MICROCHIP IMPLANT IN HUMANS

– RISKS FOR INDIVIDUAL & SOCIETY

Bachelor's thesis in Informatics

Emil Andersson
Axel Bengtsson

Spring 2019KANI42

Title: Microchip implant in humans – risks for the individual & society

Year: 2019

Authors: Emil Andersson & Axel Bengtsson

Supervisors: Stefan Cronholm

Abstract

The purpose of this study was to investigate what opinions people have regarding microchip implant in humans. The report is limited and focused on the risks concerning the microchip implant. To answer the purpose a research question was formulated*: "What is the opinion about microchip implants in humans for 18-30-year-old people in Borås, when it comes to risks in their daily life and the society?"*. This study is constructed through two studies, a qualitative and a quantitative. The first step in the study was qualitative interviews with six different individuals. These interviews were the basis for the upcoming step, which was the quantitative survey. The quantitative survey was a questionnaire where 100 people were asked. The result showed that the people were not knowledgeable about microchip implants in humans and had a lot of different opinions about the technology. Some saw the risks as a big threat and others saw them as a less of a threat. In the end, the results showed that most of the participants were against microchip implants in humans and would not get chipped. The conclusion showed that the people between ages 18-30, in general, had the same opinions regarding risks that scientific articles and theories mention.

Sammanfattning

Syftet med denna kandidatuppsats var att undersöka vilka åsikter människor har gällande microchip-implantat i kroppen. Rapporten är begränsad och har fokus på riskerna rörande mikrochip-implantat. För att svara på syftet formades frågan *"Vilken åsikt har människor i Borås, i åldrarna 18–30 år gällande mikrochip-implantat när det kommer till risker i det dagliga livet och samhället?"*. Denna rapport är gjord genom två studier, en kvalitativ och en kvantitativ forskningsmetod. Första steget i uppsatsen var en kvalitativ intervju med sex personer. Dessa intervjuer var grunden till nästkommande steg i uppsatsen, vilket var den kvantitativa undersökningen. Den kvantitativa undersökningen var en enkätundersökning där 100 personer var tillfrågade att medverka. Resultatet visade att respondenterna inte hade kunskap om mikrochip-implantat i kroppen. Resultatet framför även ett flertal olika åsikter kring teknologin. Somliga såg riskerna som ett stort hot medan andra såg riskerna som ett mindre hot. Slutligen visade resultatet att de flesta deltagarna var emot mikrochip-implantat och ville inte bli flisade. Sammanfattningsvis visar studien att vetenskapliga artiklar och människor mellan 18–30 år generellt har likande åsikter gällande riskerna kring mikrochip-implantat i kroppen.

Keywords: Microchip, Implant, RFID, Biohacking, Chip, Risks

Acknowledgements
First of all, we want to give a special thanks to our supervisor Stefan Cronholm for the help and guidance through this research by providing valuable opinions and guidelines. Also, a big thank you to all the people who participated and helped us. Without you, our study would not be possible and we are happy that by all your help we came up with a result that completed our study.

All the best, thank you!

Emil & Axel
Borås, January 2019

Table of content

1 Introduction

People want to live an easy life where every day is smooth and simple. Today, it is getting more and more common that people insert microchips into their own bodies just to make their daily life easier for them. Now, more than 5 000 Swedish people have a microchip inserted into their own body (Forskning 2019). Microchip is also called an integrated circuit. A microchip has four components: diodes, resistors, capacitors, and transistors. The four components are integrated and are all placed on a little disk called microchip (Nationalencyklopedin 2019).

The microchip for humans is called Radio-frequency identification (RFID). You place one RFID- chip under the skin which can contain a lot of information and be used for many different things. The RFID- chip has one unique code that connects to the system. RFID is a passive chip which means it gets power when it connects to the reader, otherwise the chip has no electronic power and therefore it cannot send signals. The passive chip makes it difficult to track the chip (Biohacking 2019). This technology can be used for different kinds of payments, like at SJ (The state's railways), as keys and can probably develop in the future to prevent aging so that people can live longer. Biohacking, which is the name for modifying your body is getting more common each day and more people are doing it (Forskning 2019). Biohacking comes from transhumanism which is a Philosophy that speaks and works for making our mental and physical characteristics better through (Forskning 2019).

According to "Wis. company To Offer Microchip Implants To Employees" there is an American company, who state that they are the first company in the United States, to be using this for easier access for their employees to open different doors and to easier log in to their computers through having something that they call a "chip party". This is available to all their employees if they so wished (Szal 2017). In Mexico, a hospital put a chip into over 1 000 patients with information about blood type, allergies and to look at earlier treatments which helped the nurses in their work with the patients (White 2005).

The microchip comes with a lot of advantages but also some disadvantages. The microchip is, in its current state, passive which means that it needs to be active to use for more purposes. An activate microchip is more sensitive and with an active chip, there are some risks. Especially when a new technology is invented and many other devices get established. The world has constantly been tested in history for risks and more risks will appear in the future. The big question is if the people are ready for the new evolution and for the risks that come with it? By following the questionnaire of this study, the purpose is to see what the opinion for the ages between 18-30 years old is about the risks regarding biohacking into humans and to later do a research about it.

1.1 Background

Historically humans have taken the technology-evolution to new levels. Integrated circuit has been and is placed in almost all electronical devices and after electronical devices, they started to put microchips into animals like cats and dogs (Sime 2016).

The development is moving forward and today an implant of microchips is possible on humans as well. The microchip is around one centimeter in size, meaning that you can easily have it under your skin without noticing it. The microchips are dedicated to simplifying life and is useful in a lot of different areas. In the current state it is limited to more accessible devices like id-cards, keycards and payment cards (Mårtensson 2018). Microchips are already inserted into

humans but are still a new technology to our society. The second step is to upgrade the chip and to make it more effective and powerful. There are many questions and debates regarding the updates and what the microchips consequences are on both the individual and society in the future.

1.2 Problem discussion

With the new technology, that microchips are implanted into humans, new and different issues can occur (Randall 2012). Problematic areas that will be mentioned in the report are costs, harmfulness on the human body, privacy, robbery, tracking and monitoring.

The technology of microchipping is moving forward, both the system and how the chip is used included. Today the passive chip is used more, but in the future the active chip can be used more since an active chip can have more data and a bigger range of usage. But an activated chip also means that it is easier to obtain sensitive data (Randall 2012).

One main problem is the risk of being hacked. While the chip is getting developed, hackers can develop their hacking skills to be able to steal the sensitive data stored in the microchips of their victims. By developing their own skills while, following the development of the chip, there might be a possibility of the hackers learning how to get their hands on the sensitive data in an easier way (Randall 2012). Another problem is the integrity alien. This can be a problem because of the future possibility of when users are using their microchip there might be a huge risk in having all data collected in the same place. This can lead to wrong people having the ability to reach all of your personal data instead of just parts of it (Gadzheva 2007). Tracking and monitoring are also huge problems and one of the most mentioned risks in theoretical framework. The RFID- chips information can easily be obtained and the user has no clue who monitors them (Rodriguez 2019). Tracking is another aspect that also can be obtained from different society actors which makes it an even more sensitive subject considering it is under the skin and has the possibility of surveillance at all times. To have a valuable device under the skin will increase the risk of getting hurt if a robbery occurs. If you wear a microchip and a thief decides to rob you, the thief needs to cut out the microchip from the inside of your hand. The incident may cause physical and mental harm. The chip does not need its personal owner to be used and that makes robbery a big risk, especially through violent methods of robbing you of your personal information through stealing the chip in your arm (Gadzheva 2007).

Other problems that can occur with the chip can for example be that it is harmful to the body when it stops working. Infections and other medical reactions are risks that can come while having or installing a microchip in the body. Irritation under the skin can be a problem because the chip may move around while irritating the skin and to get away and fix the problem, a professional surgery might be necessary. If it stops working a surgery will probably be necessary as well (Gadzheva 2007). These are some of the problems with microchip that can make users not feel safe having one. To solve this problem and make the usage of the microchip safer might make even more people to start using it. People can be hurt both physically and mentally which make people more doubtful to get the microchip. People want their life to be easy (Forskning 2019) but by always having these risks in their mind might make the chip feel more as a disadvantage than an advantage.

1.3 Purpose and Research Question

The purpose of this report is to:

- Investigate what people think about microchip implants
- If they are willing to use this technology even with the knowledge of the risks that come with it

Consequently, the research question are as follows:

- *What is the opinion about microchip implants in humans for 18-30-year-old people in Borås, when it comes to risks in their daily life and in society?*

1.4 Target group

Main focus are people who are interested in getting chipped and want to read more about possible risks. Everyone including companies and society actors can be interested in reading this because it gives more information about the new technology microchip implants in humans.

1.5 Limitations

This research focuses on the risks concerning microchip implants for humans, otherwise the investigation would be too large. The study is further limited to: The target group ages and the location where the study took place. Another aspect to mention is that this research is based on the participants opinions and knowledge and this is presented in the results.

2 Methodology

This research contains a qualitative and a quantitative analysis where the purpose was to see what people between the ages 18 to 30 years old hold as opinions and understandings about getting a microchip implemented into the human body. A triangulation method was used because it increases the reliability which gives a more trustful survey (Recker 2012).

To start this project, a semi-structured interview (Recker 2012) was done to collect a lot of important data that later on was the start for the study that is going to bring all the data that is needed and later on be analyzed to see what the opinion is of microchip implants for 18 to 30-year-old people. In this chapter, the whole process will be described from the very first interview and how the data has been collected through different studies.

2.1 Research design

This part starts with a description for the research design, thereafter, the specific methods will be explained in chapter 4 and 5, where respectively the studies are presented. Deduction and induction are two themes for research design. This study has inductive and deductive design included. Inductive design is when the researcher's specific observations by analyzing patterns and commonalities to, later on, connect and develop to theories study (Recker 2012). From the observed data theories can be created; in other words, the theories are based on the studies.

Inductive design is a qualitative strategy. One example of inductive design is a case study (Recker 2012).

Inductive design was applied at the beginning of this study through interviews. Answers from the interviews have later on received support from existing scientific articles that include facts and theories. Inductive research design is suitable for the study but is insufficient to draw conclusions that are completely sure and correct (Recker 2012). Deductive design is when the study is based on theories, therefore the researchers are trying to prove the concept from the theories and apply a new study. This design is a quantitative strategy and must be performed with caution because still, the conclusion could be incorrect (Recker 2012). Deductive design was applied for this study and the study is based on the first study and scientific articles that have facts and theories. Deductive design is important for the study to get relevant data that concerns the research question. Research does not always go in the same direction, validation and rationalization may differ depending on which method that is applied. To combine inductive and deductive designs give a higher quality text for the research and the conclusion gets more reliable. A combination of different research designs can set the theories against each other, then they can be carefully examined (Recker 2012).

In this research, a qualitative and quantitative methodology have been performed in two different steps. Qualitative was used at the first, to dig deeper into the topic and to get an understanding of what the interviewees think and what they have for opinions. Later on, was a quantitative method used to create the survey where data was collected through the survey that was based on the qualitative interviews. A combination of quantitative and qualitative strategies is called Mix methods (Recker 2012). Mixed method is used to find new and important points in the study that are reliable and relevant to the study (Cronholm, Hjalmarsson 2011). This method can be performed simultaneously or sequentially (Recker 2012). The meaning of doing both quantitative and qualitative study is to keep the strengths in the study and decrease the weaknesses by doing the study twice and use a mixed method (Cronholm, Hjalmarsson 2011). Cronholm and Hjalmarsson (2011) mentions that the two different researches become stronger if they are used together instead of just one at a time.

Case study is a research method you can use when you want to clarify a context situation “case”. The strategy is for a single case or a few more related cases. This method focuses on getting a deeper understanding and a detailed examination of one case (or a few related cases) you want to get more knowledge about (Colin, 2002). The qualitative strategy was performed as a case study, there the answers from the interviews gave qualitative data. From the qualitative data a study was created. The meaning of the qualitative study was to bring more understanding and knowledge about the interviewees opinions and also bring high-quality questions to the next survey. The next study characterizes as a quantitative strategy (Recker 2012).

The interviews and the survey research method are probably the best way to collect necessary data because then you know that the asked person's focus is at its best and that the answers will be honest and good to analyze. The method is also more suitable for this study than the cross-sectional study because it is during a short period (Colin, 2002).

Research strategies can be differentiated by dimensions, quantitative and qualitative research methods include different high degrees of different dimensions. The dimensions are divided into Controllability, Repeatability, Deductbility, Generalizability, Complexity and Explorability (Recker 2012). This research has combined all dimensions, providing a mixed method that contains various characteristics and benefits.

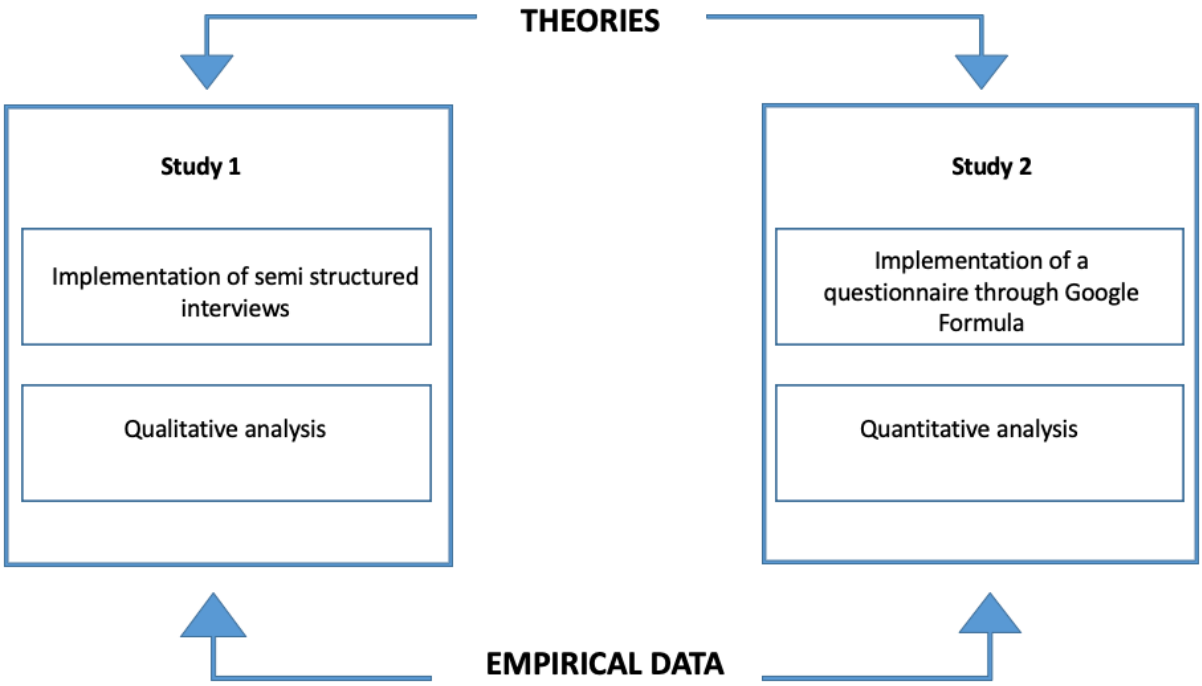


Figure 1. Model over the two studies, a mix method.

2.2 Respondents for both studies

To only ask the target group that was chosen carefully is because it creates a picture of what the first "real" generation thinks. The development of microchip implants will affect the people in this age the most and that is why the focus is on their opinions. The target group is people, both men and women between 18-30 years old in Borås. This target group is relevant because this group is going to be affected and the "first real" generation to use the microchip inside their body.

Some people have already started using microchips into their bodies but since it is not that common yet and not that many have started using it, this group is probably the first generation to use it and is in the process of getting more common in different environments, for example in stores as a payment method. Borås is a medium-large city and an accessible place for the study. It is big enough to get a good sample and the range of age fits the target group since it is a student city with a lot of people of different ages.

2.3 Ethical considerations

The answers can be affected depending on the participant's ethnicity and where they come from. This can be a problem when it comes to ethical considerations like religion and cultural aspects. All participants have their own opinion and because of different backgrounds and values in life, the answer can be different between all participants. All participants have a big impact on the final result. These aspects are important to consider and mention when the answers have been analyzed.

This research has followed the Swedish rules (SFS 2003:460) that say that all participants have to be informed of the study's purpose and if there are any risks. This is a measure that will minimize any confusion (Lunds Universitet 2019). The participants are anonymous in this study

which probably is the reason that so many people attended and took part in it. The questions were objective and to get the best result as possible the language was easily written to understand medical terms and other difficult words, just to minimize misunderstandings between the participants and the interviewers and the survey. It is important that all the participants had time to attend and answer considerately. A stressful environment and a stressful participant could affect the answers negatively.

3 Theories

Theories according to the topic are based on a literature review but also similar technology that can be likened to microchip implants.

3.1 Literature review

The main material comes from scientific articles with trustworthy sources that ensure the arguments in the work. To get relevant sources for the literature review keywords such as Microchip, Implant, RFID, Biohacking, Chip, Risks have been used during the research. Newsmagazines and websites were also used to look at relevant facts that describe the microchip and the impact it has on not only the individuals but also society as a whole. The sources are trustworthy and have a big range of knowledge. All sources are based on research from people who work with the subject in some way, though all the information aren't from scientific articles. Some of the information are from research institutes where the researcher creates their articles based on their work according to the topic. You can never be sure that sources like research articles and websites have the same quality as scientific articles.

Microchip and the implementation of microchips is going to have a big impact in society. Big parts of the implementation are about issues like control and privacy (Michael, Michael 2013). When you insert a microchip into the arm of a human, there is a risk that people can be tracked at all times and lose their privacy if you compare to how it was before the use of microchips. One of the biggest fears in implants into humans is that all dignity and individuality is going to be lost and more seen and treated as an inventory and also be supervised at all times. To have a chip that can be tracked can frighten people and be a challenge for how people are going to keep their privacy against public goals (Gadzheva 2007). Tracking is a threat to the individual and it will be easier to stalk, surveillance and spy (Monahan, Fischer 2010).

Today the implementation of a microchip can be considered for limiting people's freedom because of the risks of being tracked and monitored (Gadzheva 2007). Identity documents and other sensitive information can easily be read and copied by identity thieves (criminals), organizations or governments. E.g. without the person's knowledge their passport can be shared or obtained. Other data concerning people’s history, preferences, and habits can also be of interest in some substitute. The data is a private document and analyzing this data will encroach on people’s integrity (Monahan, Fischer 2010). Microchip implants are a threat against privacy and people's own body. In healthcare the microchip is an easy way of identification of the patient and the patient's health information. If the microchip is used incorrectly it can generate privacy issues and health risks. Therefore, is it important to introduce laws and regulations on how the technique can be performed (Monahan, Fischer 2010).

Because of the pretty new development and implementation of microchips it is hard to be sure about all risks and negative effects that can come with it. The FDA (U.S Food and Drug Administration) said that the VeriChip, which is one of the most common chips, is not completely safe. A letter FDA sent out said it has a few health and security risks about the microchip like;

- Failure of implanted transponder
- Failure of inserter
- Failure of electronic scanner
- Electromagnetic transponder
- Electrical hazards
- Magnetic resonance imaging incompatibility and needle stick

Of these examples the incompatibility is the most serious risk because it is not possible to give lifesaving medical means to a patient with a microchip. By implementing an RFID microchip there can be risks if it, for example, moving around inside the body and then start to irritate or give other reactions. If this happens, it means that you have to remove the chip and you need to do a surgery that can cause other damages (Gadzheva 2007).

Microchip implants have a lot of advantages in some areas. Future microchips will be used for more purposes like mobile computing. The mobile computing has generated issues when it comes to internalization. Microchip implants are not an exception and RFID implants will probably have the same problems and risks that mobile computing has brought (Katina, MG 2013).

Security concerns are a huge topic according to the implementation of microchips into human bodies. People who are against it have argued against the chips on technical grounds and says it is possible to clone an implemented chip by using a reader to collect the information and then do another one that is the same. Then someone else has all your personal information and can use your chip for their own winning (Gadzheva 2007). There is a fear that microchip implants can be coercion for people in the future, for a reason to control, monitor and regulate people. Parents can probably decide to implant a microchip in their children. Another example is to implement an RFID- chip in patients who have a psychological disease. In some cases, it can give a good result to coercion people to implant a microchip, but it is an ethical question that must be criticized and adapted to the society by apply sharp regulations and laws (Monahan, Fischer 2010).

3.2 Body area network

Body Area Network (BAN) is a wireless technology with a purpose to oversee the health and emergency medical response (Lu, Ming, Shucheng, Jiawei 2013) (Li & Kohno 2011). The technology has the ability to anticipate eventual diseases that decrease medical costs. Sensors are placed on the body and they understand wireless connectivity and can communicate with vital signals (Li & Kohno 2011).

The intelligent sensors sizes differ but ordinarily, they are small, therefore they could easily be implanted inside the body or be placed outside the body. The signals from these sensors are treated by a controller called CU. The collected data is processed by doctors and they can

analyze real-time diagnoses (Lu, Ming, Shucheng, Jiawei 2013). It is possible to connect BAN to other devices for healthcare and medical purposes (Li & Kohno 2011).

Safety implications and integrity are some issues/aspects that avoid BAN to expand and revolutionize homes, hospitals, and operating rooms. The process is a risk to keep the patient sensitive information safe. It is a risk for the patient if the wrong person (hacker) gets access and connects to BAN because the person can sabotage and control the patient's health. There are many types of research regarding how you keep wireless networks safe with authentication but BAN has requirements because of its unique functions and area of use (Lu, Ming, Shucheng, Jiawei 2013).

3.3 Wireless personal area network

Wireless personal area network (WPAN) is a flexible technology that has become very popular for consumers and it has replaced wired devices (Kim, Kim, Fang & Wong 2010) (Rohde, Toftegaard 2011). WPAN is a technology that connects and shares information between physical objects, smart objects, and the internet (Zhu, Chi, Tian & Leung 2016). Wireless network devices have expanded the last years in organizations and people's homes (Rohde, Toftegaard 2011).

Before there was WPAN used for traffic monitoring, intelligent transport system and other applications related to transports, but nowadays WPAN is possible in more areas of use (Zhu, Chi, Tian & Leung 2016). The expending of using wireless devices lead to issues and have an impact on the license-free frequency and it generates a high interference. Cognitive radio technology could be a solution against the high load of frequencies in the future (Rohde, Toftegaard 2011).

3.4 Theories concerning risks

The purpose of this chapter is to inform and explain some of the most mentioned and known threats that come to mind when talking about microchip implementation in humans. By asking the participants about what they believed was a threat and risk in this topic an overview was created and by creating a description of every threat/risk it is going to be easier to understand what each of them mean.

To examine these different threats and risks facts have been used to describe the different parts to strengthen the trustworthiness and to give a deeper understanding. All facts are divided into subheadings so it gives a clear and correct picture where all different threats and risks are informed that can happen while using a microchip or while implementing a microchip. The chapter is divided into the first part which is about the individual risks and later on the societal threats. The risks that will be mentioned are "human implants and their privacy", "harmful for the body", "robbery", "tracking and monitoring", "human implants and being hacked" and the last one is "costs".

3.5 RFID

Radio Frequency Identification is a technology that has been used since World War two (Gadzheva 2007). Today, RFID is used in many different areas like manufacturing, military, healthcare, livestock ranching, and warehouse management systems (Yang, Rida, Traille, Tentzeris & Russer 2008). In the beginning, the chip was limited to objects but today RFID is possible to implant in humans (Gadzheva 2007). The technology makes the identification more effective of a person or objects (Yang, Rida, Traille, Tentzeris & Russer 2008). RFID technology includes readers and microchips. The microchip has a unique number and the reader collects signals from the tag to identify the microchip. Information in the chip can be updated or changed. The microchip has different sizes depending on if the microchip is active, passive or semi-passive (Gadzheva 2007).

A microchip that is passive does not need electricity because it gets enough from the radiofrequency's signal and a passive microchip are smaller because the use is limited and therefore it has a longer life span (Gadzheva 2007). Semi-passive is the only chip that is approved to be implanted into humans, the chip becomes active when it gets a request and an active microchip has a large memory and a longer reading range which is possible because it has a battery. There probably is an active microchip available for humans in the future (Gadzheva 2007).

If there are too many RFID tags around a reader at the same time there is a risk that a collision may occur. It confuses the readers and data from the tags cannot be read correctly, this situation will lead to collisions (Jing, Vasilakos, Wan, Lu & Qiu 2014). Computer crash is another problem that may arise and it affects the use of the chip (Gadzheva 2007). It is possible to read tags from a distance in different areas where items and people are located. Track, monitor, identify and locate are some of the functions the RFID- technique offers and has the ability to perform (Rodriguez 2019).

Verichip is a glass-coated RFID microchip that is the size as big as a rice grain that you put into your arm and fill up with information about yourself for saving lives and decrease mistakes regarding medicals (Voas, Kshetri 2017). A not fully developed system that had the purpose of helping us humans to an easier life, but also gave us some risks that people are worried about instead and that cause suspicion whether or not it is worth using. The following text is about some of the biggest risks that people have regarding the implementations of a microchip according to the interviewees.

Individual concerns

3.6 Human implants and their privacy

The concept of integrity means value and dignity and stands for each person's intrinsic value. Integrity can be divided into two parts, physical and psychic integrity. Physical integrity is about the body and that no one has the right to inspect your body without your permission. Physical integrity means the individual's values in life, opinions, wishes, and mental life. Physical integrity is not to be offended and there is no room for infringement (The Swedish National Council on Medical Ethics 2019).

Personal integrity means inviolability and is about having the right to keep things to yourself. In healthcare personal integrity can be offended in some different ways, for example, breaking the professional secrecy and give away sensitive information or do different kinds of actions against your own will (The Swedish National Council on Medical Ethics 2019). This can lead to a situation where you feel offended with people that are threatening your integrity. When it comes to privacy for each person, a lot of people see microchip implementation as a really bad thing since their privacy can be threatened with risks of constantly being tracked (Gadzheva 2007). These small chips make it easier to get information about one person and can easily get personal information through just one scan. Today there are privacy concerns of issues and debates about mostly when it comes to RFID microchip implementations (Rodriguez 2019). Applied digital solutions (ADS), that was developed by Verichip, has been used all over the world in getting VIP status at bars to patients at hospitals for getting information quickly and has once said that their system has stored all information regarding Verichip. All users that has an implant are secured with a password. It has been proved incorrect that the microchips can only be read by special readers (Lockton, Rosenberg 2005).

Implementations of an RFID chip can be seen as a way to make the freedom for individuals more limited because of the risks. Such as always having the ability to be tracked or surveillanced (Gadzheva 2007). There has been criticism against the implants and the privacy which can be divided into 5 different parts. These parts show the concerns about privacy if an implant of a microchip is done.

1. That the tags can hide information and documents against the individuals without their knowledge
2. That it is possible to mass identify objects which means it is possible to track items to persons afterward when a product has been transferred or has been sold. This makes the privacy decreases.
3. The possibility to collect a lot of data and especially if it can connect personal data which makes the privacy decrease.
4. With personal identity numbers connected to the personal microchip can private persons be profiled and tracked without the knowledge and consent.
5. Privacy concerns have been created since it is possible to read a microchip from distance in many different environments which decreases privacy and integrity (Rodriguez 2019)

According to Dario Rodriguez, the main feature of RFID chips is the possibilities to track, identify and locate people (Rodriguez 2019). This shows very clear that the privacy with these chips will not be very private. And that people are concerned about the problem it makes sense to compare the study that has been made where one of the risks that are mentioned is privacy.

The biggest fear that those microchips bring privacy advocates thinks will be that the people lose all their individuality and dignity. People getting scared to live with a chip that keeps a lot of private data and challenges the balance in life between public goals and their privacy (Gadzheva 2007).

3.7 Harmful for the body

According to WHO (World Health Organization) health is defined as social, mental and physical wellness (Regeringen 2008). RFID- implant is a pretty new technology, therefore the knowledge is limited to what side-effects and risks it brings to the body. FDA: s VeriChip

implant is approved but there is nothing that assures that the chip implant is completely safe (Gadzheva 2007).

Anti-RFID activist of CASPAIN (Consumers against Supermarket Privacy Invansion and Numbering) mention several potential health risks. According to CASPIAN a microchip implant can involve health risks such as:

- The chip emits electromagnetic interference
- Negative impact on tissue reactions
- The microchip can change location in the body
- Surgery mistakes while implementing the chip
- Electronic risks

Infection and other medical reactions are risks that could emerge when an RFID implant has been performed. Therefore, it is important that the implant is performed in a medical environment that offers a sterile, cleaner and safer place for health (Gadzheva 2007). Irritation under the skin can occur because there is a risk that the microchip may move and migrate. To solve the problem could be harmful for the body and to fix is required professional surgery (Gadzheva 2007).

3.8 Robbery

If a criminal threat or violence occurs with a purpose to steal the chip it is classified as a robbery. Robbery is defined differently depending on how rough the act is (Polisen 2019).

The chip does not need its actual owner to be used in different situations and therefore there is a risk that thefts without knowledge about IT and hacking might use violence methods and cut out the RFID- chip from the victims. The violent methods can be abused instead of hacking because the criminals miss the competence of hacking (Gadzheva 2007). Things that can happen when you have a microchip implemented except a robbery are things like, fraud, harassment or blackmail. People who use a chip are going to get hurt in some way while being exposed to a robbery and it does not have to be in a way that you end up getting hurt personally. It can also hurt you economically and also other ways (Neumann, Weinstein 2006).

Individual and society concerns

3.9 Tracking and monitoring

Tracking is when you try to figure out who has left traces behind or to see what a person has done by following (IT-ord 2019). Monitoring is done on distance and you install a program on a reader or computer to collect information (IT-ord 2019).

The digitalizing society is developed in a way that it reduces the cost of monitoring and tracking. Technology has revolutionized and the progress has resulted in tracking and monitoring to be possible without financial restrictions. Society has become more interconnected through mostly of all electronic devices and is highly developed and connected to computer software. Data from electronic devices collect and get analyzed (Claypoole, Balough 2012). The individual does not know who obtains the data from the RFID- tags (Rodriguez 2019).

Tracking and monitoring the individual are facts and the interest to have control over the wielder has increased (Claypoole, Balough 2012).

Information from individual devices reaches many stakeholders. Electronic devices like cars and smartphones contain systems that analyze, collect and report information to other stakeholders. Payment systems tier names to a transaction. Every time the individual consumes it amplifies the physical trail and this supplements the tracking. Smartphones stick out of the crowd, it has several of movements that could be tracked and it is a highly sophisticated tracking tool. Smartphones have many functions and therefore it is easy to monitor every movement that the owner is performing (Claypoole, Balough 2012). Different companies that are involved in the production of the phone have access to the information and the movement from it. Beyond the suppliers it is easy for companies to track the users and also authorities that can take part in the information by request. Mobile-phone providers collect and store historical location information. To solve crime, the police in the United States ask mobile companies after information from mobile phones and in 2011 they answered on 1,3 million applications from the police (Claypoole, Balough 2012). An employer is not an exception, companies increase the monitoring and tracking over their staff. They track their staff through cars, GPS phone tracking and it is increasingly popular for companies to the employees to use RFID- chip at work. Microchip implants in the employment context is a technology that has to expand and implants in employees will probably become a standard. Chipped employees increase the risk of being tracked and monitored at the workplace and outside of work. Microchip implants are going to expand if governments don't regulate the law. A risk that can occur in the future are that employers have mandatory microchipping on their employees. If there are no regulations it is going to threaten the privacy for the employees (Rodriguez 2019).

3.10 Humans implant and being hacked

Internet use has increased and the expanded phenomenon has resulted in more criminals committing different crimes over the internet. Cybersecurity is a protection for organizations and individuals from threats from several different directions, despite the cybersecurity, there are still risks that can damage a user's information. Risks that may occur are viruses, surveillance, phishing, spyware, trojans and identity theft (van Schaik, Paul et al 2017).

The same way computers can be hacked by different kinds of threats like other people and different kinds of viruses the RFID chip can be hacked, read from or corrupted. RFID has to be read from a specially designed reader that is based on regulations and standards and for a hacker to hack into an RFID chip is all that they need, just more power to have the opportunity to read and identify information. Hackers that can reach those chips can also deploy harmful content that is almost impossible to find (Dinh 2008). Talented hackers can have the knowledge to turn RFID chips on and off because of changing information (Clarke III, Flaherty 2008) which can concern people getting it since they feel it is not worth it. Hackers have different kinds of targets when it comes to hacking. Some do with a purpose like earning money out of it and see the financial advantages and some do it just for fun and see it is a challenge for them (Muir 2007). A technical person can just buy a reader that has the technical expertise to track and find those people who use a microchip and scan them without their knowledge or consent. It has also been revealed that the microchip is vulnerable to viruses. More and more people are willing to get an RFID-implant but one of the most important challenges is that people have the proper tools to make the right choice for themselves and to be able to protect themselves and their data (Gadzheva 2007).

3.11 Costs

According to Jervis Colin, he mentions that even though the advantages are many it is important to also see the costs that come with the implementation of RFID chips. The price depends on different reasons like what frequencies and also what functions it needs. The price for basic passive tags costs 75 pence (which today, 2019-12-03 in 9,42 Swedish crowns) when buying smaller amounts. When it comes to machines, like writeable tags the cost is around ten pounds or even more, depending on higher frequencies. Door readers can cost around 2000 pounds each and just small readers that you hold, around 170 pounds (Colin 2005).

To get chipped in Gothenburg, Sweden it costs 1500 Swedish crowns and takes around 30 minutes and you decide by yourself what the chip needs to have, for example, keys, keycards or instead of the new type of bus cards that has started to be used here (Chipme 2019). By using subheadings about all different topics, the idea was to make it clear and easy to understand for the readers and let them follow the red thread in an easy manner. It is important to present the content in a way that makes the reader interested and that it is easy to read. By using small parts with valuable content under different subheadings the idea was to get a higher quality in the overall text.

4 Step one interviews

The first interview contains questions and answers that will have a big impact on the upcoming survey. First, an interview with six different individuals was made where questions regarding risks, user imagination and own opinions was asked. The participants were different genders, ages, and current occupations because the main focus was to get different answers from people with different experiences and knowledge of the topic. In the interviews there were three women and three men. The ages were between 23 and 26 and four of the six individuals were students at University of Borås and the last two were working occupants. A semi-structured interview was used during the first survey.

The method, semi- structured, that was used in this report was necessary since it is all about people's opinions and thoughts regarding microchip implants in humans. The research question says "What is the opinion about microchip implants in humans for 18-30-year-old people in Borås, when it comes to risks in their daily life and the society" and to get the answer on this question, an interview and a survey was needed since it creates an image and an overall picture of other people's thoughts. To get answers, it is important to come up with questions. By always having the research questions it is important to find and look at the results to the relevant material. This way the questions can be connected and later on get answered by looking at the results.

It is important to inform all participants about the topic and the advantages and disadvantage that come with it. The information includes integrity aspects like tracking, harmful to the body and other risks. The information and the questionaries' must be objective. If the interviews are objective it will not affect the participants and that will generate trusty and relevant data from the interviews (Colin, 2002).

4.1 Interviews

The interviews were both done face-to-face, where the meeting ended up where the participant wanted, also on phone and mail contact. One interview was face-to-face, one by mail and four were made by phone (see table1, summation of interviewees). The questions were decided before-hand and all questions were the same for each participant (see appendix 1) meaning that the interviews were done in a structure that is called a semi-structured interview. A semi-structured interview is based on the same questions to everyone who is part of the survey which means that everyone is treated the same. The advantage of this type of interview is that it gives a more relaxed feeling and is more like an actual conversation while still being serious with high professionalism (Recker 2012).

The questions were asked in a way so that it was easy for the participants to keep up and understand since the interviewed individuals all have different grasps about the topic. The survey started with some simple questions and later on more turned to more" thinking questions" where the purpose was to see if the participants came up with new risks that had not been mentioned before. At the end of the interview the participants could express their own opinion and if they were interested in implementing a microchip to themselves.

The interviews took different amounts of time depending on how the interview was done. The face to face interviews were more like a conversation where the answers were more detailed and very thoughtful which took around fifteen minutes. The phone interviews were more short answers and not as detailed as the face to face and these took a maximum of ten minutes. The mail interview was more difficult to estimate how much time it took for the participants to answer since the questionnaire was sent and the participants gave answers when they had time. The survey was sent to all participants before they answered, both to see if they were interested in taking part in it and also to have a chance to read them to give their answers well.

4.2 Data collection

The data for the step one interviews has been collected in different ways. To get necessary data both face-to-face interviews where the meeting was at a decided place, by phone when the respondent had the time and also by mail where the respondent replied when they had time.
Later on, all data from the six different individuals were compiled into a table to easier look at and compare the different answers. The data collected from the first study is what the second study is based on.

4.3 Analysis

In the qualitative part has a research method been used that is reminded of grounded theory. Grounded theory is a research method that is based on qualitative data which is collected and analyzed. Grounded theory's purpose is to build theories, by exploring and develop formulations functions that are basics from a phenomenon at the same time as data collections and observations have been performed (Recker 2012). The applied research method, which is similar to grounded theory was suitable for step one in the study because theories are built upon theoretical samplings that collect data and analyze it from the study to see if it is relevant or not to the theory (Recker 2012).

The answers from the interviews needed to be categorized and analyzed and there are many different types of techniques that can be applied (Colin, 2002). To eliminate superfluous data

from the interviews coding was an effective alternative. With this technique it was easier to analyze data by organizing and categorize it (Recker 2012).

Grounded theory consists of three main steps: open coding, axial coding and selective coding. The purpose of open coding is to group data into categories, axial coding is about relating the categories to each other and selective coding is about finding and identifying a main category that cover all other categories. In this study only, open coding has been performed, because it was not necessary to perform the other two steps because the step open coding was enough to see the connection between the respondent's answers. Open coding is one approach of coding techniques where the purpose is to name concepts from the qualitative data. With open code it is possible to compare and find data that is similar and different to each other (Recker 2012). This technique was applied by assigning a tag from every answer from the interviews which makes it easier to take out parts from the answers that were relevant for the study. The tags were summarized as keywords that had the same meaning. Participants expressed themselves differently but some answers that differ had the same meaning and these similar answers were coded with the same keywords (Recker 2012).

Later on, the similar keywords were with same meanings from the interviews distributed and divided into six different categories named "Heard about microchip implant", "Risks", "Risks to individuals", "Risks to society", "Generally opinions" and "Imagine using". These six categories were created to easily analyze and understand what the participants have as an opinion regarding microchips in humans concerning the risks for the individual and society. All categories and respective keywords were placed in a chart (see in result, chapter 5.5) there it was easy to see what the respondents had answered. When the data was categorized and organized the next step was to see if there was an interconnection between the respondent's answers. One risk could be the reason that another risk exists, like a domino effect. If one risk had been solved, it may reduce other risks as well therefore a risk maybe exists because of another risk.

Grounded theory strives to compare data and connect the new data with new concepts from the theory (Recker 2012). The new data from the interviews that were made has been compared and connected with the different answers, theories and concepts from peer-reviewed articles. Comparing the data made the first step easier to analyze the data and the result is more trustworthy when it matches and had been confirmed with the existing facts.

4.4 Respondents

The purpose of the interview was to get initial knowledge of what the target group had as an opinion about eventual risks. The interviews were the foundation to create an appropriate questionnaire for the survey. The respondents for the interviews were six people with different experiences and backgrounds. The sample of respondents were carefully selected to get a big range of multiple perspectives and the sampling was based on age, gender, and competence about IT.
These respondents were selected to get an overview of what the target group had as an opinion and their own theories regarding microchip implant in humans.

It was important to find participants who had different levels of knowledge regarding the topic because it results in different perspectives. The ones who has a lot of knowledge might think of other risks than people who have less knowledge and therefore the participants were divided into five different levels of knowledge which were "Very bad", "Bad", "Okay", "Good" and

"Very good". The mindset between women and men can be different since different genders might think differently about things in general, therefore the participants were fifty percent women and fifty percent men. Diversity gives an overall picture that summarizes all possible answers. These aspects are to get a wider range of knowledge of the target group and their thoughts about microchip implants.

One thing that can be criticized is the age of the first survey, the participants were between 23 to 26 years old. The median value and also the average value of the first interview was 24 and that is why the chosen age was from 23 to 26 years old. But as mentioned before this is a small part of the big survey since this is a possible chance for the real survey to get relevant questions that are necessary for the study. The hope is to get more inspiration and find more theories that can be useful.

Table 1, Summation of interviewees

Person	Gender	Age	Current occupation	Knowledge
1	Female	25	University student	Very good
2	Male	26	University student	Okay
3	Female	23	University student	Very bad
4	Female	23	Nurse	Very bad
5	Male	25	Fiber technologies	Good
6	Male	24	University student	Very good

4.5 Open coding

The categories that has been identified during open coding were "Heard about microchip implant", "Risks", "Risks to individuals", "Risk to society", "General opinions", "Imagine Using".

Table 2, results

Person	Heard about microchip implant	Risks	Risks to individuals	Risks to society	General Opinions	Imagine using
1	Yes	Harmful for the body, Be hacked	Robbery, Be hacked	Increased crime, System collapse,	Cool but creepy	Not now, maybe in the future
2	Yes	Harmful for the body	Be hacked	Costs	Interesting, should be developed	Not today, maybe in future
3	No	Security reasons, Be hacked, Be tracked, Monitored, Controlled	Monitored, Integrity violated	Monitored	Positive: all collected at the same place. Negative: unnatural and harmful for the body	No, never
4	No	Harmful for the body	Economical aspects, Harmful for the body	Economical aspects, Environmental aspects	Positive but scared for health risks and put unnatural stuff in the body	Yes, in future
5	Yes	Be hacked	Harmful for the body, Be hacked, Robbery risks	Increase in cimes and new types of crime	Fascinated, smooth but not neccesary	No, would never use
6	Yes	Robbery, Harmful for the body	Robbery, Be hacked , Harmful for the body	Costs	Creepy, not neccesary today	Not now, if it is common and accepted in future then yes

In the first interview, most of the participants had heard about microchip implants in humans before. While asking the individuals everyone mentioned that it can be harmful to the body as one of the main risks. In general, everyone was thinking approximately the same about risks both regarding the individual and societal. The most common risks that were mentioned was harmful to the body and the risk of being hacked. Some answers differ from each other, especially in the questions regarding "risks to society" where people who had heard about microchip implants before had different answers. For example, individual one was thinking about if the system would collapse and individual five was thinking this will create new types of crimes. Most of the people had positive thoughts about it and seemed interested in the topic, except one person (individual six) who thought it wasn't necessary today but maybe in the future. No one would use it right now but four of the six persons can maybe see themselves with a microchip in the future.

A lot of research was put in to finding information that can strengthen the mentioned risks in the theory chapter. Science articles were used to get relevant and trustfully information that could strengthen all mentioned risks. Environmental aspects were not related to the theories since it didn't feel relevant to the research question and therefore environmental aspects were chosen to not be a part of it.

5 Step two survey

This chapter contains the results of our second survey, which was based on the first survey. The result will be analyzed and also how the result has been reached. 100 individuals were asked but 73 individuals were willing to participate. Each question could be connected to the existing facts and theories (see appendix 2) regarding the purpose of each question. The questions were based on the first interview and the purpose is to get an understanding of what people in age 18-30 had as opinions regarding risks about microchip implants in humans (see appendix 3). Each question will be presented in charts with an overall picture of the participant's answers. The survey had, like the first survey, a good mix of genders, ages, and occupations.

When the interviews were done, a survey was created. The meaning with the survey was by asking even more people, in this case, 100 individuals what they believe and what they think about questions regarding the topic, microchip implants in humans. The survey is a must for getting good data that later on can be analyzed and give a result of the survey. To find the right people who were suitable for this study, the survey took place outside the university of Borås and local supermarkets. These places have a good mix of both ages and genders which gave mixed answers on the survey.

By using the survey research method, the study would give good data by asking the right individuals that were within ages 18-30 years old the right kind of questions to go forward in the survey. The survey was being produced and a lot of work was being put in the process. This was very important since the study didn't want any irrelevant data. The survey research method was both flexible and described the characteristics of a large population which seemed very useful. Another typical quantitative analysis that fits this study is the cross-sectional study. The cross-sectional study is a very popular method but doesn't match this study since it is focusing on relationships in a single group during a very short time and period. This method matches the survey research method for collecting data that are later on be.

5.1 Choice of scale

Likert scale is a scale that is formed by the American phycology Rensis Likert and is used in questionnaires where you have to choose one of the choices for the one that matches your opinion the most, for the specific statement (Psykologiguiden 2019).

A Likert scale is better to use if you use more options because then it gives a better overview of what the person thinks (SurveyMonkey 2019). Four alternatives were used because it is an even number which means that it doesn't have a "middle" answer that people can see as a neutral answer. Four alternatives make the participants take action and decide which answer they are leaning towards the most. That's why five or seven alternatives are not chosen because that could give a middle number and the meaning was to take away the neutral answers.

5.2 Data collection

The data from study two was collected through google formula and also analyzed directly after since the result of each question is presented in the formula as soon as it is handed in. The survey was based on the answers from the earlier interviews, existing facts and theories regarding microchip implants in humans (see Appendix 2 & 3).
Google Formula made the process easier, both for the interviewers but also the respondents since they could, through their phone easily answer each question. By letting each participant answer in a formula, they have the time they believe necessary and can generate high-quality answers. Google Formula saves the data in a cloud-based service which saves the data in a safe way and makes it possible to reach from anywhere. Google Formula is a tool where it is possible to create questionnaires. Google formula compiles all answers by itself and helps the users to get the work smoother. The results that the formula gives are presented in diagrams (see the link https://www.google.se/intl/sv/forms/about/).

5.3 Analysis

After the interviews were completed, the answers were compiled and analyzed. To be sure that the result from the interviews were useful to the survey the answers were compared with existing theories and facts from peer-reviewed scientific-articles, this approach can be seen as a triangulation. Triangulation is when the researcher compares studies for the same phenomena's results and explore the different methods that has been used to confirm and be sure that the results are similar (Recker 2012).

The study has been performed with qualitative and quantitative methods for data collection. Therefore, there were also mixed-methods that occurred to be able to adapt the analysis to the respective method because analysis fits differently depending on if the study is qualitative or quantitative (Recker 2012). The purpose of mixed methods is to generate theories and confirm the inquiry question that results in stronger conclusions (Recker 2012). In the first step the interviews were analyzed with an appropriate qualitative method called Grounded theory.

In step two, the survey had been analyzed with a quantitative data technique called Multivariate analysis (MVA). Multivariate analysis is a more general technique for statistical inferences and can be applied virtually for all statistical methods. The technology examines objects or individuals and the investigations are analyzed several times (Recker 2012). Multivariate analysis is part of the survey since measurements have been made on each individual answer on each question to get a final result of all participants answers that has been put together as

one on each question (Recker 2012). All the answers in the study have been answered alone by random individuals and has later on been put together in a diagram where the answers on the same question has been presented to get a total of what everyone thinks. The diagram shows an over overall picture of what the participants has answered.

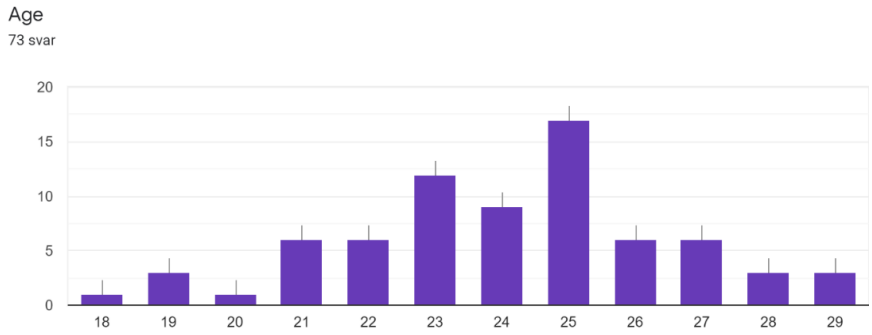
All data from the survey was collected, summarized and analyzed by Google formula. Every question can be associated with their category and all the answers were analyzed and placed in a diagram. Respective diagram manages their statistic and it was easy to read and understand the diagrams that were reported in percentages and numbers. The data from the survey was compared to the analyzed data from the interviews and existing theories and facts. Data from the interviews had been examined to see if there are any interconnections to the data from the survey and to see if there are similarities or differences. More about the results and conclusions come later in this chapter.

5.4 Respondents

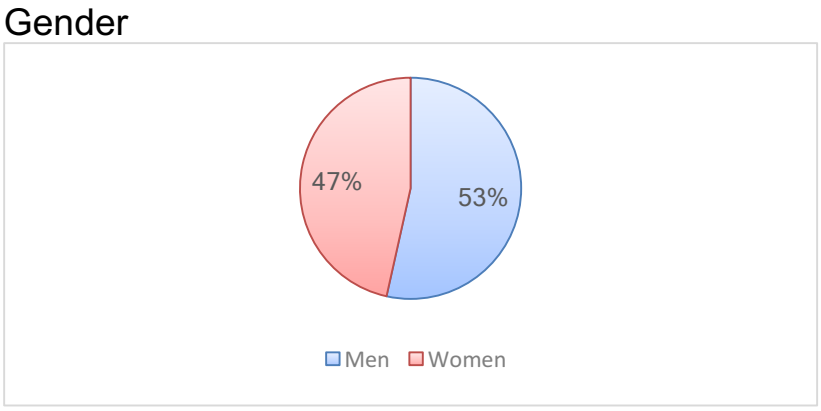
Study two was the biggest study of the entire paper and where the final result will be given. The survey had 100 individuals who were asked to participate but only 73 people who were willing to be part of it. 37 of the respondents were working, one individual was unemployed and 35 individuals were studying. The purpose of this study was to come up with an answer to the research question where a result could be presented that gave a clear and easy understanding of what the people between 18-30 years old have for opinions regarding microchip implants in humans and the risks that come with it.

In the second survey the participants were randomly selected in both age, gender and knowledge. Because of this a variety of answers were given and were made necessary for the neutral stand of the study. It was important to collect opinions from all individuals, which means that we did not just focus on one kind of individuals. People who were asked to participate were either working in different branches or studying different educations. All individuals were randomly selected. The survey was very successful and had a good mix of participants. One thing that can be criticized was the number of respondents that ended up in 73 individuals that answered out of the 100 individuals that were asked. It was still a lot who wanted to be part of this survey and it gave a good result, but the feeling was that with even more people, an even better result could be presented from the survey. The compiled result gave a good answer to the research question.

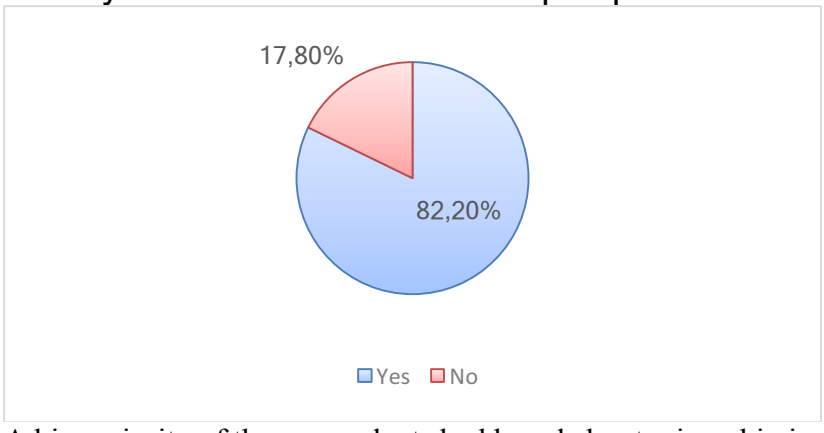
5.5 Result from the survey



The respondent's age was between 18-29 years old. The majority of age was 25 years old, 23 years old and 24 years old. The age range between 18-20 and 27-29 was a minority.

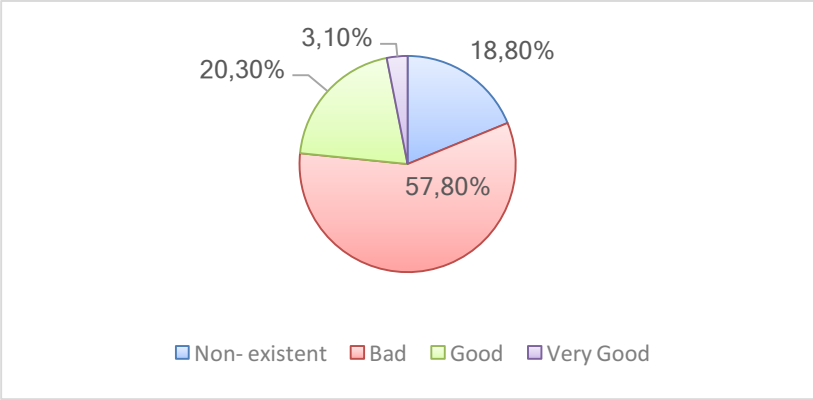


There was a good mix of the genders, there were 39 men and 34 women that attended. Men and women's opinions can differ from each other in general, therefore it is important to ask both men and women. The mix of genders generate a better result for the study and a picture that agrees with reality.



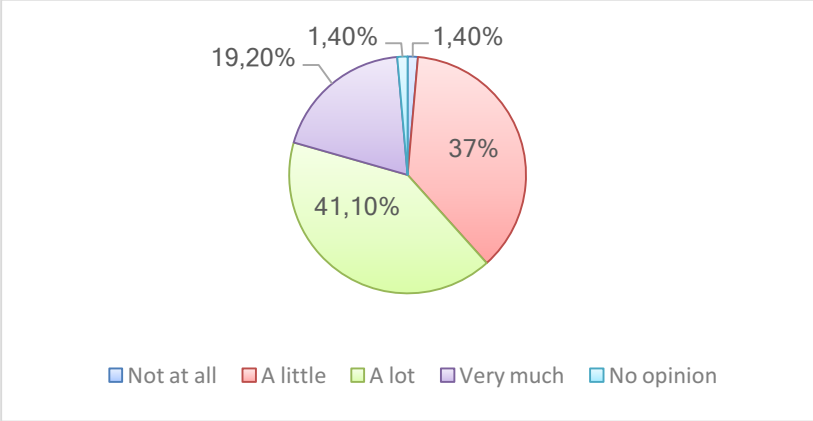
A big majority of the respondents had heard about microchip implants before, it was surprising that 82,2% had heard about microchip implants before since it is a pretty new upcoming technology that has not been popular yet.

If you answered yes, what do you currently know about microchip implants in humans?



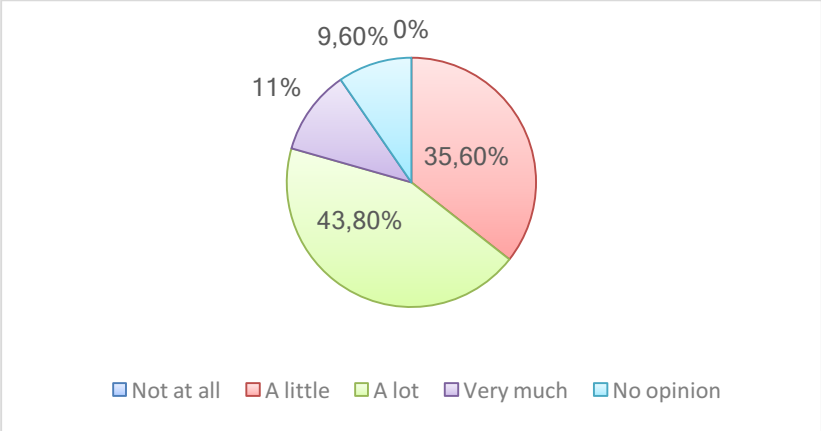
As a follow-up question, it shows that the majority do not have the knowledge that they think is needed to get a microchip. A fifth believed that they have the knowledge that is needed to implement a microchip into the body.

Do you think this is an interesting subject/topic?



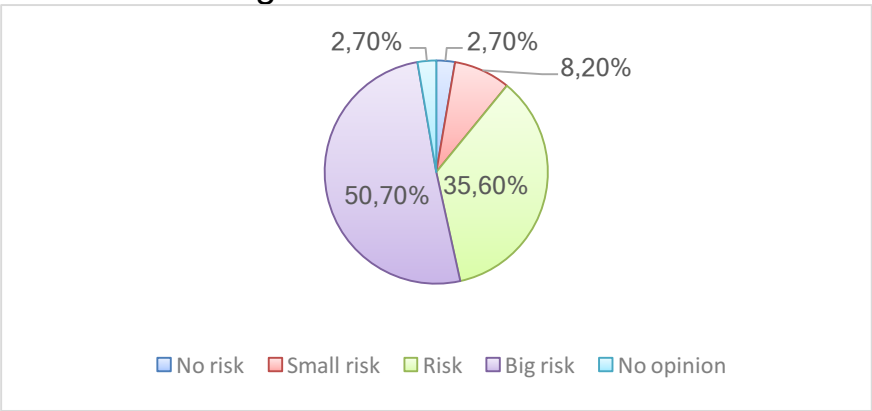
The majority considers that this topic seems more interesting than uninteresting there was only one participant that thought it is interesting at all and one participant had no opinion.

Your privacy is more at risk of getting exposed?



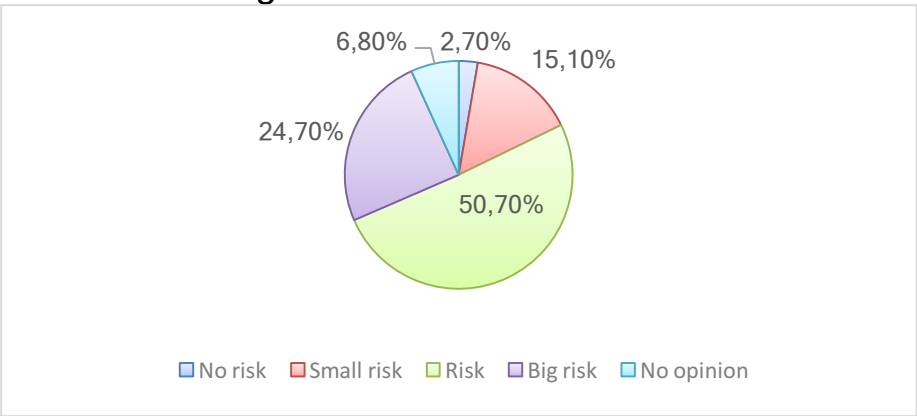
There were pretty various opinions where approximately fifty percent believes that microchip implants threaten the personal integrity and circa fifty percent believes not or have no opinion.

The risk of being tracked and monitored?



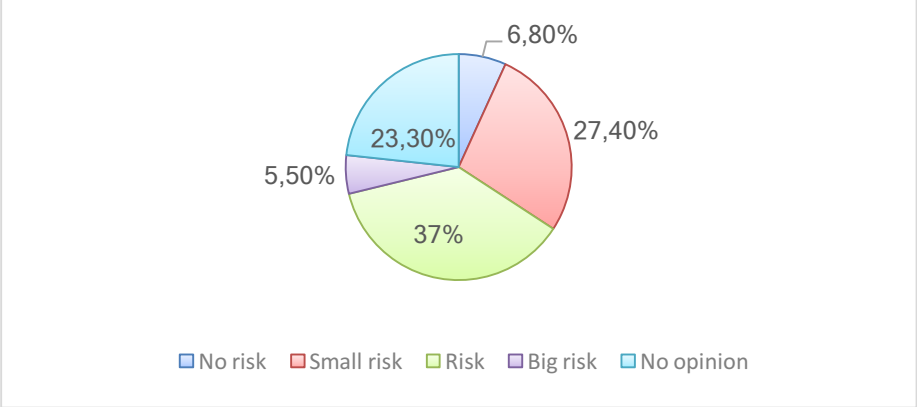
Respondents were convinced that there is a risk with microchip implants and that they can be monitored. Most of the respondents either believed that there is a risk or a huge risk to be tracked or monitored when using microchip.

The risk of being hacked?



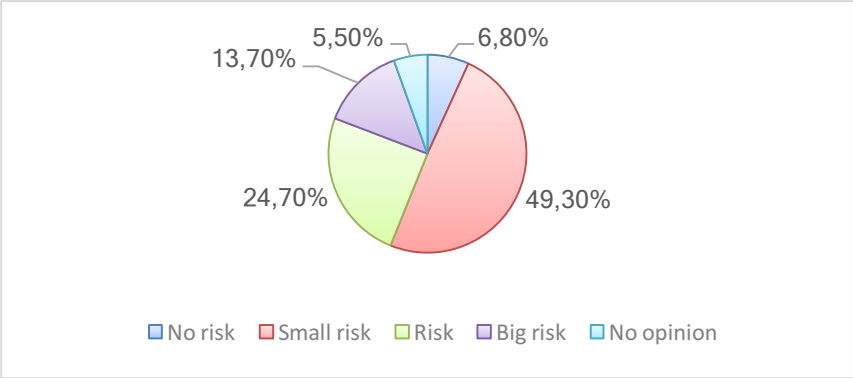
Over half of the respondents see a risk to be hacked while having a chip. A lot of respondents also see a very small risk of being hacked while having a microchip implemented.

The risk from a perspective of health?



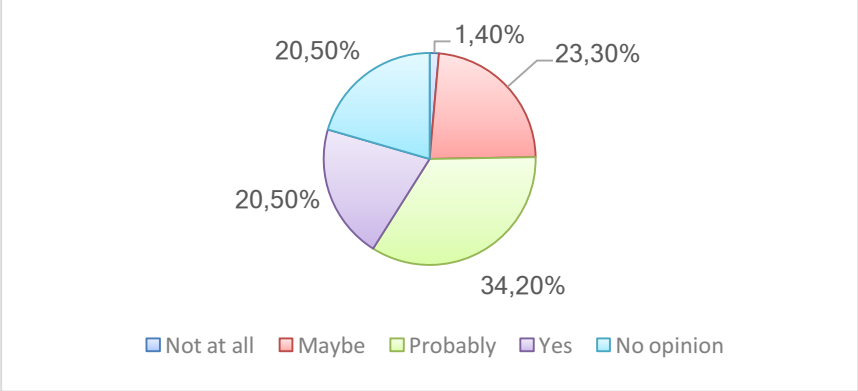
A question where the opinions were very different from each other. This question in the survey had the most answers of “No opinion” chosen. People probably have different answers since this is hard to relate to something that is similar to this.

The risk of getting robbed of your implanted microchip?



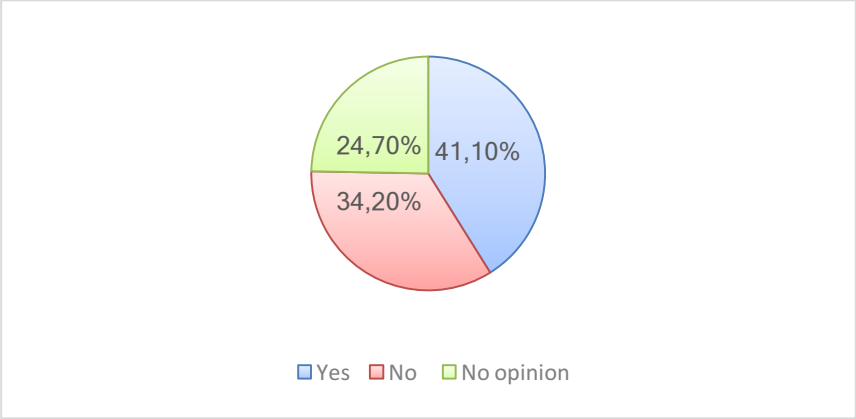
Getting robbed is a small risk according to the participants and how they chose to answer. But still circa 38 percent believe there is a risk of getting robbed.

The microchip implants generate costs for the individual and society?



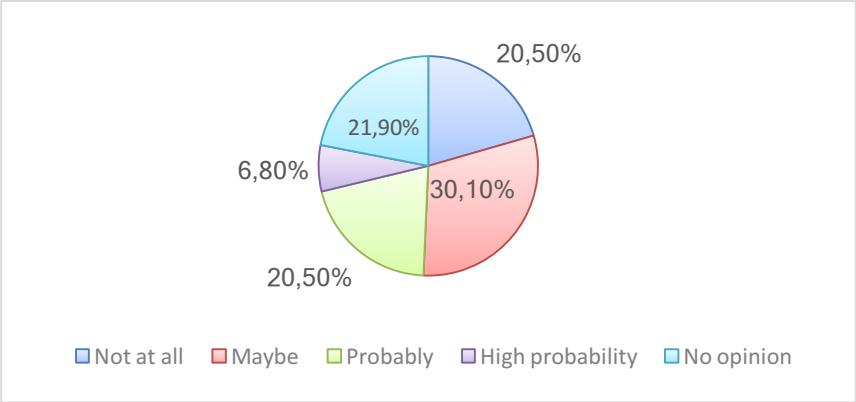
The answers from the participants were divided pretty similarly at four of the alternative and only one participant had answered: “not likely at all”. Maybe this question is a little diffuse and it can might be a reason that the answers are divided.

Is the microchip worth using if there is a chance that it can suddenly stop functioning?



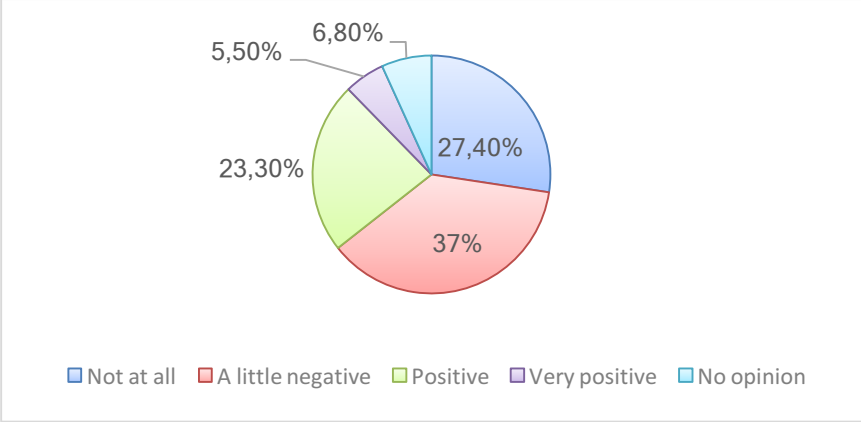
Various answers where the participants have shared opinions, but still see it as a worthy risk since 41 percent answered “Yes”.

How big is the probability of your employer or the government demanding implants of microchips into your body as a requirement in the future?



This question is intended for the future since it is not common to have a microchip implant in today's society. Still, respondents had different opinions and believed it can become a requirement.

Are you for or against the thought of having a microchip inserted into your body?



Also, very different answers, but here most of the respondents were negative to getting a chip implemented. Some have no opinion and circa a quarter were either positive or very positive to it.

6 Discussion

The purpose of the report was to see what people aged 18-30 years old think regarding implementation microchips into the human body even though there are some risks for both the individuals but also societal risks as well. The reason why we wanted to do this study is because we were interested to learn more about people's opinions regarding microchip implementation in the human body. We believe this study is relevant to informatics since it is about the connection and relationship between human and the pretty new and upcoming technology, microchip implant in the human body.

This study has through deeper research given the opportunity for the readers to learn more about what a microchip is and how it can be used in the daily life and make it easier for each individual with certain tasks. It is possible to read up on how it is used today but also how it can be used

in the future. People that are interested to get chipped also get a deeper knowledge about risks and what they can do to you. Some risks that have been mentioned, for example getting tracked and monitored can be compared to other technologies that can have same risks as microchip implants in human. For example, smartphones that has also been mentioned. We wanted to show that the risks with microchips could also be the same risks something else has, in this case smartphones and that people still are using it even with the risk of being tracked or monitored.

In this chapter a discussion and reflection about the results from the two previous studies that has been presented. The theories have been chosen because they kept reappearing while asking questions and also because of the similar technology of microchip implants. Also because of the enlightenment and of the similar technology that are getting more and more developed during the same lifetime. To make it more clear, the discussion is divided into five parts.

6.1 First study

The first study was a shorter qualitative interview where the purpose was to get more information and knowledge about what six different individuals with different levels of knowledge think about the topic. These interviews were the start of the big interview. The result from this study gave a broad consensus because the participants had quite many similar answers even though some of them had never heard about the topic beforehand which can be perceived as a little strange. Even if one of the individuals had never heard about microchip implants in humans before they still came up with relevant and possible risks that have been mentioned from both theories and other respondents. The answers were pretty much the same and the most common answers were that it can be harmful to body, be hacked-and-monitored and getting robbed. After reading different theories we saw that it is also harmful to the body and being hacked and monitored were two of the most common risks that were mentioned. One that mentioned this a lot in her articles was Maya Gadzheva (Gadzheva 2007). These answers make sense since after digging deeper into the topic these risks were those that had been discussed the most except a scenario of an actual robbery.

It is impossible to know if the participants had heard about these risks beforehand or if they just used their common sense and drew parallels of their own to digital devices like smartphones or debit/credit-cards. But still, it is interesting that most of the people that discussed the topic mentioned the same types of risks (see “table 2, results” in chapter 4.5). There was even one individual who had never heard about microchip in humans before that talked about environment aspects, which not many had done before. After the interview was done a research regarding this was done but nothing was found worth mentioning.

Something that stands out and is a bit surprising is that fifty percent mentioned a scenario of a robbery as a risk. This answer was expected by the interviewers but not to be given in such amount from unrelated individuals. All who mentioned it had heard about the microchip topic before the interviews, which was interesting. Why it is surprising is because it is a subject that is almost impossible to find in different articles and older theories. Could this maybe become a future risk that will be more common when microchips are getting used more? We see this as a possible risk but not as the biggest. It could occur that you try to steal the chip by cutting it out (Gadzheva 2007) but we believe that a robbery would more commonly occur through hacking, rather than a stereotypical robbery. Societal costs were at a similar risk as robbery when it comes to finding existing facts and theories. Costs were mentioned more than excepted but were hard to find anything relevant for the report worth mentioning.

The majority of the participants saw microchip implants as a pretty scary thing but still, some looked at it in a fascinated way and believed it was cool. A common denominator from both is that no one sees this as a necessary technology today and that it is not needed in today's society, but maybe in the future when it is even more developed and start getting more common. The RFID chip is today used in many different areas (Yang, Rida, Traille, Tentzeris & Russer 2008) but yet the usage in the human body is still limited to just a few things. For example, as a usage of payment or as a key (Forskning 2019) and that might also be one of the reasons people do not use it today. Today there are around 5000 Swedish people who have a chip in their body (Forskning 2019). These answers were quite expected after reading about it in debates and theories and also listening to the participants about the potential risks. One thing that caught us by surprise was that no one wanted to implement a microchip today and were pretty confident about it even though they could think about getting one later.

6.2 Second study

The second study was a quantitative survey that was made in Google Formula. The purpose was to get a wider understanding of what opinion people have and to get an answer and a result connected to the research question.

The majority of the participants agreed with each other that the risks are all relevant risks, according to how they have answered about microchip implants in humans. Even though many of the participants see the risks in the microchip implants a third of the participants could see themselves using a microchip in the future. But in total, the majority is not interested in getting a chip implemented. Despite this, there's a majority that believed it would be worth it to get a chip implemented even with the risk of it not functioning. We thought this was pretty interesting because of the arguments against each other. The majority are against getting chipped but the majority can also think of getting chipped even though the potential risk of it malfunctioning. We think this answer was because of different reasons. One is that the question might have been a little too hard to understand correctly. The other is that some people contradict themselves and we also believe this answer occurs because of the lack of knowledge that over 75 percent said they had. What we think is interesting is that many of the respondents think of this as an interesting subject while not knowing very much about it. We find it a little strange that something they like or feel is interesting does not make them more curious about the subject. This does not lead to anything relevant or anything we can use for the study, but we think that something that so many consider as interesting would be fun to be more knowledgeable about, especially in regards to today’s technology where you can easily get the information you are looking for, as long as you look for it.

The knowledge varied between the respondents and a lot of them said they were not knowledgeable but still many individuals had an opinion regarding the questions and risks. We thought it was odd to have an opinion about something that you do not know that much about and felt it was strange to comment on it. We did not believe it was very trustworthy to be listening to someone that did not have the knowledge but still had an opinion about the subject. We thought there were going to be more responses to the “No opinion” option since it was more logical to answer with a no if you do not have the knowledge about the subject. On four of the ten questions where the option of “No opinion” was available to have as an answer, we saw that only ten percent or more used that option. For us, that is a pretty low number since almost 77 percent were not knowledgeable enough about the topic which resulted in us believing there were going a more number of individuals that would had that as their answer.

The questions that mention integrity, tracking and monitoring and hacking are the questions that gave the clearest picture of what people thought. The majority agreed with the risks and what they could cause which was also backed up by what the previous theories said. We think that this was an expected result on the answers but we were a little surprised that the questions regarding if it is harmful for the body was not a part of this since this question was mentioned the most in the scientific articles that we read.

A lot of the participants believed that getting chipped could become a requirement from the employers in the future but did not want to get chipped according to the studies. How could this problem be solved? We believed it was important to maybe explain it in another way instead of forcing everyone to have a microchip inserted into their body. For example, they could say that this would help them as an employee and also the company could limit the functions on the inserted microchip. We also thought that it was really interesting that 22 percent of the participants did not have an opinion about a question like this that could potentially have a big impact on each person and instead have an opinion concerning more fact-oriented questions. An interesting thought while we looked at the answers was that around 30 percent could consider getting a chip but on the answers regarding the risks there was around 30 percent that saw it as a no- or a small risk. Could those be the same individuals that filled in these answers? It was nothing we could be sure about but only something we speculated about. We saw it as an interesting and worth mentioning observation. We thought it made sense but could not be sure that it was like that.

6.3 Comparing the two studies

The two studies had been very important for the study since these were the two steps that were needed to get a result that could be presented as an answer to the research question. The two studies had been in different sizes which meant that to compare these two to each other, all of the comparing was going to be presented in percentages because of the different numbers asked.

6.4 Differences

Between the two studies, some huge differences were seen. Harmful for the body was something that the six individuals in the first study saw as a huge problem and that everyone mentioned as a risk. In the survey, there were very divided opinions and the respondents did not see this as that big of a risk as much as the first respondents. In total there was 100 percent of the participants in the first survey and the second survey, there were 64,7 percent divided into the categories “Small risk” and “Risk” that saw harmful for the body as a risk. Another risk that was mentioned as different from each other was the risk regarding robbery. In the first study, there were 50 percent who mentioned robbery and in the second study, they were a little bit less, at around 38 percent. We believed it could have been like this because in the second survey the participants could perceive the question in a different way than the first participants did, for example, some might think robbery and being hacked was the same type of crime and therefore did not see this as a bigger or smaller problem.

In the interviews nobody mentioned integrity as a risk. Instead, tracking and monitoring were mentioned a lot which could be seen as a similar meaning to the concerns of the integrity aspects. The interview was more like a discussion with an open dialog where we had more of a conversation because we wanted the individual to be open and honest about all the risks that

they could come up with regarding microchip implementation in humans. The second study was more of a strict interview where we wanted the individual's opinion on already decided questions.

Some risks could be chosen even though they might not have even thought of it as a risk beforehand. This could have been due to someone mentioning a random risk in the first interview which then made it to the second interview as its own question. Because all questions were mandatory, they had to take a stand and share their opinions. One example of this type of question can be the risk regarding costs. There were only 33 percent in the first interview who had thought of it as a risk but when the question was asked again in the second interview circa 55 percent saw it as a risk, which was much higher.

In the first survey 100 percent said that they would not have a microchip implanted into their body and in the second interview there were 64,4 percent that were against microchip implants into their own body. We thought it was very unexpected that the opinions differed in each of the interviews. In the interview in the first study there were more open questions that were asked and therefore there were a lot of risks that had never been mentioned in the second study. In the survey the respondents could see different potential risks because the questions mentioned the most common ones. In the first study there were no alternatives to choose from for the respondents and therefore the participants did not get any information about potential risks. In the first interview no one could imagine themselves getting chipped but in the second study, more respondents were open to get one, around 29 percent were open to getting one.

6.5 Similarities

We believed it was important to have a mix of our respondents in both gender and age. Gender, because of the curiosity in different things and therefore we believed it was very important to have both men and women's opinions included in the result. The first interview was answered by fifty percent women and fifty percent men and in the second interview the participants were more randomly chosen to participate but was still almost fifty/fifty of men and women. This was a similarity we believed was important for our result since like mentioned above, interests can differ between genders in different topics and we wanted everyone's opinion in the ages 18 to 30 years old.

In both studies the majority of the participants had heard about microchip implants in humans before. Because this was a pretty new technology, we were a bit surprised that that many had heard about it. Answers that were similar to each other in the two studies were the questions regarding tracking, monitoring, and hacking. These results obviously showed that these risks are the biggest and most common opinions regarding microchip implants. It was expected that the respondent's answers would be the same concerning these risks because tracking, monitoring, and hacking are the risks that are mentioned and discussed most in existing facts and theories (Gadzheva 2007) (Claypoole, Balough 2012) (Muir 2007) (van Schaik, Paul et al 2017). Also, these risks are an issue in different areas for other electronic devices in society today. For example, smartphones, etc. Therefore, people recognize these risks that already exist and see this as the most common and biggest risk for microchip implants in humans as well.

7 Conclusion

Through combining the two conducted studies with previous theoretical framework and research, it is possible to answer the research question and create some conclusions regarding it. The study's research question is:

- *What is the opinion about microchip implants in humans for 18-30-year-old people in Borås, when it comes to risks in their daily life and the society?*

Based on the result from the studies, the following conclusion could be drawn:

- Knowledge: The majority of the respondents from the studies have heard about microchip implants in humans and seem interested but they do not have that much knowledge about it.
- Negative opinions: From the respondents, the majority have negative opinions about the technology. Their standpoint was that they would not implant a microchip into their own body.
- Harmful for the body: Harmful for the body is an opinion that is divided. One part of the target group sees it as the biggest risk and another part is the complete opposite and does not believe it would harm the body.
- Hacking & Tracking: The most obvious risks regarding microchips according to the target group is hacking, tracking and being monitored. These are the risks people are the most afraid of and these risks are connected to integrity and therefore the conclusion could be drawn that integrity was the biggest risk concerning microchip implant in human bodies.
- Necessity: Regardless of all risks that have been mentioned the majority of the target group does not seem to think that microchips are a necessary tool in daily life.

Hacked, tracked and being monitored can become a collective term that is identified as integrity. Integrity is one aspect that is common in theories and the two studies in this research. It seems like people and the general society are more afraid of mental injuries rather than physical injuries. Being mentally injured can be a risk of always feeling monitored, the risk of being hacked and damage to the one's personal integrity. Physically injured meaning, for example, harmful to the body. One factor that could probably affect the people feeling this way is the different views media and social actors have on the subject.

To compare what the participants, the facts and the theories says regarding the topic is it a result that is united to each other according to the risks if it is being chosen to get chipped or not. The facts that are used and given can as a result of this study be seen as matched to what people's opinions are in ages between 18-30 years old.

7.1 Further research

This research has been quite extensive and we feel it would have only been possible to go deeper into a few parts, for example only the integrity aspects including, being hacked, monitored and tracked. As further research, we suggest further qualitative in-depth studies of the subject in matters concerning knowledge, negative opinions, harmful for the body, hacking and tracking and last necessity. Instead of collecting even more data an in-depth study could be possible. An in-depth study includes a deeper analysis and uses the two steps axial and selective coding that has been described in the grounded theory.

Other aspects have not been mentioned in this report since the thesis did not contain relevant information that would have helped or strengthened the result but can still be of some interest to other parties. For example, there were no advantages in the survey since the focus was on risks, like the thesis says. But that does not mean that advantages were not an interesting aspect. It was simply an aspect that was not a part of this survey.

This study answered a research question on what opinion people have about a technology that is arising and still pretty foreign for people that they have no experience of microchips yet. Because of this, there was more interest in repeating this study again later on in the future when getting chipped is more accepted and common in our society and the possible use of the chip for different things like payments and keycards, compared to today. This technology can be compared to, for example, the internet that simply came and took over. People were a little skeptical about it and did not believe it was a necessary invention. Later on, the internet has taken over the world. We have no clue but maybe the chip will have some kind of similar impact on the individual and society in the future if this has been more accepted and common like the internet had on the society.

8 References

Biohacking (2019). *Allt om RFID-implantat.* https://biohacking.se/allt-om-rfid-implantat/ [2019-09-29]

Chipme (2018). *CHIPPET.* https://www.chipme.se/chip-under-huden [2019-12-18]

Clarke, Irvine & Flaherty, Theresa B (2008) RFID and Consumer Privacy. *Journal of Internet Commerce*. [Online] 7 (4), 513–527. [online]. Available from: http://www.tandfonline.com/doi/abs/10.1080/15332860802507370.
DOI: 10.1080/15332860802507370

Claypoole, Ted & Balough, Richard (2012) LOCATION TRACKING AND US LAW: HOW TECHNOLOGY ALTERS EXPECTATIONS. *Journal of Internet Law*. 24–31. [online]. Available from: http://search.proquest.com/docview/1151852328/.

Colin, R. (2002). Real World Research. 8.edition., Malden: Reference literature

Cronholm, S., Hjalmarsson, A. (2011). Mixed Methods in Use: Experiences from Combining Qualitative and Quantitative Approaches. *In proceedings of the 10th European conference on Research Methodology for Business and Management Studies*. Caen, France, June 20-21, 2011. / [ed] Marie Ashwin, 2011

Dinh, Angela (2008) RFID Systems in Healthcare. *Journal of AHIMA*. 79 (1), 62–63. [online]. Available from: http://search.proquest.com/docview/212619238/.

Forskning. (2019). *Fler hackar kroppen- för ett bekvämare liv.* https://www.forskning.se/2019/02/05/fler-hackar-kroppen-for-bekvamare-liv/ [2019-09-25]

Gadzheva, Maya (2007) Getting Chipped: To Ban or Not to Ban. *Information & Communications Technology Law*. [Online] 16 (3), 217–231. [online]. Available from: http://www.tandfonline.com/doi/abs/10.1080/13600830701680537.
DOI: 10.1080/13600830701680537

IT-ord (2019). *track.* https://it-ord.idg.se/ord/track/ [2019-12-18]

IT-ord (2019). *Remote monitoring and management.* https://it-ord.idg.se/?s=monitoring [2019-12-18]

Jervis, Colin (2005) RFID: security aid or breach of privacy? *The British Journal of Healthcare Computing & Information Management*. 22 (2), 41–43. [online]. Available from: http://search.proquest.com/docview/197279025/.

Jing, Qi et al. (2014) Security of the Internet of Things: perspectives and challenges. *Wireless Networks*. [Online] 20 (8), 2481–2501. [online]. Available from: http://search.proquest.com/docview/1612830100/

Kim, Byung-Seo et al. (2010) Feedback-assisted MAC protocol for real time traffic in high rate wireless personal area networks. *Wireless Networks*. [Online] 16 (4), 1109–1121.

Li, Huan-Bang & Kohno, Ryuji (2011) Standardization on Body Area Network and a Prototype System Based on UWB. *Journal of Medical Systems*. [Online] 35 (5), 1255–1263.

Lockton, Vance & Rosenberg, Richard (2005) RFID: The Next Serious Threat to Privacy. *Ethics and Information Technology*. [Online] 7 (4), 221–231.
Lunds Univeristet (2019). *Forskningsetik.* https://www.hb.se/Biblioteket/Skriva-och-referera/Referera-till-kallor/Guide-till-Harvardsystemet/Webbsidor-forum-bloggar-programvaror/Webbsidor-/ [2019-10-09]

Lu Shi et al. (2013) BANA: Body Area Network Authentication Exploiting Channel Characteristics. *IEEE Journal on Selected Areas in Communications*. [Online] 31 (9), 1803–1816.

Michael, Katina & Michael, MG (2013) The future prospects of embedded microchips in humans as unique identifiers: the risks versus the rewards. *Media, Culture & Society*. [Online] 35 (1), 78–86.

Michael, K., & Michael, M. (2013). The future prospects of embedded microchips in humans as unique identifiers: the risks versus the rewards. *Media, Culture & Society*, *35*(1), 78–86. https://doi.org/10.1177/0163443712464561

Monahan, Torin & Fisher, Jill A (2010) Implanting inequality: Empirical evidence of social and ethical risks of implantable radio-frequency identification (RFID) devices. *International Journal of Technology Assessment in Health Care*. [Online] 26 (4), 370–376.

Muir, Scott (2007) RFID security concerns. *Library Hi Tech*. [Online] 25 (1), 95–107.
DOI: 10.1108/07378830710735885

Mårtensson, R. (2018). Ökat intresse för att sätta in mikrochip i handen. *SVT Nyheter*. 8 april https://www.svt.se/nyheter/inrikes/stort-intresse-for-att-chippa-sig-i-handen

Nationalencyklopedin (2019). integrerad krets.
https://www.ne.se/uppslagsverk/encyklopedi/l%C3%A5ng/integrerad-krets [2019-09-25]

Neumann, Peter & Weinstein, Lauren (2006) Risks of RFID. *Communications of the ACM*. [Online] 49 (5), 136.
DOI: 10.1145/1125944.1125971

Polisen (2019). *Rån- utsatt.* https://polisen.se/utsatt-for-brott/olika-typer-av-brott/ran/ [2019-12-10]

Psykologiguiden (2019). *Likertskala.*
https://www.psykologiguiden.se/psykologilexikon?Lookup=Likertskala [2019-12-18]

Randall, A. (2012). RFID Can be Hacked: Here's How, & What You Can Do To Stay Safe. *Makeuseof.* 25 October https://www.makeuseof.com/tag/rfid-hacked-stay-safe/

Recker, J. (2012). *Scientific Research in Information Systems.* Queensland: Reference

Regeringen (2008). *Svensk bedömning av multilaterala organisationer-Världshälsoorganisationen, WHO.*https://www.regeringen.se/49c842/contentassets/ca2ecf234d214181a4ef508945d5c562/varldshalsoorganisationen-who)[2019-12-18]

Richardvanhooijdonk. (2017). Human Microchipping, The Benefits And Downsides. https://richardvanhooijdonk.com/blog/en/human-microchipping-the-benefits-and-downsides/?fbclid=IwAR1HtjgC5d6YBEMdVd6VaQUuGm0TBGeDlxEck5pm-CSjo55DR--v2oNs0xk [2019-09-25]

Rodriguez, Dario (2019) Chipping in at Work: Privacy Concerns Related to the Use of Body Microchip ('RFID') Implants in the Employer–Employee Context. *Iowa Law Review*. 1581–1611. [online]. Available from: http://search.proquest.com/docview/2212658515/.

Rohde, John & Toftegaard, Thomas (2011) Adapting Cognitive Radio Technology for Low-Power Wireless Personal Area Network Devices. *Wireless Personal Communications*. [Online] 58 (1), 111–123.

SFS 2003:460. *Lag om etikprövning av forskning som avser människor.* Stockholm: Utbildningsdepartementet.

Sime, M. (2016). St. Paul Animal Hospital Urges Microchipping Pets During Times of Change. *M2 Presswire ; Coventry*

Springer Proceedings in Physics, Time Domain Methods in Electrodynamics, pp.283-301

The Swedish National Council on Medical Ethics (2019). *Integritet.* http://www.smer.se/etik/integritet/ [2019-12-10]

SurveyMonkey (2019). *Variationer på den vanliga flervalsfrågan.* https://sv.surveymonkey.com/mp/multiple-choice-questions-everything-you-need-to-know/ [2019-12-18]

Szal, A. (2017). Wis. Tech Company To Offer Microchip Implants To Employees. *Manufacturing Business Technology; Rockaway.*

van Schaik, Paul et al. (2017) Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*. [Online] 75547–559

Voas, Jeffrey & Kshetri, Nir (2017) Human Tagging. *Computer*. [Online] 50 (10), 78–85. https://ieeexplore-ieee-org.lib.costello.pub.hb.se/document/8057311/references#references DOI: 10.1109/MC.2017.3641646

White, L. (2005). FDA Okays Implanted Chip for Health Care. *Information Management Journal.*

Yang, Li; Rida, Amin; Traille, Anya; Tentzeris, Manos M; Russer, Peter (Editor); Siart, Uwe (Editor) 2008

Yi-Hua Zhu et al. (2016) Network Coding-Based Reliable IPv6 Packet Delivery Over IEEE 802.15.4 Wireless Personal Area Networks. *IEEE Transactions on Vehicular Technology*. [Online] 65 (4), 2219–2230.

Appendix 1-First survey, interview

9 Interview: Microchip implant in humans

We are writing our bachelor thesis and examine the subject about microchip implants in humans. We are studying international marketing and IT at Borås University.

The purpose of our bachelor thesis was to find out what people of ages 18-30 years old think and their opinions about microchip implants in the human body. We will also investigate the interest in implementing and using microchips despite possible risks that can arise.

We are going to do six interviews with both men and women and we are going to choose individuals with varied skills regarding IT. The answers were to be put together and analyzed and later on we created create a survey that was based on the first six interviews. The intention with this was to get a survey in very high quality in both questions and answers.

To participate was optional and you had the right to cancel at any time. The participants were anonymous and when the result was done the participants would have a chance to get the report and the final result, which would be finished by January 14th.

Since microchip implants in humans is a new technology, we needed to give a brief explanation of what it was before we could start asking our questions.

A microchip implant is a small chip (around one centimeter in size) that you place into your arm under your skin. Today, the chip is a passive chip which means it is inactivated and therefore limited to a few applications like id-card, different kinds of payment methods and keycards.

To develop and expand the views and uses of the chip, the chip needs to be activated. A chip contains sensitive data and an activated chip has a greater risk that sensitive data can be exposed to various threats and risks.

Age:

Gender: Male Female

Knowledge about IT: Very bad
Bad
Okay
Good
Very good

1. Have you heard anything about microchip implants before?

2. What risks do you think microchip implants can cause?

- Why do you think these risks?

3. How would you describe the risks for the individual?

4. How would you describe the risks for the society?

5. What is your opinion about microchip implants?

6. Can you see yourself with a microchip in your body?

Appendix 2 – Survey construction

10 Survey questions based on interviews and existing theories

To get a deeper understanding of the survey, we wanted to show what the questions were based on and why the questions were a part of the survey and also with the facts that strengthen the relevance for each question. Each number specified each question in the survey.

1.This question was based on earlier a questionnaire from the first interview that was made.

2.This question was based on the earlier question, as a follow-up, to see how knowledgeable the participant was regarding the subject.

3.This question was relevant for the survey, with a purpose to reflect over the answers and analyze if there were eventual connections.

4.This question was based on an earlier interview where the anonymous participants believed that a threat to their own privacy was one of the risks.

According to Gadzheva, she says that microchip implementation is a bad thing since their privacy can be threatened and constantly be tracked (Gadzheva 2007). Today privacy concerns are one of the issues in talks and debates regarding implementation of microchip (Rodriguez 2019).

5. This question was based on the respondents where one of the respondents described it as the biggest risk. One of six individuals talked about this specific risk, this question was relevant since this was mentioned often in many contexts concerning microchip implants.

Society is, today, interconnected and electronic devices are highly developed and most of the devices are connected to computer software. The data collects and analyzes which makes it easy for stakeholders to track and monitor individuals. The information reduces the integrity and different interests get more control over inhabitant and individuals (Claypoole, Balough 2012).

6.The question was based on one of the mentioned risks from the previous questionnaire where the participants saw this risk as an important one.

By buying a reader that has the technical expertise to for example track and find people that use microchips and later on scan them without their consent/knowledge (Gadzheva 2007). Hackers have the chance to steal content from a microchip and get away with it since it is almost impossible to find them (Dinh 2008).

7.The majority of the respondents mentioned that microchip implants are probably harmful to the body. The risks about health was a relevant question because biohacking humans is a pretty new technology and people seem to be scared since a lot of them mention it in the interview.

Facts: Nothing gives assurances that a microchip implant is completely safe for the body. There are several potential health risks and side effects like electronic risks, impact on tissue reactions and surgery mistakes (Gadzheva 2007).

8.A lot of the respondents mentioned that one of the risks was being robbed in some way of your chip that is inside your body. This risk was very relevant because there are many people who are thinking about the same thing.

The chip does not need its actual owner to be used, which makes the risk of getting robbed higher. Robbers without knowledge about IT or how to hack might use more violent methods to try and steal the chip (Gadzheva 2007). You can also be hurt in an economical way by the robbers obtaining the chip (Neumann, Weinstein 2006).

9. This question was based on an earlier interview where one of the mentioned risks for our society was the cost that could emerge, both for the individual and the public.

The price depended on different things such as, what it is going to be used for, the frequency and what different functions the tag needs (Colin 2005). For an individual living in Sweden, the cost to put it into their body is 1500 Swedish crowns and takes around 30 minutes (chipme.se 2019).

10.This question is based on the first interview where some were wondering what would happen if the chip stopped functioning.

There could be a collision between the RFID tags and the readers in different situations if there were too many chips around the reader at the same time. It would confuse the readers and data from the tags could not be read correctly, this situation would lead to collisions (Jing, Vasilakos, Wan, Lu & Qiu 2014). Computer crashes might arise and affect the use of the chip (Gadzheva 2007).

11.Monitoring is a risk that can occur from community actors. The respondents raised that aspect in the interviews and described it as an important question. An offer to chip an employee has become more common and the technology has expanded which would probably become standard in the near future. If it continues at the same rate, there is a risk that employer will mandatorily chip their own employees in the future (Rodriguez 2019).

12. This question is based on the opinion that the people have, and since our purpose of this thesis was to know if they had positive or negative thoughts about microchipping even when they knew of the risks. This question was mentioned in our first interview where the majority were positive towards using it in the future if it had been more developed than it is today and was necessary for our results.

Appendix 3 – Second survey

11 Survey: Microchip implant in humans

We are writing our bachelor thesis and we are examine the subject about microchip implants in humans. We are studying international marketing and IT at Borås University.

The purpose of our bachelor thesis was to find out what people of ages 18-30 years old think and have for opinions about microchip implants in the human body. We will also investigate the interest in implementing and using microchips despite possible risks that can arise.

To be able to do our study and get more knowledge on the subject we used a survey. We needed a big sample and therefore asked 100 individuals to answer twelve questions.

This survey question was based on earlier interviews where respondents with varied ages, genders, and skills about IT answered questions regarding microchip implants in humans. The intention was to get a survey in very high quality in both questions and answers.

To participate was optional and you had the right to cancel at any time. The participants were anonymous and when the result was done the participants would have a chance to get the report and the final result, which would be finished by January 14th.

Since microchip implants in humans is a new technology, we needed to give a brief explanation of what it was before we could start asking our questions

A microchip implant is a small chip (around one centimeter in size) that you place into your arm under your skin. Today, the chip is a passive chip which means it is inactivated and therefore limited to a few applications like id-card, different kinds of payment methods and keycards.

To develop and expand the views and uses of the chip, the chip needs to be activated. A chip contains sensitive data and an activated chip has a greater risk that sensitive data can be exposed to various threats and risks.

This survey had “Yes” or “No” questions and also questions with 1-4 options where one is the lowest and four is the highest. There was also an alternative “No opinion”/” never heard” option that equals a zero.

Age: _____ Years old

Gender: Female Male

Current occupation: _____

Mail: _____

Please, ring that option that best suits you.

Have you ever heard of microchip implants in humans before?

Yes No

This question is based on earlier questionnaire from the first interview that was made.

If you answered yes, what do you currently know about microchip implants in humans?

1 2 3 4

This question was based on the earlier question, as a follow-up, to see how knowledgeable the participant was regarding the subject.

Do you think this is an interesting subject/topic?

1 2 3 4 0

This question was relevant for the survey, with a purpose to reflect over the answers and analyze if there were eventual connections.

The risks that the participants talked about in the earlier interview is this down under, do you agree that this is relevant risks as a private person?

Your privacy is more at risk of getting exposed?

1 2 3 4 0

This question was based on an earlier interview where the anonymous participants believed that a threat to their own privacy was one of the risks.

According to Gadzheva, she says that microchip implementation is a bad thing since their privacy can be threatened and constantly be tracked (Gadzheva 2007). Today privacy concerns are one of the issues in talks and debates regarding implementation of microchip (Rodriguez 2019).

The risk of being tracked and monitored?

1 2 3 4 0

This question was based on the respondents where one of the respondents described it as the biggest risk. One of six individuals talked about this specific risk, this question was relevant since this was mentioned often in many contexts concerning microchip implants.

Society is, today, interconnected and electronic devices are highly developed and most of the devices are connected to computer software. The data collects and analyzes which makes it easy for stakeholders to track and monitor individuals. The information reduces the integrity and different interests get more control over inhabitant and individuals (Claypoole, Balough 2012).

The risk of being hacked?

1 2 3 4 0

The question was based on one of the mentioned risks from the previous questionnaire where the participants saw this risk as an important one.

By buying a reader that has the technical expertise to for example track and find people that use microchips and later on scan them without their consent/knowledge (Gadzheva 2007). Hackers have the chance to steal content from a microchip and get away with it since it is almost impossible to find them (Dinh 2008).

The risk from a perspective of health?

1 2 3 4 0

The majority of the respondents mentioned that microchip implants are probably harmful to the body. The risks about health was a relevant question because biohacking humans is a pretty new technology and people seem to be scared since a lot of them mention it in the interview.

Facts: Nothing gives assurances that a microchip implant is completely safe for the body. There are several potential health risks and side effects like electronic risks, impact on tissue reactions and surgery mistakes (Gadzheva 2007).

The risk of getting robbed of your implanted microchip?

1 2 3 4 0

A lot of the respondents mentioned that one of the risks was being robbed in some way of your chip that is inside your body. This risk was very relevant because there are many people who are thinking about the same thing.

The chip does not need its actual owner to be used, which makes the risk of getting robbed higher. Robbers without knowledge about IT or how to hack might use more violent methods to try and steal the chip (Gadzheva 2007). You can also be hurt in an economical way by the robbers obtaining the chip (Neumann, Weinstein 2006).

The risks that the participants talked about in the earlier interview is down under, do you agree that these are relevant risks as a society?

The risks that the participants talked about in the earlier interview is this down under, do you agree that this is relevant risks as a society?

The microchip implants generate costs for the individual and society?

1 2 3 4 0

This question was based on an earlier interview where one of the mentioned risks for our society was the cost that could emerge, both for the individual and the public.

The price depended on different things such as, what it is going to be used for, the frequency and what different functions the tag needs (Colin 2005). For an individual living in Sweden, the cost to put it into their body is 1500 Swedish crowns and takes around 30 minutes (chipme 2019).

Is the microchip worth using if there is a chance that it can suddenly stop functioning?

Yes No No opinion

This question is based on the first interview where some were wondering what would happen if the chip stopped functioning.

There could be a collision between the RFID tags and the readers in different situations if there were too many chips around the reader at the same time. It would confuse the readers and data from the tags could not be read correctly, this situation would lead to collisions (Jing, Vasilakos, Wan, Lu & Qiu 2014). Computer crashes might arise and affect the use of the chip (Gadzheva 2007).

How big is he probability of your employer or the government demanding implants of microchips into your body as a requirement in the future?

1 2 3 4 0

Monitoring is a risk that can occur from community actors. The respondents raised that aspect in the interviews and described it as an important question.

An offer to chip an employee has become more common and the technology has expanded which would probably become standard in the near future. If it continues at the same rate, there is a risk that employer will mandatorily chip their own employees in the future (Rodriguez 2019).

Are you for or against the thought of having a microchip inserted into your body?

1 2 3 4 0

This question is based on the opinion that the people have, and since our purpose of this thesis was to know if they had positive or negative thoughts about microchipping even when they knew of the risks. This question was mentioned in our first interview where the majority were positive towards using it in the future if it had been more developed than it is today and was necessary for our result

HÖGSKOLAN
I BORÅS

Besöksadress: Allégatan 1 · Postadress: 501 90 Borås · Tfn: 033-435 40 00 · E-post: registrator@hb.se · Webb: www.hb.se