Phonopticon: The age of mobile surveillance.

by Mudit Ganguly

A thesis exhibition presented to OCAD University

in partial fulfillment of the requirements

for the degree of Master of Design in Digital Futures

Toronto, Ontario, Canada, April 2018

Copyright Notice

Author's Declaration

I hereby declare that I am the sole author of this thesis.

This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I authorize OCAD University to lend this thesis to other institutions or individuals for the purpose of scholarly research.

I understand that my thesis may be made electronically available to the public.

I further authorize OCAD University to reproduce this thesis by photocopying or by other means, in total or in part, at the request of other institutions or individuals for the purpose of scholarly research.

Mudit Ganguly

Mudit Ganguly, OCAD University, Phonopticon: The age of mobile surveillance, Master of Design, Digital Futures, 2018

Abstract

Smartphones play an intimate role in everyday life. What many users don't know is that these devices have unparalleled access to their data. Companies like Facebook, Apple and Google commodify and share personal data with third parties. This data passes back and forth between third parties but also makes its way to governments. The controversy that followed Edward Snowden's revelations is an ideal segue into current problems of surveillance and privacy.

This thesis argues that knowledge about privacy breaches carried out by mobile applications leads to awareness about privacy. Research through design was used to create the Phonopticon, an immersive installation that gives viewers knowledge about privacy breaches. Just like Jeremy Bentham's panopticon enables guards to observe prisoners without their knowledge, the applications on our smartphones gather and share our data without our knowledge. This thesis contends that we're living in a Phonopticon – the age of mobile surveillance.

Keywords: Data Visualization, Data Breach Literacy, Mobile Applications, Surveillance, Panopticon.

Acknowledgments

This thesis would not have been possible without the unconditional support of the faculty and staff at OCAD University. I would like to especially thank my advisors, Isabel Meirelles and Kate Hartman for their guidance and valuable feedback and would like to acknowledge the assistance of Reza Safaei, Roxanne Henry and Katie Micak in the development of the prototype. I am grateful to all the wonderful participants of this project who volunteered their precious time and feedback. Without the assistance of Joshua Paglione, David Macintosh and Sayeda Akbary this thesis would have been entirely speculative. I would additionally like to acknowledge the unending support I receive from my parents, Mali Ganguly and Alin Ganguly. Lastly, I wish to thank all my peers and friends especially Stefani Joane Germanotta, Afaq Ahmed Karadia and Samah Ahmed for their support.

I would like to acknowledge OCAD University for their support in the form of the Ontario Graduate Scholarship in the completion of this research.

Table of Contents

-

List of Figures

PHONOPTICON: THE AGE OF MOBILE SURVEILLANCE.

Introduction

A tiny bit of paranoia can be healthy (Dillian, 2017). What if there were entities that were always watching, listening and storing our every move? The idea that there exists an entity that has endless information about users might seem very far fetched. However, it is far from impossible. Facebook knows our social network. It knows what users look like, as well as what their friends and families look like and knows what their political affiliations are (Dillan, 2017). If users ever feel that Facebook knows them intimately, that's because it does (Komando, 2016). Amazon knows our tastes in movies, books, electronics, and clothes. Amazon's Alexa knows what we sound like and catches every conversation we have around it. Google has information about our movements, our voice, our internet searches and even records the ads we click on. How far-fetched does the idea of an entity watching our every move sound now?

Since the introduction of the first iPhone in 2007 and the introduction of the first Android smartphone in 2008, the number of smartphone applications has grown. As of 2017, the Android App Store had 2.8 million applications, and Apple's App Store had 2.2 million applications (Statista, 2018). The utility of these applications cannot be denied, and they use a smartphone's numerous components to give users essential services and exciting features. Examples of these components are the front and back cameras, microphone, text messages and call logs. Applications can even use WiFi points and GPS data to track user locations. As useful as mobile applications are, users must consider how access to these components allow applications to intrude on a user's security and privacy.

There exist numerous applications that can turn any smartphone into a sophisticated, wireless surveillance device, and such operations are undetectable to the average user (Raphael, 2008). Many applications collect sensitive data behind our backs. For example, Facebook was found to be uploading users' contact lists to their servers. So even if you did not have a Facebook account, but your friend did, Facebook would still have your phone number because your friend has your number on their phone (Grobart, 2011). The crux of privacy issues around applications is more than just poor communication or privacy controls (King, Lampinen & Smolen, 2011).

There is a difference between what an application does and what it claims to do that leads to unrealistic expectations regarding privacy. This might occur because the information sharing model of applications is complex, and users find themselves lost in the legal and technical jargon used. Various researchers have examined concepts of user privacy and smartphones and have proposed different solutions. Some researchers were concerned about protecting users' privacy by analysing the applications themselves (Chin, Felt, Greenwood & Wagner, 2011). Other researchers assessed user concerns (Felt, Egelman &Wagner, 2012) and user behaviour (Felt, Ha, Egelman, Haney, Chin & Wagner, 2012). Some researchers offered users privacy control in the form of mobile applications that give false data to third parties like Mockdroid (Beresford, Rice, Skehin & Sohan, 2012). Others thought of changing the system architecture of the smartphone itself (Hornyack, Wetherall, Han, Jung & Schecter, 2011) or adding a new 'privacy mode' to smartphones that limit what data applications can take (Zhou, Zhang, Jiang & Freeh, 2011). While these frameworks are suitable, they focus on users making changes to their behaviour to protect themselves or relied on users changing something about their smartphones. In this thesis, I focus on raising awareness and educating users so that they make informed decisions regarding the applications they download.

Users today have little support in making trustworthy decisions about what applications to install. Current solutions rely on users to opt-out of these applications sharing their data because by default the applications are designed to share data. What if we invert this relationship? What if applications only shared data when they were asked to do so by the users? Such a scenario would give users more control over their data. But for it to work effectively users must know precisely what data an application gathers, what data an application shares, and with whom does it share that data. However, that is not the case and many users have an uninformed opinion of what an application does with their data. In an ideal world, the user's opinion aligns perfectly with what the application does. By giving users insight and knowledge into widely recognized misconceptions about applications, this thesis attempted to inform users about privacy breaches so that they can make informed decisions about smartphone applications.

This thesis used Ken Wilber's All Quadrant All Level (AQAL) as a theoretical framework to guide it. This framework enabled the thesis to look at the subject of mobile surveillance holistically.

The first step was to compare the surveillance carried out by smartphone applications to the surveillance carried out in Jeremy Bentham's panopticon. Following that this thesis examined what users understand about smartphone applications and whether more knowledge in that field would lead to privacy-conscious attitudes. A prospective cohort study of six participants was used to investigate how users view applications, what they know about applications and how their knowledge relates to their privacy concerns. A prospective cohort study is a study that examines a group of individuals over time (NCI, 2018). An open source application, NetworkStatsManager, was deployed within the group to find out how much data each application on their smartphones gave away to third parties. The goal was to examine whether more knowledge about how applications, such as Facebook, that send data to third parties would lead to an alignment in the user's cognitive model. Simultaneously, this thesis also used research through design and Barry Boehm's Spiral Model of Software Development to develop a physical installation, the Phonopticon, that serves as a data visualization tool which informs users about how mobile applications spy on them. The Phonopticon is a representation of the surveillance carried out by applications that are installed on smartphones.

This thesis sheds light on the growth of ubiquitous surveillance carried out by our smartphones and proposes a possible solution for understanding how mobile applications spy on us. The following research questions drove this thesis:

1.What are the similarities between surveillance carried out in our mobile devices and the surveillance structure proposed by Jeremy Bentham's Panopticon?

This question is addressed in Chapter 2 of this paper which includes the literature review. The literature review begins with an introduction to the panopticon and then it draws parallels between the panopticon and existing surveillance systems embedded in smartphone applications. Once it was established that smartphones and the applications on them are the new age panopticon, the focus of this literature review

shifted towards investigating user awareness about privacy breaches along with a viable way of educating users about data breaches using data visualizations. Examples of such work are in Chapter 3 which also serves as the contextual review of this thesis.

2. Do users see value in having more education about surveillance?

This thesis aimed to find out if users cared about surveillance and privacy. For this purpose, a prospective cohort study was carried out to access user opinion. Chapter 4 contains a detailed explanation of this cohort study. Pew Research Center carried out a survey in 2015 titled *Americans' Attitudes About Privacy, Security and Surveillance*. This survey covered surveillance as a vast subject but did not touch upon the surveillance carried out by smartphone applications specifically. This thesis aimed to investigate this less researched area and used Pew's survey as an inspiration.

3. How can data visualization be used as a meaningful tool to educate users about surveillance?

The answer to this question presents itself in the form of the Phonopticon. The Phonopticon is an immersive installation that uses data visualizations to educate and inform users of privacy breaches along with methods to shield themselves from surveillance. Research through design was used in the development of the Phonopticon, and a prospective cohort study was used to assess user feedback. Chapter 5 contains the detailed description of the prototype, the rationale for the design decisions as well as the specific tools and techniques used. Additionally, it includes descriptions of the implementation approach used in user testing sessions and focus groups. The prototype uses an artistic data visualisation that contains distortions. The prototype is explained in detail in Chapter 5 of this thesis.

This thesis ends with Chapter 6 which contains the conclusions of this thesis study followed by future research that could be undertaken.

Readers of this thesis must be aware of its scope and limitations. This research dealt with giving users education and information regarding privacy breaches but did not oversee if this led to change in user behavior. There was no way to isolate users to make sure any change in behavior was a result of only

the education and information given to them. Additionally, the time provided to carry out this research was too short to assess any change in behavior. The prospective cohort study was limited to Android users, and members of the cohort group were individuals based in Toronto, Canada. The size of this cohort was too small to make any generalizations. NetworkStatsManager was deployed within the cohort group and calculated the total data the applications on the member's smartphone sent to third parties. But this study did not investigate the details of that data, or to whom that data was sent to. The prototype developed in this study, the Phonopticon, visualises the qualitative data that viewers provide it but does not give viewers an accurate depiction of the surveillance carried out on them by smartphone applications.

This introduction offered a summary of this thesis. It began with an explanation of how applications use the various capabilities of a smartphone to spy on users and was followed by mentioning other research done in the field of mobile application and user privacy which placed this thesis amongst other contemporary work. The introduction also mentioned the framework and methodologies used in the development of the thesis. And it concluded with the three research questions of this thesis along with the scope and limitations of this thesis.

1. Theoretical Framework

This thesis looked at surveillance carried out via applications on mobile devices in 2018 and needed a lens that allowed for the observation of the bigger picture as well as the observation of minute details. The theoretical framework used was the All Quadrant All Level (AQAL) framework. AQAL is a part of the Integral Theory developed by Ken Wilber. The Integral Theory enables the examination of ourselves and the world around us in comprehensive and effective ways (Wilber, 2005). Additionally, it allows for the examination of diverging theories and thinkers into one framework. Wilber developed the All Quadrant All Level (AQAL) framework (Figure 1) within Integral Theory.

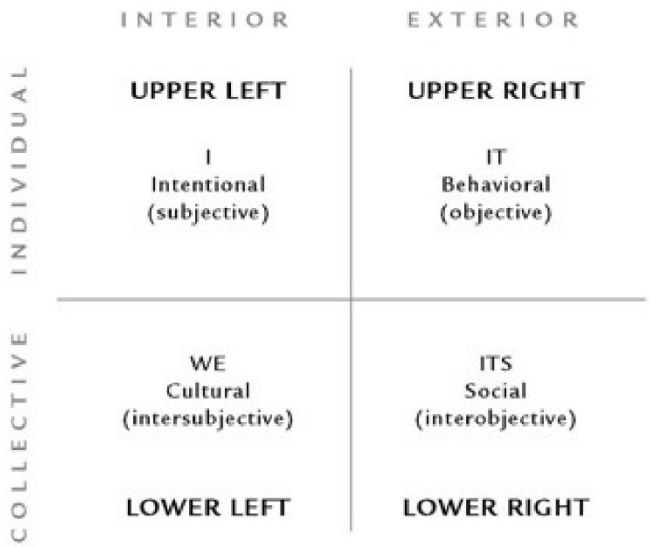


Figure 1. The Four Quadrants (Esbjörn-Hargens 2009, p.3)

AQAL was used as the theoretical framework to guide this research because this framework argues that all knowledge and experiences can be plotted onto a grid that is divided into four quadrants. These quadrants are exterior individual, exterior collective, interior collective and interior individual (Wilber, 2010). Wilber argued that AQAL offers a comprehensive outlook on a subject and using AQAL, this thesis was able to examine the similarities between the panopticon and the Phonopticon as well as the differences. The AQAL lens gave this research a holistic view of surveillance. Surveillance involves both individual users and systems, it relates to both introspection and expression and deals with both

interpersonal and intrapersonal relationships. Since each quadrant of the AQAL framework has a relationship with this paper; Ken Wilber's diagram was reinterpreted (Figure 2) to suit this thesis's needs.

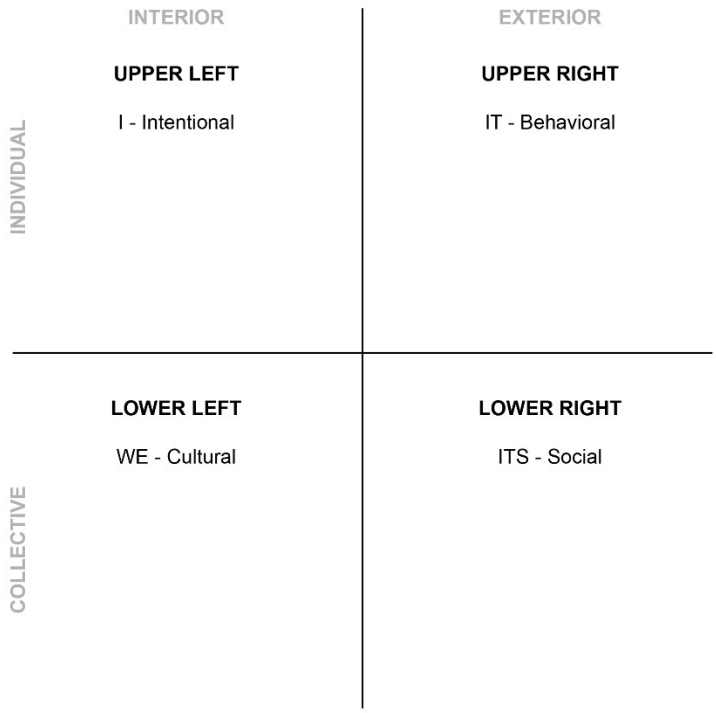


Figure 2. My interpretation of Wilber's AQAL framework

Surveillance is singular, plural, internal and external. And the four quadrants of the AQAL framework gave this thesis the ability to examine the many facets of surveillance. These quadrants are:

IT or Exterior individual (upper-right): This quadrant interprets the users' behaviour. How do internal thoughts influence those behaviours? How does a user behave, both online and offline, when they know they are under surveillance?

ITS or Exterior collective (lower-right): This section interprets the behaviour of society. How have societies in the past resisted surveillance? How do countries and governments protect their citizens? For example a few years ago, the European Union passed a law that allowed its citizens to the 'Right to be Forgotten,' forcing Google to remove "outdated" links in searches (Woods, 2014).

WE or Interior collective(lower-left): This quadrant interprets the collective consciousness of society. This section deals with what society thinks of surveillance and privacy. For example, 56% of Americans believe that the National Security Agency (NSA) is justified when it tracks telephone records to investigates terrorism (Dimock, 2013).

I or Interior individual (upper-left quadrant): This quadrant interprets the users' interior experiences and focuses on interpersonal concepts. Are users aware of privacy breaches happening? Do they know that they are under surveillance?

This research investigated what privacy meant to users, and what all users thought of it collectively. Privacy and surveillance not only change how users see themselves but also affect how users view each other. This section outlined the theoretical framework used in this thesis. The AQAL framework not only guided the structure of the literature review but also guided the prospective cohort study and directed the development of the Phonopticon. The following section discusses the literature review.

2. Literature Review

This literature review begins with an introduction to the panopticon. This review then breaks down the panopticon into its characteristics after which it examines the cognitive dissonance shared by users along with the use of education to reduce that dissonance.

2.1. Introduction to the Panopticon

Because the panopticon is brought up numerous times in this thesis, the section below offers a brief introduction to the panopticon for clarity. The word panopticon is made up of two words, pan and optikon. Pan meaning ‘all’ and optikon which relates to the eye or vision (Merriam-Webster, 2018). When combined they mean a vision or gaze that can see everything.

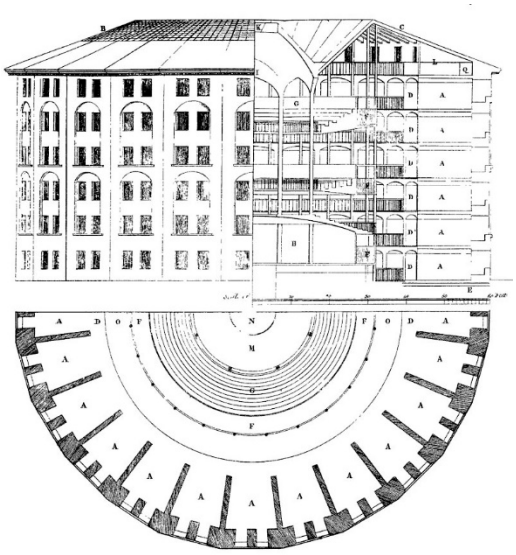


Figure 3. Elevation, section and plan of Jeremy Bentham's Panopticon penitentiary (Reveley 1971)

Bart Simon’s description of the panopticon is clear and concise. He describes it as a circular building which has a watch tower at the center (Simon, 2002). The tower contains windows that open onto the inner section of the building. The outline of the building is lined with prison cells, and each cell goes all the way through the whole width of the building. Each cell contains two windows, one that looks towards the tower and the other that lets light into the prisoner's room. The arrangement of windows

creates a backlight effect that allows the guard to observe the prisoner without being seen (Figure 3). After that, the cells need to be populated with prisoners and the tower needs to be populated with any number of guards. There are numerous cells, each with a lonely prisoner, segregated and constantly visible (Foucault, 1979). The panopticon was designed by Jeremy Bentham who was a philosopher and believer in prison reform. However, it is Michel Foucault, a historian and philosopher who is responsible for the panopticon's popularity (Foucault, 1979). He studied modern institutions and the relation of power in those institutions and perhaps his most popular analysis of such institutions was the panopticon. What is important for Foucault's adaptation of Bentham's plan is that the prisoner must be aware of the presence of the guard (Foucault, 1975). Simon paints a dystopic image of the panopticon when he says that the panopticon copies the helplessness individuals often feel in the face of overwhelming institutions like prisons, hospitals and schools (Foucault, 1979).

This thesis argues that users carry a miniature panopticon in their pockets in the form of smartphone applications. Such users can run but cannot hide from surveillance systems embedded in the applications installed on smartphones. The next section explains this further by drawing parallels between the panopticon and existing surveillance systems embedded in smartphone applications. The following literature review is structured on the AQAL quadrants.

2.2. Exterior Individual

This section focuses on watching the users from outside. It examines the users' external behaviour that is a result of their internal opinions and ideas. The guards, the prisoners and the relationship between them are vital to the functioning of the panopticon. This relationship contains two main components that are essential to its functioning as a tool for surveillance. These are the "visibility" of a guard and the "unverifiable" act of being gazed upon (Foucault, 1979.p. 200). Foucault defines "visibility" as the ability of the prisoners to observe the tower that spies on them. He defines "unverifiable" as the prisoners who never know if the guard in the tower is watching them but must be assured that they are always being watched (Brown n.d.).

There are similarities and differences between the panopticon and the Phonopticon. We examine the similarities first. Edward Snowden said “I watched NSA tracking people's Internet activities as they typed. I became aware of just how invasive U.S. surveillance capabilities had become. I realized the true breadth of this system. And almost nobody knew it was happening” (Zetter, 2014). Snowden’s words are eerily like the environment inside the panopticon. This quote connects the panoptic system of surveillance to contemporary methods of surveillance. Third-party services gather data about users in exchange for their service and sometimes the need to access this data is essential for an application to function. For example, Uber needs to know a users’ location to give that user a list of nearby drivers. Applications could, and do, send such personal data elsewhere. They can do this because they are developed by combining third-party libraries (Rodriguez & Sundaresan, 2017). These libraries are a treasure of confidential data, data which can be transmitted to online servers – or to other companies altogether. A network of such libraries might be able to create detailed digital profiles of users. For example, a person might give Uber permission access to their location, and another application Facebook access to their contacts. Even though they are two separate permissions, one for each application, what would happen if both apps incorporate the same third-party library? The library’s developer could combine both incoming data sets and complete a digital profile of a user. These applications rely on in-app permissions to get users to agree to this data transfer.

Even though mobile phones give users the ability to enable or disable permissions for each application, this method contains many shortcomings. Firstly, users are unaware that when they give these applications permissions to access their data, they enable third-parties to access it as well. Secondly, users do not know which applications share their data with the same third-party services, and they remain in the dark about the substantial amounts of data that those third parties collect. Users might have some awareness that an application is sending data to third parties, but they have no idea who these third parties are, and they would never know such information because applications are not required to disclose the software libraries they use (Shields, 2011). Even if applications disclose such information, they do so in the form of long legal documents that average users won't read let alone comprehend (Sunyaev, 2015).

Examples of sharing data with third parties were brought to light in 2017 by the Haystack Project. The Haystack Project found that more than 70% of smartphone applications share personal data with third parties like Google Analytics (Razaghpanah et al., 2018). Thus, there is evidence that several applications share private data with third parties without the users' knowledge. This supports the argument that there is some similarity between the panopticon and the Phonopticon, which is that both the users and prisoners are always being watched.

The difference between the panopticon and the Phonopticon lies in the behaviour of the prisoner and the mobile phone users. In the panopticon, the prisoners behave themselves because they fear punishment. The prisoners conform as there is no room for deviations in behaviour. Edward Snowden says, "Under observation, we act less free, which means we effectively are less free." (Germanos, 2014). Glenn Greenwald seems to think so too. "A citizenry that is aware of always being watched quickly becomes a compliant and fearful one." (Porter, 2014). Snowden and Greenwald believe that constant surveillance in contemporary times might lead to users censoring their online behaviour. However, mobile phone users do not regulate their behaviour when using their smartphones. We often send pictures, messages and say things on our mobile phone that might get us into trouble if they became public. Smartphones allow to express themselves over the internet freely. Twitter and Facebook are examples of where users' express opinions that might be considered deviant depending on the context. Example of such events are the Iranian election protests that followed the 2009 Iranian presidential election. These protests were known as the Facebook Revolution because videos of the protests went viral on Facebook (IBO, 2009) and the revolution picked up traction and followers following the online spread of content on Twitter (Moscaritolo, 2009). During the Iranian Revolution Twitter was used by protesters to hire hackers to launch cyber warfare tactics against the Iranian government. Such behaviour puts users in an even more precarious situation than the prisoners of the panopticon because when users do not censor themselves they allow third parties to look at their unfiltered and uninhibited data.

2.3. Exterior Collective

This section looks at society from outside. It examines current surveillance scenarios and steps taken by governments to resist or accept surveillance.

Societies of Control, developed by Gilles Deleuze in the *Postscripts on the Society of Control* (1992), offers an insight into our contemporary society. Societies of Control is a concept that is useful in considering and questioning how control and freedom and our orientation towards control and freedom are increasingly interconnected in a technological and surveillance driven world. In its simplest explanation, Societies of Control is as an evolving form of discipline, where discipline moves beyond enclosed structures and outward into a sophisticated network of installed systems. In Societies of Control, the shift in the governing of a population is not limited to enclosed spaces like the office or factory but instead is freed up to operate in open systems and networks (Deleuze, 1992). Deleuze recognised the advancement in technology as the major force in the creation of societies of control. Technologies like smartphones create the ultimate form of mobility for users because users are constantly connected to the internet through their smartphones. It is relevant to note that Deleuze believes that "control is not discipline" (Deleuze, 1995. p. 322). For example, highways that allow travellers to move quickly between distant places. We cannot confine travellers with such highways, but by making highways we multiply the means of control as we decide where the travellers can go and where they cannot go. So even though users can travel freely without being confined they can still be perfectly controlled. In other words, while living in a Society of Control can feel incredibly freeing at times, it also comes with increased surveillance and that is the trade-off. Smartphones are freeing, and they let users access the internet, but they also exhibit new forms of control. The mobile applications on smartphones collect data about user interactions, the websites they visit and who they talk to. In Societies of Control, the technology embedded in smartphones provide the freedom to work anywhere and buy anything with a few taps on screen. However, they also trap users in a network that they cannot escape. Living in Societies of Control might seem convenient, but it is difficult to remove ourselves from the networks created by technology.

There are certain governments that are taking steps to counter these Societies of Control. The European Union passed a law that entitled its citizens to the ‘Right to be Forgotten’, forcing Google to remove “outdated” and “irrelevant” links in searches (Woods, 2014). Such laws are now gaining traction across the globe in countries like India (Gargi, 2016), Spain (Peguera, 2017) and South Korea (Lim, 2016). In these cases, change arose when users demanded to be protected from surveillance. Thus far we’ve seen examples of users asking for protection from surveillance but there are cases where users have asked for more surveillance instead. Edward Snowden’s revelations in 2013 exposed the government of Singapore as a third party that was providing many countries, like the United States of America, data about Singaporeans phone data. The citizens of Singapore paid little attention to this news (Lee, 2013). The fact that the government had resources to spy on its citizens should have raised questions, but the citizens were in favor of such surveillance. The existing laws in Singapore are such that the government can access mobile data like text messages, email, call logs and surfing history without needing legal permission from courts. On the other hand, in Canada, a warrant is needed to obtain data without the user’s knowledge. The citizens of Singapore don’t seem to mind living with this surveillance in exchange for a better security system. In fact, in 2012 Members of Parliament spoke about the lack of an advanced surveillance system to tackle crimes in the country (Lee, 2013). This outlook towards surveillance might have something to do with how crime and terrorism are now easily imagined. Edward Snowden said, “Bathtub falls and police officers kill more Americans than terrorism, yet we've been asked to sacrifice our most sacred rights for fear of falling victim to it” (Houston, 2013). Singapore is one such example of where populations did not mind giving up their privacy in exchange for security that was offered by more surveillance.

Many users who support surveillance might say that they have done nothing wrong, and so have nothing to hide. To them one might ask, ‘do you have curtains at home?’ The ‘I have done nothing wrong’ argument forgets that the definition of what is ‘wrong’ is always up for discussion and often it is our governments that define what's wrong. Greenwald (2013) summarises the current state quite well, “the way things are supposed to work is that we're supposed to know virtually everything about what they

(the government) do: that's why they're called public servants. They're supposed to know virtually nothing about what we do: that's why we're called private individuals".

How long must we wait until a government decides to crack down on a community and uses mobile surveillance to target them? This may sound extreme but is already happening. Egyptian police officials used data gathered from Grindr, a geolocation-based application that connects queer individuals across the globe, to locate and arrest its queer users (Culzac, 2014; Payton, 2016; Bo, 2017). Homosexuality is illegal in Egypt, and police officials used Grindr to get the location of users they suspected of being queer. Cardinal Richelieu famously said, "If one would give me six lines written by the hand of the most honest man, I would find something in them to have him hanged" (Hoyt, 1896). Given enough data about an individual, Richelieu could find something to arrest or blackmail them with. What happens if tomorrow the government decides that something that is legal today is no longer legal? For users to agree with the 'I have done nothing wrong' argument, users must have complete trust in their public servants to do the right thing.

2.4. Interior Collective

This section discusses the collective consciousness of our society. It discusses how culture is segregated by algorithms after which it examines the transformation of the physical static panopticon into the digital mobile Phonopticon.

The panopticon is a kind of microscope and to see an object under a microscope requires the transformation of that object. When an object is observed under a microscope it is dismembered, isolated, confined from the larger whole of which it is a part. The isolation and separation of the prisoners of the panopticon have similarities with how algorithms use social sorting to isolate and distinguish human populations. Social sorting is one of the outcomes of contemporary surveillance. Our lives have always included social and personal categorization and the algorithms in mobile applications amplify such categorization. There is a distinction between data collection and data analysis that must be mentioned

here, and the distinction is that even though mobile applications are used to collect data, it is the algorithms behind these applications that are responsible for analyzing that data.

Algorithms act as gatekeepers that allow users access to certain events or restrict access to certain events (Lyon, 2003). This can be found in China where algorithms are managing a "social credit" system that is made to rate everyone's trustworthiness (Botsman, 2017). Applications like Alipay and WeChatpay are used by Chinese citizens to pay for goods and services. Alipay includes a service called Zhima Credit which tracks user transactions made through Alipay and gives each user a score between 350 and 950. Based on these scores users are given perks and rewards. Hvistendahl says "It uses big data to conduct an objective assessment. The higher the score, the better your credit." (2017). This credit system not only tracks user transactions but also includes information about their education and the score of their friends (Hvistendahl, 2017). Zhima Credit is just one of the many credit scoring services in China. Another such service, Sesame Credit, is an example of how these algorithms are used to control users. Users who have a high credit score on Sesame Credit might get benefits like expedited airport security checks (Ming, 2017). However, users who have a low credit score have penalties enforced on them that prevent them from buying plane tickets, buying property or asking for loans. These users are part of a blacklist that is available to government officials, banks and enterprises. This blacklist includes 9.59 billion users (Pak, 2018).

There is no reason why one cannot substitute the operations of the guards of the panopticon with an algorithm. In the Phonopticon, we are not watched by individuals but rather surveyed by algorithms. These algorithms are tied to users because they are responsible for categorising those users. However, these algorithms are created by developers, and they should be accounted for as well. Algorithms that assess users should be screened for prejudice. Unfortunately, there is evidence that algorithms can amplify the effects of prejudice (Devlin, 2017). If algorithms are given prejudiced data, they make prejudiced decisions. This was explored in a study titled *Semantics derived automatically from language corpora contain human-like biases* (Caliskan, Bryson & Narayana, 2017) in which researchers focused on

a machine learning tool which interprets speech and text. The algorithm built a mathematical representation of language based on words that appear next to one another. For example, words for flowers related to pleasantness and words for insects were related to unpleasantness. Similarly, words like 'female' and 'woman' were associated with jobs in the field of arts or humanities, and words like 'male' and 'man' were associated with engineering professions. Sandra Watcher, a data ethics and algorithms researcher, believes that even though algorithms present a threat they might be used as a tool to address prejudice and counter it. She says, "We can, in principle, build systems that detect biased decision-making, and then act on it," (Devlin, 2017). Watcher believes that users need a regulatory body to ensure transparency and fairness with regards to the decision-making process used by algorithms (Sample, 2017).

This section highlighted how algorithms play the part of the guard without the material enclosure of the panopticon as they are not bound to physical structures. Users should not be concerned because third parties are looking at their data, users should be concerned because third parties have the power to look at their data in the first place and that's what makes it surveillance (Schiner, 2014). And no user is safe because the power of digital computing allows for the surveillance of diverse users who are not bound to physical structures.

This physical structure of the panopticon is important because not only does it make constant monitoring feasible, but it also forces self-discipline upon the prisoners (Bauman, 2000). Once there is nowhere left to hide conformity makes sense, but as soon as the walls disappear the system becomes harder to oversee. Without an enclosed area the prisoners have nothing holding them back and can escape the panopticon. This condition of enclosure, isolation and immobility that the Panopticon enforces is absent in our contemporary society, and so some may consider the metaphor to be invalid (Boyne, 2000). Where the panopticon signals immobility through an enclosure, the urban mobile landscapes allow users to come and go at will. Our global population cannot be confined to a physical space and thus cannot be isolated (Mare, 2016). Users cannot be held in place long enough for the panoptic mechanism of 'being seen without being able to see' to work its magic (Simon, 2002). These critiques are valid and might lead

one to think that the panopticon is limited to its enclosure. However, this thesis argues that the panopticon must not be perceived as a physical building but as a metaphor for power. The panoptic machine of Bentham is static; it is a prison after all. But Foucault argues that the panopticism is mobile and can produce the effects of enclosure wherever users might be found. Think of an airplane, even while flying, are passengers not caught in an immobilizing structure? The expansion of panoptic standards of supervision beyond the structural limits of the static prison is precisely what Foucault had in mind. Even though users are not confined to a physical space and have the freedom to move around, they are still under this panopticism.

Users may believe that identifying individuals from mobile phone location data might be difficult, but researchers say otherwise. Scientists at the Massachusetts Institute of Technology (MIT) believe that it is extremely easy to identify a user with a few pieces of location information. At MIT researchers studied 1.5 million users' mobile phone records for 15 months (Palmer, 2013). Even though these data sets were anonymous the researchers were able to find "mobility traces" - evident paths of each mobile phone. Researchers found that only four locations and times were enough to identify a particular user (Montjoye, 2013) Compare that to Edmond Locard's research conducted in the 1900's that showed that 12 points are needed to identify a fingerprint (Champod, 2005). The amount of data needed to track and identify users has reduced in comparison to what it used to be. Users can run, but users cannot hide because the structure of the panopticon has evolved from being an architectural building to a mobile limitless system.

2.5. Interior Individual

This section focuses on the personal thoughts and opinions of users that determine their behaviour. When examining the panopticon under this section, this thesis focused on the prisoner. This section ends with an analysis of user's opinions and awareness regarding the surveillance carried out on them.

The primary function of the panopticon is to instil a state of permanent visibility in its prisoners that allows it to maintain the status quo (Foucault, 1979). The prisoners believe they are being watched

and so are careful not to anger the guards who they think are always watching. The prisoners in the panopticon monitor their own behaviour because they fear punishment and as a result, they discipline themselves. In our current surveillance environment there exist examples where users are monitoring themselves. One such example is the Quantified Self Movement. Users now track many facets of their lives with the help of devices and applications and this trend is called the Quantified Self Movement (Ballano, 2014). According to Pew Research Center's study, 69% of Americans regularly track their weight, diet or exercise activity (Fox, 2013). The quantified self movement is now in its golden age because of the amalgamation of numerous factors such as technology, health, and popular culture.

Critics may argue that the prisoners monitor themselves out of fear while smartphone users monitor themselves because they want information about their lives, and these critics have a point. But even though the motives behind self-surveillance are different, it is still considered surveillance. There is another difference as well, the difference being that even though these Quantified Self Movement practitioners are aware that their data is being tracked, they do not know who else has access to their data. Quantified self practitioners might be unaware of where their data goes, and this can lead to dangerous situations. One such example is what happened with Strava users in 2018. Strava is a jogging application that collects geolocation data about its users. It is used to track their jogging movements for health and lifestyle benefits. Strava knows where it's users are, where they are going and how long they spend in various places. In January 2018 Strava released an interactive heat map of the world (Figure 4) showing 13 trillion GPS locations that it tracked (Strava Labs, 2018).

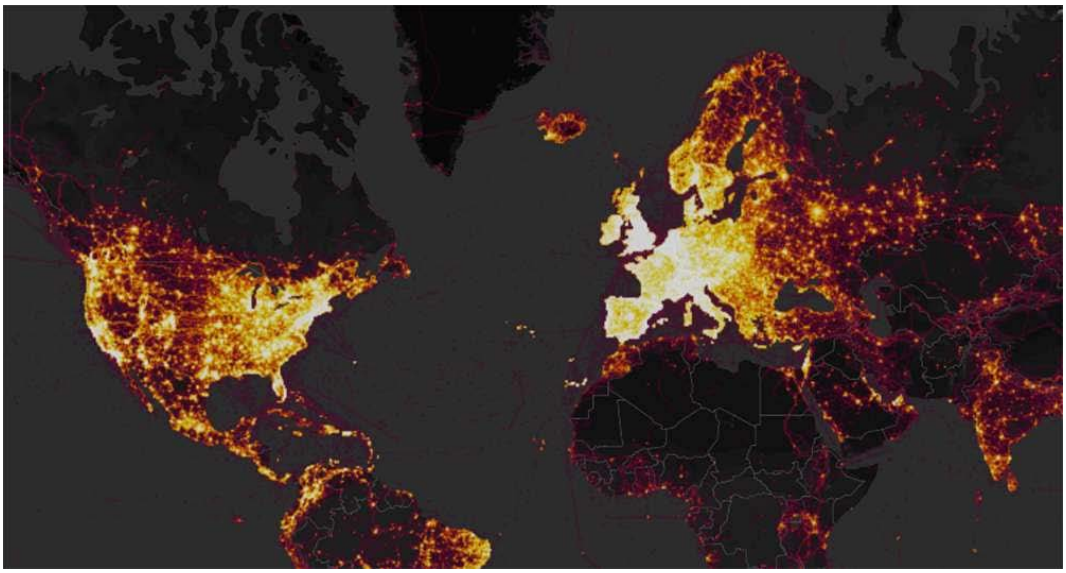


Figure 4. Strava's heat map visualization (Felton 2018)

Unfortunately, a lot of United States military personnel have their location tracking enabled on Strava which led to viewers locating where these personnel train, and consequently led to revealing the location of military bases worldwide. Additionally, by scraping the data if a viewer wanted they could also identify other individual Strava users and track their movements. (Felton, 2018)

Figure 5. The National Security Headquarters viewed in Strava's visualization (Al-Bassam, 2018)

Ironically, the data also showed that there were Strava users within the National Security Agency headquarters in Maryland, USA (Figure 5). It is worth noting here that the National Security Agency (NSA) is known to collect confidential data from our smartphones and aims to use that data to try and identify terrorists. The word 'collect' is used because the Department of Defence (DoD) has a special

definition of that. They only consider data to be ‘collected’ when it has been used by an employee of the DoD as part of that employee’s official duties. James Clapper, the American Director of National Intelligence, compared this scenario to a library. Clapper spoke of how the NSA has books about user data stored in shelves but only a few are read. So only the books that they have read are the ones they claim they have ‘collected.’ (Schiner, 2014).

The panopticon metaphor falls flat without a sign to remind users that they are being viewed. The applications on smartphones might be sending data to third parties without notifying the users who remain unaware of the privacy breach taking place. However, this section argues that the signs are always present for the users to view and analyze. These signs are present in the form of terms and conditions that users must agree with before they can use smartphone applications.These terms and conditions specify what the applications can do with user data. However, these terms and conditions are often long and are designed to be skimmed through if they are read at all (Lomas & Dillet, 2015). *Choice*, a technology magazine in Australia, hired an actor to read aloud the Terms and Conditions of the Amazon Kindle. It only took the actor nine hours to do so (Hunt, 2017). And all of this is assuming the user even reads the Terms and Conditions, which they do not do (Lomas & Dillet, 2015). Users have access to signs that inform them of the data they give up, but they do not pay attention to these signs. Such user behaviour might lead to the conclusion shared by many critics that the panopticon is not a suitable metaphor for current surveillance systems that are carried out by our mobile devices because users do not read the terms and conditions.

However, there is one extremely vital piece of evidence that proves that even though many users do not read these terms and conditions, they are still aware of surveillance carried out by smartphones. That piece is Edward Snowden. On June 5th of 2013, *The Guardian* released an exclusive report revealing a secretive court order from the United States government that forced Verizon, a cellular provider, to give the government the phone records of millions of Americans. Following the first story, *The Guardian* then published information that proved the existence of the PRISM program, a program that gave the NSA access to citizens data from Google, Apple and Facebook, was revealed to the public. These corporations denied the accusations and the President at that time; President Obama defended the

program by saying that having complete security and simultaneously complete freedom and privacy is impossible. On June 9th the whistleblower who leaked the information to *The Guardian* revealed his identity and stated that he did not want to hide because he believed that he did nothing wrong. In just a few days Edward Snowden went from being a computer professional to a whistleblower to a household name (Sheridan, 2016) (Greenwald, 2013).

Snowden's revelations brought the panoptic surveillance architecture back into view. Previously the awareness of such technology was very limited, some might have even considered it a conspiracy theory, but Snowden brought it back into the limelight as news channels and publications covered the story extensively. The Snowden revelations have brought about a change in user opinion (Pew, 2015). Users might not be able to stop third parties from gathering their data, but they are now more informed. In response to the Snowden revelations, Pew carried out a survey where they gathered data about American opinions after the Snowden revelations and found that 34% of its participants who were aware of the surveillance programs took at least one step to shield their information from the government. Steps such as changing their privacy settings on social media; using social media less often, avoiding specific applications and uninstalling applications (Pew, 2015). Snowden's goal was to help users move away from fear and look towards reason and resilience and he aimed to achieve that goal by telling the truth.

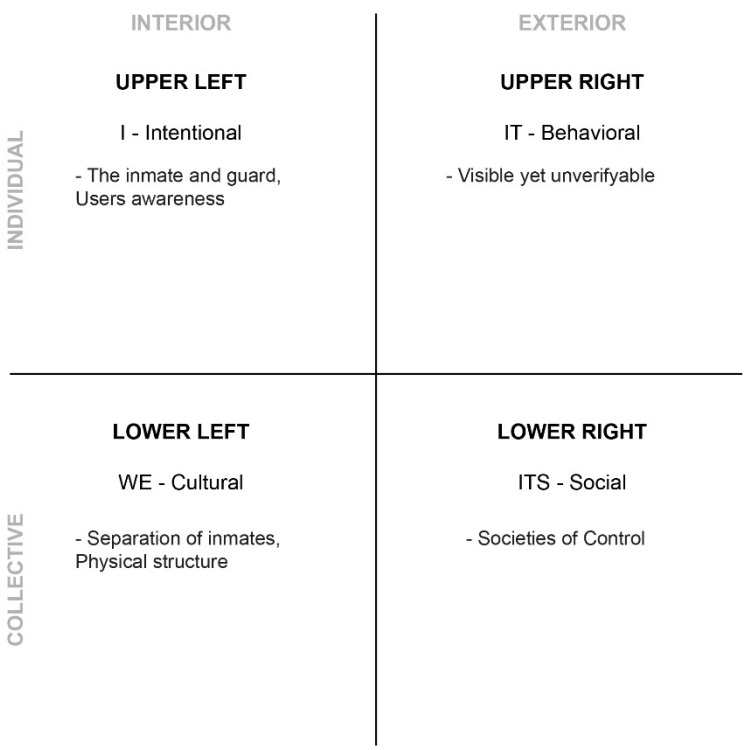


Figure 6. Summary of comparison between surveillance carried out in the panopticon to surveillance carried out by mobile applications on our smartphones overlaid onto the AQAL diagram.

The section above summarises the findings of the literature review after comparing the surveillance carried out in the panopticon to surveillance carried out by mobile applications on smartphones. The findings of the literature review were put onto the AQAL diagram for clarity (Figure 6). The literature review looked at the similarities and differences between the surveillance structure of panopticon and surveillance carried out by mobile applications and concluded that there exists a cognitive dissonance in the minds of users. Users know that applications are spying on them, but they continue to use them. This topic is further explored in Chapter 4.

2.6. Using education as a tool

The previous section of the literature review highlighted how the applications on smartphones betray users. In the following section, this thesis explores what users think about this betrayal and what might be the best way to solve such problems. The research included examining surveys such as the one done by

Pew Research Center titled *Americans' Attitudes About Privacy, Security and Surveillance* (2015). The main findings of Pew's research were that 34% of its participants took at least one step to protect their data from the government after they were informed of surveillance programs. A similar survey was carried out among the prospective cohort group as well. Detailed summaries of these findings can be found in Chapter 3 of this paper. One of the main findings of this study was that even though the participants did not trust the applications on their smartphones, they continued to use them. This is where a cognitive dissonance was noticed.

When we have contradictions between our attitudes and behaviours, it leads to what Leon Festinger calls Cognitive Dissonance (Festinger, 1957). According to Festinger's theory of Cognitive Dissonance, people feel discomfort when they hold two conflicting beliefs. Festinger emphasizes on the role of exposure to information in creating or destroying this dissonance (Festinger, 1957). Such exposure to information created an opportunity to use education as a tool to reduce the cognitive dissonance. As a result, the main argument of this thesis revolves around educating and giving users knowledge about the surveillance carried out by the applications on their smartphones along with giving them information about protecting them from such surveillance. In this manner, this thesis attempted to reduce the cognitive dissonance that participants had using education. The following contextual review contains examples of projects that educate users about data breaches that are carried out by smartphone applications.

3. Contextual Review

This contextual review is divided into two main parts. The first part contains examples of tools and applications that use data visualization to inform users of data breaches both in mobile phones and on the web, and the second part contains examples of projects that inform and educate users about surveillance.

The first application examined was Lumen Privacy Monitor. Lumen monitors a user's mobile device and identifies applications that collect sensitive information and lists the third parties which collect that user data. However, users must grant Lumen all sorts of permissions to analyze their data. Lumen is not an open source application and cannot be implicitly trusted. Its creators claim that they are only concerned about where the user's data goes (ISCI 2017). Lumen visualizes the data breaches happening in a users' smartphone by using donut graphs and supplements these graphs with information (Figure 7).

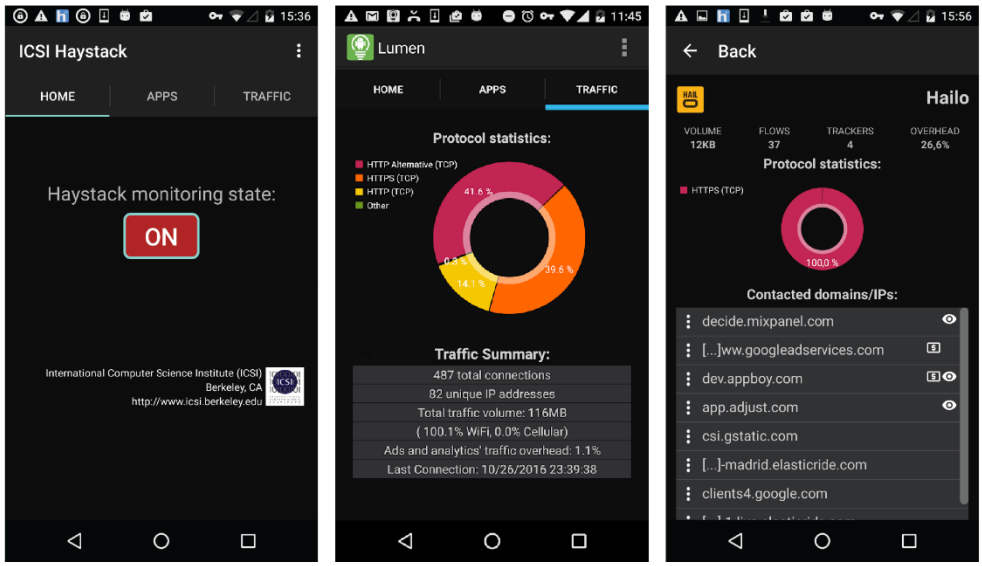


Figure 7. Screenshots of the Lumen Application (ISCI 2017)

The second application examined was XPrivacy, created by Marcel Bokhorst, that lets users control permissions for each application on Android phones. XPrivacy gives other applications fake data or no data at all. It can also restrict data like location or contacts, from being used by all applications (Figure 8). However, the downside was that the Android phone must be rooted before you can install XPrivacy.

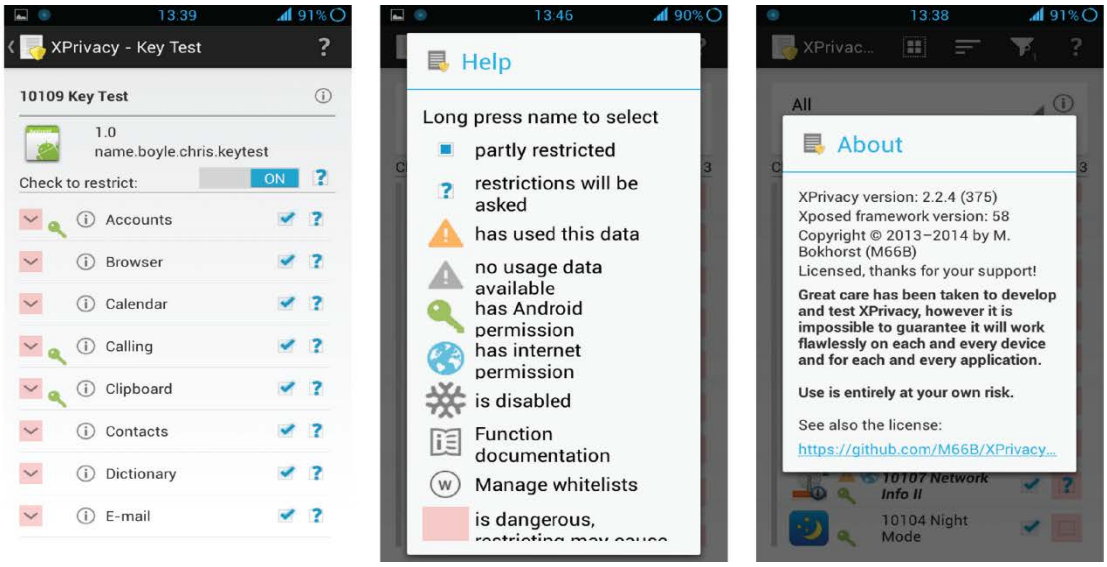


Figure 8. Screenshots of the XPrivacy Application (Toombs 2013)

This thesis needed an open source application that did not require the cohort to modify their smartphones in a significant way. NetworkStatsManager is a class and set of functions within the Android operating system that calculates all the data that is uploaded from each application from a user's phone. The class does not tell users what kind of data is uploaded or whom it goes to. It just provides users with how much data gets uploaded. Furthermore, an open source application that uses NetworkStatsManager was found on Github which was used for the prospective cohort study. NetworkStatsManager presented the data as text (Figure 9), which was not the most effective way to communicate such information, but it got the job done. It was an application that could be trusted because its code was available for examination. The code used in developing the application along with the data readouts for the members of the cohort study in Appendix A of this paper. Additionally, NetworkStatsManager was only available for Android devices which was a minor setback, but it was overcome by including only Android users in the cohort group. NetworkStatsManager was not the first application examined, but it was the first one that suited the needs of this research. The members of the cohort study were given knowledge about how NetworkStatsManager worked beforehand and they consented to it being downloaded on their smartphones.

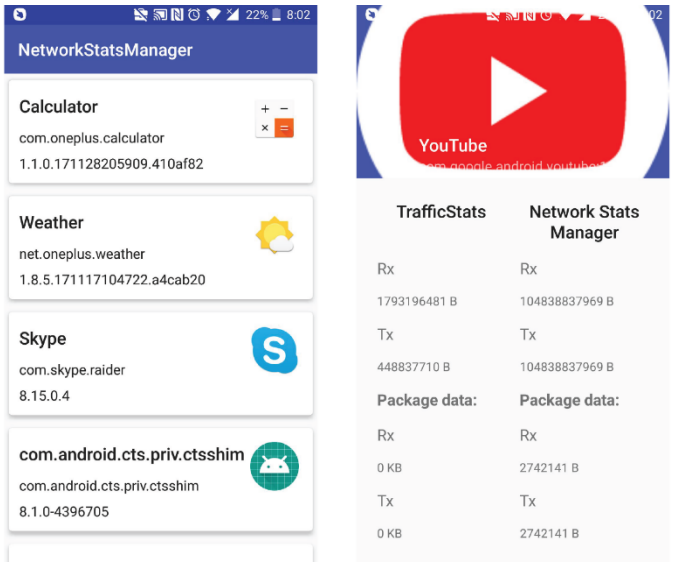


Figure 9. Screenshots of the NetworkStatsManager Application

Moving from mobile-based visualizations to web-based visualizations this research looked at David McCandless's visualization titled World's Biggest Data Breaches. McCandless conceptualized and designed a visualization of the world's largest data breach in the past decade. In the visualization (Figure 10), users can see when the attack happened, who it happened to, and how large the impact was. Clicking on any breach brings up news events associated with that breach. This was an excellent example of using both quantitative and qualitative data to educate viewers. (McCandless, 2018).

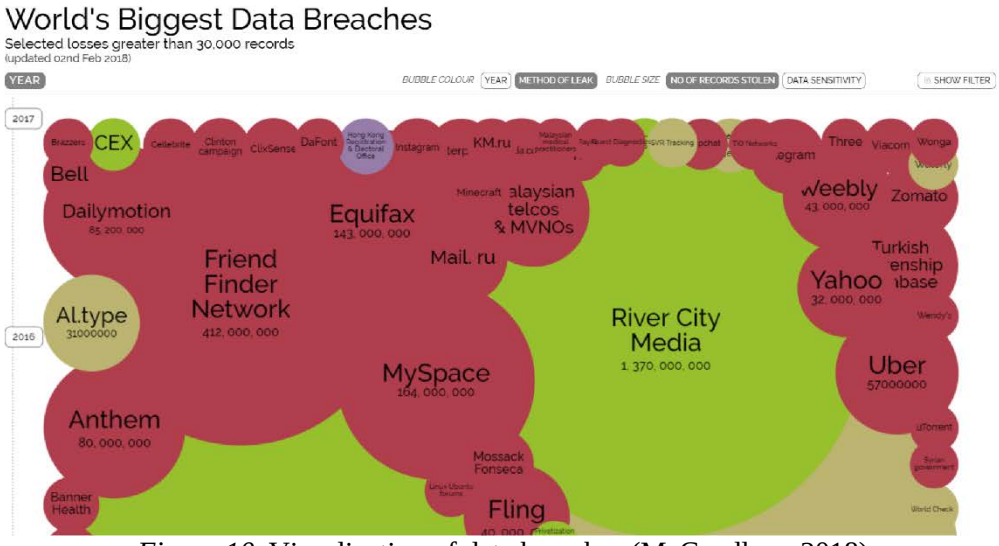


Figure 10. Visualization of data breaches (McCandless, 2018)

After analyzing these examples, the strengths of visualizing such data were examined. Giving users information about data breaches could be used as a tool for raising public awareness. However, this information should be informative and personal to the user. One could write multiple pages on how applications are giving up our data, but that would not be the best way to engage viewers. Instead, one could rely on visuals to do the job. These are some examples of tools that are available for users that inform users about privacy breaches. The next section of this contextual review contains projects and installations that inform users of surveillance and privacy breaches.

Figure 11. Installation view of the wall of mechanical objects (background) and robotic arms (foreground) (Filippetti 2011).

Seiko Mikami's Desires of Code (Figure 11) was made to emulate the workings of memory in our contemporary society. Desire of codes is made up of three parts: first, a wall composed of 90 mechanized rods which contain lights, cameras, and sensors; second, six large robotic arms that are suspended from the roof; and lastly, a sculpture placed on a wall which resembles a large compound eye, divided into 61 hexagonal video screens (Figure 12). The video that is played on these 61 screens is a remix of footage from the cameras on the rods as well as footage from surveillance cameras around the world.

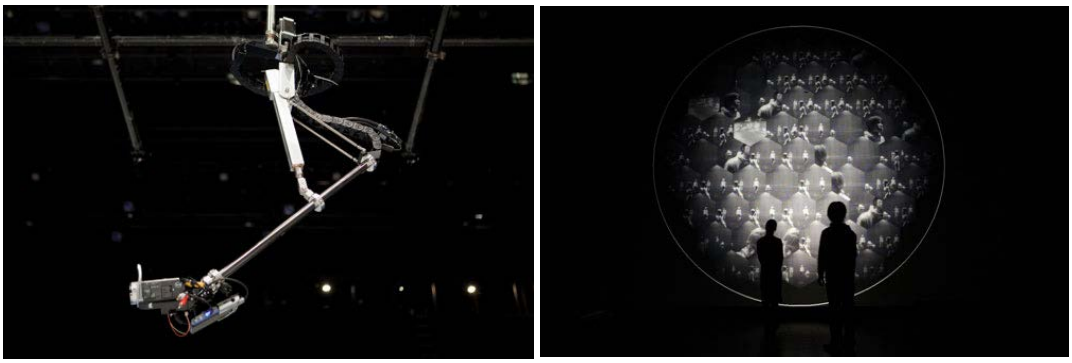


Figure 12. Closeup of the mechanical arms © ryuichi maruo, courtesy tama art university department of interaction design (Filippetti 2011).

'Desires of Code' helped this thesis understand how the 'gaze' of cameras could be used as a tool to induce introspection. The Phonopticon aimed at replicating a similar feeling of being seen and being followed. It also aimed at giving users visual feedback in the form of seeing their own image, again similar to what one experiences in Seiko's work. Desires of Code allowed for the examination of the effect cameras have on visitors.

Artist Ai Weiwei in collaboration with architects Jacques Herzog and Pierre de Mueron created Hansel & Gretel an immersive installation that not only allows participants to experience surveillance but also informs them of how such surveillance takes place.

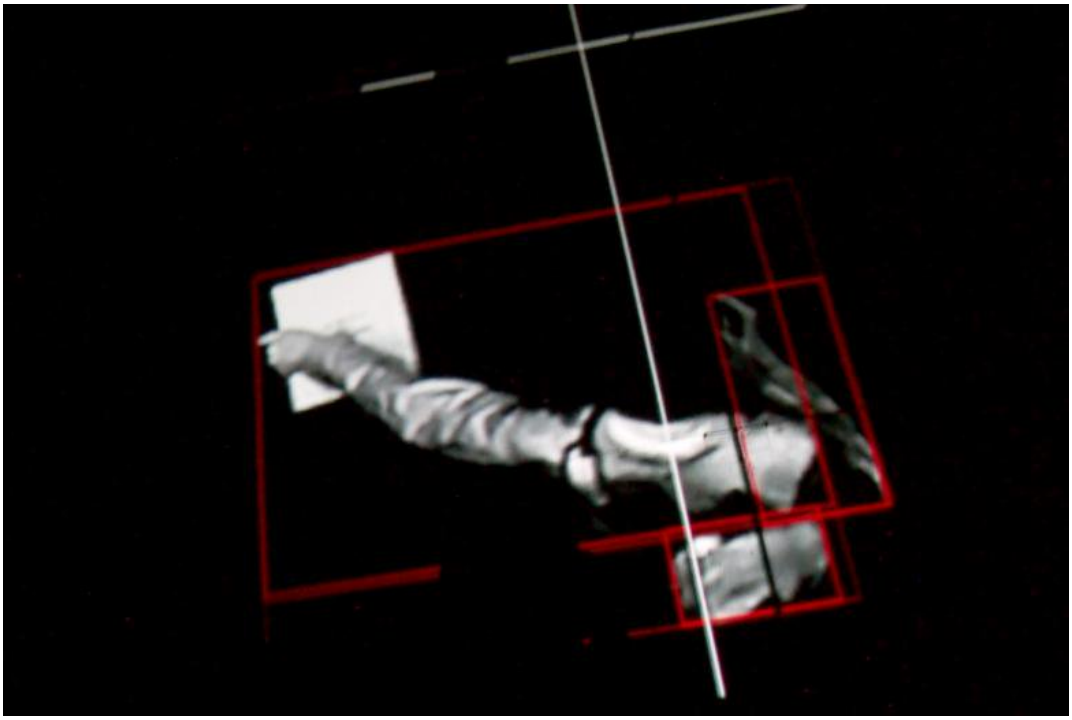


Figure 13. Projections of the participants on the floor of the hall. © John Hill/World-Architects (Hill, 2017)

The experience begins with participants walking through a narrow entranceway into a hall. The hall itself is lit with rectangles that are projected on the floor and red squares that follow the participants around. After a while participants recognise themselves being projected onto the floor (Figure 13) and realise that there are cameras that are watching them. There are drones on the ceiling that create a buzzing sound that adds to the effect of the experience.

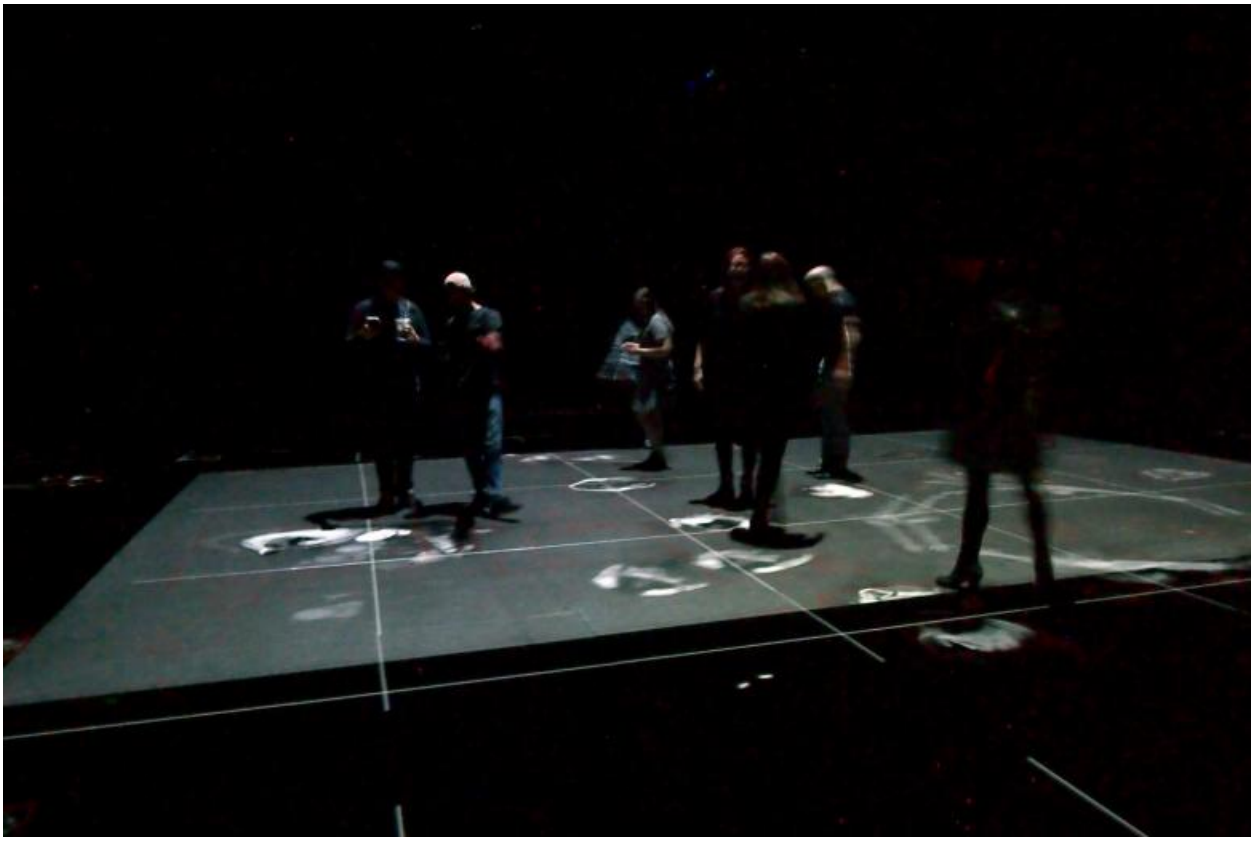
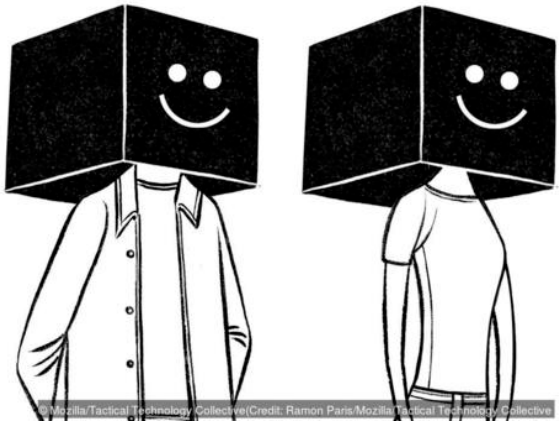


Figure 14. Participants interacting with the projections on the floor. © John Hill/World-Architects (Hill, 2017)

Participants are encouraged to make body movements, dance or lie down on the floor and experience how their image is projected onto the floor (Figure 14). Once they exit the hall they are led onto the second part of the experience where they can view other participants. The second part of the installation contains many iPads that show the faces captured by the cameras (Figure 15). Participants may use the iPads to identify themselves and can also view a livestream of other participants as they enter the building.

Picture 15. Participants interacting with the iPad's © John Hill/World-Architects (Hill, 2017)

They are also informed that all this video is publicly available online. Once this realisation has settled in the participants are informed of various drone surveillance technologies that exists and are used by governments. There are also books about surveillance and privacy breaches that are available that participants can purchase. This exhibit was a good example as it not only offered participants an immersive experience, but it also gave them knowledge about surveillance systems.



Picture 16. An illustration depicting digital anonymity. (Credit: Ramon Paris/Mozilla/Tactical Technology Collective)

Another project that aimed to help users was the Data Detox Kit. This was designed by non-profit groups Mozilla and the Tactical Technology Collective for a pop-up experience in London called The Glass Room. This experience invited visitors to look at what happens to their data. The project realised that online behavior that has happened in the past cannot be changed however they could help users make informed decisions about their data. It consists of steps that users can take to reduce their 'data bloat'.

Participants of the Data Detox are required to spend 30 minutes everyday for 8 days and take steps that make users think differently about their data. The project also informed users of alternative applications that can be used and also suggested weekly or monthly goals that users can strive towards to reduce their 'data bloat'.

This section outlined various visualization projects that allowed users to walk away more informed and gave them the ability to form their own opinion about the subject matter. The first part of this section discussed various tools that can be used by individual users while the second part of the section discussed visualisations and projects that ~~were~~ aimed at educating users about data privacy. This thesis used NetworkStatsManger within the cohort group to examine if giving users information and education through data visualisation would lead to a change in their cognitive models. The details of this examination are provided in the next chapter of this thesis.

4. Summary of the prospective cohort study

This section provides a detailed explanation of the prospective cohort study carried out in this thesis. It is divided into two parts. The first part is a summary of the research plan used in this study and is followed by the findings of the research. The literature review of this thesis shed light on how there exists a cognitive dissonance in the minds of some users regarding the applications on their smartphones. The goal of this prospective cohort study was to examine if the cognitive dissonance in the mind of a user, specifically about what mobile applications can do with user data, can be reduced by giving a user education about how mobile applications share user data.

The first step of the process was securing research ethics approval. This approval was received from the Research Ethics Board at OCAD University on the 23rd of November 2017. This printed ethics approval is in Appendix A of this thesis.

For clarity, the users who took part in this study are referred to as members in this paper. This research needed six members to be part of its study who needed to have Android smartphones because NetworkStatsManager only works on Android devices. Once the members were picked, they were asked for their signed consent to be a part of this thesis. After their consent was received, the members were asked to answer a questionnaire. This questionnaire and any other material used in this prospective cohort study are in Appendix A of this thesis. The questions that were asked were inspired from surveys carried out previously by Pew titled *Americans' Attitudes About Privacy, Security and Surveillance* (2015) and the Office of the Privacy Commissioner of Canada titled *Survey of Canadians on Privacy* (2016). The questions were also connected to the All Quadrants All Levels (AQAL) framework.

After answering the first questionnaire, the entire cohort group met for the first time as a focus group. This focus group discussed topics such as surveillance, mobile applications and user privacy. After the focus group was over, NetworkStatsManager was installed on the members' smartphones. The application was installed after the first questionnaire and the first focus group were carried out because this thesis wanted to access their opinion and thoughts before any information was provided to them. NetworkStatsManager was installed on the smartphones of four of the members and they kept it on their

smartphones for the duration of the study while the other two members served as controls. This was done because this thesis also wanted to evaluate if having general knowledge would be enough or would members need personal real-time data to help bridge their cognitive models. The data provided by NetworkStatsManager was recorded in spreadsheets. These data readouts are in Appendix A of this thesis. After this first meeting, the members later met with the researcher individually, and an interview was conducted to learn how the members felt about the applications on their smartphones. This interview was repeated after some time had passed to see if the attitudes and opinions of the members had undergone any change.

All the members and the researcher met one last time during the second focus group. During this session topics such as surveillance, privacy and mobile applications were discussed again. The aim of this focus group was to identify any change in the opinions of the members. This was a brief summation of the research plan used in this thesis.

The next section provides a detailed description of the results gathered from the interviews and focus groups. Because these questionnaires and interviews were aimed at identifying any change in user opinion the figures presented in this section below represent the answers to both the first and second questionnaire. The summary of the research is divided into four parts based on the four segments of the AQAL framework.

Using the AQAL lens this research first examined the exterior individual segment which involved looking at the applications used by the members of the cohort group. Members of the cohort group were asked how many applications they had on their smartphones. The members had many applications on their smartphones (Figure11), and even after learning about how applications were spying on them, only two out of the six members (Member 5 & Member 6) of the cohort group deleted a few applications.

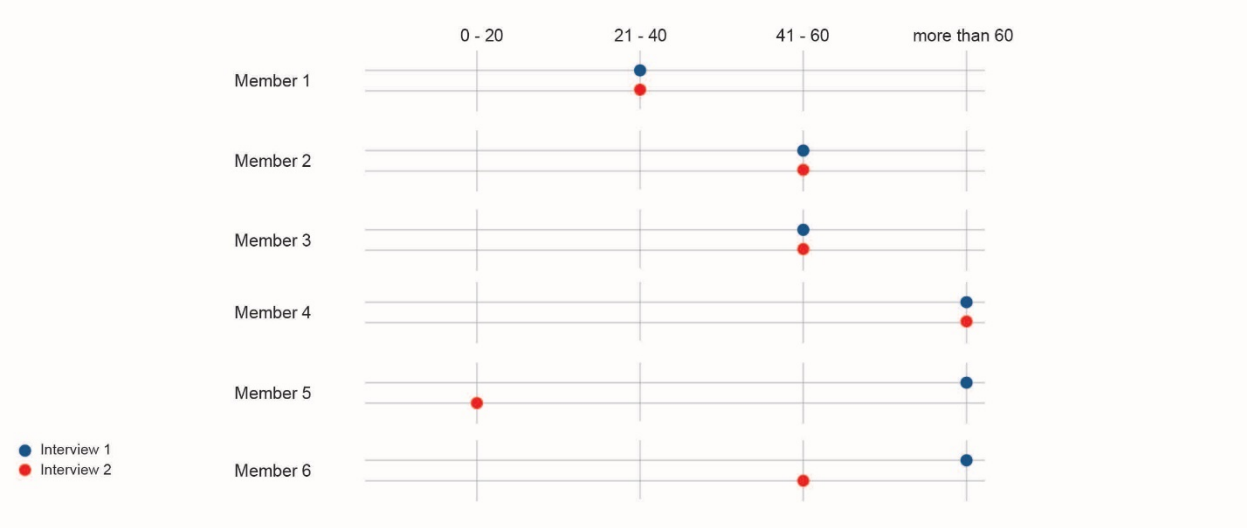


Figure 17. How many applications do you have on your mobile device?

When asked about their daily application use the answers were varied (Figure 17). Member 4 used up to 5 applications daily but had over 60 on their smartphone. Whereas Member 3 had about 0 - 20 applications on their phone and used almost all of them daily. However, after they were provided with information about privacy breaches, it was observed that Member 3 reduced their application use from 0-20 to up to 5 applications per day.

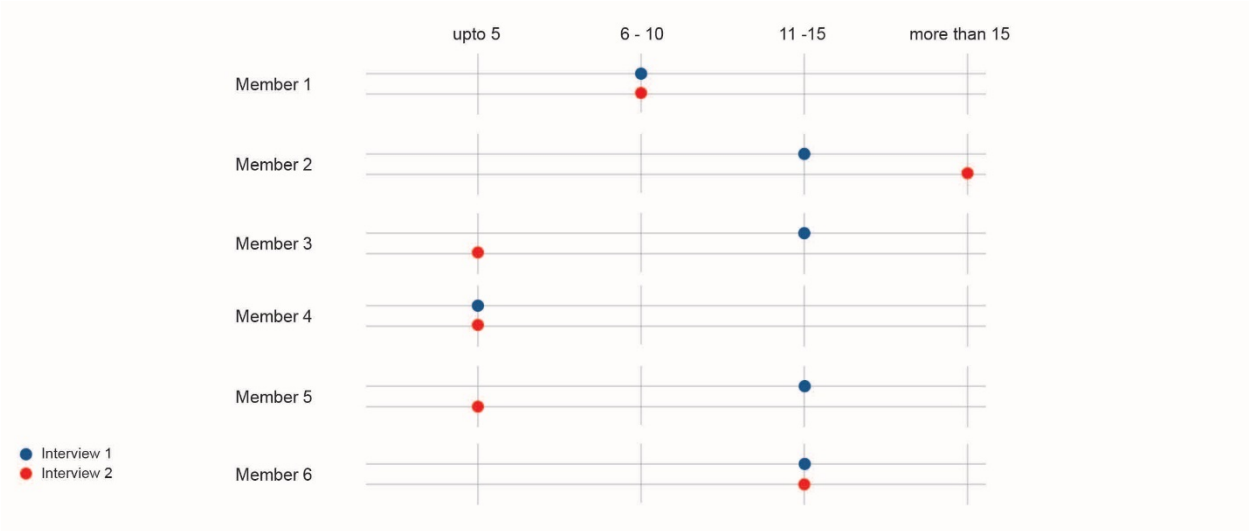


Figure 18. In the course of one day, how many applications do you use?

The next question was related to the privacy policy of mobile applications. Usually, if a smartphone user wants to know what an application does they can access the terms and conditions that are provided in the privacy policy section of the application. However, none of the members in this study read them (Figure 19). Having access to information about data breaches did not have any effect on their answers.

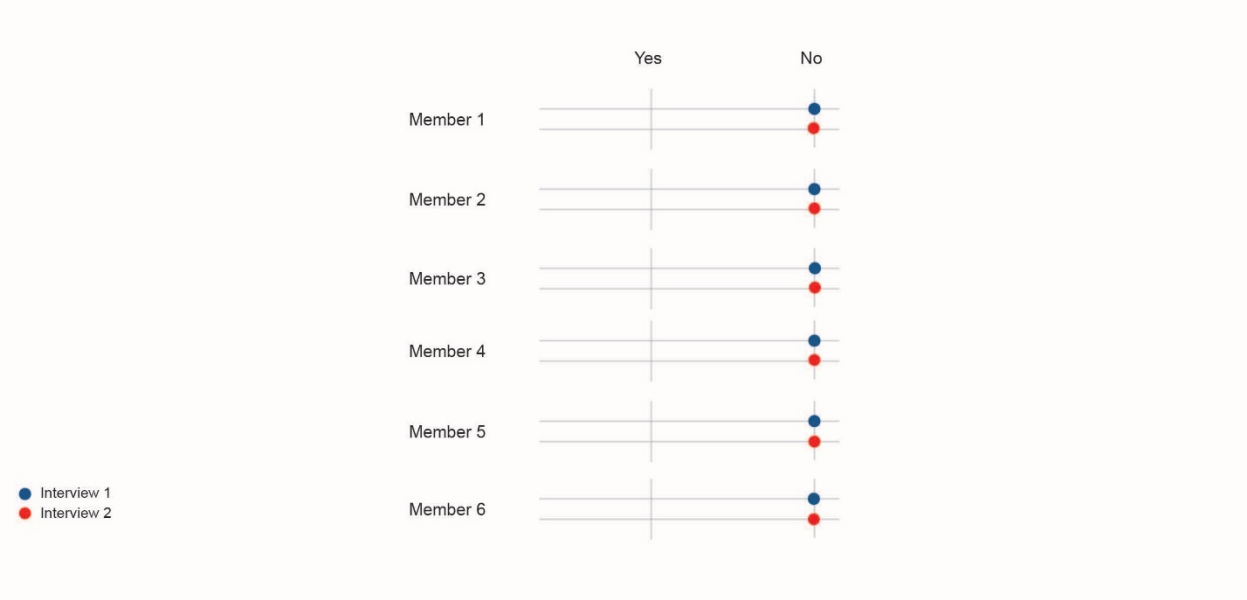


Figure 19. Do you read the privacy policy for applications before you download them?

When questioned as to why they didn't read them, Member 4 felt that the language used was obscure and boring. They went on to say, "When you sign up for an app the onboarding and UX (User Experience) is made to be as cool as possible, but the terms and conditions are tedious and boring.". Member 1 echoed these sentiments when they said, "It's long and uses words and terms I don't understand". Members did not understand how the applications on their mobile phones work because the language used in the terms and conditions was not user-friendly which led misinformation. Most of the members of the cohort group used many applications even though they had no idea what the application could do with their data. They used them because they valued the utility the application provided over their privacy. This could explain why the difference in their cognitive models exists.

In the context of the exterior collective view of the AQAL lens, the literature review examined the Right to be Forgotten. The cohort group was introduced to the Right to be Forgotten, and the members were asked about their opinion on such legal safeguards. Member 6 felt that the Right to be Forgotten was a clever idea. “I wish that had happened here (in Canada)”. Member 5 said that they would remove their data “in a heartbeat”, and Member 2 said, “I don't want what I said on the internet when I was twelve years old to be available to anyone now”. The members viewed the Right to be Forgotten favorably and given the chance they would invoke it because they cared about their data that was on the internet. There might be some users who do not care and are comfortable sharing their data with third parties. However, none of the members of this cohort study fell under that category.

In the context of the interior collective, the questions revolved around how the cohort group interacted with other users. Members were asked if knowing about how applications are tracking them led them to have conversations with other users about this topic. Member 1 was surprised by what others had to say. “What surprised me was when I talk about data breaches to people they’re okay with it, because they feel that they are not important enough. I think the more people talk, the more awareness we have”. Member 2 spoke about data breaches with their partner and the response they got was “Okay, I don’t care” whereas Member 6 received the opposite reaction “My partner deleted HQ (a trivia game application) after I told her how horrible it was”. Surprisingly Member 3, who was a control in this study, had these conversations as well. “I did mention how cell phones were listening to our conversations with other people and they actually became much more aware and paranoid because of that conversation. The ripple effect was very interesting. They didn't believe me at first and then they checked all of their security settings and went through all their applications like Facebook and Gmail and that was very interesting”. Member 6 later added that awareness and education are better ways of informing users of such data breaches. This sharing of information was very valuable to this research because even with information that was not specific to a user, they still passed on knowledge about privacy breaches onto others.

The following section deals with the interior individual view of the AQAL lens. The aim of the interviews and focus groups was focussed on assessing the cognitive model of the participants. The questions investigated their assumptions around what an application does with their data compared to the reality of what an application does. The members were asked if they trusted the applications on their smartphones. 5 out of 6 members did not trust the applications on their smartphones (Figure 20), and this did not change even after they were informed of data breaches.

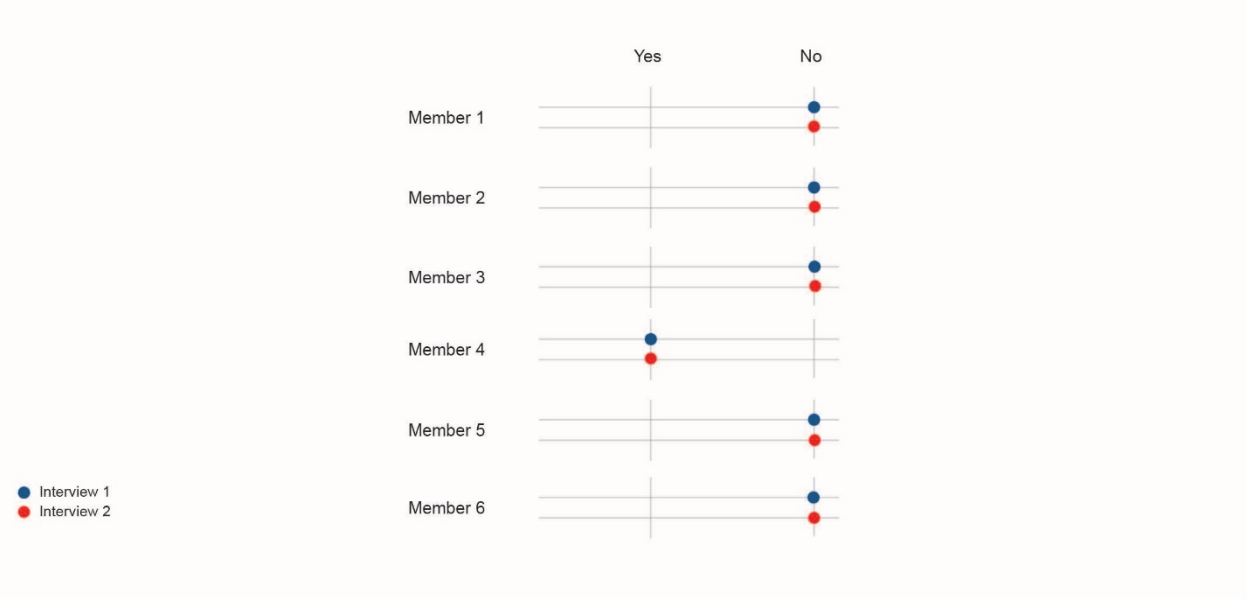


Figure 20. Do you trust the applications on your phone?

When asked to elaborate as to why they still use applications they don't trust the members had varied responses. Member 1 thought that "There's no other alternative" while Member 3 used the applications because of convenience. They said "It's a cost-benefit situation. I do understand my privacy is at stake but I'm still okay with giving it up". Member 4 was the only one who trusted the applications on their phone, and when asked why they trusted those apps they said "I have very few applications anyway, so the ones I have I know I can trust"

Because the members of the study did not read the terms and conditions, they were unaware of the amount of data the applications were sharing about them (Figure 21). Before they were given information about how applications share user data only 16% of members felt that they were aware of the amount of data transmitted by applications on their mobile device.

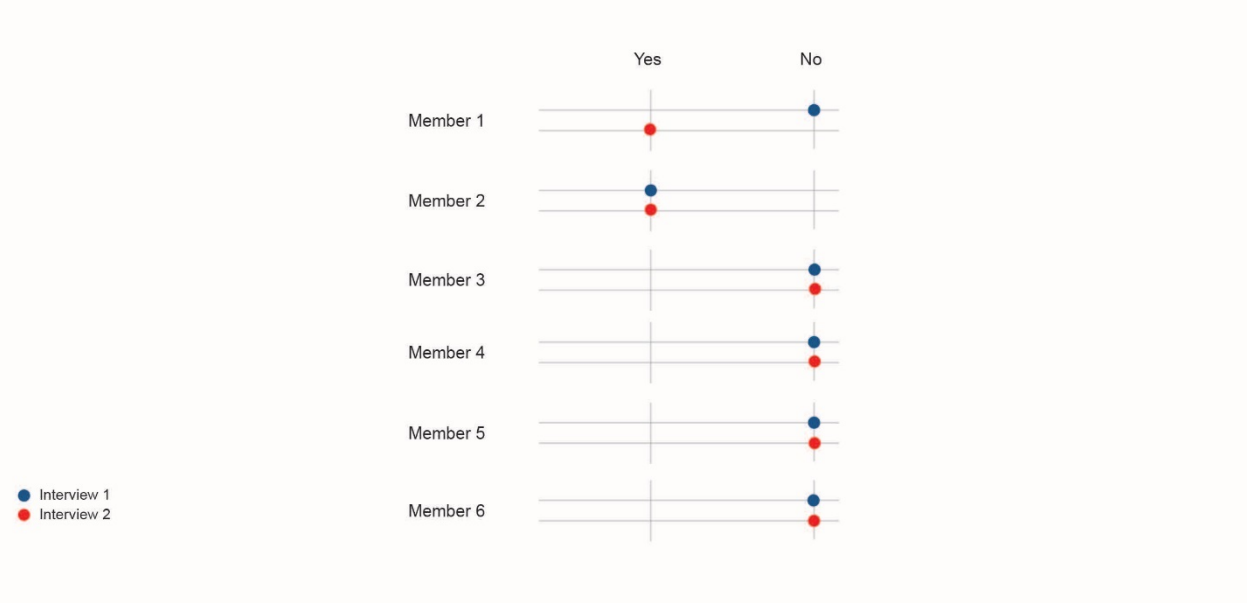


Figure 21. Are you aware of the amount of data used and transmitted by the applications on your mobile device?

Member 2 was the only one who thought they were aware of how mobile applications share data. However, after NetworkStatsManager was downloaded on their smartphone, they realised they were mistaken. The Netflix application on their phone was found to be transmitting more data than they thought which they found surprising. They later deleted the Netflix application. Member 1 felt that they had enough awareness about data transmitted by applications after they were provided information about that subject matter while the rest were still not confident about their awareness.

All the members felt that their mobile phones were unsafe or extremely unsafe from third parties that wanted access to their data (Figure 22). These opinions remained unchanged even after the members were provided with information regarding privacy breaches.

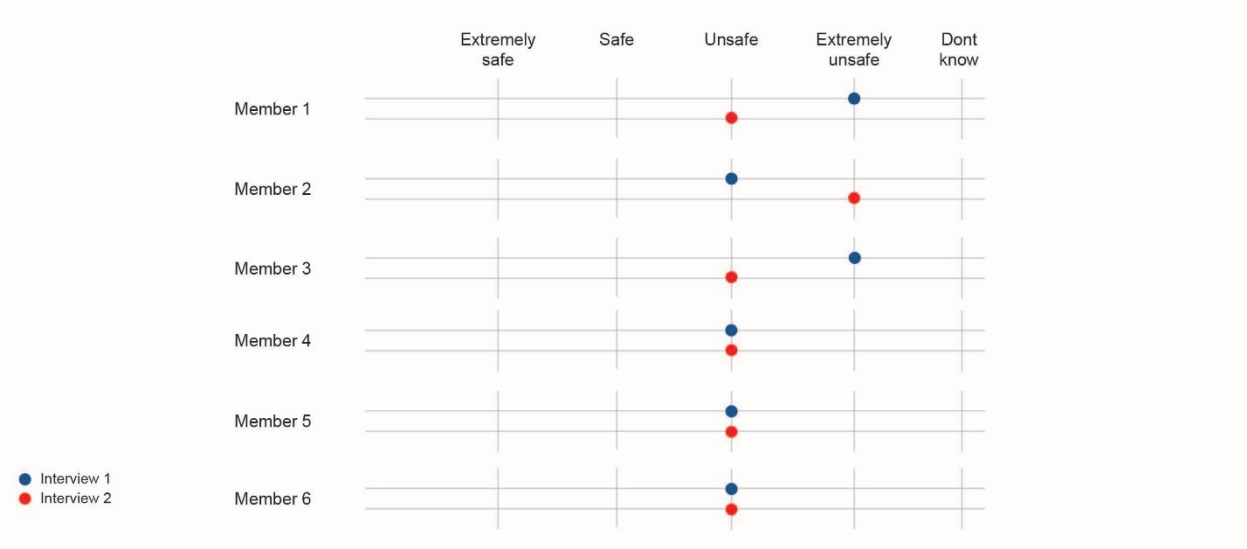


Figure 22. How safe do you think your mobile phone is from third parties that want to access your data?

The next question asked was if the members valued knowing how applications are giving away their data. The answers were unanimously positive (Figure 23). These options remained unchanged even after being informed about how applications carry out privacy breaches.

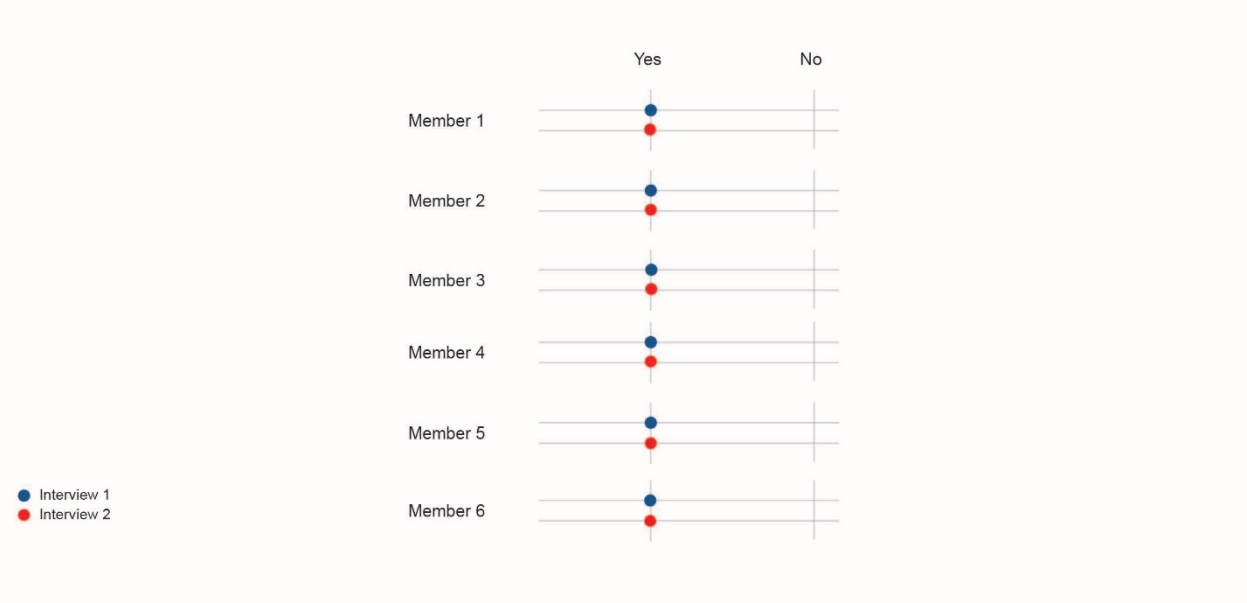


Figure 23. Do you think you would benefit from having more information about how applications are giving away your data?

When asked about what kind of information they would like, Member 5 asked for specific details "I'd like specifics of how the data is being collected, who has access to this data and what is done with it" while Member 3 wanted "a general overview of what's (data) being sent".

The members were also asked if they were aware of the NSA leaks made by Snowden in 2013. Every member was aware of the Snowden leaks (Figure 24). This proved that though the members knew that smartphones could be used to spy on them, but they still ended up using them.

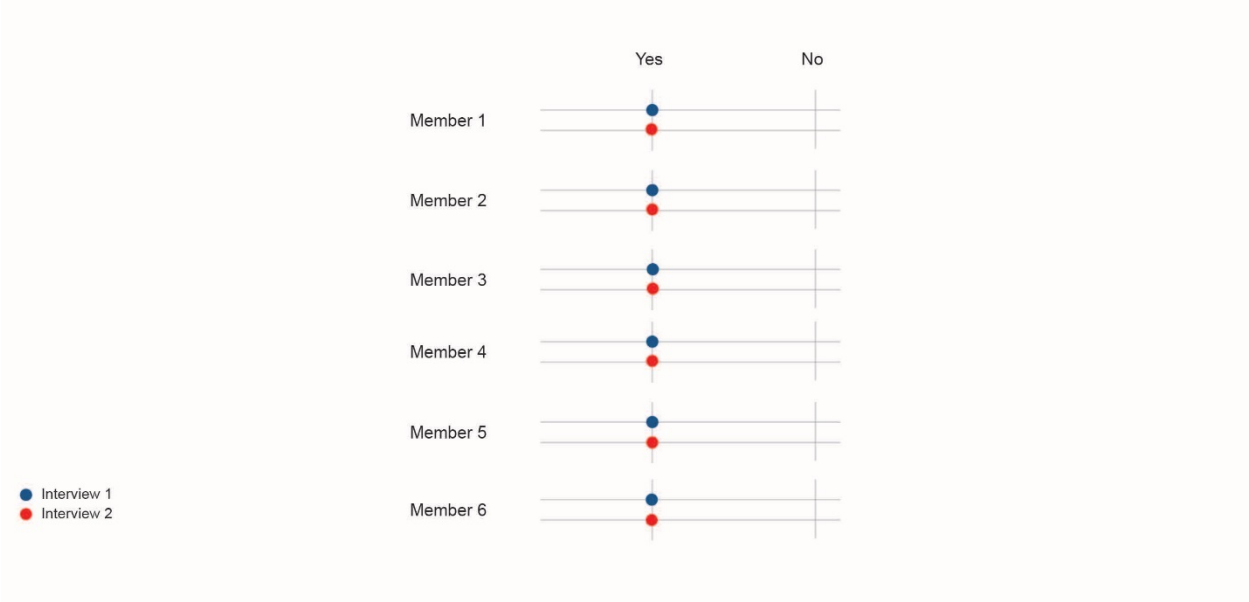


Figure 24. Are you aware of the National Security Agency document leaks carried out by Edward Snowden in 2013?

The section above focussed on individual opinions and allowed us to access the cognitive model of the cohort group. Something valuable learned from this study was that members wanted to know about privacy breaches. They also admitted to having misinformation about the data policies of the applications on their smartphones and wanted to be more informed.

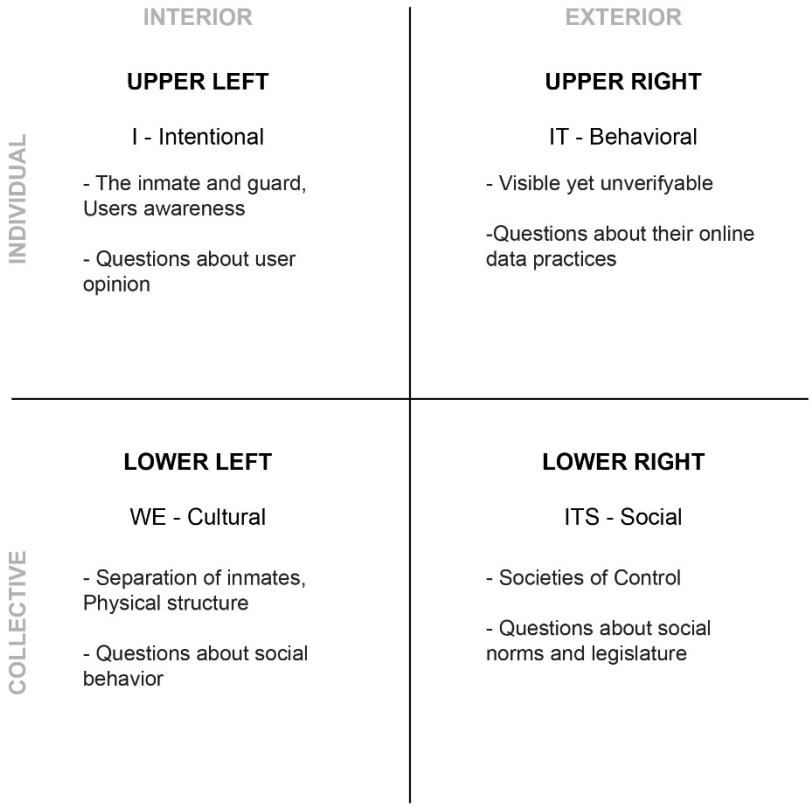


Figure 25. Summary of questions asked in the prospective Cohort Study overlaid onto the AQAL diagram.

The figure above (Figure 25) is a summary of the prospective cohort study; it shows how the questions were divided to give a holistic view of the cognitive models of the members. In conclusion, this thesis learnt that the members of this study have many applications on their smartphones that they do not trust yet they used those applications because of the utility provided by the applications. The members did not trust those applications because they did not understand how the applications functioned and even though there were ways to learn about this, like reading the terms and conditions, the members refused to do so because they felt that the terms and conditions were boring and tedious. Because the members failed to read the terms and conditions they were unaware how the applications on their smartphones were sending their data to third parties. They also knew that their smartphones were not protected from third parties that want access to their data. The goal of this prospective cohort study was to examine if the

cognitive dissonance in the mind of a member, specifically related to what mobile applications can do with user data, could be reduced by giving the member education about how mobile applications shared their data. The result of that examination was that even though education was provided to the members, their opinions about applications did not change. However, not only did the members see value in education about privacy breaches taking place through smartphone applications but they also passed on this knowledge to others who were not a part of this study. This point of sharing knowledge was instrumental in the development of the prototype.

This section provided a brief introduction of the research plan used in this thesis, followed by an analysis of the interviews and questionnaires answered by the members of the prospective cohort study.

5.0. The Phonopticon

This section describes the Phonopticon, an installation that uses data visualization to inform and educate users about surveillance carried out by applications on smartphones. The previous chapter explained how members wanted more information about privacy breaches and that insight was vital in the development of the Phonopticon. This section begins with an explanation of the methodologies used, followed by previous versions of the prototype that were developed and explains the current version of the prototype. This section concludes with the feedback received on the Phonopticon.

5.1. Methodology

This section elaborates on how research through design was used as a methodology in the developed of the prototype. Research through design focuses on the understanding that is learned through a design process. It relies on this understanding to provide a simplification of complicated problems. It involves looking at the design process as research and includes the creation of new prototypes and experimentation with new processes and materials. However, the prototype is not the goal of the process, the goal is to get gain knowledge and understanding about a subject (Godin & Zahedi, 2014) and this knowledge and understanding are gained through the development of the prototype. According to Zimmerman the “process of iteratively designing artifacts as a creative way of investigating what a potential future might be” (2010, p. 312) is research through design. Thus, the design process used in making the Phonopticon involved many iterations that were improved based on feedback. Since many design processes include feedback loops, the Spiral Model of software development by Barry Boehm was used as a research method. This model emphasizes feedback and continuous improvement of a prototype. Boehm proposed a risk-driven process that integrates risk management and subsequent development (Boehm, 1988). The process is made up of multiple spiral loops and (Figure 26), each loop is one iteration of the prototype (Zsolt, 2014). Even though the model was developed for software, it was beneficial in the creation of the prototype due to its focus on making iterations and feedback.

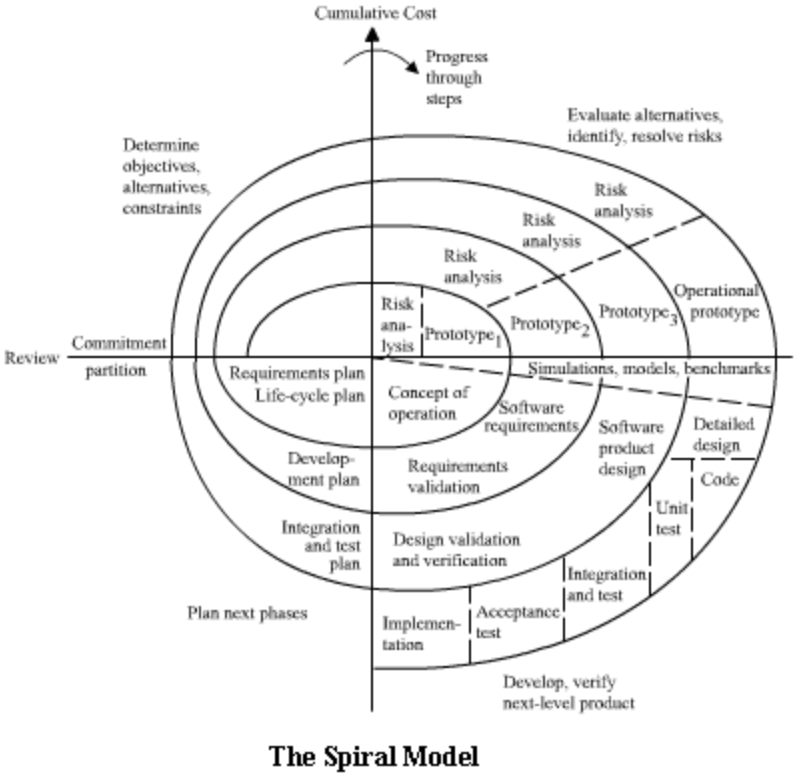


Figure 26. Barry Boehm's Spiral Model of Software Development (Boehm 1988. p. 25).

Each loop of the Spiral Model of Software Development is divided into four parts, and each part represents a stage of development of the prototype.

1) Setting the objective- Before each iteration was made, the intended objective of that iteration was decided, along with the goals and the limits of that iteration. Prototype risks were identified that could cause problems in the future had they not been accounted for. Based on those risks, backup plans were thought of and kept ready. For example, one of the objectives set in the initial stages of development was to educate users about the data that was given away to third parties by the applications on their smartphone. The risks of this were that users might get bored of just textual information and in response, videos along with a narration were used.

2) Risk assessment - For each of the identified prototype risks, an analysis was carried out. If those risks could not be eliminated, steps were taken to reduce their effect. For example, users who tested the early variations of the Phonopticon found certain aspects of the prototype to be non-essential, and

those aspects were then removed from future variations. Aspects such as linking users to news articles on websites that would draw them out of the installation were removed from future iterations.

3) Development and validation- After assessing the risks, the process for the following version is decided upon. For example, in previous iterations, users felt that there was too much text on the mobile interface and it distracted them from viewing what was presented on the screen. These risks were addressed in the development. For example, text on the mobile interface was kept to a bare minimum.

4) Planning- The prototype is critiqued, and if it is found to be satisfactory, the process comes to an end. But if it is not then the process continues along a new loop of the spiral (Gabry, 2017). For example, based on the user testing feedback the shape of the prototype kept changing while the use of the webcams was carried onto future iterations.

This spiral method allowed this thesis to identify problems and drawbacks. Most importantly, it allowed for those drawbacks to be addressed effectively. The prototype and its previous iterations could only be developed once feedback was received and a prospective cohort study was used to get that feedback from users. These individuals had certain common traits but also shared differences with one another. For example, participants who only used Android devices were recruited but these participants used those devices in diverse ways. Even though many of the participants had the Uber application on their smartphones, some used Uber to travel all the time while others just use it to check the prices of taxis. In conclusion, the development of this prototype relied on research through design as a methodology and Boehm's spiral model of development as a research method to develop the Phonopticon. Additionally, questionnaires and interviews were used as research methods to get feedback about the different iterations.

5.2. Previous Versions

This section describes the previous versions of the Phonopticon that led to its current form. These versions were developed over a period of nine months between 2017 and 2018 and were tested with students and teachers at the OCAD University. The design for the Phonopticon has been through many variations, but each variation includes topics such as vision, power and surveillance.

Figure 27. User testing the first iteration.

The very first iteration of the Phonopticon was going to be a smart mirror (Figure 27). The mirror would receive data from an application on a singular user's smartphone and would display the amount of data each application on the user's smartphone uploads to third parties. The idea behind this was that a user could get their readout once a day and that would cause a change in user behaviour. The visuals displayed on the mirror were simple heads-up display (HUD) elements. The visuals were made up of quantitative data that users would be able to read quickly and understand. This prototype was speculative, and after a few rounds of feedback, it was found that users would not want this in their homes. Also due to the restraints of time and resources, this thesis would not be able to assess a change in user behaviour. Additionally, this mirror would give users information that would scare them every day and most users

would not want that. Suggestions were made to convert it from a product to a research object, like an installation in a public space as opposed to a product that would be present in someone's private space.

Figure 28. User testing the second iteration.

The second iteration of this prototype was developed after early research into the panopticon was carried out. It was made up of an array of webcams that were connected to servo motors that covered or uncovered the webcams depending on how users answered a few questions on their smartphone (Figure 28). The webcam feed was shown on a screen in front of the user. The screen displayed multiple feeds of the same webcams in a grid to replicate the many prisoners of the panopticon. Feedback received for this iteration was that users were too occupied with the interface on their phones and were missing out the interface on the screen. Additionally, the servo motors were unreliable and had to be discarded in future iterations.

Figure 29. User testing the third iteration.

In the third version users approached a display and using a mouse answered questions regarding the applications they use and their data practices. The display contained a grid that was made up of feeds from various webcams that were aimed at the user. Depending on the user's answers the grid started to change (Figure 29). The feedback we received at the end of this user testing session was that the user's smartphone needed to be included in the interaction. The visual metaphor worked, but users did not feel the connection between the visual metaphor and their mobile devices.

The creation and iteration of these prototypes were instrumental in the development of the Phonopticon. The current version is a prototype that has potential to be improved upon. Boehm's spiral model of development encourages numerous variations of the prototype until satisfactory results are achieved.

5.3. The Phonopticon

This section describes the current version of the Phonopticon. It describes the visuals used, the physical structure, the mobile interface and the software used in its development. Following that the prototype is analyzed by using the AQAL lens. For clarity in this section, the term viewer is used to denote a single user that interacts with the Phonopticon.

The Phonopticon is an immersive installation that has three main goals. The first goal is to inform its viewers of cases where mobile phone applications have violated user privacy, the second goal is to visualize the surveillance carried out by mobile phone applications, and the last goal is to educate its viewers of what they can do to shield themselves from breaches of privacy. Data visualization was used to achieve these goals because it allows viewers to digest enormous quantities of data efficiently. Data visualization also challenges viewers to think about the data rather than the design, or the methods used to create the visualization. Additionally, backing data visualization with facts and information leads to impactful responses (Centerline Digital, 2015). The Phonopticon does not visualise quantitative data. Instead, it visualises qualitative data that is a representation of the viewer's input.

The Phonopticon was made to emulate the workings of the panopticon in our contemporary information society and is made up of three parts that work simultaneously to offer an interactive experience to a viewer. The first part is a set of visuals that are projected from the outside onto the walls of a hexagonal structure. These visuals can be viewed in OCAD University's Open Research Repository and are located in the same section as this thesis document. The second part is a hexagonal enclosure onto which the visuals are projected. The viewer stands inside this enclosure which has six webcams mounted in various locations around it. The last part is a mobile interface by which a viewer can interact with the Phonopticon.

The following section describes a viewer's journey in the Phonopticon and offers a detailed description of the visuals that are projected onto the walls of the enclosure. When a viewer approaches the installation, they see an iPad along with a set of wireless headphones (Figure 30). The iPad has a visual

that warns users that they are under video surveillance. It also tells users to open a specific web link on their smartphones and enter the installation.

Figure 30. The sign viewers see outside the Phonopticon.

After entering the installation with their smartphones, the viewer can see visuals being projected on the walls of the Phonopticon. At the same time, the webpage on their smartphones displays a 'Start' button (Figure 31). The visuals were edited in Adobe After Effects and were organized and controlled using a Processing script. The full list of software used in this thesis can be found later in this chapter.

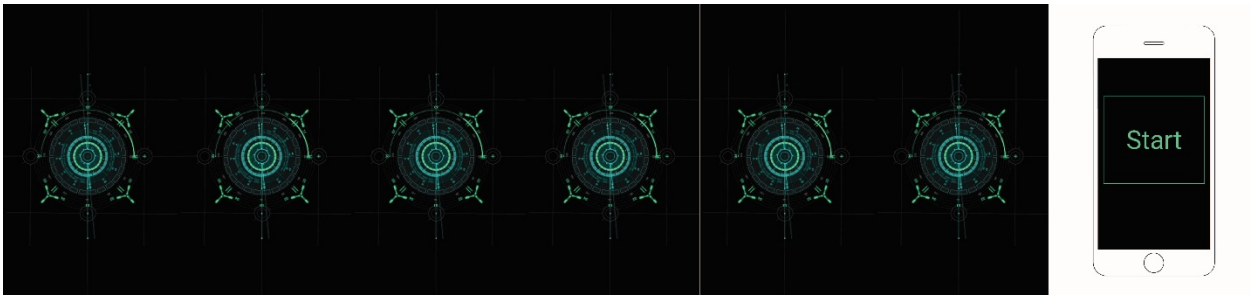


Figure 31. The first visuals displayed in the Phonopticon along with a webpage screenshot of the visitor's phone.

When the viewer presses the 'Start' button, the visuals change, and an audio narration begins. The narration is played through the wireless headphones provided and guides the viewer through the entire interaction. The visuals include brief text about the Phonopticon and gives the viewer instructions about what they must do while they are inside the enclosure (Figure 32). The viewer is informed that they must

answer six questions about the applications on their smartphones after which the Phonopticon will visualize the surveillance carried out by those applications. Once the viewer has understood the instructions, they press the ‘Okay’ button on their smartphones.

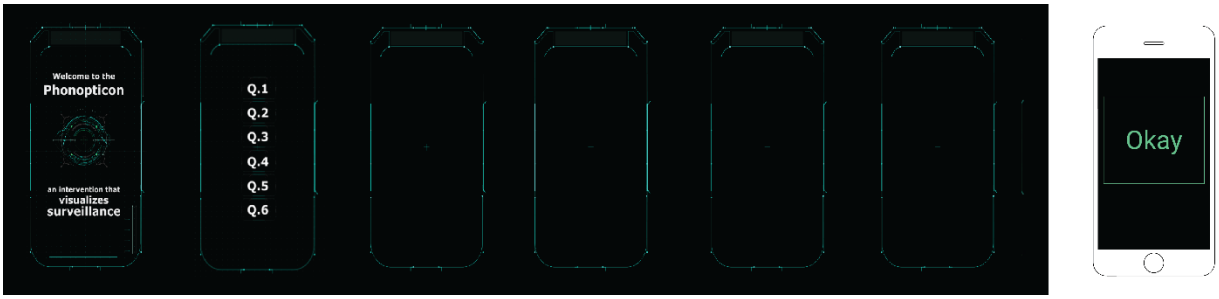


Figure 32. The introduction visuals displayed in the Phonopticon along with a webpage screenshot of the visitor’s phone.

The visuals change, and the first question is displayed which is ‘Do you have the Instagram application on your smartphone?’ (Figure 33). This question is displayed in text and is also repeated through the narration. The viewer must click on the ‘Yes’ or ‘No’ button on their smartphones to answer the question.

Figure 33. The first question displayed in the Phonopticon along with a webpage screenshot of the visitor’s phone.

Once the viewer has provided their answer, the question disappears and is replaced with information about how Instagram has rights to the images uploaded on its platform and can sell those images to third parties (Figure 34). The visuals also include news articles where Instagram has been found guilty of giving away data to third parties. These news articles were included because the first goal of the Phonopticon was to inform and educate the viewer about breaches in data privacy taking place through

smartphone applications. However, the visuals alone were unable to convey that information to viewers. In earlier iterations of the prototype, all the information was provided through text and images, but viewers felt that there was an information overload. In response, the narration was introduced to the prototype because it allowed for easier communication. Text that would take many pages to display and a lot of time to read was replaced by a narration. Thus, the visuals rely on the narration to explain the details of privacy breaches. This allowed the viewer to understand the information in an uncomplicated way. This narration can be read in Appendix C of this paper. Once the narration is done talking about Instagram, the second question loads. The second question asks the viewer 'Do you have the Uber application on your smartphone?'

Figure 34. The first answer along with the second question displayed in the Phonopticon along with a webpage screenshot of the visitor's phone.

This entire question and explanation process is repeated until the viewer has answered all six questions (Figure 35). These questions are about Instagram, Uber, free games, fitness tracking applications, terms and conditions and Facebook. These applications were picked because not only are they common among users, but because they have all been known to give away data to third parties. The question about terms and conditions was included because it reflects the viewer's data practices. In the prospective cohort study, it was found that none of the members read the terms and conditions and this question was included in the prototype to find out if the viewers read the terms and conditions before using an application. Many users do not read them (Lomas & Dillet, 2015) and might be unaware of how applications such as Netflix and Dropbox have terms and conditions that justify their sharing of user data with third parties. The question about free games was included after examining the data readouts of the

prospective cohort study in which it was found that the free games used by members of the cohort shared a lot of data. The six applications were also chosen because they cover various kinds of data. Instagram gives away images to third parties, Uber and fitness tracking applications give away geolocation, the free games give away audio data that is captured from a smartphone's microphone, the terms and conditions are used by companies to get users to agree to their terms of service and Facebook shares contact details with third parties.

Figure 35. The screen displayed when all the questions in the Phonopticon have been answered along with a webpage screenshot of the visitor's phone.

Once the viewer has answered all six questions and has been informed of how these applications share their data with third parties, the visuals change to depict a circular loading bar appears (Figure 36) that tells the viewer when their surveillance visual has loaded. Once this progress bar reaches 100%, the viewer is meant to press 'Initialize' on their smartphones to begin the next visualization.

Figure 36. The loading screen displayed in the Phonopticon along with a webpage screenshot of the visitor's phone.

Unknown to the viewer there are six webcams located around the installation. Each webcam is linked to one question the viewer previously answered. The webcams are positioned around the enclosure

in a specific way. The webcam associated with Instagram is pointed at the face of viewer, the webcams associated with Uber and fitness tracking applications are pointed at the feet of the viewer, the webcam associated with free games is pointed at the hands and fingers of the viewer, the webcam associated with terms and conditions are pointed at the enclosure itself and finally the webcam associated with Facebook is located at the top of the enclosure and is pointed downward at the viewer. These webcams are constantly capturing live feeds of the viewer. These live feeds are not visible to the viewer but when they press the 'Initialize' button these life feeds begin to be displayed on the walls of the Phonopticon. These feeds are displayed as a grid (Figure 37), and in the beginning each application has 2160 feeds which add up to a total of 12960 feeds coming in from the six webcams.

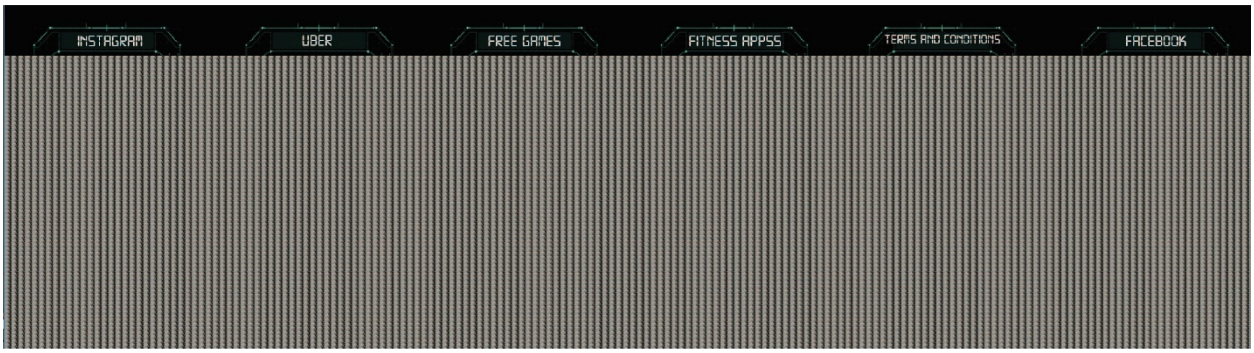


Figure 37. The grid visualisation displaying 12960 live feeds.

Depending on the viewer's answers these feeds can change. For example, if a viewer answered 'Yes' to having the Instagram application and answered 'No' to the other five questions, the live feeds related to Instagram reduce in number every five seconds (Figure 38) until there are only two feeds left. Simultaneously, as the number of live feeds reduces the size of each feed doubles.

Figure 38. The grid visualization displaying how the live feeds change.

This continues until only two feeds are left (Figure 39). The intended effect was to make the viewer think that the Instagram application is watching them closely as compared to the other mobile applications that are not because the viewer does not have those mobile application installed on their smartphone.

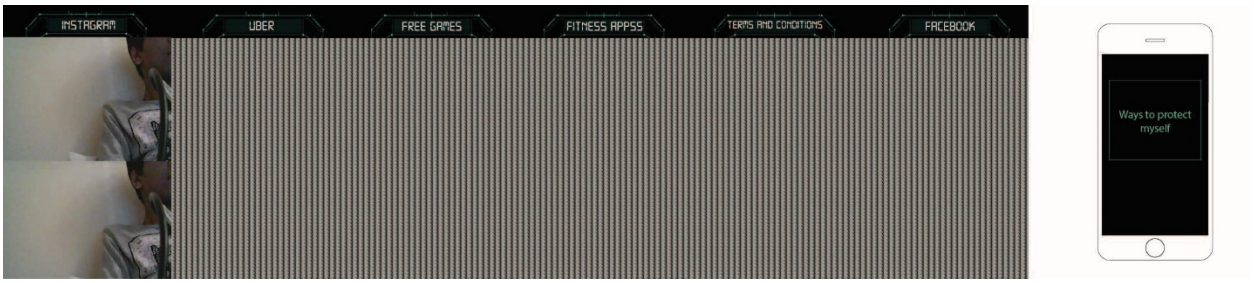


Figure 39. The grid visualisation displaying how the live feeds change along with a webpage screenshot of the visitor's phone.

The feeds related to the other five applications do not change but are still visible because even though the viewer might not have those applications on their mobile phone, those applications could still have their data. In 2011 it was found that Facebook had access to phone numbers of users who did not have Facebook accounts. They got this data by looking at the contacts of users who did have Facebook accounts and added everyone from those Facebook users' contacts to their servers. (Grobart, 2011). Even if a viewer does not have certain applications, they cannot be sure that their data is safe. The narration in this section identifies each application and the webcam associated with it. It also identifies where these webcams are so that the viewer can see them. The narration also informs the viewer that in the next segment they will be told of ways to shield themselves from such surveillance.

This entire segment was added to the Phonopticon because the second goal of the prototype was to visualize the surveillance carried out on mobile phone users. This grid visualization serves as an artistic data visualization. The term artistic data visualization is defined as "visualizations of data done by artists with the intent of making art." (Viégas & Wattenberg, 2007). Viéga and Watternberg outline two conditions a visualization must meet for it to be considered an artistic data visualization. The first is that

the artwork must be based on real data, not metaphors, and second is that there needs to be artistic intent behind the visualization. The grid visualization used in the Phonopticon is based on real qualitative data that is sourced from the viewer's answers, and the intent of the visualization is to create an artistic representation of how mobile applications are surveying the viewer. The grid visualization is not a completely accurate representation of the surveillance carried out by mobile applications because different viewers might use the same application in different ways, some may use Facebook all the time, but others might use it sparingly, ultimately the visualization for both scenarios would be the same. However, that does not reduce the value of the visualization. Artistic data visualizations acknowledge that there are "distortions" (Viégas & Wattenberg, 2007) embedded in them. But these misrepresentations are not mistakes. The value of such visualizations relies on their power to put forth a point of view. In the case of the grid visualization, this point of view is that the mobile applications are always monitoring users.

The viewer can watch the grid visualization for as long as they would like to and when they are ready to move onto the next section, they can press the 'Ways to protect myself' button that is visible on the viewer's smartphone (Figure 40).

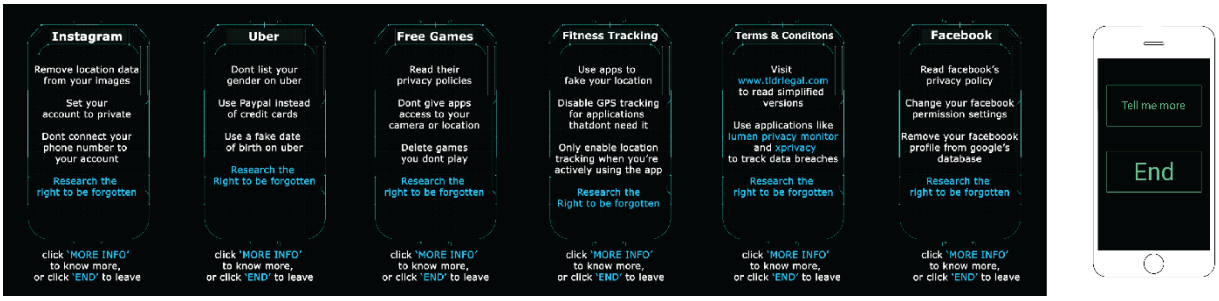


Figure 40. The information screen displayed in the Phonopticon along with a webpage screenshot of the visitor's phone.

The next segment was added because of the last goal of the Phonopticon which was to educate viewers by informing them of what they can do to shield themselves from surveillance carried out by the applications on smartphones. This segment lists various practices that can be carried out that can protect

the viewer. It also includes alternative applications that can be downloaded to shield the viewer from surveillance.

Once the viewer has read them, they may choose to either exit the Phonopticon or gain more information about the Phonopticon. This choice was added because after carrying out user testing it was found that some viewers felt that there was too much information being provided to them and they wished to end the visualization. However, it was important to convey more information about the Phonopticon, and so a compromise was reached wherein viewers were given a choice to either get more information or end the visualization. If a viewer wanted more information, they can click the 'Tell me more' button on the webpage or if they want to leave they can click the 'End' button. If they click the 'End button' the Processing script restarts and once the current viewer leaves the installation the Phonopticon is ready for the next viewer.

If the viewer clicks on 'Tell me more' then the final visualization begins (Figure 41). This visualization explains how users are currently living in a new age panopticon. It offers a brief explanation of Bentham's panopticon and informs users about the Right to Be Forgotten that exists in the European Union.

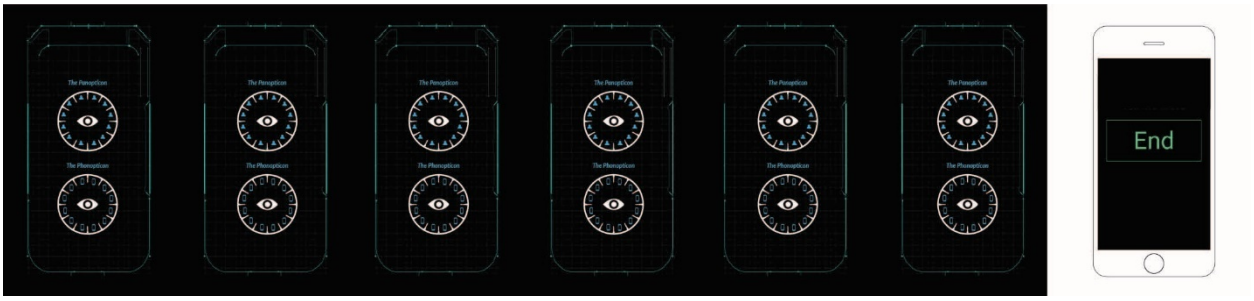


Figure 41. The last screen displayed in the Phonopticon along with a webpage screenshot of the visitor's phone

When these visualizations end the viewer is expected to press the 'End' button which restarts the Processing script, and once the viewer leaves the enclosure the Phonopticon is ready for the next viewer. However, even if the viewer does not press the 'End' button, the entire script restarts after 4 minutes of

inactivity (Figure 42). On exiting, the viewer can take an A4 sized card that includes details about privacy breaches and steps to shield themselves from mobile application surveillance for their own reference.

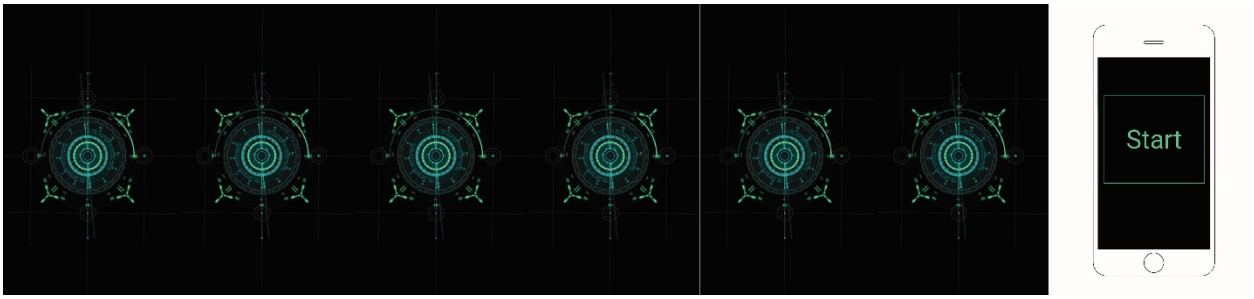


Figure 42. The first visuals displayed in the Phonopticon along with a webpage screenshot of the visitor's phone.

The section above offered a detailed description of a viewer's journey in the Phonopticon. The following section sheds light on the other parts, the physical structure and the mobile interface.

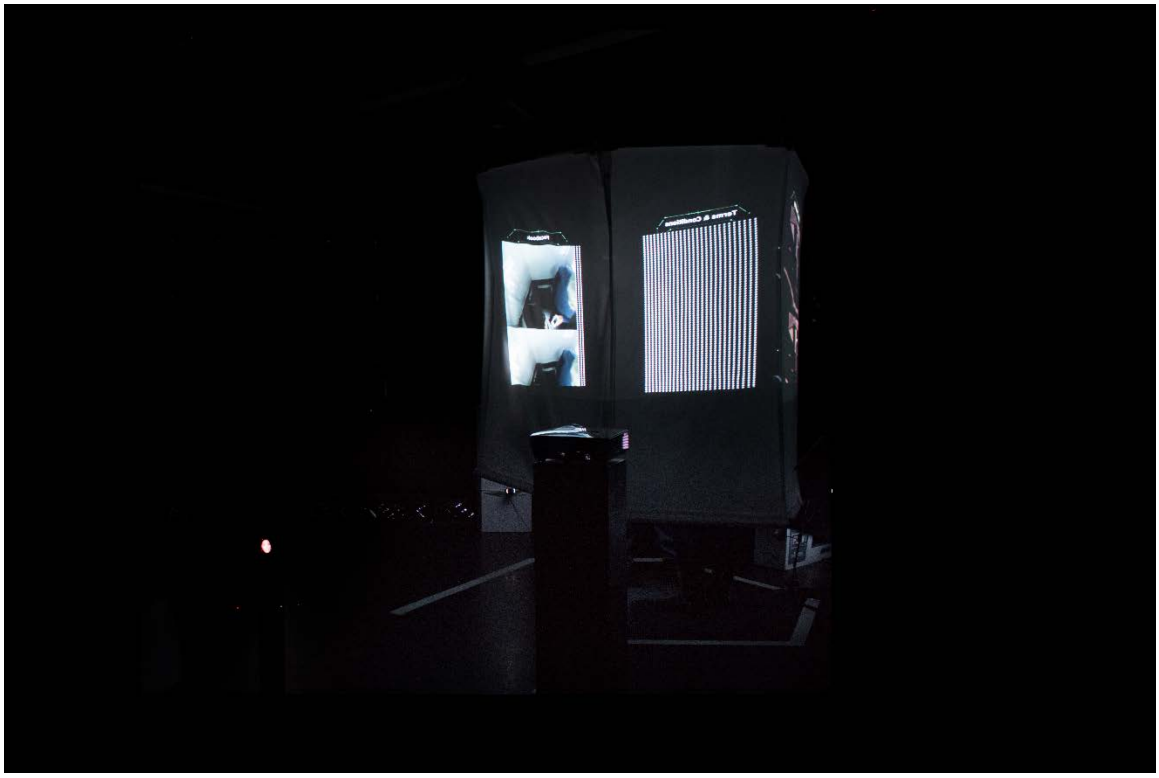


Figure 43. The physical structure of the Phonopticon.

The Phonopticon is made up of a hexagonal enclosure that has an opening for users to enter. The diameter of the enclosure is 6.5 feet, and it is 9 feet high (Figure 43). Surrounding the enclosure are three short throw projectors that project visuals on the walls of the enclosure. At various points around the enclosure are attached six webcams that transmit live video to a computer that is connected to the projectors.

Figure 44. The mobile interface used to interact with the Phonopticon.

The mobile interface (Figure 44) was designed using Javascript and Pubnub to communicate with the Processing script. This communication system was crucial for the interaction between the viewer and the Phonopticon because without it there would be no way to connect the viewer's smartphone to the Processing script.

This paragraph gives a brief description of the software used in the development of the Phonopticon. Adobe After Effects is a video editing software that was used to edit the visuals and add the narration. Processing is an integrated development environment designed for visual arts. It was used to organize and play the visuals based on input from a viewer's phone and was also used to create the grid visualization. Atom is a text editor that was used to code the mobile interface and the programming

language used to do so was Javascript. The communication between the mobile interface and the Processing script was carried out by PubNub which is a data stream network that enables messaging across the internet. Resolume Arena 5 is a projection mapping software that was used to project the visuals onto the walls of the prototype and Spout is a software that enables visuals from Processing to be displayed by Resolume Arena 5.

The following section looks at the Phonopticon through the AQAL framework. The framework is used to explain design decisions made in the development of the Phonopticon.

In the Exterior Individual segment, the behaviour of the viewer is examined. The Phonopticon needed a method to gain information about the viewer's behaviour, or what applications they have on their mobile phones and this information was gathered by asking them questions. The question and answer segments were added as it was one way for the visualization to be somewhat specific to each viewer. Otherwise, a viewer may not feel like the data visualized on the walls is a representation of their personal data.

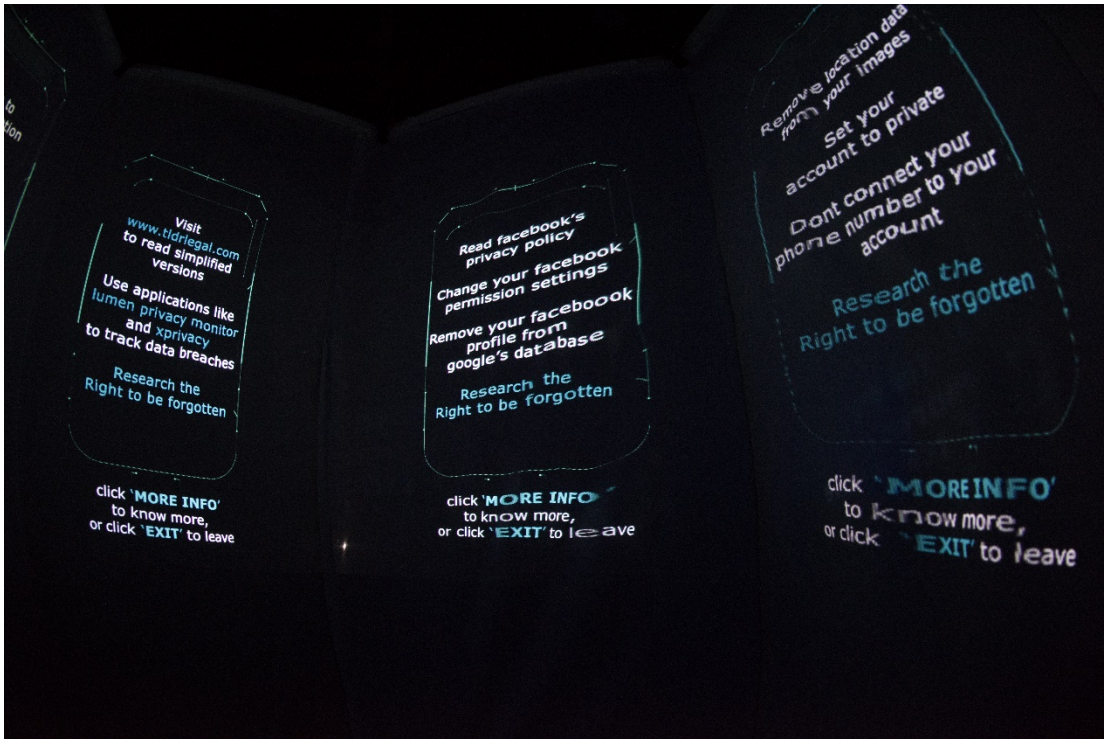


Figure 45. The text on display on the walls of the Phonopticon.

In the Exterior Collective segment, our global environment is examined. In the Phonopticon, aspects such as information about the Right to be Forgotten was included with the aid of the narration alongside the visuals. Parts of the narration offer information about the growth of ubiquitous surveillance and the emergence of our smartphones as the new panopticon.

Within the Interior Collective segment, our culture is examined. While designing the Phonopticon, the aspects of isolation and social sorting had to be included. The viewer had to be physically separated from their environment, which explains the enclosing structure of the Phonopticon. The material used for separating the viewer from their surroundings allows shadows to pass through. So, when one viewer is inside the Phonopticon, they will be able to see shadows of other viewers outside. However, they will not know the identity of those viewers. Additionally, even though the total height of the prototype is 9 feet, the height of the walls is 6 feet. This allows for viewers outside the Phonopticon to see part of the viewer inside. This also allows viewers inside to see part of the viewers outside. The element of social sorting was brought out with the use of the surveillance score that separated viewers based on their answers. The webcam feeds were designed to look like a grid because they represented the cells of the panopticon. Just as the prisoners inhabited the cells of the panopticon, the viewer's images inhabit the cells of the Phonopticon.

Within the Interior Individual, user opinion and thoughts are examined. The aspects of user awareness and knowledge about privacy breaches needed to be addressed in the prototype. Therefore, the Phonopticon had visuals that aimed to change the viewer's opinion about smartphone applications through education.

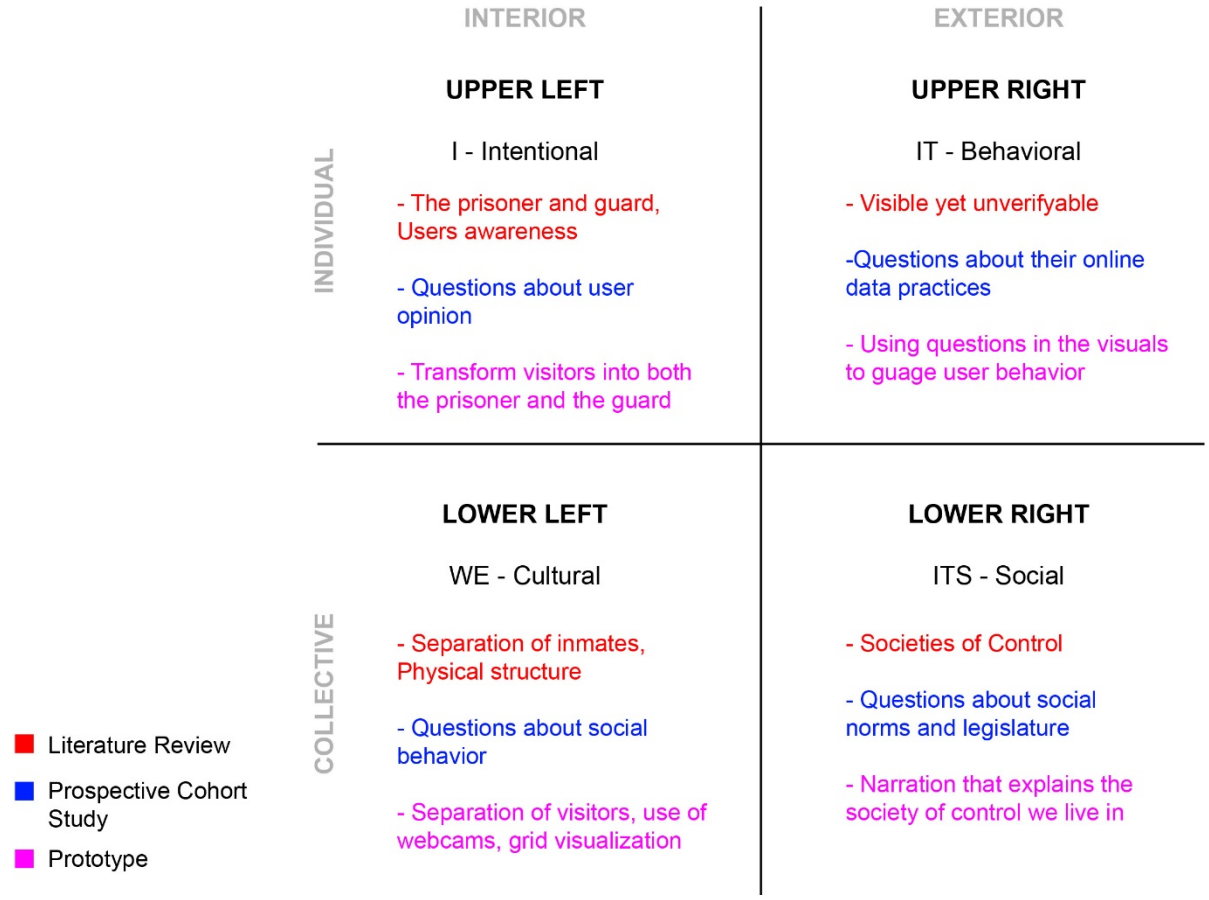


Figure 46. Summary of my research (literature review, prospective cohort study and development of the prototype) overlaid onto the AQAL diagram.

The figure above (Figure 46) shows how the AQAL framework was applied to all parts of this thesis, specifically the literature review, the prospective cohort study and in the development of the prototype.

In conclusion, there has been no other work that has influenced the development of the Phonopticon more than Bentham's panopticon. The Phonopticon reflects the panopticon in both its working and its physical form. Just like Betham's structure, the Phonopticon is circular and puts an individual in the center of the structure. However here lies the vital difference between the two. In the Phonopticon the guards and the prisoner can be the same person, whereas in the panopticon they are

different entities. Additional influences that were used in the development of the Phonopticon are mentioned in Appendix B.

5.4. Feedback

The feedback process for the Phonopticon involved individual user testing sessions with the members of the cohort group. Members felt that the physical structure was intimidating but were curious to explore it. Once they approached the Phonopticon, they were informed of the web-link they could access to interact with it. Once inside, members took a while to get used to the enclosure. Even though they were not completely covered, they did feel claustrophobic and isolated. The visualizations were perceived as being futuristic, and members felt like they were in a science fiction movie. The voice of the narration added to this effect. The members navigated the six questions at their own pace. Some took their time to digest what was being shown while others rushed through the questions. Ultimately, they finished answering the questions after which the Phonopticon displayed the loading animation. Most of the members were surprised and taken aback when the visuals of the webcams were displayed. There was some confusion in the beginning, but as the narration cleared things up, they understood what they were looking at. At this point users turned around on their own to view the different webcam feeds. Some users tried looking around to find the location of the webcams. It did make them feel uncomfortable which was the desired effect. Users moved their hands to see the visuals representing those movements. The next section was where users spent most of their time. The section informed them of things they could do to protect themselves from the applications on their smartphones and users read these tips to gain knowledge. They also learnt about the Right to be Forgotten. On ending the interaction with the Phonopticon, members left the enclosure feeling a little relieved but also a little paranoid.

6. Conclusions and future research

The concluding chapter of this thesis summarises the research that was carried out. It highlights the goals of this thesis, examines if those goals were reached and elaborates on what this research learnt in the process of reaching those goals. It also includes a section on how the current prototype could be improved. This chapter ends with a description of the future research that can be carried out in similar fields.

Firstly, this thesis found that smartphone users make uninformed decisions when it comes to downloading smartphone applications. Smartphone users have an idea of what an application can do with their data, which is not necessarily the same as what application does. The literature review drew comparisons between Bentham's panopticon and the surveillance smartphone applications. This comparison found that users have a cognitive dissonance that can be reduced by educating users about the surveillance systems embedded in smartphone applications. This finding influenced the direction of the prospective cohort study and also answered the first research question about the similarities between surveillance carried out in mobile devices and the surveillance structure proposed by Jeremy Bentham's Panopticon. The answer is that the panopticon is an effective metaphor for contemporary surveillance. The core value of Foucault's analysis of the panopticon is that the prisoners discipline themselves because they do not know when they are being watched and even though this thesis did not examine user behavior future research into this matter could offer valuable insights into how users regulate their own behavior and thoughts when it comes to surveillance carried out by mobile applications.

Secondly, the goal of the prospective cohort study was to examine if the cognitive dissonance in the mind of a user, specifically about what mobile applications can do with user data, can be reduced by giving a user education about how mobile applications share user data. Education such as information about data and privacy breaches carried out by mobile applications was provided to the members of the cohort study. The principle findings of the cohort study were that the members of the cohort group did not change much even after they were given education about surveillance systems embedded in smartphone

applications. Even informing the members of examples where user data was shared to third parties was not enough to change their views on smartphone applications because the members valued the utility provided by mobile applications more than their privacy. However, the members saw value in education about privacy breaches and this influenced the development of the Phonopticon. They not only valued the information provided but also shared that information with other users who were not a part of this study. The findings of the prospective cohort study also answered the second research question which was about users finding value in education about surveillance.

Lastly, the Phonopticon had three main goals. The first goal was to inform its viewers of cases where mobile phone applications have violated their privacy, the second goal was to visualize the surveillance carried out by mobile phone applications and the last goal was to educate its viewers of what they can do to shield themselves from breaches of privacy. These goals were met by the prototype. The development and feedback of the Phonopticon helped answer the last research question of this thesis which was about using data visualization to educate users about surveillance. The findings of the Phonopticon were that data visualization can be used as a tool to educate users about surveillance.

These were the main findings learnt in this thesis. The next section elaborates on future research that can be carried out in similar fields.

Because the prospective cohort study was limited to Android users, future research could include iPhone users to get a better understanding of other smartphone users. The size of the cohort group was too small to make any generalizations, and the data collected as part of this thesis is not substantial enough to make assumptions regarding general data practices. Future research into this topic could increase the size of the cohort group to more diverse users. The Phonopticon needs to be tested with more users to get diverse feedback that can be used to access its effectiveness as a tool. The grid visualization used to represent surveillance is currently based on visual metaphors. However, not all applications are watching users and some, like Honey Quest (Maheshwari, 2017), might be listening too. Given enough time and resources, future prototypes could record visitor audio and use that audio to represent surveillance. Additionally, given more time a version of the Phonopticon that connects directly to

NetworkStatsManager can be developed, so that the visualization is completely personalized to every visitor who views the prototype.

This paper scratched the surface about surveillance carried out by smartphone applications, but future research can go even deeper. The conclusions about the effectiveness of education in aligning the cognitive models of the users point us in the direction of future research. Researchers can explore other tools, like applications or software, which could align the cognitive models of users. On one end we have countries like China and Singapore that embrace surveillance systems, and on the other end, we have Argentina and the European Union that resist it. Research into how these governments embrace or resist surveillance will be very useful for users who want to escape contemporary surveillance.

Some users might not have a problem with the panopticon we live in and would not mind sharing their data with third parties. The consequences of such behavior need to be researched. What happens if Google gets hacked tomorrow? There is nothing users could do about their data then, but there might be something users can do about their data now. Users cannot opt out of this environment because we still need our phones to function as members of society. Tools like Mockdroid allow us to confuse the surveillance systems, but they do not solve the problem. The development of applications like XPrivcay and Lumen and represented a change in user perspective regarding data privacy and surveillance. This change in user perspective needs to be researched in detail. The ethics around surveillance carried out by smartphone applications need to be assessed as well.

Experts like Schneier believe that we are slowly but surely moving towards a scenario, like Oceania from George Orwell's *1984* (1949), where the citizens live under constant surveillance. When asked about his opinions regarding the current surveillance state Schneier says "I am regularly asked what the average Internet user can do to ensure his security. My first answer is usually 'Nothing; you're screwed" (2008.p.112). There is no place to hide: the technological gaze is potentially all over the place. Schneier believes that we have lost the fight against surveillance, that there is no hope for us. However, there is hope. A global movement has begun that recognizes privacy as a human right and not just an abstract concept. The European Union is a leader in this movement, and other governments like India

(Gargi, 2016), Spain (Peguera, 2017) and South Korea (Lim, 2016) may follow. The start of this movement will be Edward Snowden's legacy. Such movements will gain more followers once users are aware of the existence of the current panoptic surveillance state, and this awareness can come when users start talking about surveillance and mobile applications.

Smartphone users need to revaluate how they perceive their smartphones because every smartphone is a miniature panopticon. The steady growth of the mobile application industry validates the main point that this thesis is trying to make, that we're living in a Phonopticon – the age of mobile surveillance.

7. References

Al-Bassam, M. (musalbas) (2018, January 28). Fitbit heatmap inside GCHQ building (left) is more hot than inside NSA building, probably because it rains all the time in the UK [Twitter Moment]. Retrived from https://twitter.com/musalbas/status/957676620386590722/photo/1

Andrejevic, M. (2006). *The discipline of watching: detection, risk, and lateral surveillance. critical Studies in Media Communication.* Retrieved from http://people.southwestern.edu/~bednarb/media-culture/articles/andrejevic.pdf,

Ballano, B., Wueest, C., & Lau, H, (2014). How safe is your quantified self? Retrieved from https://www.symantec.com/content/dam/symantec/docs/white-papers/how-safe-is-your-quantified-self-en.pdf

Bauman, Z. (2000). *Liquid Modernity*. Cambridge, Polity Press. Print

Beresford, A., Rice, A., Skehin, N., & Sohan, R. (2012). *MockDroid: trading privacy for application functionality on smartphones*. United Kingdom: University of Cambridge. Print.

Berenson, A. (2013). Snowden, Through the Eyes of a Spy Novelist. Retrieved from http://www.nytimes.com/2013/06/25/opinion/snowden-through-the-eyes-of-a-spy-novelist.html

Bertrand, M & Mullainathan, S (2003). *Are Emily and Greg more employable than Lakisha And Jamal? A Field Experiment On Labor Market Discrimination.* MA: National Bureau Of Economic Research. Print

Bo, H. (2017). Activists Aren't Backing Down After Egypt's Massive LGBTQ Crackdown. Retrieved from www.vice.com/en_us/article/bjvbg4/activists-arent-backing-down-from-egypts-massive-lgbtq-crackdown.

Boehm, B. (1988). A Spiral Model of Software Development and Enhancement. Retrieved from http://csse.usc.edu/TECHRPTS/1988/usccse88-500/usccse88-500.pdf

Botsman, R. (2017). Big data meets Big Brother as China moves to rate its citizens. Retrieved from http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion

Boyne, R. (2000). Post-Panopticism. Retrieved from http://www.tandfonline.com/doi/abs/10.1080/030851400360505

Brown, F. (n.d.). The power of panopticism. Retrieved from http://home.moravian.edu/public/eng/writingCenter/prize/Faith_Brown.pdf

Bujold, N [Nathalie Bujold]. (2015). Textile de cordes [Video file]. Retrieved from https://vimeo.com/97258089

Caliskan, A., Bryson, J., & Narayanan, A. (2017). *Semantics derived automatically from language corpora contain human-like biases.* Retrieved from http://science.sciencemag.org/content/356/6334/183

Centerline Digital. (2015). The Importance of Data Visualization. Retrieved from https://www.slideshare.net/Centerline_Digital/the-importance-of-data-visualization

Chin, E., Felt, A.P., Greenwood, K., Wagner, D., (2011). *Analyzing Inter-Application Communication in Android*, Berkeley: University of California. Print

Christophe Champod, C., Lennard, C., Margot,P ., Stoilovic, M. (2016). *Fingerprints and Other Ridge Skin Impressions*. Florida: CRC Press. Print

Crain, C. (2013). Living in a Society of Control. Retrieved from http://www.mantlethought.org/philosophy/living-society-control

Culzac, N. (2014). Egypt's police 'using social media and apps like Grindr to trap gay people. Retrieved from www.independent.co.uk/news/world/africa/egypts-police-using-social-media-and-apps-like-grindr-to-trap-gay-people-9738515.html.

Deleuze, G. (1992). Postscript on the Societies of Control. Retrieved from https://cidadeinseguranca.files.wordpress.com/2012/02/deleuze_control.pdf

Deleuze, G. (1995). Two Regimes of Madness, Revised Edition, Texts and Interviews. Retrieved from https://www.scribd.com/doc/147698164/Gilles-Deleuze-Two-Regimes-of-Madness-1975-1995

Devlin, H. (2017). AI programs exhibit racial and gender biases, research reveals. Retrieved from https://www.theguardian.com/technology/2017/apr/13/ai-programs-exhibit-racist-and-sexist-biases-research-reveals

Dick, B. (2000) A beginner's guide to action research. Retrieved from http://www.uq.net.au/action_research/arp/guide.html

Dillan, J. (2017). 1984 Was a Warning, Not an Instruction Manual. Retrieved from http://www.mauldineconomics.com/the-10th-man/1984-was-a-warning-not-an-instruction-manual#

Dimock, M, et al. (2013). *Majority Views NSA Phone Tracking as Acceptable Anti-Terror Tactic.* Pew Research Center. Print.

Enck, W., Octeau, D., McDaniel, P., & Chaudhuri, S., (2011). *A Study of Android Application Security*. United States: The Pennsylvania State University. Print

Enck, W. (2011). *Defending Users against Smartphone Apps: Techniques and Future Directions.* United States: North Carolina State University. Print

Epstein, R. (2013). Google's Gotcha. Retrieved from https://www.usnews.com/opinion/articles/2013/05/10/15-ways-google-monitors-you

Esbjörn-Hargens, S. (2009). An overview of Integral Theory. Retrieved from http://www.cybertech-engineering.ch/research/references/Esbjorn_2009/Integral%20Theory_AQAL%20By%20K.%20Wilber%203-2-2009.pdf

Felt, A., Egelman, S., & Wagner, D. (2012). *I've got 99 problems, but vibration ain't one: A survey of smartphone users' concerns*. Berkeley: University of California. Print

Felt, A., Ha, E., Egelman, S., Haney, A., Chin, E., & Wagner, D. (2012). *Android Permissions: User Attention, Comprehension & Behaviour.* Berkeley: University of California. Print

Felt, A.P., Wang, H., Moshchuk, A., Hanna, S., & Chin E. (2011) *Permission Re-Delegation: Attacks and Defenses*. Berkeley: University of California. Print

Felton, J. (2018). Fitness App Releases Data, Accidentally Reveals Top-Secret Military Information. Retrieved from http://www.iflscience.com/technology/fitness-app-releases-data-accidentally-reveals-topsecret-military-information/

Festinger, L. (1957) *A theory of cognitive dissonance*. CA: Stanford University Press. Print

Filippetti, J. (2011). Seiko Mikami: desire of codes installation. Retrived from https://www.designboom.com/art/seiko-mikami-desire-of-codes-installation/

Foucault, M. (1979). *Discipline and Punish: The Birth of the Prison.* NY: Vintage Books. Print pp. 200–201, 205, 207, 215–216, 218, 211

Fox, S. (2013) “Tracking for Health”, Pew Research Center’s Internet & American Life Project, Washington DC. Print

Gabry, O. (2017). Software Engineering—Software Process and Software Process Models, Retrieved from https://medium.com/omarelgabrys-blog/software-engineering-software-process-and-software-process-
Models-part-2-4a9d06213fdc

Gargi, A. (2016) Delhi banker seeks `right to be forgotten' online. Retrieved from https://timesofindia.indiatimes.com/india/Delhi-banker-seeks-right-to-be-forgotten-online/articleshow/52060003.cms

Germanos, A. (2014). Al Gore: Snowden Revealed Crimes 'Way More Serious' Than Any He Committed. Retrieved from https://www.commondreams.org/news/2014/06/10/al-gore-snowden-revealed-crimes-way-more-serious-any-he-committed

Gianotti, H. (2015). Michel Foucault's Panopticon. Retrieved from https://tbaw.ca/2015/09/21/michel-foucaults-panopticon/

Godin, D., & Zahedi, M. (2014). Aspects of Research through Design: A Literature Review. Retrieved from http://www.drs2014.org/media/648109/0205-file1.pdf

Greenwald, G. (2013). On Whistleblowers and Government Threats of Investigation. Retrieved from https://www.commondreams.org/views/2013/06/07/whistleblowers-and-government-threats-investigation

Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily. Retrieved from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Grobart, S. (2011). The Facebook Scare That Wasn't. Retrieved from http://gadgetwise.blogs.nytimes.com/2011/08/10/thefacebook-scare-that-wasnt/

Hampton-Smith, S. (2017). The designer's guide to Gestalt Theory. Retrieved from https://www.creativebloq.com/graphic-design/gestalt-theory-10134960

Hill, J. (2017). Hansel & Gretel & Herzog & de Meuron & Ai Weiwei. Retrieved from https://www.world-architects.com/ca/architecture-news/headlines/hansel-and-gretel-and-herzog-and-de-meuron-and-ai-weiwei

Hvistendahl, M. (2017). Inside china's vast new experiment in social ranking. Retrieved from https://www.wired.com/story/age-of-social-credit/

Heath, B. (2014) Racial gap in U.S. arrest rates: 'Staggering disparity'. Retrieved from https://www.usatoday.com/story/news/nation/2014/11/18/ferguson-black-arrest-rates/19043207/

Hornyack, P., Wetherall, D., Han, S., Jung, J., & Schecter, S. (2011). These Aren't the Droids You're Looking For" Retrofitting Android to Protect Data from Imperious Applications. Washington DC: University of Washington. Print.

Houseton, W. (2013). Foiled plots and bathtub falls. Retrived from https://www.economist.com/blogs/democracyinamerica/2013/06/cost-benefit-analysis-and-state-secrecy

Hoyt, J. (1896). The Cyclopedia of Practical Quotations. New York: Funk & Wagnalls company. Print.

Hunt, E. (2015). Amazon Kindle's terms 'unreasonable' and would take nine hours to read, Choice says. Retrieved from https://www.theguardian.com/australia-news/2017/mar/15/amazon-kindles-terms-unreasonable-and-would-take-nine-hours-to-read-choice-says

IBO. (2009). Basij shots to a young woman in Tehran's Saturday June 20th protests. Retrieved from https://www.youtube.com/watch?v=185vPe_gROA

ISCI (2017). Lumen Features. Retrieved from https://haystack.mobi/

Jaivin, L (2014). The end of secrets. Retrieved from https://www.themonthly.com.au/issue/2014/june/1401544800/linda-jaivin/end-secrets

King, J., Lampinen, A., Smolen A., (2011). *Privacy: Is There An App For That?* Berkeley: University of California. Print

Komando, K. (2016). Facebook is watching and tracking you more than you probably realize. Retrieved from https://www.usatoday.com/story/tech/columnist/komando/2016/03/18/facebook-watching-and-tracking-you-more-than-you-realize/81803796/

LaMorte. E. (2016). Principles of Graphical Excellence from E.R. Tufte. Retrieved from http://sphweb.bumc.bu.edu/otlt/MPH-Modules/BS/DataPresentation/DataPresentation3.html

Tufte. E. (1984). Visual Display of Quantitative Information. CT: Graphic Press. Print

Lee, T. (2013). Singapore an advanced surveillance state, but citizens don't mind. Retrieved from https://www.techinasia.com/singapore-advanced-surveillance-state-citizens-mind

Lim, J. (2016). South Korea Releases Right to Be Forgotten Guidance. Retrieved from https://www.bna.com/south-korea-releases-n57982070847/

Lomas, N., & Dillet, R. (2015). Terms And Conditions Are The Biggest Lie Of Our Industry. Retrieved from https://techcrunch.com/2015/08/21/agree-to-disagree/

Lyon, D. (2003). *Surveillance as Social Sorting Privacy, risk, and digital discrimination.* Canada: Routledge. Print.

Madden, M., & Raine, L. (2015). Americans' Attitudes About Privacy, Security and Surveillance. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Maheshwari, S. (2017). That Game on Your Phone May Be Tracking What You're Watching on TV. Retrieved from https://www.nytimes.com/2017/12/28/business/media/alphonso-app-tracking.html

Mare, A. (2016). A qualitative analysis of how Investigative Journalists, Civic Activists, Lawyers And Academics are adapting to and resisting communications surveillance in South Africa. Retrieved from https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/duncan_2_comm_surveillance.pdf

McCandless, D. (2018) World's Biggest Data Breaches. Retrieved from http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

McMullan, T. (2015). What does the Panopticon mean in the age of digital surveillance? Retrieved from www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham

Ming, C. (2017) FICO with Chinese characteristics: Nice rewards, but punishing penalties. Retrieved from https://www.cnbc.com/2017/03/16/china-social-credit-system-ant-financials-sesame-credit-and-others-give-scores-that-go-beyond-fico.html

Montjoye, Y., Hidalgo, C., Verleysen, M., & Blondel, V. (2013). Unique in the Crowd: The privacy bounds of human mobility. Retrieved from https://www.nature.com/articles/srep01376

Moscaritolo, A. (2009). Iran election protesters use Twitter to recruit hackers. Retrieved from https://www.webcitation.org/5ic0PcGvi?url=http://www.scmagazineus.com/Iranian-election-protestors-use-Twitter-to-recruit-hackers/article/138545/

NCI. (2018). Definition of prospective cohort study - NCI Dictionary of Cancer Terms. Retrieved from https://www.cancer.gov/publications/dictionaries/cancer-terms/def/prospective-cohort-study

Office of the Privacy Commissioner of Canada. (2016). Survey of Canadians on Privacy Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/

Orwell, G. (1949). *1984*. New York: Harcourt. Print

Pak, J. (2018). Inside China's "social credit" system, which blacklists citizens. Retrieved from https://www.marketplace.org/2018/02/13/world/social-credit-score-china-blacklisted

Palmer, J. (2013). Mobile location data 'present anonymity risk'. Retrieved from http://www.bbc.com/news/science-environment-21923360

Panopticon. 2018. In Merriam-Webster.com. Retrieved from https://www.merriam-webster.com/dictionary/panopticon

Payton, M. (2016). Egyptian police 'are using Grindr to find and arrest LGBT people'. Retrieved from www.independent.co.uk/news/world/africa/egyptian-police-grindr-dating-app-arrest-lgbt-gay-anti-gay-lesbian-homophobia-a7211881.html.

Peguera, M. (2017). Right to be forgotten and global delisting: some news from Spain. Retrieved from http://cyberlaw.stanford.edu/blog/2017/12/right-be-forgotten-and-global-delisting-some-news-spain

Porter, H. (2014) No Place to Hide review – Glenn Greenwald's compelling account of NSA/GCHQ surveillance. Retrieved from https://www.theguardian.com/books/2014/may/19/no-place-to-hide-review-glenn-greenwald-nsa-gchq-surveillance-edward-snowden-spying

Raphael, JR. (2008). Cell Phone Spying: Is Your Life Being Monitored? Retrieved from https://www.geeksaresexy.net/2008/05/05/cell-phone-spying-is-your-life-being-monitored/

Razaghpanah et al. (2016). Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem. Retrieved from https://www.ftc.gov/system/files/documents/public_comments/2016/10/00038-129143.pdf

Retaildesignblog. (2011) Adris Pavilion at WMF by Brigada, Rovinj – Croatia. Retrieved from http://retaildesignblog.net/2013/11/30/adris-pavilion-at-wmf-by-brigada-rovinj-croatia/

Reveley, W. (1971). The works of Jeremy Bentham vol. IV. Retrieved from https://en.wikipedia.org/wiki/Panopticon#/media/File:Panopticon.jpg

Sample, I. (2017). AI watchdog needed to regulate automated decision-making, say experts. Retrived from https://www.theguardian.com/technology/2017/jan/27/ai-artificial-intelligence-watchdog-needed-to-prevent-discriminatory-automated-decisions

Sagor, R (2000). Guiding School Improvement with Action Research. Virginia: Association for Supervision and Curriculum Development. Print

Schneider, T. (tobiaschneider) (2018, January 27). Somebody forgot to turn off their Fitbit. Markers trace known military outposts, supply and patrol routes. [Twitter Moment]. Retrieved from https://twitter.com/tobiaschneider/status/957319340394799104/photo/1

Schneier, B. (2014). NSA robots are 'collecting' your data, too, and they're getting away with it. Retrieved from https://www.schneier.com/blog/archives/2014/03/surveillance_by.html

Schneier, B. (2014). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. USA: WW Norton. Print.

Schneier, B. (2008). *Schneier on Security*. USA: Wiley. Print.

Shields, T. (2011). Mobile Apps Invading Your Privacy. Retrieved from https://www.veracode.com/blog/2011/04/mobile-apps-invading-your-privacy

Shahani, A. (2014). Smartphones Are Used To Stalk, Control Domestic Abuse Victims. Retrieved from https://www.npr.org/sections/alltechconsidered/2014/09/15/346149979/smartphones-are-used-to-stalk-control-domestic-abuse-victims

Sheridan, C. (2016) *Foucault, Power and the Modern Panopticon.* Connecticut: Trinity College. Print

Simon, B (2002). *The Return of Panopticism: Supervision, Subjection and the new Surveillance.* Canada: Concordia University. Print.

Statista. (2018). Number of smartphone users in Canada from 2013 to 2022 (in millions)* Retrieved from https://www.statista.com/statistics/467190/forecast-of-smartphone-users-in-canada/

Statista. (2018). Number of apps available in leading app stores as of March 2017. Retrieved from https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Strava Labs. (2018). Global Heatmap. Retrieved from https://labs.strava.com/heatmap/#2.46/-79.63379/46.41187/hot/run

Sundaresan, S., Valinna-Rodriguez, N. (2017). 7 in 10 Smartphone Apps Share Your Data With Third-Party Services. Retrived from http://observer.com/2017/06/7-in-10-smartphone-apps-share-your-data-with-third-party-services-mining-security/

Sunyaev, A., Dehling, T., Taylor, P., & Mandi, K. (2015). Availability and quality of mobile health app privacy policies. Retrieved from https://doi.org/10.1136/amiajnl-2013-002605

Toombs, C. (2013). [New App] XPrivacy Gives You Massive Control Over What Your Installed Apps Are Allowed To Do. Retrived from https://www.androidpolice.com/2013/06/23/xprivacy-gives-you-massive-control-over-what-your-installed-apps-are-allowed-to-do/

Viégas, F. & Wattenberg, M. (2007). Artistic Data Visualization: Beyond Visual Analytics. Retrieved from https://www.ninalp.com/ART/Papers/artistic-infovis.pdf

Wilber, K. (2005). Introduction to the Intergral Approach. Retrieved from http://www.kenwilber.com/Writings/PDF/IntroductiontotheIntegralApproach_GENERAL_2005_NN.pdf

Wilber, K. (2010). AQAL Glossary. Retrieved from http://aqaljournal.integralinstitute.org/public/Pdf/AQAL_Glossary_01-27-07.pdf

Woods, B. (2014). Google is now removing search results following EU ‘right to be forgotten’ ruling. Retrieved from https://thenextweb.com/google/2014/06/26/google-now-removing-search-results-following-eu-right-forgotten-ruling/

Zetter, K. (2014) Glenn Greenwald's Pulse-pounding Tale Of Breaking The Snowden Leaks. Retrieved from https://www.wired.com/2014/05/greenwald-no-place-to-hide/

Zhou, Y., Zhang, X., Jiang, X., & Freeh, V. (2011). Taming Information-Stealing Smartphone Applications (on Android). North Carolina: North Carolina State University. Print.

Zimmerman, J., Stolterman, E., & Forlizzi, J. (2010). An Analysis and Critique of Research Through Design. Retrieved from http://research.cs.vt.edu/ns/cs5724papers/zimmerman-dis10.pdf

Zsolt, U. (2014). Software development processes and software quality assurance. Retrieved from http://www.tankonyvtar.hu/en/tartalom/tamop412A/2011-0042_szoftverfejlesztesi_folyamatok_angol/ch02.html#Az_2_1_Spiral_model_of_requirements_and_design_

Appendix A: REB materials

Research ethics application approval

Student Email by Google

Mudit Ganguly [redacted]

Application approved

[redacted] Thu, Nov 23, 2017 at 5:21 PM

To: "Mr. Mudit Ganguly (Graduate Researcher)" [redacted] "Prof. Isabel Meirelles (Principal Investigator)" [redacted]

November 23, 2017

Prof. Isabel Meirelles
Faculty of Design
OCAD University

File No: 101 118
Approval Date: November 23, 2017
Expiry Date: November 22, 2018

Dear Prof. Isabel Meirelles,

The Research Ethics Board has reviewed your application titled 'Phonopticon'. Your application has been approved. You may begin the proposed research. This REB approval, dated November 23, 2017, is valid for one year less a day: November 22, 2018. Your REB number is: 2017-54.

Throughout the duration of this REB approval, all requests for modifications, renewals and serious adverse event reports are submitted via the Research Portal.

Any changes to the research that deviate from the approved application must be reported to the REB using the amendment form available on the Research Portal. REB approval must be issued before the changes can be implemented.

To continue your proposed research beyond November 22, 2018, you must submit a Renewal Form before November 15, 2018. REB approval must be issued before research is continued.

If your research ends on or before November 22, 2018, please submit a Final Report Form to close out REB approval monitoring efforts.

If you have any questions about the REB review & approval process, please contact the Christine Crisol Pineda, Manager, REB secretariat at [redacted].

If you encounter any issues when working in the Research Portal, please contact our system administrator via research@ocadu.ca .

Sincerely,

Nancy Snow
Acting Chair, Research Ethics Board

Table 1: Member 1 Data Readout

Application Name	Bytes Sent
Fido	10880553
Timeplay	4039094
Futurism	3614185
Chrome	2794416
Slack	802447
Shazam	654725
Google Maps	591747
Google Backup	205705
Google news	188318
Twitter	138742

Note: Data readouts taken for Member 1, for the top ten applications that were uploading the most data.

Link to NetworkStatsManager repository: https://github.com/RobertZagorski/NetworkStats

Table 2: Member 2 Data Readout

Application Name	Bytes Sent
Podcast Addict	1154572340
Netflix	132780873
Snapchat	49374522
360 background	39178202
Gem Quest	35509087
Uber Eats	14952945
Gmail	12796843
Bubble Shooter 2	9927033
Messenger	7125143
Facebook	6953447

Note: Data readouts taken for Member 2, for the top ten applications that were uploading the most data.

Link to NetworkStatsManager repository: https://github.com/RobertZagorski/NetworkStats

Table 3: Member 5 Data Readout

Application Name	Bytes Sent
Hearthstone	1567279547
Buried Bornes	43572515
Quizlet	39839337
Steam	26554894
Waze	10511292
Talon	6742568
Reddit	6500436
Google Play Store	4001878
Lift	2492926
Goodreads	2168501

Note: Data readouts taken for Member 5, for the top ten applications that were uploading the most data.

Link to NetworkStatsManager repository: https://github.com/RobertZagorski/NetworkStats

Table 4: Member 6 Data Readout

Application Name	Bytes Sent
HQ	84360836
Facebook	61180221
Tap tap	28175221
Twitter	11096209
Pinterest	10173784
Spotify	8316361
Instragram	5602177
Slack	4425473
Chrome	4019144
Messenger	2469300

Note: Data readouts taken for Member 6, for the top ten applications that were uploading the most data.

Link to NetworkStatsManager repository: https://github.com/RobertZagorski/NetworkStats

Questionnaire 1

In this survey we'd like to explore your views about some important issues regarding Surveillance, Privacy and the Applications on your mobile phones.

Q1.) Which of these statements more accurately describes you:

a) I am generally a private person and like to keep to myself

b) I am generally an open person who enjoys sharing with others

Q3.) How many applications do you have on your phone right now?

a) up to 20

b) 21 - 40

c) 41 – 60

d) more than 60

Q4.) In the course of one day, approximately how many applications do you actively use?

a) up to 5

b) 6 to 10

c) 11 to 15

d) more than 15

Q5.) You might use your mobile phone through the day. You might use it to look for transport, to buy products online, check in on social media, use maps to find your way around or use search engines. How much control do you feel you have over how much information is collected about you and how it is being used?

a) A lot of control
b) Some control
c) Not much control
d) No control at all

Q6.) Are you aware of the amount of data used and transmitted by the applications on your phone?

a) Yes
b) No

Q7.) Do you trust the applications you have on your phone?

a) Yes
b) No

Q8.) If your answer to the previous question was No, why do you continue to use those applications?

If the answer was Yes, please answer n/a

a) _____

_____

_____

Q9.) How safe do you think your mobile phone is from third parties that want access to your data?

a) Extremely safe

b) Safe

c) Unsafe

d) Extremely Unsafe

e) Don’t know

Q10.) How would you rate your knowledge of your privacy rights?

a) Very Good

b) Good

c) Neither Good nor Bad

d) Poor

e) Very Poor

Q11.) How would you rate your knowledge of the surveillance systems that target your mobile phone?

a) Very Good

b) Good

c) Neither Good nor Bad

d) Poor

e) Very Poor

Q12.) In general, how concerned are you about the protection of your privacy?

a) Extremely Concerned

b) Concerned

c) Somewhat

d) Not concerned

Q13.) Have you ever adjusted settings to limit personal information shared via applications?

a) Yes

b) No

Q14.) Do you read the privacy policy for apps before you install them?

a) Yes

b) No

Q15.) If the answer to the previous question was ‘Yes’, has reading the policies affected your decision to use the application?

a) Yes

b) No

c) Somewhat

Q16.) Have you felt confused by the information provided in a privacy policy?

a) Yes

b) No

Q17.) Have you changed your mobile phone use in recent months in any way to avoid having your data activities traced or noticed?

a) Yes

b) No

Q18.) If your answer to the previous question was Yes, do you feel as though you already do enough to protect the privacy of your personal information online. If the answer was No, please pick n/a

a) Yes

b) No

c) n/a

Q19.) How concerned are you with the collection and use of information from your phone like calendars, GPS location, and camera data?

a) Extremely Concerned

b) Concerned

c) Somewhat

d) Not concerned

Q20.) Are you aware of the National Security Agency document leaks carried out by Edward Snowden in 2013?

a) Yes

b) No

Q21.) Have you carried out your own research into how you can protect yourself from surveillance?

a) Yes

b) No

Q22.) Do you think you would benefit from having more information about how applications are giving away your data?

a) Yes

b) No

Q23.) If your answer to the previous question was No, why do you think so?

If the answer was Yes, what kind of information would you like to receive?

a) _____

_____

_____

Thank you for your participation.

Focus Group Questions 1

a) Please think about smart-phones. What comes to mind?

b) What are your favorite applications on your mobile phones?

c) Do you normally read the agreement text before using apps?

d) Have you ever refused to provide an application with permission to access your data?

e) What does privacy mean to to you?

f) So, what do you consider a breach of privacy?

g) Are you comfortable with third parties (people or companies who make applications) having access to your phone or the data generated by your phone?

h) Are you comfortable with third parties (governments) having access to your phone or the data generated by your phone?

i) What do you think are the pros and cons of surveillance?

j) What do you do to protect yourself from surveillance?

k) What do you think is the solution to mass surveillance?

l)

Let's go around the room and discuss any final thoughts or points any of you may have.

Thank you for your participation.

User Testing Questions: 1

a) According to the data we've collected the applications on your mobile phones that transmit the most data are (insert application names here). How does that make you feel?

b) Is there a reason why you think those applications are uploading that much data?

c) (insert application name here) is known to have given up user data to third parties in the past. (insert details of this event here) How does that make you feel?

d) Does this new information change your opinion of the application?

e) There are many ways to prevent this from happening (insert preventive methods here) Would you practise these methods?

f) Now that you've been educated and informed about these events, would you make any changes to the way you use these applications?

Prototype Questions:

a) Does this prototype make you feel a certain way? Pick any of the following emotions that you feel.

Terrified

Fearful

Panicky

Shocked

Apprehensive

Threatened

Insecure

Uneasy

Cautious

Nervous

Worried

Anxious

Pleased

Glad

Satisfied

Cheerful

Thrilled

Excited

Elated

What exactly makes you feel that way?

b) How do you feel about seeing your face/body/data on the screens?

c) There are certain visual effects that have been applied to the screens (eg. Change in color, size, distortion), how does that make you feel?

d) What do you think about the placement of the cameras and the screen in relation to you?

e) The last screen shows how well you fare in comparison to others, how does that make you feel?

f) What changes would you make to the prototype? Why would you make these changes?

Thank you for your participation.

Appendix B: Prototype Influences

This appendix serves as the horizon scan for the Phonopticon. It includes works that I have come across that influenced the development of the various aspects of the Phonopticon.

Adris Pavilion at WMF by Brigada, Rovinj – Croatia

Figure 47. The Pavillion (Retaildesignblog 2013).

Brigada developed the concept for Adris Group's exhibition which involved visualising the annual reports of the Adris Group from the past ten years. For the exhibition, Brigada installed ten cylinders, each a "mini pavilion" presenting one annual report (Figure 44). When visitors entered each of these cylinders they created their own private space in which they could isolate themselves from the outside and view the exhibition material in peace. The enclosed spaces designed by Brigada influenced the physical design of the Phonopticon walls. It was a perfect example of private spaces in public places. The enclosed structure allows for introspection, isolation and contemplation. By entering the pavilliion, visitors are offered a private space where they get away from "external noise" and view the visuals in isolation.

Textile de cordes - Nathalie Bujold

Figure 48. Screenshots of Textile de cordes (Bujold, 2015).

This artistic video by Nathalie Bujold served as an inspiration for the visuals of the webcams. The video starts with a lone cellist playing the cello. However, her image is multiplied in a grid; and the image is eventually multiplied 67108864 times. Every 10 seconds the number of images in the grid reduces by half while the size of each image doubles in dimensions until all we're left with is one singular image of the cellist, Isabelle Bozzini (Figure 45)+.

Appendix C: Phonopticon Narration Script

The following text is the script of the narration that plays alongside the visuals inside the Phonopticon

Welcome to the Phonopticon

An intervention that visualizes the surveillance carried out by mobile applications. You must answer 6 questions after which the Phonopticon will visualize the surveillance carried out by the various applications on your smartphones.

Press Okay when you are ready

Question 1

Do you have the instagram application on your mobile device? Press Yes or No on your mobile device to answer the question.

When users upload images to Instagram, they give Instagram rights to sell those images to advertisers You probably don't care if they sell that photo of your lunch, but you may care if they sell photos of your face. Images on instagram also include metadata about the location and time they were taken allowing third parties to track your movements.Instagram can legally sell your data to third parties without your knowledge

Question 2

Do you have the Uber application on your mobile device? Press Yes or No on your mobile device to answer the question.

In 2012, Uber identified users who used uber to have one night stands. It monitored users who took an Uber between Friday or Saturday night. Then it looked at when these users returned home early next morning. They published this data online calling it the ‘Uber Rides of Glory’ .They found out which neighbourhoods in north american cities were having the most one night stands. if you thought Uber would never use that data you’d be wrong. In China, Uber used tracking to find drivers that were attending taxi protests and threatened to terminate them as drivers.

Question 3

Do you have free game applications on your mobile device? Press Yes or No on your mobile device to answer the question.

Gaming apps like “Honey Quest” and “Beer pong trickshot” monitor the viewing habits of their users even when the games aren’t being played. These apps use Alphonso, a software that uses a phones microphone to analyze background audio. The software can identify what users watch by identifying TV ads and shows, sometimes even identifying the places users visit and the movies they see. This information is used to target ads more precisely and works even if a phone is in a pocket or if the apps are running in the background.

Question 4

Do you have fitness tracking applications on your mobile device? Press Yes or No on your mobile device to answer the question.”

Fitness tracking applications Like Strava use a phone's GPS to track a user's exercise activity. In 2017 Strava released a map that shows the activity of its users. However the map revealed locations of soldiers who use Strava when they exercise and also revealed military bases across the world. In locations like Afghanistan and Syria, the users of Strava seem to be almost exclusively foreign military personnel. Twitter users have identified locations including a suspected military base in Iraq and a secret spy station in Australia.

Question 5

Do you read the Terms and Conditions of an application before you download it? Press Yes or No on your mobile device to answer the question.”

Terms and conditions have hidden clauses that users blindly agree to. When you use Dropbox you give Dropbox employees permission to access your data whenever they feel they have a legitimate reason to

do so. These permissions extend to third-parties as well: So you grant access to unknown third parties to store and scan your data. Netflix can do so as well and cannot be held liable if it gets hacked and your personal info is stolen. Because when you click I agree you agree that you will not sue them in court. So if Netflix were to tweet about your data, it would be legal

Question 6

"Do you have the Facebook application on your mobile device?

Press Yes or No on your mobile device to answer the question."

Cambridge Analytica, a voter profiling company with a link to Donald Trump's campaign, collected private information from 50 million Facebook users without their permission. The information was gathered via an app that asked for consent before accessing user data, the information was being used for a purpose that wasn't transparently disclosed to the users. They had been told it was for "academic purposes," but the Facebook data was sold to Cambridge Analytica, a foreign company funded by right-wing billionaire and Trump donor Robert Mercer, and then used to create psychographics or demographics that help in targeting voters. People expect that Facebook will use their data to create ads, but not to help a political candidate win. Fiesler says what Cambridge Analytica did was an "expectation violation." People are willing to allow access to their Facebook data "so they can take a quiz and find out what *Game of Thrones* character they are," knowing the company behind the quiz is mining their data and that of their Facebook friends for advertising purposes. But in the case of Cambridge Analytica, which got its information second-hand from an app created by Kogan, who in turn got access with Facebook's permission, there was a sense of safety.

Thank you for your answers, your visualization will load soon. Your personal visualization is ready, press Initialize to begin.

What you're seeing right now are multiple live feeds of you. In a few moments some of these videos might be amplified based on your answers. They reflect how closely these mobile applications are looking at you through your data. The larger the image, the more data they have about you. Each feed representing how these applications monitor us. The first one represents how strava tracks your location and is pointed at your feet, the second one represents how Terms and conditions cover every application, so the feeds show you the entire Phonopticon, the next feed represents how Uber watches our every move and is connected to our bank accounts, so the camera is pointed at your purses or pockets. The next feed represents how Facebook watches over everything and so the camera is on top. The next feed represents how Instagram watches us and the camera is pointed at your face. And the last feed represents how games we play spy on us and so the camera is pointed at your fingers.

I encourage you to stay here for a while and look around as the visualization changes to represent our current surveillance state. When you're ready to move on, press 'Ways to protect myself' to find out how to shield yourself from such surveillance.

What happens if Google gets hacked tomorrow? There is nothing you or I could do about our data then, but there might be something we can do about our data now. These are suggestions that can help you take control of your data. If you would like to more press 'More Info' or if you'd like to exit the installation press "End". Thank you for your time. And good luck

We are living in an environment where the applications on our mobile phones are observing, listening and gathering data about us without our knowledge. The applications offer us utility, but they take user data in return. That difference between what an application does and what it claims to do leads to unrealistic expectations regarding privacy. The Phonopticon aims to bridge that gap. Now that it has told you what applications have the potential to do with your data it's time to tell you how to protect yourself. Click "Next" on your mobile device to move onto the next section

PHONOPTICON: THE AGE OF MOBILE SURVEILLANCE.

This installation is called the Phonopticon because it is based on Michel Foucault's Panopticon. The panopticon is a circular prison. It has prisoners on the outer edge and in the center is a guard tower. It is built in such a way that the guards can watch any prisoner at any time, but the prisoners don't know when they're being watched. In the same way our phones right now might be under surveillance and we might have no idea. Even the word ‘pan-opticon’ means something that watches over everything. Compare that to Google. Each of us has a tiny panopticon in our pockets and it’s way more powerful than we imagine.

The solution to mass surveillance is not to stop using our smartphones or to stop using applications. The solution is to have laws that protect the privacy of users. In the European union they have the ‘Right to be forgotten’ which gives users the power to remove their personal data from internet databases when there is no justification for its collection. Users can go to Facebook and say “delete the data you have about me” and facebook has to comply. Or atleast justify why it needs that data. Users can only ask for laws like this if they know how dire the situation is, If you’re not aware how apps are sucking up your data you’re not going to be pissed off. That’s what the Phonopticon does, it informs, educates and empowers.

Thank you for your time, you may now leave the installation, but you may never be able to leave the Phonopticon.