear characteristics	• Sleeping habits
• Odour	• Workout patterns
• Brain Waves	• Foot weight distribution
• Heartbeat (wave)	• Lip motion
• Footprint	• Foot dynamics
• Thermography	

Table 1: currently measurable biometric identifiers, divided into physical and behavioural characteristics (Information gathered and combined from different sources)

Biometric systems are used in a variety of different fields and for different purposes. They range from identification and access control in public and private settings, over the usage in the area of health and fitness, to the simple purpose of increased convenience and entertainment. With the ability to uniquely identify a natural person, the primary and oldest purpose of use for biometric data is identification in the governmental context and authorization in enterprise (Secure Identity Alliance, 2019). Biometrics are one of the safest ways to identify a natural person and the specific features of biometric identifiers offer better protection than for example a password, which is easier to copy and decrypt. They cannot be copied as easily, and “normal” hackers would not take the time and effort it currently takes to steal a digital identity. Although security is constantly evolving and improving, no security solution is 100% secure and biometric data is of course, like any other data, vulnerable to hacking and spoofing. Biometric systems are also not invulnerable to errors and false positives or negatives can occur (ibid.). In a serious context such as border control, such mistakes can have a massive impact on the individual's life.

Despite these risks, the usage of biometrics is growing rapidly, especially in the consumer market. In their report on best practices and recommendation guidelines for biometrics from June 2019, the Security Identity Alliance predicted that by 2020 ”nearly all smart devices including mobile phones, tablets and wearables will have some form of biometric security enablement“ (p.7). Biometrics systems that are using fingerprint and face recognition are present in consumer products since several years. Using Touch ID or face recognition became a known and accepted technology that is also trusted by banks. The increased implementation of biometric technologies in consumer products leads especially fast to acceptance if they are designed for personal entertainment and fun. Ellebrok describes that the playful use of controversial technologies shifts them from a serious and hard to a less threatening context, making them user-friendly. The use of these technologies can therefore provide pleasure, convenience, and personal entertainment (2011). The increased and playful usage of biometrics also helps to develop these technologies faster and can eventually establish some standards (ibid.). In the more serious context of biometrics for identification purposes, the Security Identity Alliance is calling for standardisation to create and protect a trusted digitally ”root“ identity (2019). While on the one hand standardisation can create more security, on the other hand it makes it easier for biometric data collected in different systems to be combined and supplemented. As a result this can also lead to a higher risk of leakage, creating harm (Ellerbrok, 2011)

2.1.2. Biosignals

The term biosignals or biological signals refers to electrical, chemical and mechanical biological events like the beating of a heart or the contraction of a muscle. These signals can be measured, monitored and analysed. They are containing useful information which can be used to understand physiological mechanisms (Enderle & Bronzino, 2012). Biosignals can be distinguished in electric and non-electric signals. (Kozlíková, Granja & Leroy, 2010). They are existent in any living creature and can provide information in an active or passive way. In addition, biosignals can be divided into signals that originate from the organism and can be measured based on its own activity, and signals that can be measured by exposure to an external source. (idid.). Based on their physiological origin, biosignals can further be categorized into six types: bioelectric, biomagnetic, biochemical, biomechanical, bioacustic and bio-optical (Enderle & Bronzino, 2012). The most known biosignals in these categories are :

Bioelectrical signals	Electrocardiogram (ECG), electrical activity of the heart, Electroencephalogram (EEG), electrical activity of the brain
Biomagnetic signals	Magnetocardiography (MCG), magnetical activity of the heart magnetoencephalography (MCG) , magnetical activity of the brain
Biochemical signals	Blood oxygen, Blood sugar
Biomechanical signals	Blood pressure
Bioacoustic	Activity of the respiratory system
Bio-optical	Signals that are generated by the optical or light induced attributes

Table 2: Most known types of biosignals in the six categories of physiological origin

Unlike biometric data, most biosignals cannot be used as unique identifier of an individuum as they are time, space, or space-time dependent recordings (ibid.). Nevertheless, brain waves or the curve of a heartbeat, for example, can be used as biometric data. In combination with biometric identifiers, biosignals can provide information about a person's state of health in addition to identifying them.

Biosignals are mostly used in the medical context but are also increasingly present in consumer products. Fitness trackers are for example aimed to improve one’s fitness, well-being and sleeping behaviour. Health gadgets serve medical but also personal purposes. They can be used for self-monitoring of biological parameters, for example to determine fertility intervals in child planning. More and more products are also designed to control and train the activity of biological signals to achieve more mindfulness.

2.2. Critical Play & Activist games

The term “critical play” was coined by Flanagan and generally encompasses the approach of using games to critically challenge established norms, to question reality, to make social and political criticism or to convey a message of subversion. (2009). In the theoretical framework of critical play, the role of the designer involves the careful examination and analysis of social, cultural, and political issues. Developing critical play in form of critical games should involve a diverse test audience to ensure that the conceptual, thematic and technological aspects of the game deliver the same message and meet the desired goals at the end of the project. Since criticality requires to a certain degree the taking of a stand for one side, the goal of the theoretical reference system of critical play includes the interest of the designer in exercising criticism as well as the use of the medium of play for it. (Flanagan, 2009). Critical games are well suited to address issues that might be uncomfortable. They raise questions and provide information about the subject area addressed by the game. The aim is not to win but to create a reflection and discussion on a topic within a safe space. (Flanagan, 2009)

Activist games are one type of critical games and a result of using the framework of critical play as a design approach. They are characterised by addressing current “real” problems or aspects in the socio-political, socio-economical and cultural context (Flanagan,2009; Flanagan & Lotko,2009) and can enable players to critically think about their ideological assumptions. Therefore, observation and research is necessary to understand how things are actually working to be able to transfer these into the game (ibid). Furthermore, they are didactic and have an inherent tension between the message they want to convey and the entertainment value of a game. An artistic aesthetic approach is not the right one when developing an activist game or critical game (Flanagan & Lotko, 2009 ; Flanagan, 2009). The political aspect in such types of games lies in the mechanics and is achieved through the technique of simulation. Due to the simulation of “real world” events and mechanisms in the game , “what players are doing, what choices are available, and the activities and habits of the players matter”(-Flanagan & Lotko, 2009, p.2). To simply paint an existing game with a new theme may not allow it to exercise criticism and question existing norms. Sicart also examines what makes play in general political and goes one step further (Sicart, 2014). He argues that it is not even enough to simulate political mechanisms with the mechanics and rules of a game. Political meaning arises from the playing community and from the way in which the game brings together context, form, and situation (ibid).

3. Related Work

Existing games that address the issue of data privacy can be divided into two types. Games that aim at security training and education and games that aim at raising awareness and informing about the issue by putting the player in a different role.

3.1. Spot The Risk

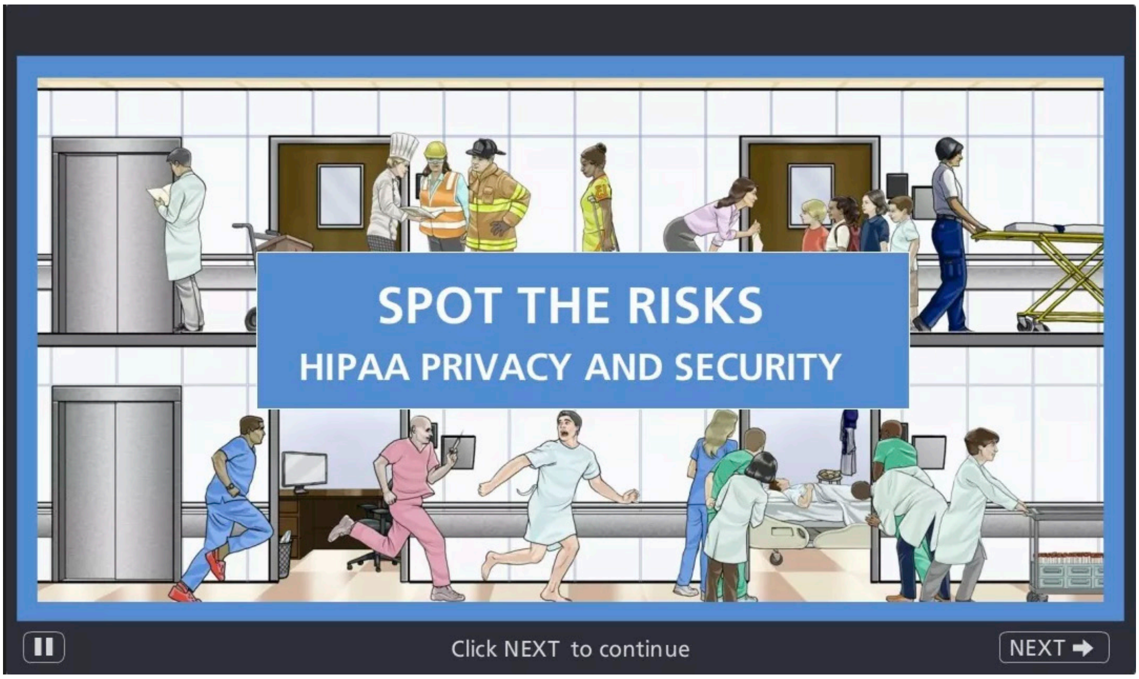


Figure 1: "Spot the risks" game education module to train employees on data protection and security

The company TeachPrivacy offers a variety of computer-based training courses for employees in various industries, focusing on data security and privacy awareness. The game "Spot The Risks" is a module of their training offer on data protection and security. As the name indicates it is a spotting game in which trainees are asked to spot and click on every security and privacy risk parameter in each scene.

3.2. [d0x3d!]

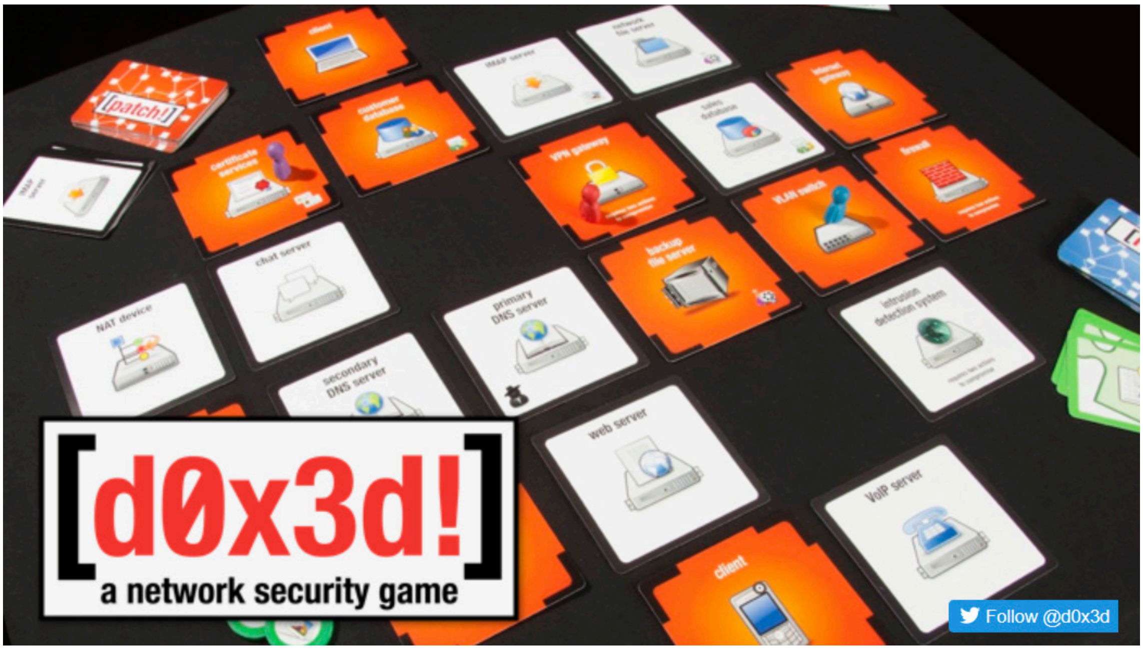


Figure 2: "d0x3d!", an educational game on network security

d0x3d! is an open source board game addressing computer science students on the topic of network security teaching them relevant terminology, attack end defends mechanics and basic computer security concepts.

3.3. Control-Alt-Hack

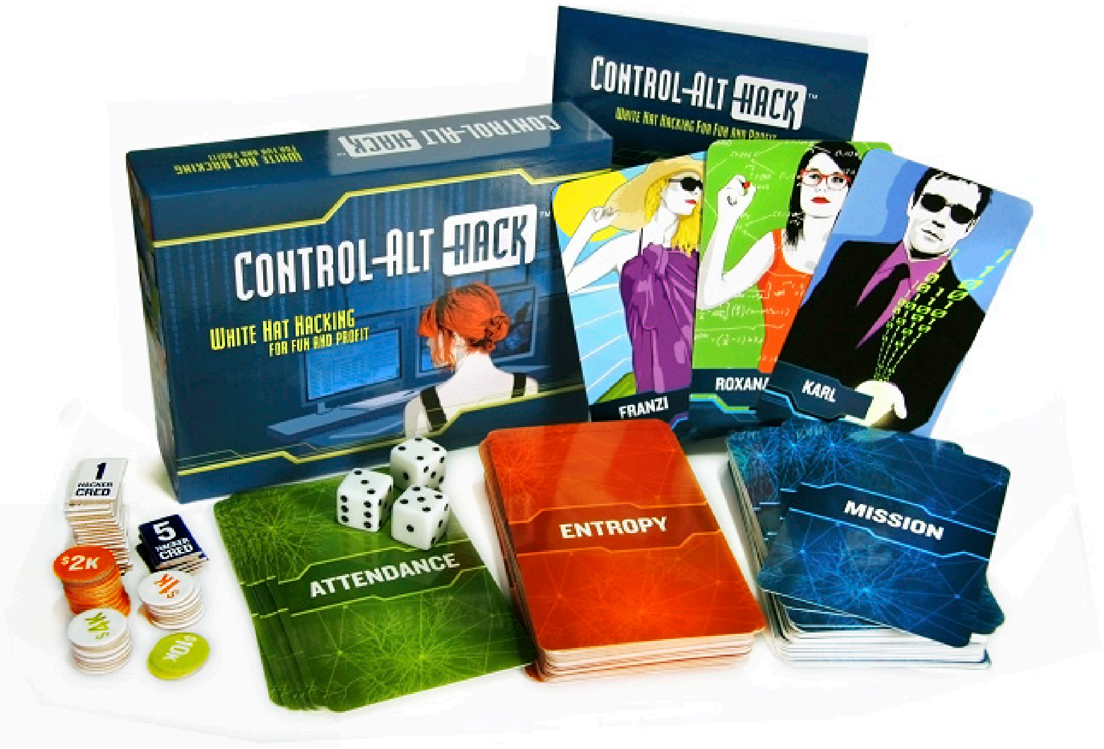


Figure 3: "Control-Alt-Hack^{TM}" card game

Control-Alt-Hack™ is a tabletop card game about white hat hacking. Players take on the role of a hacker working for the computer security company Hackers, Inc. Missions are played to conduct security audits and provide consulting services by applying their hacking skills.

3.4. Unveiling Interfaces

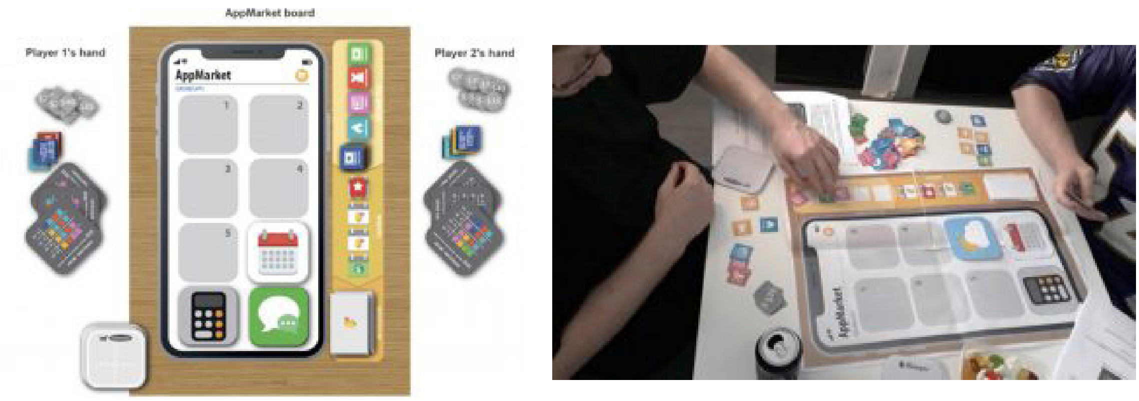


Figure 4: "Unveiling interfaces" board game

Unveiling interfaces is a Euro-style board game which was developed as part of a thesis project. It aims to create awareness of algorithms in the players' everyday life and to promote algorithmic literacy. Players are put in the role of a developer and should try to disguise the algorithms behind a social media app. The goal of the game is to hide them behind user friendly icons and publish the app on an imaginary mobile app market for profit.

4. Methodology

The methodological approach that is used in this project is Research through Design (RtD). RtD is the commonly used approach in Design research and it describes the usage of design practice within the research process to create new knowledge that can contribute to design theory (Zimmerman, Forlizzi & Evenson, 2007). The practical-explorative character of RtD manifests itself in the inclusion of many iterative cycles within the research process through which multiple perspectives on a problem can be gained.

4.1. Interviews (Unstructured and semi-structured)

In this thesis project, unstructured and semi-structured interviews were conducted in the ideation phase and in the context of play testing. The strength of unstructured interviews lies in the fact that the loose structure gives the respondent more control and relevant aspects - which were not considered before - can be discovered (Wilson, 2014). Semi-structured interviews contain pre-defined questions that ensure that certain information can be gathered while still leaving room for further perspectives (ibid).

4.2. Sketching

Within the more practical and exploratory approach of research through design, sketching represents an embodied form of thinking used by designers. The act of sketching and resulting sketches can take many different forms, but they all serve the purpose of exploring and conceptualizing a variety of directions (Buxton,2007). There is an implicit knowledge behind the way designers think and solve problems (Cross, 2010). The core lies in the exploration, the experiencing and the doing. Most steps in a thinking process cannot be reproduced by the designer in verbal form but take on the form of sketches (Buxton,2007). Sketching is a method that is used throughout the entire design process, but above all characterizes the ideation phase (ibid.)

4.3. Prototyping

An essential feature of prototypes is that they represent a manifestation of an idea but differ from a sketch in so far as they serve a different purpose (Buxton,2007). Prototypes are also representations of the final design, which were created before the development of the actual artefact (Buchenau & Suri,2000) and which facilitate the development of the design problem and its solution (Fällman 2003). Prototypes can be physical or digital and range in quality from low to high. Low-fi prototypes usually consist of cheaper materials and are easier and faster to modify while High-Fi prototypes are offering a higher degree of functionality (Holmquist, 2005).

In this project only physical prototypes were created to simulate and explore the handling of private data on an abstract level with game mechanics and materials. The advantage of physical prototypes is that they allow players to focus on the game rather than the technology. Especially prototypes made of simple materials like paper allow multiple iterations in a shorter amount of time. Furthermore, it is possible to react directly to feedback from the tests and make changes on the go (Fullerton , 2014).

4.4. Playtesting

Playtesting is a method that comes from game design but can be applied in many other fields when “interaction between a created experience and a participatory audience” is involved (Fullerton & Zimmerman, 2014, p.283). It describes the testing of “work in progress” projects with an audience, whose results are used to make changes and upon which the design process continues. Playtesting is also to be understood as an approach that emphasizes problem solving through iteration and collaboration in the design process (ibid.). It should be involved in the development process from the beginning on, to create a constant loop of idea generation, evaluation, and revision (ibid). Initial early testing should be done in a self-test to explore fundamental mechanics and to identify and correct problems at an early stage. Afterwards it is useful to test with friends and family to get a new perspective. Since friends and family are objectively influenced by the relationship to you, further testing should be done with external people (ibid.). According to Fullerton it is crucial to recruit the right playtesters, which are people out of the target group. As in this project no clear target group exists, the playtesters were not selected according to specific criteria. Furthermore, the main goal of the project is not to develop a compelling and fun game, but to use it as a tool to uncover aspects and mechanics that are useful for interaction designers outside the game design industry to raise awareness and inform about data privacy issues. It was only tried to gain people as testers whose attitude towards data protection and trust in new technologies differs as much as possible.

4.5. Ethical and societal considerations

In accordance with The General Data Protection Regulation (GDPR), data that was collected containing personal information was handled to the best of my abilities according to the guidelines.

4.5.1. Collecting & Storing Data

During the project data was collected in form of a survey, interviews as well as in form of audio and video recordings. The survey was done with the program Sunet survey which is provided by Malmö University to guarantee a certain level of data protection. Interviews that are held remotely were done with the video conference tool Zoom and the messengers Telegram and Signal. Some interviews held online or in person as well as play tests were audio or video recorded if consent is given. All collected data was stored on my private data repository. The data will be stored until the thesis project is finished, graded and uploaded to the Malmö University publishing platform.

4.5.2. Information & Consent

Interviewees and test participants needed to give their consent before the interview or test. They could give their consent orally when audio or video recorded or in form of signing a consent form. Consent forms containe information about the thesis project, information on how the data will be stored and for which time period it will be saved, the right to revoke their consent at any time. Two additionall points were included to give consent for recording interviews and tests and the usage in the thesis paper.

4.5.3. Types of collected and/or used Data

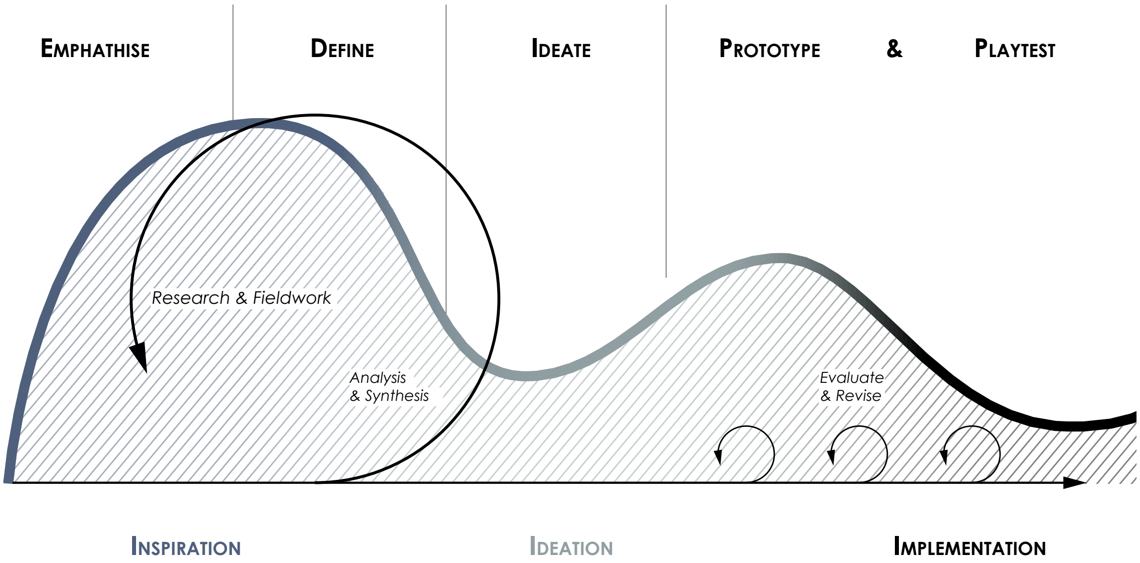
In the surveys and in interviews personal data like age group and country of residence were collected. User / play tests were video recorded and/or documented by photographs. Biometric data in form of facial characteristics are visible in some of that visual documentation material.

4.5.4. Sustainability

For all steps in the design process and for the construction of prototypes, as much material as possible was reused from older projects. Electronic material that was used in the ideation process was lent out for exploration.

5. Design Process

5.1. Process structure



5.2. Inspiration Phase 1

The initial starting point for this thesis was to explore how biosignals can be represented and shared in a more physical way other than numbers and graphs. By that an inwards experience of the own body should be created, leading to mindfulness. Another aspect was the focus on sharing that body data in real time with other people. It was assumed that the shared and more physical experience can also raise the question of data privacy and thus create awareness on how private data is handled. Although the focus in this first round of research and fieldwork was a different one, a few results and observations were building the starting point for the final project and are relevant to it. Besides desktop research a survey and a self-test was conducted in that first phase.

The survey was focusing on the usage of fitness trackers, health gadgets and smart watches to get insides on how and why people are tracking their data, what impact it has on their life and their opinion on data tracking, storage and sharing.

General survey information:

Number of participants	55
Main age group(s)	20-30 (48%) and 31 -40 (44%)
Gender identity	56% of the participants identify themselves as female, 43% as male and 1% as other
Continent living on	78% Europe, 14% Asia, 8% North America
Usage of fitness/health tracking devices	68% are currently using a fitness tracker, health gadget, smartwatch or similar, 32% have used one before

The following results from the survey were relevant for the final topic and provide insights on attitudes and knowledge about private data and data privacy within this group of people. They are also complementing the information that has been gathered through desktop research and interviews.

68% of the participants stated that very regular or constant measuring and tracking of their biosignals is important to them. This number is consistent with the number of participants currently using a fitness/health tracking device. The three most common reasons given were to train better, more effectively and to achieve set goals, to identify possible health problems and to learn more about one' s own behaviour and body. Four answers included the concern that constant tracking can make one more worried than necessary, especially as each body is different and the general public does not have the expertise to properly assess values and trends and questions the provided normative values and interpretations of such devices and apps. About half of the participants are or were sharing their fitness and health data with others, mostly friends (48%). In case of medical health trackers, the data is only shared with the doctor. Reasons to share the tracked data are competition (45,5%), medical reasons (36,4%) and accountability and motivation (18,2%). When it comes to data security of the device they use, about half of them stated that they had thought about it (52%) and 66% have thought about how the tracked data is used and processed. When asked if they would be willing to share and store their data with doctors, medical research centres or the health system if it could improve their health and minimise health risks, 44% answered with yes, 42% with "only if I can and must confirm it each time", 14% said no and 8% were not sure. In some comments, it was noted that it is a difficult question to answer, as it is very context-dependent when considered over a longer period of time. It was also mentioned that even if one gives their data for medical or research purposes, there is always an underlying and uncomfortable idea that it might be in some way lucrative for research centres, doctors or other institutions.

To get a feeling for what it is like to track oneself, I conducted a self-test. Over a period of 1.5 weeks I wore a fitness tracker wristband, with which I not only tracked the automatically recordable data, but also consciously entered values for recording and analysis. Although I do not belong to the target group of such devices and found wearing the wristband awful and uncomfortable, I surprisingly realized that from the fourth day on I started to check in the morning how my sleep had been. This fact confirms the statements in later interviews for me that one gets used to technology very quickly if it brings you comfort or if it makes you believe to learn more about yourself. A significant event that occurred after I had completed the test and which contributed to changing the focus of the work was that I received an email informing me that my period was to begin in 3 days.

5.3. Inspiration Phase 2

The second inspirations phase was mainly characterized by desktop research and interviews. This provided more in-depth information on the topic of personal data, in particular biometric data and biosignals, and data protection. The question in which context and for what purpose these data are used also led to the subject of data as a currency and commodity, and consequently to the issue of surveillance and surveillance capitalism. Information found in reports, survey results and statistics on what motivates consumers to give their data and their attitude towards data privacy were used as a basis for subsequent interviews.

5.3.1. Interviews

Nine people in an age range of 29 to 52 were asked in an unstructured interview about their knowledge and attitudes to the topic of private data, data protection and their handling of private data. The general attitude towards the handling of private data ranges from extremely cautious to mostly unconcerned. Two people can be said to be extremely cautious when it comes to the topic of private data and are sceptical about its use. they can be characterised as such based on the fact that they are using a fairphone or not a smartphone at all. Furthermore, they are always looking for more secure alternatives to commonly used applications, services and programs. Two more interviewees also stated that they regularly look for alternatives, for example using Telegram and/or Signal instead of WhatsApp or the facebook Messenger. They also read in part or always the general terms and conditions and information on data privacy. However, it also depends on the context, and if the decision has to be made relatively quickly whether to have access to some services or to receive some benefit from it, this step is skipped. Regarding the question of how much knowledge about private data exists, it turned out that all respondents have a basic idea of what can be considered private data. However, it is not known what exactly biometric data are or which data can be classified as particularly sensitive according to the GDPR. It was assumed that all data relating to the physical body, including biosignals, are biometric data. The idea that behavioural data can also be biometric data was surprising for three of the interviewees. When they were informed about what can currently be used as biometric identifiers, all participants were amazed but not surprised that most of them are using biometric technology. Five interviewees said that they have heard of the GDPR. Only three of them stated that they knew what it actually is about. However, almost all of the participants said that they had noticed that something had changed since the introduction of the GDPR and that they were constantly being asked to give their consent to various things, both analogue and digital. And especially the digital requests in screen-based products are perceived as disturbing. The general perception is that in very few cases one has the choice to disagree in order to continue using certain products and services. Three statements indicated that it would be good to have a choice between consent, rejection or partial consent and to accept restrictions in return for more security and privacy. One point that each interviewee mentioned was that the information that is provided is often not the information that would be interesting to know. The information provided leaves one in the dark to a certain extent, is often very vaguely formulated and sometimes linguistically difficult to understand. From the interviews it was generally apparent that there is a perception and feeling of powerlessness. It has been said several times that in most cases one does not have a choice or is even forced to provide personal data in order to participate in social life. There is also the belief that once collected, data cannot be deleted, and if it cannot be used and monetized now, technological progress will make this possible sooner or later. Interviewees who are less concerned about the protection of private data stated that they value the advantages over privacy and security more in most cases. In addition, they feel that they are not so important that their data would be valuable in any way.

5.4. Ideation & Exploration

In order to develop ideas on how to raise people’s awareness of the handling of private data, to encourage them to reflect critically and to inform them about the topic in general, the collected information was first sorted and mapped. Data that can be defined as biometric was listed and categorised in physical and behavioural. The sources used to determine which biometric identifiers exist did not categorise them all in the same way. Based on the purposes for which this type of data is used, areas of application were roughly defined. The defined areas are: Security and Authentication, Medicine and Health, Fitness and Wellbeing, Games and Entertainment, as well as Art and Performance. In addition to this classification and categorization, research was done on which sensors and other electronic components can be used, how they can be obtained, and which data recordings would have to be simulated. The measuring and use of biosignals was included in these considerations

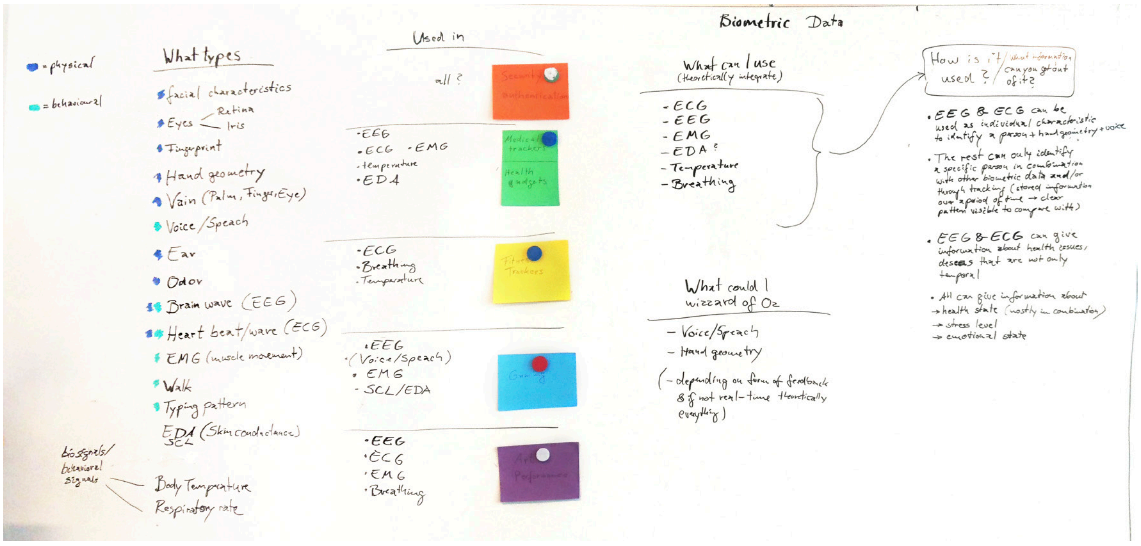

= physical
= behavioural
What types
facial characteristics
Eyes Retina Iris
Fingerprint
Hand geometry
Vain (Palm, Finger, Eye)
Voice / Speach
Ear
Odor
Brain wave (EEG)
Heart beat/wave (ECG)
EMG (muscle movement)
Walk
Typing pattern
EDA SCL (Skin conductance)
biosignals/ behavioral signals
Body Temperature
Respiratory rate
Used in
all ?
Security authentication
·EEG ·ECG ·EMG ·temperature ·EDA
Medical trackers
Health gadgets
·ECG ·Breathing ·Temperature
Fitness Trackers
·EEG ·(Voice/Speach) · EMG - SCL/EDA
Gaming
·EEG ·ECG ·EMG ·Breathing
Art Performance
Biometric Data
What can I use (theoretically integrate)
- ECG
- EEG
- EMG
- EDA ?
- Temperature
- Breathing
How is it used ? / what information can you get out of it?
• EEG & ECG can be used as individual characteristic to identify a person + hand geometry + voice
• The rest can only identify a specific person in combination with other biometric data and/or through tracking (stored information over a period of time → clear pattern visible to compare with)
• EEG & ECG can give information about health issues, deseas that are not only temporal
• All can give information about
→ health state (mostly in combination)
→ stress level
→ emotional state
What could I wizzard of Oz
- Voice/Speach
- Hand geometry
(- depending on form of feedback & if not real-time theoretically everything)

Figure 5: Mapping of biometric identifiers and a few biosignals on a whiteboard

An OpenBCI kit, a heart rate, muscle, temperature, SpO2 sensor and other electronic components could be borrowed to test them and explore their use in the project. Since most of the borrowed electronics must be attached to the body and the outbreak of Covid-19 would have made it difficult to test with other people, early ideas of building playful wearable objects were discarded. Instead, it was decided that the recording of biosignals should be simulated and pre-recordings should be used for feedback if they were to be integrated into the project.

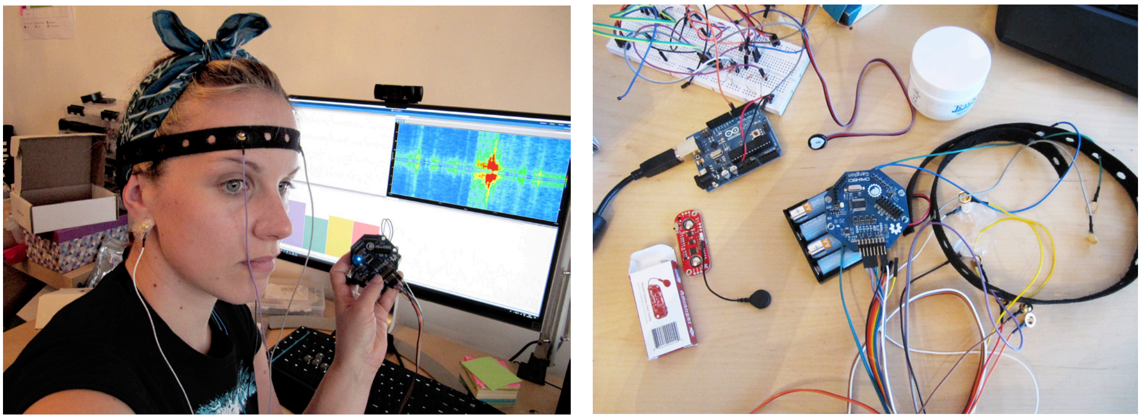


Figure 6: Testing of different biosensors

Since most people have little knowledge about the handling of private data and their use and processing, the idea was born to use the analogy of the black box. First ideas were sketched out how this analogy could transfer into an object that might be part of a tabletop game. The basic idea was to place the black box as the centre of the game in the middle of a table. The players should record their biometric identifiers and/or biosignals to be able to progress in the game. The more data would be fed into the system, the more the box would grow. One goal could be to access the collected data and thus "own" the personal data of the other players. This would bring into the game the property of data to be used as currency as well as commodity or material.

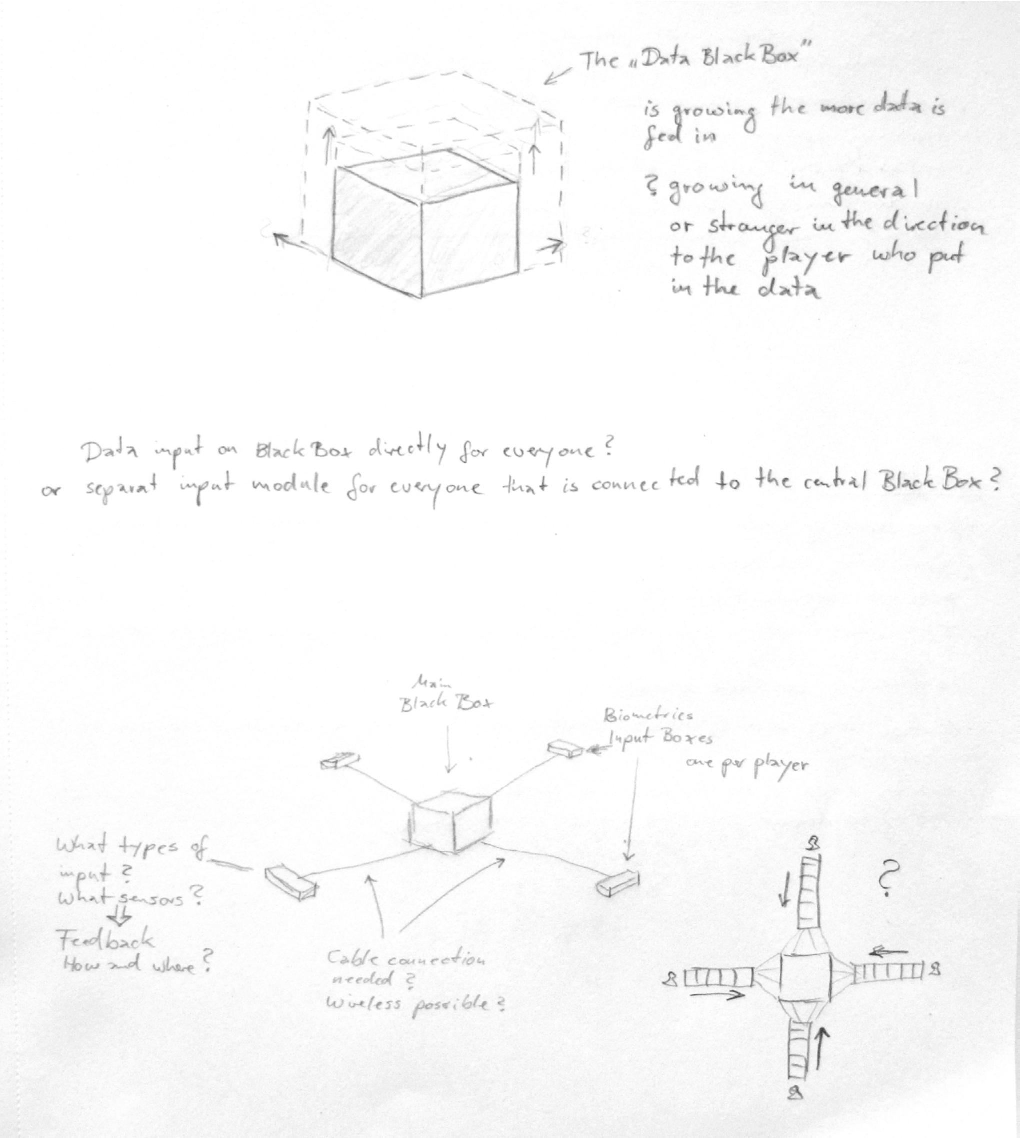

The „Data Black Box"
is growing the more data is fed in
? growing in general
or stronger in the direction to the player who put in the data
Data input on Black Box directly for everyone?
or separat input module for everyone that is connected to the central Black Box?
Main Black Box
Biometrics Input Boxes one per player
What types of input?
What sensors?
Feedback
How and where?
Cable connection needed?
Wireless possible?
?

Figure 7: First sketches of possible game setup and mechanical behaviour of the "black box"

5.5. PROTOTYPING & PLAYTESTING

The phase of prototyping and testing follows the "critical Play" Game design model. Although Flanagan describes this model also as a method, I see it more as an iterative design process enriched with the goal of critical play of intervention, disruption, and subversion of socio-political, socio-economic and cultural issues.

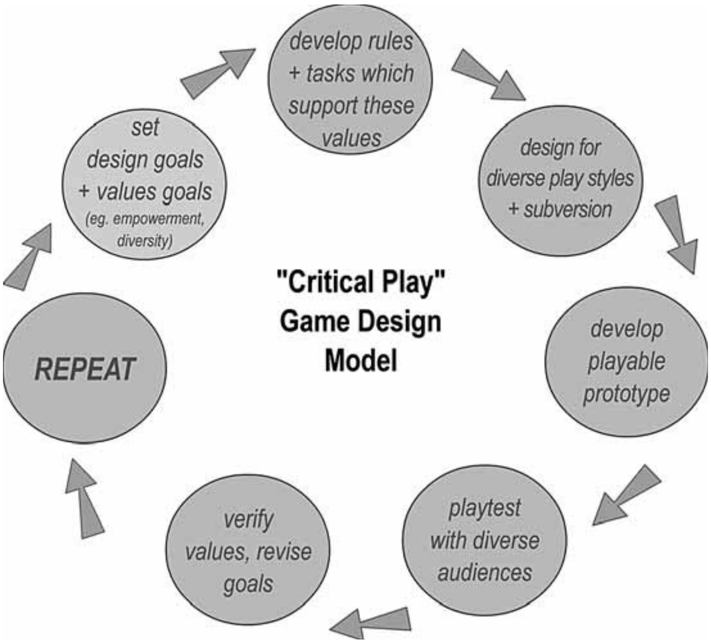

develop rules + tasks which support these values
design for diverse play styles + subversion
develop playable prototype
playtest with diverse audiences
verify values, revise goals
REPEAT
set design goals + values goals (eg. empowerment, diversity)
"Critical Play" Game Design Model

Figure 8: Mary Flanagan, model of critical play method (Flanagan, 2009)

A selection was made which biometric identifiers, biosignals and other private data should be used in the game. All the selected data are currently or will soon be used in everyday life. Based on the frequency of use, their sensitivity level and identification value, they were scored and a number of times they can be used in the game was determined .(see appendix 1)

The concept of the digital doppelgänger was integrated at this point to serve as a losing condition. The idea behind is that if a certain amount of data points is spent, the "black box system" gathered enough information of the player to create a digital copy and no further data is needed to "keep it alive". The term digital doppelgänger or digital twin, data-proxy, data double or data body generally refers to the assemblage of data that is willingly and unwillingly collected and can be associated with a natural person, building a kind of digital copy of that person and an identity that can even outlive the person it originates from. (Bode & Kristensen,2016; D. Haggerty, Richard V. Ericson, 2000; Smith, 2016; Lupton, 2016; Adee, 2012).

Since a critical reflection on one’s own behaviour in dealing with private data is to be achieved, categories were created which represent motivations why people provide their data. Various reports (Castro & McLaughlin, 2019) (“Global Fraud Report 2019 | Experian”, 2019) (Global Alliance of Data-Drive Marketing Association & UK DMA & Acxiom, 2018), survey results and statements from the interviews were used as the basis. General use cases for the selected biometric data, biosignals and a few more were researched, and several more specific use cases were formulated in such a way as to communicate the benefits of them. These use cases were mapped to the motivation categories and data costs were assigned to them. Based on the specific use case it was determined who has to pay; yourself, other players, all players or combinations (see appendix nr). From this composition playing cards were created. To simulate that in real life one has the choice to accept or decline the use of private data, the cards can be played or discarded. The motivation categories were transferred into a kind of player statistics that can be levelled-up. This made it possible to document the reasons a player has played cards, which in return can lead to self-reflection.

To test this first basic mechanics and dynamics, a short self-playtest was done with only a few physical components. The cards, showing the use case description, the costs that need to be played and colour-coded categories they belong to, were printed and cut out of paper. It revealed that there were not enough use cases to cover certain categories. Thus, more cards needed to be created.

5.5.1. Playtest session 1

The first playtest was conducted with three participants, from which two were friends. In addition to the materials used in the self-play test, a carton box representing the “black box” . Each player received a game figure and a game board which was roughly sketched on paper, leading to the box. The paper pieces representing the data were additionally outlined with a thin coloured line based on what type of data it is.

The basic instructions that were given were:

1. **The game is played round wise**

   a player draws a card and decides if they want to play it or not. If they play it they need to pay the respective type and amount of data into the "black box" and can move their statistics one level up in the category(s) the card belongs to but also moves one step up on the doppelgänger scale. If the card is discarded nothing happens. After that the players moves their game figure one field up towards the box

2. **There are two goals**

   one is to reach the "black box" and get all the data that is in it. The other one is to level up all categories

3. **There is a loosing condition**

   If a player reaches the last point on the scale, saying digital doppelgänger, the player is out of the game.

Nr. of players	3
Game Board	Hand drawn, V1.: 19 steps, moving one step round by round V2: 6 steps
Digitalisation meter	Hand drawn, 13 steps
Stats	Hand drawn, colour-coded categories, 15 steps, colour-coded paper snippets to indicate level
Cards	Printed, small format, categories colour-coded on top of card, other only plain text event
Data	Small paper snippets, colour-coded outline for data type, data name
Changes, additions in the Rules	
V2: levelling up two steps when a card belongs to only one category	

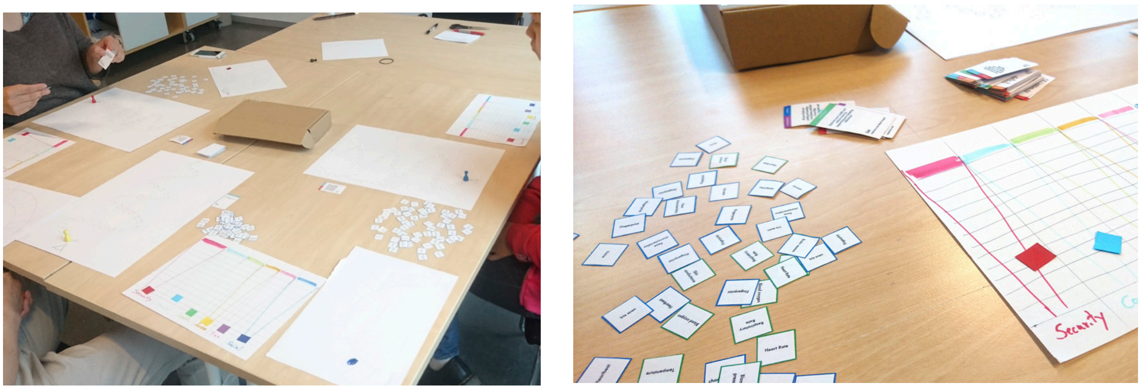


Figure 9: First playtest session with simple, mostly hand drawn paper prototype

It was obvious directly after the session has started, that the play field does not make sense if all players are moving their game figure one field up each round automatically. Nevertheless, the game was run a few rounds, to observe how the other components work, how the gameplay develops and to collect feedback on the game experience and mechanics.

The test was stopped after four rounds and first feedback collected. Surprisingly the playtesters did not saw the essential problem with the game board but only mentioned that it was too long, and the game would profit from a shorter game board, thus less rounds. The suggestion was made that if a card is assigned only to one category, one could level up two steps in that category. As discussions around the topic of the game already emerged in the first rounds and the players wanted to continue playing, these two changes were made directly, and the session continued.

After playing this first revision, the feedback was given that there was no motivation to reach the box, as one would get a step closer each round anyway. Furthermore, it was hard to find the right data fast, as the paper pieces with only the text on it were quite small.

5.5.2. Playtest Session 2

Nr. of players	2
Game Board	Hand drawn on paper , 19 fields, randomly marked fields for event cards, different on every board, rolling a dice to move forward V2: up and down slides (snakes and ladders like) added
Digitalisation meter	Same as previous session
Stats	Printed colour-coded categories, 10 steps, colour-coded paper snippets to indicate level
Cards	Action Cards: Printed on paper, categories colour-coded on top of card, use case description, info if not (only) you need to pay, colour-coded costs Event cards: Printed on paper, black and white cards for positive or negative event
Data	Colour-coded tokens with name of data + icon
Changes, additions in the Rules	

V1: if the game figure of a player lands on marked field an event card needs to be drawn and played

V2: if the game figure of a player lands on a field with an arrow connection to another field, the game figure is moved to the field the arrow is pointing to

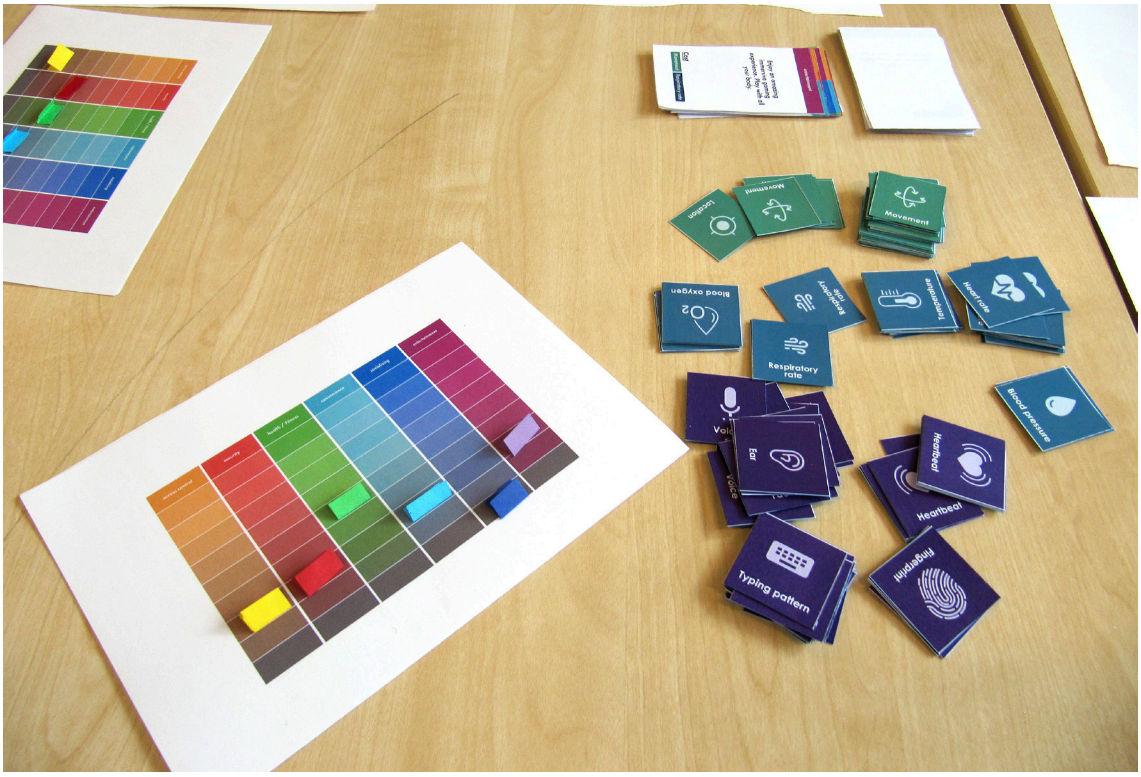


Figure 10: Motivation category statistics and data tokens from playtest session 2

The introduction of the Event cards brought a certain tension into the game. Making the tokens that are representing the data bigger, colour-coded and adding aa central icon, the players could find the needed data faster and the game picked up speed.

By using a dice to move forward, the number of fields on the board was too small. One player reached the box already in the second round. One playtester also suggested that if a player is more focused on reaching the “black box”, the introduction of an element of chance that does not allow for continuous progress might make the game more interesting and challenging. The game boards were revised, and another game round was started. Besides adding fields on the board, arrows have been drawn on some fields, which lead up or down to another field. If a player lands on one of these fields, the game figure will be moved to the field the arrow is pointing to. Since the players compared how they would behave and decide in real life, the criticism came up that there was not enough choice in the game.

5.5.3. Playtest Session 3

Nr. of players	4
Game Board	Hand drawn on paper , 19 fields, randomly marked fields for event cards, different on every board, up and down slides (snakes and ladders like) , rolling a dice to move forward
Digitalisation meter	Printed on cardboard, graphic instead of labelling of the sides, 10 steps
Stats	Printed on cardboard, 5 steps, color coded paper snippets to indicate level
Cards	Same as previous session
Data	Coloured thicker paper glued to the back (player colour)
Changes, additions in the Rules	
If a card is discarded the digitalization meter moves down the number of steps that data would have been payed V1: the drawn card needs to be played or discarded V2: each player always has three cards on hand to build a better strategy and play	

In this session some new mechanics related to the digitalisation meter were introduced. The meter was printed and designed graphically and the labelling on each side removed. Thus, a factor of ambiguity was added. The number of steps was reduced from 13 to 10. When a player discarded a card, the meter was set back by the number of steps that would have been paid in data. The boards of all players were structured uniformly. Besides the change in dynamics for the digitalisation meter, the first part of the session was played as the one before. After several rounds the game was started again and each player would always have three cards on hand.

The greater choice and the opportunity for players to plan more strategically increased the level of involvement and the overall game experience. It took 6 rounds for a player to reach the box, which was now perceived as too fast after the change. Furthermore, it remained somewhat unclear why the data is divided into types, as it has no impact on the game.

5.5.4. Playtest Session 4

Nr. of players	4
Game Board	Hand drawn on paper , 13 fields
Digitalisation meter	Three scales, one for each type of data, general private data 20 steps, biosignals 16 steps, biometrics 10 steps
Stats	Same as previous session
Cards	Same as previous session
Data	Same as previous session

Changes, additions in the Rules
Every player has three cards on hand to choose and plan more strategically If a player reaches the “black box”, they get the data that is inside and the game figure is moved to the starting field on the players game board and the game continues

To include the differentiation and value in terms of identification grade into the game, the digitalisation meter changed. It now consisted of three scales which were colour -coded according to the data types. As biometrics are the most sensitive data, only 10 steps are necessary to reach the other side of the meter. For biosignals 16 steps are necessary and for general private data 20.

In this session it was mentioned that specifically the physical representation of the data would make one more aware that personal data is something real and that it can be continuously collected in daily life. Based on this statement, combined with time problems, the decision was made not to include any electronic elements at this point. Instead, it was decided to focus on further testing to understand how the interplay of the game elements and the degree of simulation of aspects of the real world influence the players’ reflection and the discussions between them.

5.5.5. Playtest Session 5

Nr. of players	3
Game Board	Same as previous session
Digitalisation meter	Same as previous session

Stats	Printed on cardboard, 5 steps, slides to move up the level
Cards	Same as previous session
Data	Same as previous session
Changes, additions in the Rules	
The game ends if one player has reached the maximum in all categories Winner is the player who owns the most data	

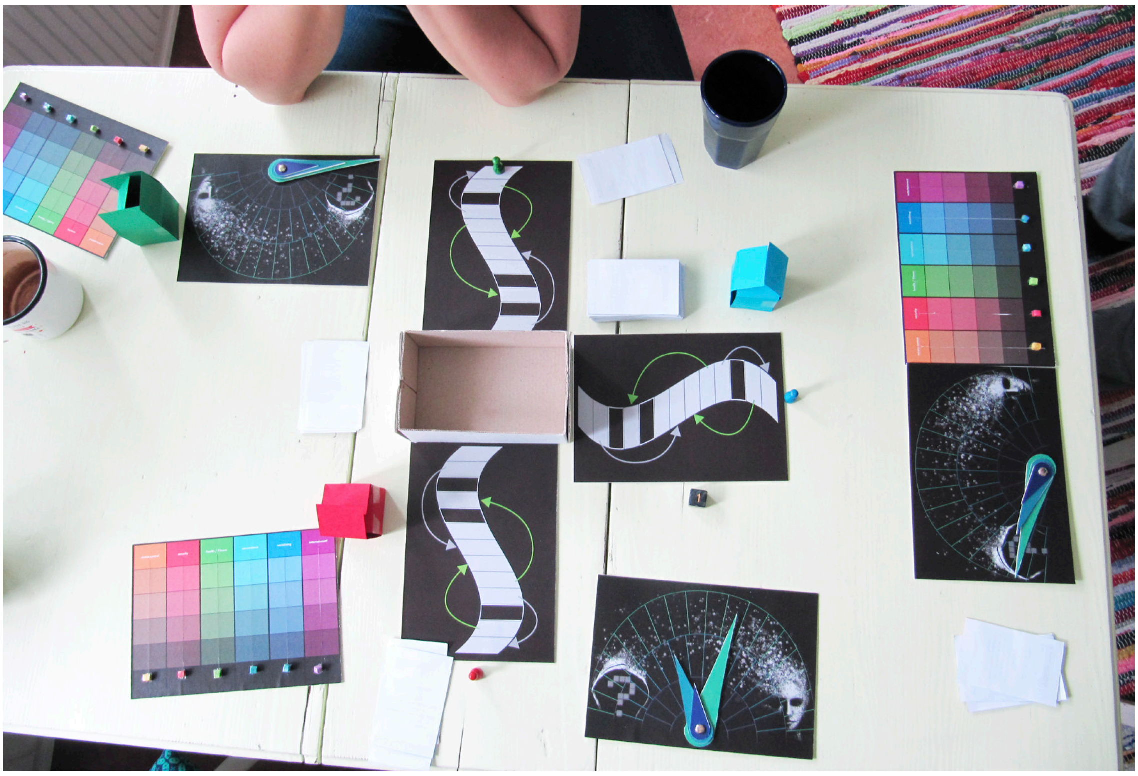


Figure 11: Playtest session with 5th iteration of the game prototype

Since with the last changes the game would not end when a player reaches the "black box", an ending condition had to be defined. The game would now end when a player has reached the maximum in all motivation categories. However, winner of the game would be the player who collected the most data.

5.5.6. Playtest Session 6

Nr. of players	3
Game Board	Game boards printed on cardboard
Digitalisation meter	Same as previous session
Stats	Same as previous session
Cards	Same as previous session
Data	Same as previous session
Changes, additions in the Rules	

For this session no adjustments were made. Based on the feedback that some formulations on the cards sounded almost mandatory, for the next Playtest some cards were marked as mandatory.

5.5.7. Playtest Session 7

Nr. of players	4
Game Board	Same as previous session
Digitalisation meter	Same as previous session
Stats	Same as previous session
Cards	Some cards are marked as mandatory to play
Data	Same as previous session
Changes, additions in the Rules	
Some cards need to be played and cannot be discarded Data types are given different value to be counted as final game point by the end of the game (biometrics 3 points, biosignals 2 points, general private data 1 point)	

Pictures from the playtesting sessions and the different prototype stages of the game elements can be found in the appendix.

6. Results

Through the interviews conducted at the end of the playtests, it became clear in the first session already that the behaviour of the players in the game mostly reflects their normal behaviour of handling private data and their attitude towards the topic of data privacy. In three playtests, in which the participants knew each other quite well, the players tried to convince each other to play a card and pay the data by referring to personal stories or pointing out characteristic behavioural patterns. This was particularly evident in the playtests, where players did not have three cards on hand, but had to make an immediate decision whether to play or discard a card. Although it was suggested in the first two sessions that more competition should be included, a later playtest showed that more competition leads to less reflection and discussion. Competition may increase the fun part in a game but it does not support the strived for goal of this game. The degree of conversation also depended on the composition of the players. Besides the personality, the factor if and how often one plays games as well as the general attitude and behaviour regarding private data played a decisive role. Participants who are in general rather careful in handling their data were often the ones who triggered reflective discussions by criticising use cases and explaining why they are discarding a card within the game. A few participants who are playing games more regularly mentioned that as soon as they are sitting in front of a game, they put themselves in the mode of playing and winning. They stated that they had only started to think more about the topic and what was going on in the game when it ended, respectively in the following feedback discussion. However, it could be observed and analysed from the video recordings that these participants also made comparisons to their daily behaviour and tried to justify some decisions. It should also be mentioned that some participants gave more feedback a few days later. They reported that they had continued to think about what kind of data they were actually sharing in order to receive something in return and how it is balanced against each other.

The given use cases in combination with the motivation categories was the aspect that enabled the connection to real life. It was pointed out that the description of actual and prospective use cases led to self-reflection. It made the players aware that personal data can be used in cases that are "absolutely normal " and where they would not necessarily think about it. In particular, the use of biometric data was surprising to most of them. Learning about different types of private data and the specific nature of biometric data led in some cases to a general rethinking of attitudes towards data privacy. One player referred to biometric data and partly also biosignals as their "real" data, their "real me". Some participants began to consider the handling of this data as generally dangerous. On the one hand because one cannot be sure in all cases where the data really goes and how it is used. On the other hand, the increased dependence on having one's biometric data recorded was criticised. As an example, the scenario of an unregistered immigrant was used and the potential problems they may face in parts of the world through the use of biometric data. Use cases that were surprising or even disturbing to some participants brought up stories that had been heard or read and some darker scenarios were imagined. In later playtests, the division of the meter into three scales in combination with the concept of the digital doppelgänger brought a deeper understanding that there are different levels of sensitivity to personal data.

By replacing the labelling on the digitalisation meter with graphic elements, an ambiguity factor was created and the dilemma with biometric data made visible. Playtesters questioned the losing condition and noted that you need a "digital face" if you want to participate in everyday life these days. However, it was also stated that the losing condition of spending too much personal data and making a digital copy of oneself has led to a more critical thinking about the collection of personal data and the fact that data can be reproduced indefinitely. The digitalisation meter took sometimes a lot of attention as soon as the pointers/marker was close to the last line. It would be interesting to test in a next step whether this fact changes when a digital component is used, and the active movement of the pointers is replaced by automatic feedback.

The transfer of the aesthetics of the digital and abstract into the analog and tangible was addressed by all participants and evaluated as positive and enlightening. The physical representation of something abstract such as data in combination with actual and/ or prospective use cases was described as particularly effective. It was mentioned that the manipulation of the different parts highlighted the interdependency, the pull and push factor between data, benefit and degree of digitalisation. What the participants wished for was more information about where the data would go in the specific use cases. In the subsequent feedback discussions, however, it was often recognized that the “black box” represents exactly this question and reflects this problem in reality.

An interesting aspect that was indicated in one of the previous interviews and confirmed in one of the interviews at the end of a playtesting session was that two people who deal with security issues and personal data management as part of their work do not transfer the awareness for data privacy to their private lives.

7. Discussion

The outcome of this project is an activist board game which addresses the issue of data privacy by simulating real world mechanics. It is not a fully developed and balanced game and rather to be understood as a concept that functions as a tool to create awareness of the issue of data privacy, provide information on different types of personal data and encourage self-reflection in this area.

The results show that with the help of an activist game an awareness for the topic of data privacy can be created amongst a wide range of people. A crucial point here is that the players do not take on a different role but are allowed to bring in their natural behaviour in dealing with private data and act according to their own values. Through the presented real and potential use cases a close connection to reality could be established and in combination with the motivation categories self-reflection was made possible, even if for some participants consciously only afterwards.

Although it is known that companies like facebook or google are constantly collecting data from people and using it for monetization purposes, the new knowledge about the types of private data and their different value made it more personal and real. In particular, the characteristic of biometric data to serve as a unique identifier of a natural person, combined with the concept of the digital doppelgänger, has led to a more critical view of what data is shared in return for what reward.

It is not enough to use the approach of critical play to design a game that acts as a tool to address a serious real world issue and create awareness as well as critical self-reflection about it. To achieve the desired goal, it is important to find the right balance between the effect the game should have on players and the gaming experience itself. As Flanagan formulates it,
"These play spaces [games] must retain all the elements that make a game enjoyable

while effectively communicating their message. Either component can be lost in the attempt to manifest the other, resulting is a game that is dull and didactic, or entertaining but hollow."(2007, p.249).

The observation that more competition was rather counterproductive to achieve the desired effect on the players, but was something that the participants suggested to make the game more entertaining, confirms that problem. In this respect, the decision to conduct more playtests and focus on the interplay of the game elements and their effect on the players, rather than integrate electronic components to simulate real world automatisms, was the right choice. The interconnected aspects of motivation, knowledge of private data, the accumulation of personal data and the often open question of where this data ends up are reflected in the game mechanics and only in combination allow for the desired result to be achieved. This reflection of connections and effects of real life in activist games makes "[the] game's mechanics (...) its message" (Flanagan, 2007,p. 185).

Unlike other games that address the issue of data privacy, this work is not designed to teach players about privacy in order to apply it in the work environment, nor is it intended to raise awareness by letting the player take on a different role. As two interviews revealed, knowledge of data privacy and data security is no guarantee that this will be transferred to private life. How it behaves in the other case cannot be estimated here. However, it was shown that the real and everyday examples of use and the possibility to still be oneself in the game were decisive for the self-reflection that resulted in a greater awareness.

The overall results of research, interviews and game feedback showed that a big knowledge gap in the area of data privacy exists. Although the introduction of the GDPR resulted in a higher awareness of data privacy in the development of digitally connected products and services and results in providing more transparency, the information and the way this information is communicated to the user is often perceived as annoying or not informative enough. Having the impression that it is most of the time the same template that is used and that one needs to give consent to almost everything results rather in carelessness or the feeling of powerlessness than being informed. As shown, informing people about what personal data is and what types of data are considered particularly sensitive and why, can create a higher level of awareness in dealing with one' s own data and respectively the issue of data privacy. It is not only important to provide information but also the way it is provided is important to have an educational effect and create awareness. Effective information on personal data protection gives users the possibility of active participation in the handling of their data, which in surveillance capitalism are on the one hand a kind of currency and on the other hand a commodity that can be monetized by companies. Besides making the abstract material of data visible and tangible, the different kind of interaction was also crucial to achieve the research goal. This quality is not directly transferable to other areas but provides a space for exploration of what types of interactions can be used in which context to communicate privacy information and, above all, to ensure that consent is given knowingly, actively and informed. Interaction designers are involved in the conception and design of a large variety of products and solutions that are equipped with an ever increasing number of sensors and which may also be involved in this respect. Smartphones alone contain a multitude of sensors. The fingerprint sensor, for example, could be directly included in the information about biometric data or the gyroscope, proximity sensor and light sensor could be used to give different levels of consent and so on.

Taking a look at games to identify qualities that can be advantageous in other areas and using a more playful approach for example for motivation or education is quite common. When it comes to biometric data, a playful approach is often used to make biometric technologies acceptable to users (Ellerbrok, 2011). How the view on games can contribute to explore possibilities to inform about biometric data and its use is currently not investigated. The development of this game offers a first approach for further research on how to effectively inform about the handling of personal data and data privacy in general.

Due to time constraints and the additional shift in focus in the thesis project it was not possible to include electronic parts in the game to test how and in which way dynamics are eventually changing and if the aimed for effect still remains. Digital components and the interaction with them in the game could reveal further insights that could be relevant to be transferred into the design of digital artefacts.

8. Conclusion

This thesis project aimed to create awareness of the issue of data privacy and encourage critical self-reflection on one’s own handling with personal data through critical play in form of an activist game. Furthermore, on the basis of the results, qualities should be identified that can be useful for interaction designers in the development of digitally connected artefacts, in order to efficiently inform users about the issue of data privacy and thus enable them to have a greater say in how their personal data is handled in the long run.

By using critical play in the form of an activist game, it was possible to address a topic of socio-economic, political and cultural importance and let the players explore correlations in the context of sharing personal data within the safe space of a game. With the focus on biometric data and the information about types of personal data with different degrees of sensitivity, the players were made aware of the different values of data. Actual and prospective use cases in combination with motivation categories that reflect why people are willing to share their personal information enabled self-reflection on their own behaviour when dealing with personal information. Including the metaphor of the digital doppelgänger and defining the sharing of too much sensitive information as losing condition the special characteristic of biometric identifiers was highlighted and brought up to a certain extend the dilemma of the use of biometric data. The ”black box” in which the data in form of tokens was given reflected the open questions of where shared data is actually going and who owns it. The question of owner ship was not directly addressed but brought in in later versions of the prototype by defining the winner of the game is the person who has collected the most data out of the ”black box”. Unfortunately, the inclusion of electronic elements to simulate automatisms in the real world was not possible due to time constraints but the transfer of the aesthetics of the digital and abstract into the analog and tangible perceived as explicitly enlightening and made the abstractness of data and its function as a kind of currency and commodity at the same time more graspable and real.

Not all aspects that contributed to answering the research question can be transferred to other areas, but they open up opportunities for further exploration. The insight gained through research, interviews and playtest feedback that there is a large knowledge gap regarding personal data and that people feel to a certain extent powerless when it comes to data protection, shows the importance of not only informing users in general about the handling of personal data and requesting permission to access it, but also to deal with the characteristics of different data. Another form of interaction can help users to make more informed consent decisions and raise awareness of privacy issues. Further research is needed on how this can be implemented in practice when designing digital connected solutions.

9. References

Adee, S., 2012. Digital doppelgangers: building an army of you. New Scientist, 215(2877), pp.38-41.

Adriaan Odendaal, Karla Zavala 2018, Unveiling Interfaces, board game. Available at: http://analoggamestudies.org/2018/12/black-boxes-out-of-cardboard-algorithmic-literacy-through-critical-board-game-design/ [Accessed 26. May 2020]

Beck, E., 2015. The Invisible Digital Identity: Assemblages in Digital Networks. Computers and Composition, 35, pp.125-140.

Bode, M. and Kristensen, D.B., 2016. The digital doppelgänger within. A study on self-tracking and the quantified self movement. Assembling consumption: Researching actors, networks and markets, pp.119-135.

Buchenau, M. & Suri, J (2000, August). Experience prototyping. In Proceedings of the 3rd conference on Designing interactive systems: processes, practices, methods, and techniques (pp. 424-433). ACM.

Castro, D., & McLaughlin, M. (2019). Survey: Majority of Americans Willing to Share Their Most Sensitive Personal Data. Retrieved 17 May 2020, from https://www.datainnovation.org/2019/01/survey-majority-of-americans-willing-to-share-their-most-sensitive-personal-data/

Cavoukian, A., 2009. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada.

Christl, W., & Spiekermann, S. (2016). Networks of control - A Report on Corporate Surveillance, Digital Tracking, Big Data & Privacy. Vienna: Facultas Verlags- und Buchhandels AG, facultas Universitätsverlag, Vienna, Austria.

Crawford, C. (1984). The art of computer game design. Berkeley, Calif.: Osborne/ McGraw-Hill.

Cross, N., 2010. Designerly Ways Of Knowing. London: Springer.

D. Haggerty, Richard V. Ericson, K., 2000. The surveillant assemblage. British Journal of Sociology, 51(4), pp.605-622.

Davis, K., & Patterson, D. (2012). Ethics of big data. Farnham: O'Reilly.

Ellerbrok, A. (2011). Playful Biometrics: Controversial Technology through the Lens of Play. The Sociological Quarterly, 52(4), 528-547. doi: 10.1111/j.1533-8525.2011.01218.x

Enderle, J. and Bronzino, J., 2012. Introduction to biomedical engineering. Academic press. pp.668.

European Commission - European Commission. n.d. What Is Personal Data?. [online] Available at: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en> [Accessed 29 April 2020].

European Parliament. (2018). REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL (pp. Article 4 (14).

Flanagan, M. (2013). Critical play. Cambridge: MIT Press.

Flanagan, M. and Lotko, A., 2009. Anxiety, Openness, and Activist Games: A Case Study for Critical Play. In DiGRA Conference.

Fullerton, T. and Zimmerman, E., 2014. Game Design Workshop. Boca Raton: CRC Press / Taylor & Francis.

Gamewright, [d0x3d!], board game. Available at:http://d0x3d.com/d0x3d/welcome.html [Accessed 26. May 2020].

Global Alliance of Data-Driven Marketing Association, UK DMA, Acxiom. (2018). Global data privacy: What the consumer really thinks. Global Alliance of Data-Driven Marketing Association.

Global Fraud Report 2019 | Experian. (2019). Retrieved 17 May 2020, from https://www.experian.com/decision-analytics/global-fraud-report-2019

Holmquist, L., 2005. Prototyping. interactions, 12(2), p.48.

Kipker, D. (2015). Privacy by Default und Privacy by Design. Datenschutz Und Datensicherheit - Dud, 39(6), 410. doi: 10.1007/s11623-015-0438-0

Kozlíková, K., Granja, C. and Leroy, C., 2010. Biological Signals In Medical Diagnostics.

Lupton, D., 2016. Digital companion species and eating data: Implications for theorising digital data–human assemblages. Big Data & Society, 3(1), p.205395171561994.

Secure Identity Alliance, 2019. Biometrics In Identity: Building Inclusive Futures And Protecting Civil Liberties. [online] Available at: <https://secureidentityalliance.org/resources/publications/entry/biometrics-in-identity-building-inclusive-futures-and-protecting-civil-liberties> [Accessed 4 May 2020].

Sicart, M., 2014. Play Matters. MIT Press.

Smith, G., 2016. Surveillance, Data and Embodiment. Body & Society, 22(2), pp.108-139.

Statistics/Different Types of Data/Quantitative and Qualitative Data - Wikibooks, open books for an open world. (2019). Retrieved 16 May 2020, from https://en.wikibooks.org/wiki/Statistics/Different_Types_of_Data/Quantitative_and_Qualitative_Data

Steve jackson Games Incorporated 2012, Control-Alt-Hack, board game, University of Washington.

Storni, C. (2014). The problem of de-sign as conjuring. Proceedings Of The 13Th Participatory Design Conference On Research Papers - PDC '14. doi: 10.1145/2661435.2661436

TeachPrivacy, Spot the Risk, computer game
Wilson, C. (2014). Interview techniques for UX practitioners (pp. 47 - 49). Waltham, MA: Morgan Kaufmann.

Zimmerman, J., Forlizzi, J., & Evenson, S. (2007, April). Research through design as a method for interaction design research in HCI. In Proceedings of the SIGCHI conference on Human factors in computing systems (pp. 493-502).

Zimmerman, J., Stolterman, E., & Forlizzi, J. (2010, August). An analysis and critique of Research through Design: towards a formalization of a research approach. In proceedings of the 8th ACM conference on designing interactive systems (pp. 310-319). ACM.

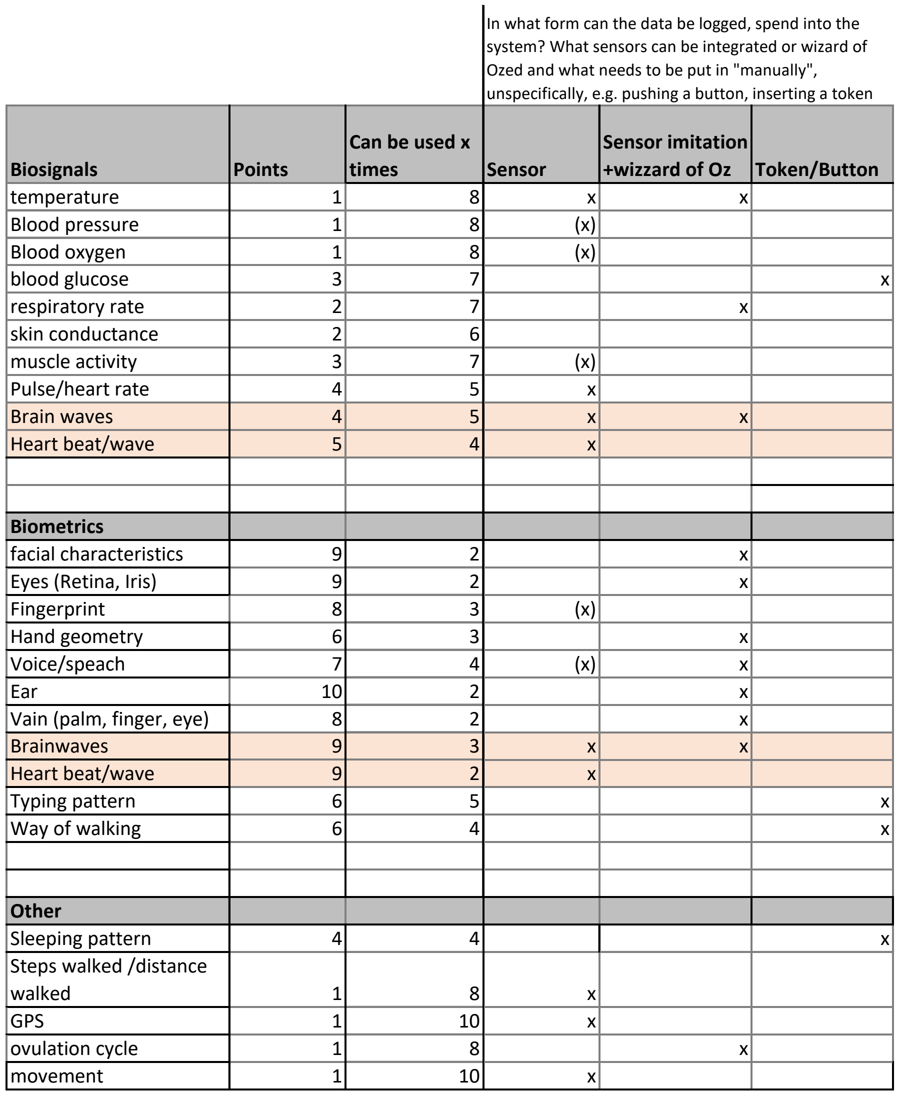
Zuboff, S., 2015. Big other: Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology, 30(1), pp.75-89.

Zuboff, S., 2016. Google As A Fortune Teller: The Secrets Of Surveillance Capitalism. [online] FAZ.NET. Available at: <https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html> [Accessed 29 April 2020].

10. Appendices

Appendix 1

Game Planning Spreadsheets



In what form can the data be logged, spend into the system? What sensors can be integrated or wizard of Ozed and what needs to be put in "manually", unspecifically, e.g. pushing a button, inserting a token

Biosignals	Points	Can be used x times	Sensor	Sensor imitation +wizzard of Oz	Token/Button
temperature	1	8	x	x	
Blood pressure	1	8	(x)		
Blood oxygen	1	8	(x)		
blood glucose	3	7			x
respiratory rate	2	7		x	
skin conductance	2	6			
muscle activity	3	7	(x)		
Pulse/heart rate	4	5	x		
Brain waves	4	5	x	x	
Heart beat/wave	5	4	x		
Biometrics					
facial characteristics	9	2		x	
Eyes (Retina, Iris)	9	2		x	
Fingerprint	8	3	(x)		
Hand geometry	6	3		x	
Voice/speach	7	4	(x)	x	
Ear	10	2		x	
Vain (palm, finger, eye)	8	2		x	
Brainwaves	9	3	x	x	
Heart beat/wave	9	2	x		
Typing pattern	6	5			x
Way of walking	6	4			x
Other					
Sleeping pattern	4	4			x
Steps walked /distance walked	1	8	x		
GPS	1	10	x		
ovulation cycle	1	8		x	
movement	1	10	x		

Action Cards		12	21	14	10	16	10	32	6	1
Benefit	**Cost**	access control	convenience	security	entertainment	health / fitness	social participation	you	other players	you + one other player of choice
Secure your phone and safe time by using Touch ID	fingerprint	x	x					x		
Secure your phone and safe time by using Face recognition	face characteristics	x	x					x		
Secure your phone and safe time with a blink of an eye	eyes	x	x					x		
All your friends are posting and sending around pictures with that new face filter. Don't be an outsider and get it too	face characteristics				x		x			x
make sure your medical records are not getting mixed up with other patients records	add your fingerprint to your health profile			x		x		x		
	add your ear characteristics to your health profile			x		x		x		
	add an iris scan to your health profile			x		x		x		
	save your heartbeat pattern as identifier			x		x		x		
travel fast and safe. identify yourself by just being you. avoid the long pass control queuing	provide eyes and iris scan		x	x				x		
travel fast and safe. identify yourself by just being you. avoid the long pass control queuing	face characteristics		x	x				x		
you are offered a higher position in your company with more responsibility. to enter a specific part of the building you need to identify yourself	provide fingerprint and hand geometry scan	x		x				x		
are you sick of switching on and off your electric devices and lights in your house by pressing a button? just tell them what they should do by using voice control	record your voice		x		x			x		
make sure your employees are payed for what they are really working. integrate a biometric attendance system	every other player needs to provide a fingerprint and finger vein scan	x	x						x	
	every other player needs to register their face characteristics and an iris scan	x	x						x	
	every other player needs to register their voice to be able to unlock their computer	x	x						x	
heavy keychain? get rid of having all that key to enter your house, the garage, the cellar, the apartment, and more. install a biometric door lock to lock and unlock your doors handsfree	face and iris scan		x	x				x		
heavy keychain? get rid of having all that key to enter your house, the garage, the cellar, the apartment, and more. install a biometric door lock to lock and unlock your doors handsfree	ear scan		x	x				x		
get a car or let your car upgrade with a accident prevention system	face characteristics, temperature, heartrate		x	x				x		
start your car with one touch	fingerprint		x					x		
for safety don't look and press around on /in the entertainment system of your car, use voice control instead. but at the same time make sure that not every person that is sitting with you in the	connect your voice to your car entertainment system		x		x			x		
rental cars/ carsharing. the carsharing companies in your area/town are collaborating. you don't need 5 different apps anymore. use one app and use touch ID to login in the app and also unlock the car	fingerprint/ face characteristics/ eye, iris scan/ heartbeat	x	x					x		
e-scooter companies in your area/town are collaborating. you don't need 5 different apps anymore. take the scooter of the brand that is closest to you	fingerprint/ heartbeat	x	x					x		
rental bikes companies in your area/town are collaborating. you don't need 5 different apps anymore. take the bike of the brand that is closest to you	fingerprint/ heartbeat	x	x					x		
make cash free payments easier and more secure. you don't need to remember all the pins for payment and transactions over your phone, with your card with a tan generator,etc. just pay	fingerprint		x	x				x		
you don't like your little sister/brother to use your beloved headphones. make sure only you can listen to music with them by using ear recognition	ear characteristics				x			x		
enjoy a new amazing gaming experience. play a game that reacts to your mood	heartrate, skin conductance, respiratory rate				x			x		
play a game with your mind	brainwaves				x			x		

for safety don't look and press around on /in the entertainment system of your car, use voice control instead. but at the same time make sure that not every person that is sitting with you in the	connect your voice to your car entertainment system		x		x			x		
rental cars/ carsharing. the carsharing companies in your area/town are collaborating. you don't need 5 different apps anymore. use one app and use touch ID to login in the app and also unlock the car	fingerprint/ face characteristics/ eye, iris scan/ heartbeat	x	x					x		
e-scooter companies in your area/town are collaborating. you don't need 5 different apps anymore. take the scooter of the brand that is closest to you	fingerprint/ heartbeat	x	x					x		
rental bikes companies in your area/town are collaborating. you don't need 5 different apps anymore. take the bike of the brand that is closest to you	fingerprint/ heartbeat	x	x					x		
make cash free payments easier and more secure. you don't need to remember all the pins for payment and transactions over your phone, with your card with a tan generator.etc. just pay	fingerprint		x	x				x		
you don't like your little sister/brother to use your beloved headphones. make sure only you can listen to music with them by using ear recognition	ear characteristics				x			x		
enjoy a new amazing gaming experience. play a game that reacts to your mood	heartrate, skin conductance, respiratory rate				x			x		
play a game with your mind	brainwaves				x			x		
you have raised blood pressure caused from stress. monitor your blood reassure and heart rate regularly for some time	blood pressure, heart rate					x		x		
towards mindfulness. train your relaxation and brainwaves	brainwaves					x		x		
send your kids to a school that is safe	eye,			x					x	
stay in contact with your friends social network	typing pattern						x	x		
You want to get more active so you bought a fitness tracker	heart rate, blood pressure GPS					x		x		
you want to loose weight. fitness tracker	heart rate, blood pressure, GPS					x		x		
sleep tracking	temperature, heart rate, respiratory rate, blood oxygen					x		x		
you want to train in the right and healthy way. track relevant data	heart rate , blood oxygen					x		x		
right breathing can reduce stress and improve your health in general	respiratory rate					x		x		
keep track of your baby's breathing	respiratory rate					x			x	
keep track of your baby's health stay connected	heart rate					x			x	
you want to get pregnant / not get pregnant	menstruation cycle, temperature					x		x		
making transactions fast end easy over the phone is a great thing, but you are worried that somebody could see it when typing in your password. use touch ID to make transactions	fingerprint	x	x	x						
	eye	x	x	x						
towards mindfulness. train your relaxation and brainwaves with a health training game	brainwaves				x					
Towards mindfulness. Relax by training your breath with a training game	respiratory rate				x					
Right breathing can reduce stress and improve your health in general. You are joining a choir	respiratory rate					x	x			
You want to share your training success with friends	Steps, Location					x	x			
Why not earning some money and get the appretiation you deserve by sharing pictures and stories	Face characteristics, Location				x		x			
Share your greatest moments in life with your friends and the world	Face characteristics, Location				x		x			
Stay in contact with your friends the fast and easy way by using a messenger	Typing pattern, Voice						x			
throw a BBQ party in the park and invite all your friends	Typing pattern, Location						x			
Ypiu are living far away from your family. Interact with them through a smart gadget and share your love	Heartrate, Location		x				x			
							x			

1	Event Cards		1	7	2	4				
er	**Description**	**Cost**	you	all players	a player of your choice	you + one player of your choice				
	Spoofing attack	2x biometric	x							
	Spoofing attack	2x biometric			x					
	Hacker attack	1x biometric, 1x biosignal		x						
	Hacker attack	1x biometric, 1x biosignal			x					
	Hacker attack	1x biometric, 1x biosignal				x				
	The government has changed. New security regulations are introduced			x						
	TO stop a deadly virus from spreading the government intoduces a security and health tracking system			x						
	The number of terroristic attacks is increasing. Social security is in danger. A public security system is introduced			x						
		Benefit								
	New security ragulations are introduced in your country	2x biosignal				x				
	New security ragulations are introduced globally	2x biometric		x		x				
	New data privacy regulations are introduced in your country	2x biosignal				x				
	New data privacy regulations are introduced globally	2x biometric		x						
	The open source market is growing rapidly. Transparancy increases	1x biometric, 1x biosignal, 1x general		x						

Appendix 2

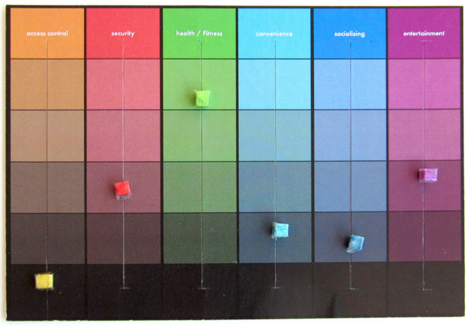
Playtests & Material

Game elements of final iteration

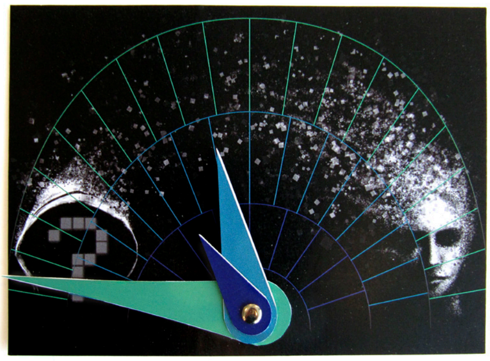
Make your phone more secure and additionally save time by using Touch ID
Cost

Action cards. Describing a use case, costs of data, information on who needs to pay , motivation categories

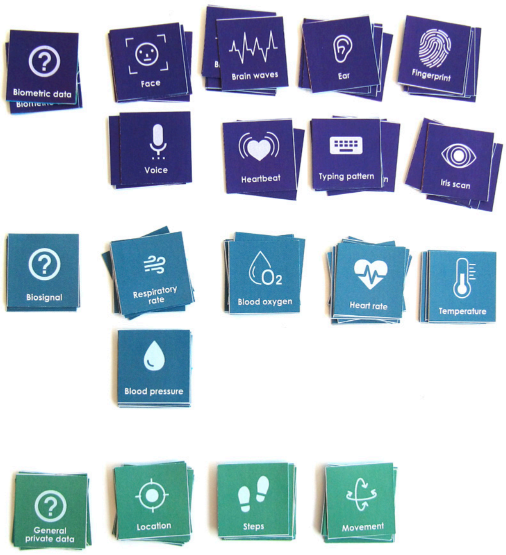
Event cards. Event description, costs of data or benefit (return of data), information on who is effected



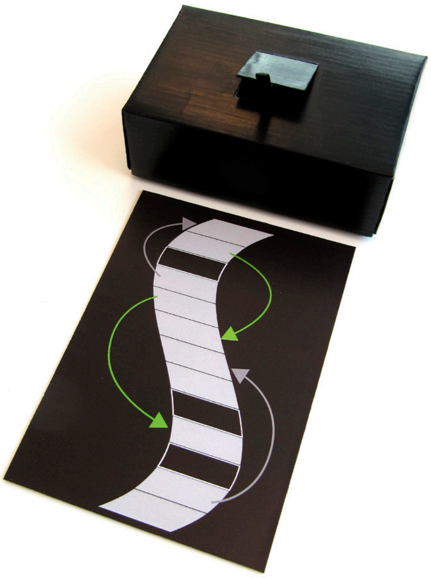
Motivation categories. Categorised in access control, security, health/fitness, convenience, socialising and entertainment



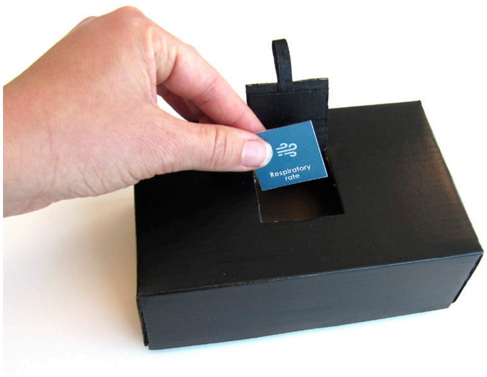
Digitalisation meter. Meter going from "Anonymous" to "Digital doppelgänger", separated in three scales, one for each type of data



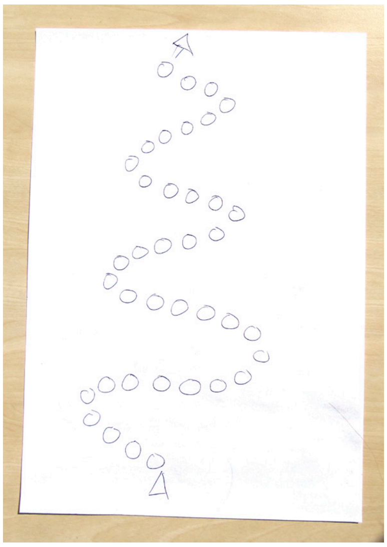
Data tokens. Categorised and colour coded after biometric data, biosignals and general personal data

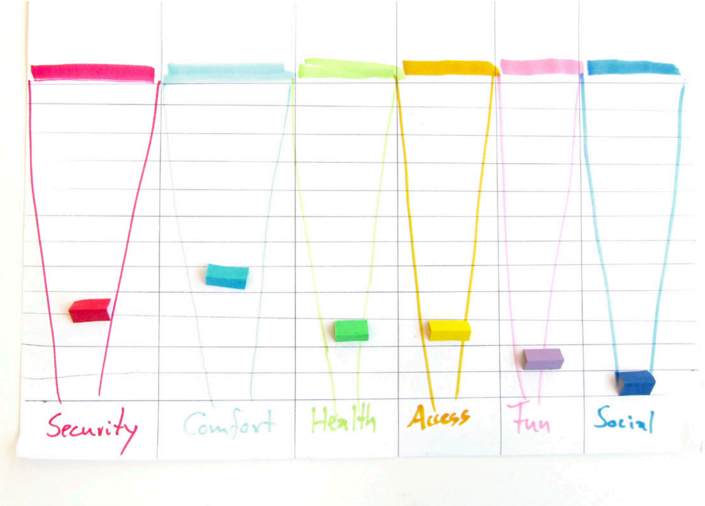


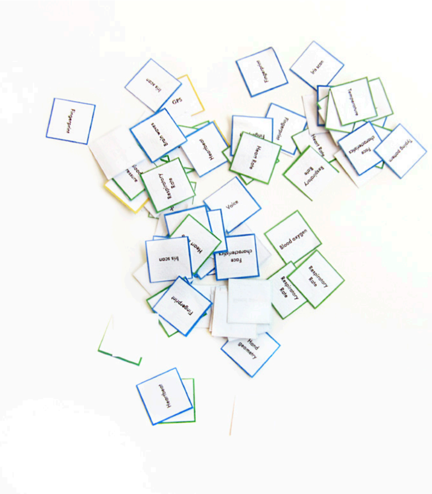
Game board & Black Box. Game board with up and down connections and marked fields for event cards. Black Box in which all the data tokens need to be "payed"

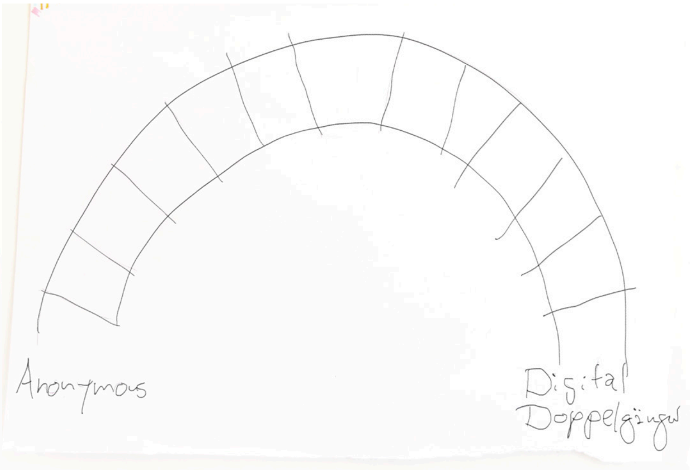


First prototype materials & Testing



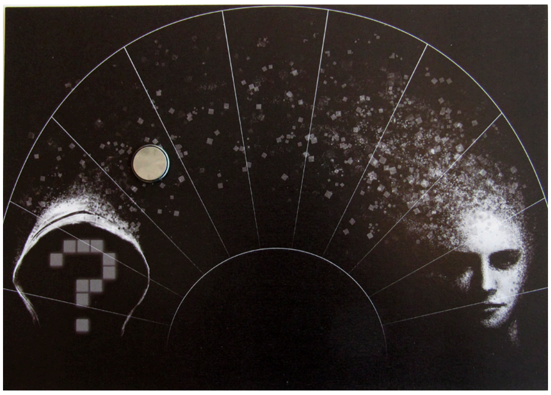


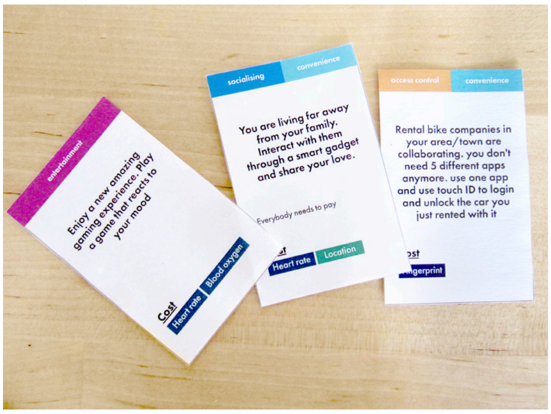


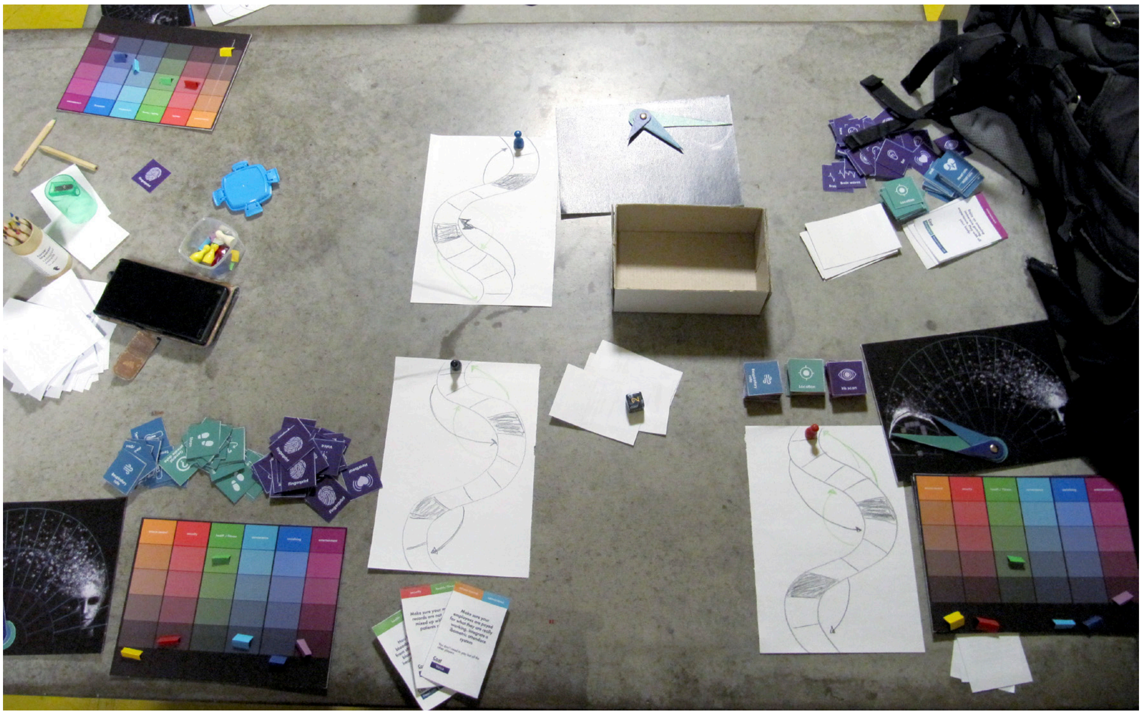


Playtest sessions

Right breathing can reduce stress and improve your health in general. You are joining a choir.
Cost
Respiratory rate
Anonymous
Digital Copy

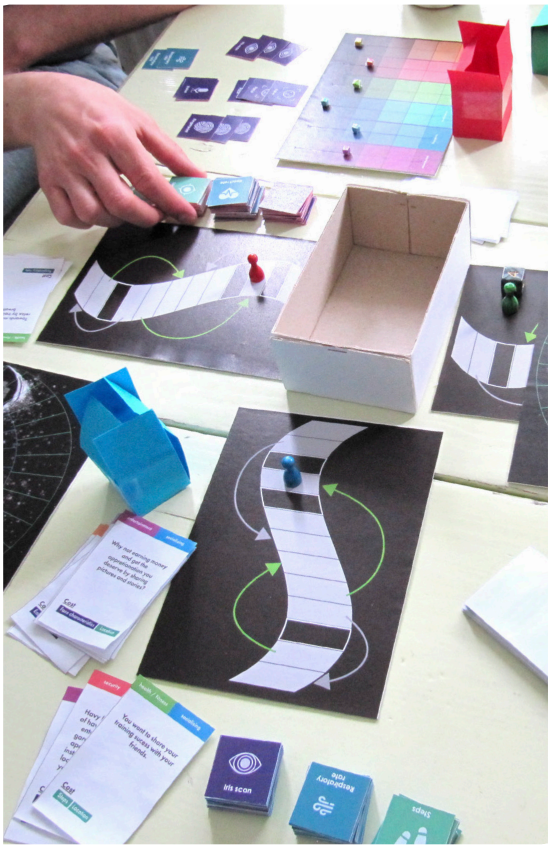



entertainment
Enjoy a new amazing gaming experience. Play a game that reacts to your mood
Cost
Heart rate
Blood oxygen
socialising
convenience
You are living far away from your family. Interact with them through a smart gadget and share your love.
Everybody needs to pay
Heart rate
Location
access control
convenience
Rental bike companies in your area/town are collaborating. you don't need 5 different apps anymore. use one app and use touch ID to login and unlock the car you just rented with it
Fingerprint



Location
Blood pressure
Blood oxygen
Fingerprint

Location
Fingerprint
Voice
Typing pattern
Iris sc
Heartbeat


Iris scan
Respiratory rate
Steps
You want to share your training survey with your friends.
Cost

Appendix 3

Quotes from Feedback & Interviews

- “Oh, yes. I’ll give away my brain for entertainment”
- “I pay! Welcome to the future!”
- “Security questions make me nervous about the future. If it’s labelled security I tend to rather pay then not”
- “Isn’t it always the question of how much freedom and privacy for how much security?”
- “It’s all just one big, swirling question mark.”
- “Seems like everybody else “owns” your digital copy, but you”
- “Biometric, biosignals, bio-whatever, it’s all me!”
- “ Now it gets personal. Do I really need to pay?”
- “ Did I collected enough different data to build a person out of it?” (moving around the data tokens on the table)
- “Ear? What do they want with my ear?”
- “Hell yeah, I own all of your fingers!”
- “ I have done that in real already. So here we go. I pay for my sins.”
- “I’ll just use drag-make-up to stay anonymous”
- “What would happen if somebody cuts off your face?”
- “Imagine you are sleeping and your partner just takes your finger to unlock your phone and search through it”
- “ It’s like truth or dare for your morals”
- “ I would like to know where all the data is really going . – Oooh! Blackbox!”
- “I try to stay informed, but it’s really hard. I mostly take the time to read through the privacy information but there is often sooo much irrelevant. And everybody seems to use the same template and just changes some names.”
- “Aren’t we living in the information age? So we are uninformed in the information age, nice.”