h e g

Haute école de gestion
Genève

The Digital Privacy Paradox

Bachelor Project submitted for the degree of
Bachelor of Science HES in International Business Management

by

Gina ZURBRIGGEN

Bachelor Project Mentor:
Gabor MARKUS

Geneva, date of submission
Haute école de gestion de Genève (HEG-GE)
International Business Management

Hes·so GENÈVE
Haute Ecole Spécialisée
de Suisse occidentale

Disclaimer

This report is submitted as part of the final examination requirements of the Haute école de gestion de Genève, for the Bachelor of Science HES-SO in International Business Management. The use of any conclusions or recommendations made in or based upon this report, with no prejudice to their value, engages the responsibility neither of the author, nor the author's mentor, nor the jury members nor the HEG or any of its employees.

Acknowledgements

First and foremost, I would like to thank my advisor Mr. Gabor Markus, Professor at the Haute Ecole de Gestion de Genève of the course Digital Marketing.

Further, I would like to express my gratitude to Mrs. Rahel Hadzi for her support. She took out the time to discuss different stages of my research. Additionally, we often debated different concepts concerning the online privacy problematic, which encouraged me to look at the issue from different angles. She helped me to stay focused on the main topic of the thesis and gave me highly appreciated constructive advice.

Lastly, I would like to thank all the survey participants for their time and participation in the experimental survey.

Executive Summary

Over the past 10 years, numerous scandals involving personal data shocked the world. In 2013, whistle blower Edward Snowden came forward and disclosed various worldwide government surveillance programs (Jill Lepore, 2019). In 2018 the Cambridge Analytica scandal erupted, revealing that the so-called behavior changing agency had without consent harvested the personal data of millions of people's Facebook profiles and used it for political advertising purposes (Steve Andriole, 2019). Those and other distressing revelations made consumers worldwide more aware of the value and misusage of their personal data. Despite the newfound awareness, consumers make little to no change to their online behavior and keep using applications that have been proven to invade their privacy. This inconstancy between the consumers privacy concerns and their behavior online is known as Digital Privacy Paradox (Spyros Kokolakis, 2015).

The Rational Choice Theory is suggesting that individuals make reasonable and logical decisions in order to create the greatest benefit or satisfaction. However, to explain the paradoxical online consumer behavior solely with this theory is over simplified, insufficient and does not lead to a substantially better understanding. The Rational Choice Approach is lacking in the necessary incorporation of emotional and of behavioral aspects. Online and offline, many actions are driven by irrational affective factors. This irrational online behavior is caused by faulty estimation of risks and potential threats. Consumer risk assessment is strongly influenced by benefit and emotional biases (Susanne Barth, Menno D.T. de Jong 2017) (Christoph Lutz, PePe Strathoff, 2014).

The mean to resolve the paradox turned out to be trust, because if consumers trusted online companies the Digital Privacy Paradox would then be solved (Christoph Lutz, PePe Strathoff, 2014). Those findings raise the question of whether tech giants or social media enterprises should change their data collection policies. Accompanying the ethical problem of invading the privacy of consumers, a climate of distrust has proven to be dissatisfying in the long run and to have a strong negative economic impact. Additionally, consumer expectations are changing. Younger generations tend to be less accepting of business culture, that is solely focused on making quick profits. Over the past few years there has been a significant systemic shift towards purposeful business and responsible capitalism. Facing the new reality, companies need to reconsider what role their organization is playing in society to ensure long-term success (Milton Cheng, 2020).

Contents

List of Tables

List of Figures

1. Introduction

1.1 Importance of the Internet

Since the invention of the internet the world is being transformed by digital innovations. Exiting technical breakthroughs such as self-driving cars, a leap forward in Artificial Intelligence and augmented reality. Digital innovation is reshaping industries by disrupting existing businesses and models. However, it also had a huge impact on society, presenting new opportunities and challenges. The cheaper and better technology is helping in creating a more connected world. In 2018, 8 billion devices are connected to the internet. It is estimated that the number of devices will increase to 1 trillion in 2030 (World Economic Forum, 2018).

1.1.1 Changes the Internet brought to Consumer

While working at CERN in Geneva, the British scientist Tim Berners-Lee invented the World Wide Web in 1989 (CERN, 2020). The World Wide Web is the most popular and widely used system to access the internet (Jessika Toothman, 2008). It was initially developed for automated information-sharing between scientists in universities and institutes around the world (CERN, 2020). Tim Berners-Lee founded in 1994 the World Wide Web Consortium to ensure that the World Wide Web was made freely available for all. In 2009 he founded the World Wide Web Foundation, which has the mission is to empower humanity and use the World Wide Web for positive change. The foundation envisions that everyone regardless of language, ability, location, gender, age or income, should be able to communicate and collaborate, create valued content, and access the information that they need to improve their lives and communities (World Wide Web Foundation, 2020). In fact, the rise of the internet in the recent decades has had transformative impact on society, including communication, social interactions and access to knowledge. The internet has become the preferred method of communication. Freed from geographical and time restrictions, there is a dizzying wide range of communication possibilities, transforming communication practices. Instead of keeping up with the news by reading the newspaper once a day, it is possible to read constantly updated news sources worldwide. Other examples are ordering food, buying clothes or sharing moments with friends. Information technology also has brought fundamental change to education, government, businesses and the way we interact with each other (Zaryn Dentze, 2013). The increased importance of the internet is visible by looking at

the amount of time consumer spend online. The global daily internet usage per capita has increased form 75min in 2011 to 170min in 2019. It is forecasted that the amount of time spend online will further increase 192min per capita in 2021 (Statista, 2019). After the recent shift towards home office and online teaching due to the coronavirus, it is likely that the increase in time spend online will be even a lot higher than forecasted by Statista in 2019.

The internet is supposed to be for everyone and connectivity around the world is growing fast. In 2019, 96.6% of individuals in developed countries are using the internet. However, worldwide only 53.6% of individuals are having access to the internet. In developing countries, 47% have access to the internet and on the continent of Africa only 28.2% have access. It is estimated that in the least developed countries only 19.1% have access. The access to the internet is essential for empowerment of underprivileged groups, especially for women. The data shows, that there is a disparity in access to the internet according to gender. Worldwide 58.3% of man have access versus 48.4% of women. Whereas the difference between male and female in the developed countries only is 1.6%, in the developing countries the difference is 12.1% and in the least developed countries 10.5% (Statista, 2019). It is important to note that to improve connectivity it is not as simple as giving people an internet connection. There a multiple, multi-dimensional factors contributing to digital divides, such as gender inequality, access to education, lack of technological skills, lack of human capacity and lack of locally relevant content. There is a risk that technological innovations create further digital inequality between those who are connected and those who are not. This inequality affects jobs, education and economic performance of countries. There is a big risk that people without proper education and access to technology will be left behind. On the other side the internet can be used to address divides within a society. In Pakistan 70% of medical students are women and most women prefer to consult a female doctor. However, due to cultural reasons only 20-30% of practicing doctors are women. New technology enables women in Pakistan to consult a female doctor by remote consultations (Erika Huizer, 2017).

While early adopters in the 90’s mainly saw the possibilities of using the internet such as the ability to express themselves openly, freely and also securely. More recently questions about the risk the internet poses have arisen. Due to the felt anonymity people speak freely, but there is often no shared moral and/or cultural code influencing how

people behave online. In the real-world hate speech can provoke actions that can threaten the personal safety of many. In 2017 the Cameroon's government shut down the internet for the English-speaking part of the country for 93 days, stating that the internet was used as a tool to spread country internal division and hatred. In that case the UN Special Rapporteur of freedom of expression condemned the government's action as an "appalling violation" of the freedom of speech (Erika Huizer, 2017). Other issues include the spread of false and misleading information, influence in elections, recruitment and radicalization of potential terrorists. Other concerns are the changes in social interaction, and whether the internet has a negative impact on social norms.

1.1.2 Changes the Internet brought to Businesses

Nowadays, it has almost become unimaginable to conduct business without relying on the internet (Vijay K Sharama, 2019). Broadband or high-speed internet access has become a basic necessity for economic and human development in both developed and developing countries. However, for many countries it is a big challenge to expand broadband access to rural areas, which can create digital inequality within countries. The digital inequality has a disproportionate impact on rural communities and the poor. These disparities hamper economic development and constrain access to pathways out of poverty (World Bank, 2020). The internet revolution did not only facilitate company internal and external communication and had a big influence on consumer expectations, but the internet created a large array of new opportunities. Businesses are able to reach, target and attract more consumers and to grow sales with engaging digital content, campaigns, personalization and branding. Using new tools such as digital marketing, cloud computing, online automation tools, e-commerce and artificial intelligence can help businesses to create a competitive advantage. Additionally, new tools enabled companies to let their staff work remotely or to develop employee's skills via online trainings. Those can have a positive effect on the employee's satisfaction and productiveness, and it can reduce costs. The ability to create growth, have marketing opportunities and make profit online had a positive impact on entrepreneurship, but has also increased the competition online (Vijay K Sharama, 2019).

To create value and built meaningful relationships with consumers, businesses must first gain a deep insight into what consumer want and need. Such insights come from good marketing information and are used to create a competitive advantage. With the internet consumer themselves are generating tons of marketing information. Companies are far from lacking information, which led in the early 2000s to the creation of the term Big Data.

Big Data refers to data that is so large, fast or complex that it is difficult to process it with traditional methods. It presents businesses both with big opportunities and challenges. Big Data can help to get precious consumer insights but accessing and sifting through the data can be difficult and time intensive. Today, businesses do not need more information, but they need valuable information (Philip Kotler, Gary Armstrong,2018).

1.2 Issue Definition

Over the past 10 years, multiple scandals involving personal data collection have shocked the world. In 2013**,** the former Central Intelligence Agency (CIA) employee Edward Snowden came forward and leaked classified National Security Data (NSA) disclosing numerous worldwide surveillance programs invading people's privacy. In 2018 the Cambridge Analytica scandal erupted, revealing that the so-called behavior changing agency had without consent harvested the personal data of millions of people's Facebook profiles and used it for political advertising purposes. The consulting firm is known to have had a role in UK's Brexit campaign and the elections of the American politicians Ted Cruz and Donald Trump. In 2019, the Netflix documentary "The Great Hack" investigated Cambridge Analytica's role in harvesting personal data and using it for political purposes. The documentary shines light on the fact, that the consulting firm has not only influenced elections in the United States and the United Kingdom, but that the firm has influenced many elections for worldwide. For example, the 2015 elections in Trinidad and Tobago, in which young citizens from a particular ethnical background where encouraged not to vote. Subsequently, the party that is alleged to have hired Cambridge Analytica won the elections. The documentary goes further and describes how data can be used to categorize people, and how companies can influence and manipulate consumer (Steve Andriole, 2019). A recent alarming report from the Norwegian Consumer Council revealed that 10 apps, among them Tinder and Grindr, had collected and sold sensitive consumer data, such as sexual orientation, political beliefs and drugs use, to over 135 different companies (City Am, 2020).

Early 2020, the New York times published an article about a new groundbreaking application called Clearview AI. The facial recognition app that goes far beyond anything ever constructed by the United States Government or the Silicon Valley. On the Clearview AI application, a picture of a person can be uploaded, and the application will display all the public photos of that person. The application has collected over three

billion photos from Facebook, YouTube, Venmo and millions of other websites. In comparison the Los Angeles police force has access to about 8 million photos and the FBI to about 411 million photos. In contrast to other similar applications, Clearview AI can process pictures of individuals wearing hats, glasses or pictures only partially showing a person's face. This leads to matches up to 75% of the time. However, it is not clear how often the tool delivers false matches and it has not yet been tested by an independent party. In 2020, multiple U.S. police forces as well as U.S. and Canadian Federal Law enforcements are testing the application. It is important to note that photos uploaded are automatically stored by Clearview AI, which enables Clearview AI to collect a data base on people searched by law enforcement. The founder of the application Ton-That was stating that despite high offers, he is not planning on making his application public or selling it to "bad" governments. It is concerning that a CEO of such a powerful application can decide to whom he is selling and that citizens must trust him on the judgement of which government is a "bad" one. Additionally, it is highly possible that a copycat of the Clearview AIapplication emerges (New York Times, 2020) (The Daily, 2020).

Those and many other shocking revelations about the increasing invasion of privacy, made consumer worldwide more aware of the (mis)usage and value of their personal data. In December 2019, Amnesty International found that more than 70% of consumer in nine countries were worried about data collection and usage. But most consumer do not change their online behavior (City AM, 2020). For example, general anger was directed to Facebook's poor response to the Cambridge Analytica scandal and for a while #DeleteFacebook was trending on Twitter, encouraging users to delete their Facebook application and their profile. Despite the huge Scandal it seems that many Facebook users stayed with the social media platform or stopped using the Facebook application, but were spending more time on Instagram, which of course is owned by Facebook (Menafn.com, 2018). In 2019, Facebook was more profitable than ever as consumer nevertheless continue to use the services that undermine their privacy (John Naughton, 2019).

In the meantime, the value of data has surpassed the value of oil. Throughout history, oil has been the most valuable resource. Those, who controlled oil have controlled the economy. However, today data is playing a crucial economical role (Therese Fauerbach, 2020). Despite the consumers new gained awareness of the collection, (mis)usage and value of their personal data and the increasing privacy concerns, consumer do not

change their privacy behavior, provide personal information online and keep using online services. The inconstancy of consumers privacy attitudes and privacy behavior is referred as Digital Privacy Paradox. Consumer seem to value convenience and personalization over privacy (Spyros Kokolakis, 2015).

In May 2018, General Data Protection Regulation (GDPR) was implemented in the EU, which impacts all companies that are either selling to or storing information about EU citizens (Jennifer Lunn, 2019). The GDPR was forcing many companies worldwide to update their privacy regulations. Currently the European Union is working on a draft called the ePrivacy Regulation. The current draft focuses on rules for advertisers accessing consumer's electronic devices. The regulation would require that consumer provide consent before a company can access their device, which includes the reading and writing of cookies (Ari Levenfeld, 2019). In the United States 25 states have laws that address data security practices of private sector entities (NCAL, 2019). The California Privacy Act has some similarities with GDPR but is not nearly as extensive. It is holding businesses that operate in the state of California or collect information about California residents responsible for how they collect, share and secure consumer information. The law is aimed to empower consumers and to give insides into what information is collected and sold (Ari Levenfeld, 2019). The state of Vermont also introduced a Privacy law that is aiming to provide further transparency for consumers and regulates what companies can do with consumer data. Canada has introduced the Personal Information Protection and Electronic Documents Act (PIPEDA) by making user consent and transparency a top priority. The law includes ten fair information principles such as accountability, consent, accuracy and safeguards (Ari Levenfeld, 2019). It is likely that in the future more governments will implement similar or other data regulation privacy laws, which will make it more difficult for companies to store or collect user data (Jennifer Lunn, 2019).

Even though, there has been extensive research to proof the existents of the Digital Privacy Paradox, it is a complex phenomenon and a very current subject that requires further research. The aim of this work is to gather existing information to gain an improved understanding of the complex paradox. Further, to offer solutions on how tech giants and social media companies can address privacy concerns of their consumers and (re)built trust, while keep being able to personalize their products and gain valuable marketing insides.

1.3 Organization of the Thesis

1.3.1 Analyzing existing data

In a first part of this work, I will analyze the research and information on the Digital Privacy Paradox. And answer questions such as: What are the reasons for such a paradox? Why are people so easily willing to give up their data? What are the advantages for companies? What effects does the new data privacy awareness have on business? How can companies not just collect consumer data and personalize their products and services, but at the same time gain consumer trust?

1.3.2 Experimental design

The second part of this work will use a survey experiment to understand more about the effects of positive and negative information concerning data collection on the user behavior and answer the following hypothesis:

H1: User's privacy concerns and behavior will change according to the content of the news article they read

H2: Depending on the article participants receive they will be willing to pay a higher/ lower price to protect their data

2. Literature review

2.1 Privacy Definition

There is no universal definition for privacy. The definition and perception of privacy differs according to societies, cultures and economic environment. Additionally, the definition of privacy depends on the concrete situation and on context; sharing the same information in different situation might be perceived differently. According to the American law professor Alan Westin, there are three different factors that affect privacy norms: the political, the socio-cultural and the personal level (Lukacs Adrienn, 2016).

Privacy can be defined as “right to be free from unwarranted intrusion and to keep certain matters from public view” (Oxford Dictionary of Law, 2015). And as such, “privacy is an important element in the autonomy of the individual. Much of what makes us human comes from our interactions with others within a private sphere where we assume no one is observing. Privacy, thus relates to what we say, what we do, and perhaps even what we feel” (MacMenemy 2016). Privacy is about the autonomy of a person and “protects our subjectivity from the pervasive efforts of commercial and government actors to render individual and communities fixed, transparent and predictable. Privacy is an indispensable feature of a democracy where an individual maintains his identity while contributing to their civic duty” (Cohen 2016) (Corpus, 2016).

Privacy can be distinguished in three different aspects: (a) territorial privacy, which concerns the physical area around a person, (b) privacy of a person, which concerns the protection against physical undue interference, such as physical research, (c) information privacy, which concerns whether and how personal data can be gathered, stored, processed and disseminated. Online data collection, usage and storage is referring to the to the third aspect of privacy (Spyros Kokolakis, 2015).

2.2 Right to Privacy

In 1945 and 1948, the Universal Declaration of Human Rights was adopted by the General Assembly. Since then, the United Nations has expanded the human rights laws to vulnerable groups of society such as children, women, persons with disability or minorities. Human rights are rights for all human beings, regardless of gender, sex, age, religion, ethnicity or any other statues. Rights include the right to life and liberty, freedom

from slavery and torture, and freedom of opinion and expression. It also includes the Right to Privacy. All governments have the obligation and responsibility to respect and protect those laws and to refrain from certain actions (United Nations website).

The Right to Privacy is a fundamental human right, essential to autonomy and protections of persons dignity. Privacy rights enables persons to create barriers and manage personal boundaries to be protected from unwanted interference in their lives such as who has access to our bodies, places and things, as well as our communication and personal information. As a result, the Right to Privacy is essential in protecting persons against arbitrary and unjustified use of power. The Right to Privacy allows persons to space to themselves without judgement, to think freely without discrimination and control over their personal information (Privacy International, 2017).

2.2.1 Universal Declaration of Human Rights

The Right to Privacy is defined in Article 12 and enshrined in the Articles 14.1 and 17.1 of the Universal Declaration of Human Rights. Additionally, it is contained in the Articles 16 and 40 in the Convention on the Rights of the Child, Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 22 of the Convention on the Rights of Persons with Disabilities and Article 4 of the African Charter on Human and Peoples 'Rights (Claiming Human Rights, 2008).

2.2.1.1 Article 12 Right to Privacy

"No one shall be subjected **to arbitrary interference with his privacy**, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks (Claiming Human Rights, 2008)."

2.2.1.2 Article 14.1 Right to Asylum

"All persons shall be equal before the courts and tribunals. In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law. The press and the public may be excluded from all or part of a trial for reasons of morals, public order (ordre public) or national security in a democratic society, or when the interest of the **private lives of the parties so requires**,

or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice; but any judgement rendered in a criminal case or in a suit at law shall be made public except where the interest of juvenile persons otherwise requires or the proceedings concern matrimonial disputes or the guardianship of children (Claiming Human Rights, 2008) ."

2.2.1.3 Article 17.1 Right to Own Property

"No one shall be subjected to **arbitrary or unlawful interference with his privacy**, family, home or correspondence, nor to unlawful attacks on his honour and reputation (Claiming Human Rights, 2008)."

2.3 Digital Privacy Paradox

The internet has become indispensable to consumers lives. Working, studying and passing time using the internet has become the norm and social networks are thriving. However, while online shopping, using e-banking, social networks or other services, consumers provide an enormous amount of personal data. This data is collected in various ways e.g. by internet companies and social networks. In this digital age, companies use the significant quantity of date available to create detailed descriptions and profiles of individuals. The resulting profiles can be used for personalized content, marketing campaigns and advertising (Christoph Lutz, PePe Strathoff, 2014).

The extend of the usage of the personal data is often unknown to consumer. The convenience of the internet stands into stark contrast with the downsides e.g. being traceable or becoming a target of personalized advertising. Many consumers embrace the online services but still worry about the risks and the negative consequences. Those sentiments are reflected in countless surveys concerning data privacy and online behavior. Many surveys show that for most consumers privacy is a primary concern, that consumers want to protect themselves from data collection and guard their privacy. The third-party usage of data is seen with particular care and that consumers have gained new awareness about the collection of data, which makes data privacy a very current topic (Henner Gimpel, Dominikus Kleindienst, Daniela Waldmann, 2018) (Spyros Kokolakis, 2015) (Christoph Lutz, PePe Strathoff, 2014).

However, despite being more aware, consumers are usually unable to estimate the risks and the amount of economic value of their data. Therefore, consumer tend to behave irrational in terms of the risk-benefit tradeoffs. They are not protecting themselves enough and disclose private information for relatively small rewards such as attention from peers. The urge to take advantage from the opportunities the internet offers seem to outweigh the concerns. The inconsistency between privacy concerns and behavior online is referred as the Digital Privacy Paradox. Privacy concerns are not correlated with taking action e.g. restricting privacy settings, using alternative search engines or deleting cookies (Henner Gimpel, Dominikus Kleindienst, Daniela Waldmann, 2018) (Spyros Kokolakis, 2015) (Christoph Lutz, PePe Strathoff, 2014).

The growth of Information and Communication Technology amplifies the data privacy problematic. Mobile applications and social media have the ability to collect an enormous amount of sensitive consumer data such as photos, location information or contact lists. Despite the knowledge of those risks, consumers continue to download install and to use mobile applications. Additionally, consumer hardly pay attention to or are able to comprehend the applications terms, conditions and permissions. Next to benefits of saving time, pleasure and practically usage, social pressure is an additional reason for many consumers to use mobile applications. The vulnerability of consumer in terms of digital services leads to the loss of control over their personal data and unwanted data disclosure. This vulnerability is exploited by digital service providers. They offer free digital services, but in exchange collet the user's personal data. Often the biggest part of those companies' revenue is based on data collection. More recently the handling of consumer data became more important, as it could have an influence on the services providers reputation, thus their economic success (Henner Gimpel, Dominikus Kleindienst, Daniela Waldmann, 2018).

The Digital Privacy Paradox has significant implications for e-commerce, social networks as well as for government regulations. E-commerce and social networks are collectors of vast amounts of personal data, a proof of the Digital Privacy Paradox encourages them to increase the collection and use of personal data. On the other hand, government policy makers justify privacy regulations on peoples increased privacy concerns. However, the inconsistency between consumers attitude and actual behavior weakens the governments justification for stricter regulations (Spyros Kokolakis, 2015).

2.3.1 Risk-Benefit Calculations

Risk-benefit calculations play a major rule in consumers assessment and the decision to share personal information. The cognitive style of decision-making during risk-benefit is both analytical and conscious, intention and actual behavior is influenced by expected benefits but also negatively affected by associated costs. The Rational Choice Theory of Human Behavior is suggesting that an individual's decisions are always made reasonable and logical in order to create the greatest benefit or satisfaction. Individuals seek to maximize utility and minimize risk through rational decision making. For example, the theory suggests that using social media, consumer base their decision making on perceived benefits such as networking with friends and acquaintances and perceived risks such as privacy intrusion. However, many researchers found that small rewards, tangible or intangible, heavily influence the consumers decision making and risk assessment. Often perceived benefits outweigh perceived risks, which leads to the neglection of privacy concerns. Meaning that the benefits of personalization, convenience and social benefits tend to outweigh the perceived risks. Seemingly consumer tend to concentrate on the benefits instead of their stated concern or potential future risks (Susanne Barth, Menno D.T. de Jong 2017).

Small rewards play a very prominent role in behavior online, such so that many scholars question whether they could be an explanation for the Digital Privacy Paradox. Many consumers despite being wary about the giving up their personal information, are willing to trade off their privacy for immediate rewards (Yong Jin Park, Scott W. Campbell, Nojin Kwak, 2012). Additionally, an interdependency between risks and benefits exits, as the evaluation of the benefits influences the risk perception. This holds true even if there is no actual relation between the benefits and the risks. For example, consumer feel they have taken adequate steps to protect their personal information by limiting their profiles visibility, but this does not necessarily lead to less of their personal data being collected. In addition, consumers are willing to exchange resources such as personal information for money, services, time, status or love (Susanne Barth, Menno D.T. de Jong 2017). It was found that many consumers value their browsing history only about 7 Euros, which is an equivalent of about a MacDonald's Big Mac meal (Spyros Kokolakis, 2015). In comparison, it has been estimated that an average American consumer's data is worth at least $240 per year. In 2016, the US digital advertising industry had a revenue of $83 billion (Wibson, 2018). Benefits such as personalization, convenience, economic

benefits and social advantages are suppressing the risk perception and while at the same time are emphasizing the benefit perception. Consumers might decide that the cost of reading the complex privacy policies outweighs the potential dangers and decide that the benefits of using the service outweighs any potential personal data abuse (Susanne Barth, Menno D.T. de Jong 2017).

However, to imply that the explanation for the Digital Privacy Paradox solely could be explained with the rational cost benefit calculation is over simplified, insufficient and does not lead to a substantially better understanding of the online consumer behavior. It is hardly possible for consumers to calculate the risks concerning the disclosure of personal information as those depend on a number for random factors and on the individual's preferences. Some consumer might find personal advertising intrusive, whereas others might find it useful to get information on products that they are interested in. Additionally, the Rational Choice Approach explanation is lacking the emotional and incorporated aspects of behavior. Online and offline, many actions are driven by irrational affective factors (Christoph Lutz, PePe Strathoff, 2014).

2.3.2 Emotional Aspect

Several authors state that emotional factors play an important role in the paradoxical consumer behavior. It has been shown that consumers evaluation of risks is heavily influenced by emotions. The problem with evaluating risks in that way is, that emotional evaluation has many flaws and is subject to cognitive biases. This still holds true, even if the flaws and biases were clearly explained beforehand. Calculating privacy risks most consumer subconsciously downplay the risks, the likelihood of threats and their potential impact. If an application like Facebook is perceived by consumer in a positive way, the benefits are estimated high and the risks low. The opposite is true if an application is viewed in a negative way, the benefits are perceived low and the risk high. This means, that as long as consumers view Facebook, Google or other companies in a positive manner, the loss of privacy is viewed solely as the cost of getting free access (menafn.com, 2018).

Tech giants have been collecting data over time, but data privacy only more recently became a widely discussed problematic. Especially amongst young consumers apathy towards data privacy concerns is a common respond. Many young consumers do care about their privacy and start to understand the risks of giving up a huge amount of personal information. However, after having used online services for most of their lives,

they feel that online services have already collected an enormous amount of their personal information and thus they feel like they have already lost control over the previously shared data. This can lead to a general feeling of resignation. Young consumers might think that tech giants and other platforms already collected a huge amount of their data, so keep using those applications will not make a difference anymore (Sarabia-Sánchez, Francisco-José; Aguado, Juan-Miguel; Martínez-Martínez, Inmaculada J., 2019) (Harry Readhead, 2020).

It also has been proven that consumer have much higher concerns about social privacy than about institutional privacy. Social privacy concerns are the fear of intrusion caused by other people. Social privacy concerns include being stalked, personal information easily found by the employer or unwanted acquaintances or being bullied online. Social privacy concerns are concerns about concrete individuals. On the other hand, institutional privacy concerns concern companies or public institutions. Those concerns are about consumers uneasiness or fear that their data is used for unwanted and unauthorized purposes. Examples are targeted Facebook ads or political spying by governments. Institutional privacy concerns are more abstract and less present in consumers day to day lives. A survey of Facebook users has shown, that many users have much higher concerns about social privacy and that only a few users are concerned about institutional privacy. Most participants of that Facebook survey had very strong privacy settings on Facebook protecting their social privacy, but they completely neglected the institutional aspects of privacy (Christoph Lutz, PePe Strathoff, 2014).

Surprisingly, a detected a high anger and disgust at the unauthorized cession of private data does not necessarily lead to a change in privacy settings. Meaning that users that are stating intense emotions concerning their privacy are not more likely to change their privacy settings, than users that are not stating intense emotions. Interestingly, the propensity to give up personal data, except for publishing photographs on social media, is not related to privacy settings. These results support the Digital Privacy Paradox, stating that intense emotional response declared before an incident of unauthorized cession of private data does not correspond to restrictive adjustments of the privacy options. One explanation for the paradoxical user behavior could be the social pressure of other members to stay active on social media (Sarabia-Sánchez, Francisco-José; Aguado, Juan-Miguel; Martínez-Martínez, Inmaculada J., 2019).

2.3.3 Trust

Trust can be a means to resolve the Digital Privacy Paradox, because if consumers trust, they are willing to become vulnerable and to rely on the other party. In the case of the Digital Privacy Paradox, if consumers trust the Internet companies or enterprises concerning their data, the Digital Privacy Paradox would be resolved. A cognitive calculative consumer statement could be “I trust a service because the benefits of trusting outweigh the costs”. An emotional consumer statement could be “I trust a service because I feel I will not abuse my data or my trust (Christoph Lutz, PePe Strathoff, 2014)”.

Trust has been defined as “a psychological state comprising the intention to accept vulnerability based upon positive expectation of the intentions and behaviors of another”. The (quasi-) anonymousness of large part of the internet and the fact that consumer experiences are limited to their devices, trust becomes the critical factor for the establishment and growth for companies online. In fact, Trust is the key perquisite for growth of online services. Consumer need a perceived sufficient level of trustworthiness to rely on the benevolence, integrity, credibility, ability and reliability of online services (Christoph Lutz, PePe Strathoff, 2014).

Consumers perceived trustworthiness depends on a variety of factors such as online experience, the consumers demographic characteristics, the consumers personality traits and the perceived attributes of the service. Social media companies rely heavily on the perceived trustworthiness of their services. They must be at least enough trustworthy for consumer to use the platform regularly (Christoph Lutz, PePe Strathoff, 2014).

Although in the survey Swiss citizens revealed a low level of trust in internet and social media companies, they do not take privacy protective measures. There is no connection between Trust and the self-reported behavior. Why then should the problem of trust be solved? A climate of distrust has been proven to not be a satisfying situation in the long run. Large scale studies have shown, that trust and social capital do have an economic impact. A more trustworthy environment might have a positive impact on the economy. Further, trust is not an isolated construct and functions with consumers privacy attitudes and behaviors (Christoph Lutz, PePe Strathoff, 2014).

2.3.4 Effect of Trust on Business

The internet revolution did not only facilitate company internal and external communication and had a big influence on consumer expectations, but the internet created a large array of new opportunities and lead many companies to switch their activity from offline to online. The advantages of conducting business online lead a large number of companies to quit traditional distribution of products and to focus solely on the new opportunities of the digital environment. However, conducting business online is often overshadowed by consumer mistrust. The intangible nature of online services and the increased skepticism of consumers can make it difficult to acquire a sufficient number of new costumers. Trust in the company has an even far greater importance on online purchase decision than the price level of the product or services offered. In fact, 49% of the people that abstain from shopping online state that they do so because of fears that range from cyber criminals to unscrupulous companies. Consumer mistrust is generated by the lack of physical contact, which creates uncertainty, makes consumers feel vulnerable and can create a fear of fraud. Trust between consumer and a company can be describe as a lengthy process of convictions, attitudes and dispositions that requires the involvement of both parties (Anamaria-Catalina Radu, Mihai Cristian Orzan, 2016) (Nathan Fillion 2020).

Consumer confidence in online services is influenced by factors such as the quality of information provided, data security, personal data protection, website reliability, guarantees, recommendations by other consumers and good communication services. Those factors can be categorized in trust in online goods, the trust in seller and online shops and the positive effects of information. For online service providers the website is acting as a mediator between the company and its consumers, and it is therefore crucial to establish trust and to help overcome consumer's uncertainty. Thus, the company website's quality is up most important, providing the consumer with the information needed and transaction safety (Anamaria-Catalina Radu, Mihai Cristian Orzan, 2016).

An example of building trust are online banking transitions. Many consumers feared the possibility of fraud or identity theft conducting their financial transactions online. Despite the increased convenience and lower cost, the fear of losing their financial resources kept many consumers from using online banking services and to instead stick with traditional transaction methods. As online transactions such as online banking increasingly was viewed as easy and useful, the level of trust was increasing. Additional

factors for creating trust are the consumers experience with other websites und the consumers overall internet skills. Also, the more familiar a consumer is with a website the more confident in the website he will be. The degree of confidence in the website depends on the costumer's satisfaction felt by previously carried out purchases. The more satisfied a consumer will be with the product or services offered, the more trusting he will become. Trust subsequently leads to more rapid purchase, fidelity and consumer loyalty (Anamaria-Catalina Radu, Mihai Cristian Orzan, 2016).

Research shows that low trust levels causes lower economic growth. The societies which are in the so called "distrust trap", craft public policy and do business in ways that benefit their own family, social class, tribe or other group. Rather than seeking projects with the highest return, in these societies people are more likely to make investments difficult for other people to seize. Examples could be Ponzi schemes or other frauds or paying a government official to secure a lucrative deal. Those actions do have a negative impact on the economy and lead to lower growth, higher regulation and more corruption. Those created negative externalities than decrease the overall trust level further (Ana Swanson, 2016).

3. Methodology

3.1 Survey (quantitative)

3.1.1 Experimental design

In the second part of this work, a survey experiment will be used to learn more about the effects of positive and negative information concerning data collection on the user behavior. It was chosen to use the website https://www.questionpro.com/ to create an online survey. QuestionPro is compliant with the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Additionally, the website is ISO 27001:2013 certified (questionpro website, 2020). Another reason was that it was one of the only survey websites that made it possible to add the full articles in the beginning of the survey. The advantages of conducting the survey online are that it is easier to share the survey with a big number of participants and therefore it is likely to get more answers. Additionally, due to the nature of my survey experiment and the questions asked, creating a paper survey and handing it out in person to participants would might have created the basis of people having less privacy to fill in the questionnaire. Less privacy could lead to participants answering the questions less truthful or participants might feel more inclined to answer all the questions instead of choosing the prefer not to answer option.

3.1.1.1 Experimental manipulations

I will be using two extracts from newspapers, that highlight either **positive or negative** aspects of personal data collection. Each participant will be exposed to only one of those articles and must rank them either positive, neutral or negative in terms of data privacy.

Measure of privacy preferences:

1. ***Disclosure of personal information***

The first measure is designed to test the impact of the previous read article on self-disclosure. It is expected that participants receiving the negative article are less likely to disclose personal data than participants receiving positive information. Participants are asked to answer 15 rather sensitive demographic and personal questions, such as gender, monthly budget/income, weekly expenditure and financial debt. The first three

of those 15 questions are standard survey questions. However, as the survey continuous the questions continue to become more sensitive. For example, the first question about consumption is about asking about chocolate, the second about the cigarettes, the third about alcohol and the fourth about illegal drugs. Participants can choose one of the answer options or choose the option “Prefer not to say”. The same effort is required to answer the question or to choose the “Prefer not to say” option. Additionally, in the last part of the survey, participants can add their contact information such as their name, email address and phone number. This last part is clearly indicated as optional and it is expected that most participants will not add their contact information. The logical assumption is that participants that read the positive article are more likely to fill in their contact information than participants that read the negative one.

2. ***Willingness to pay a price for data protection***

In the second part of the experiment, the participants are asked how much they are willing to pay to protect the data provided in the survey and how much are the willing to pay for their overall data protection. The logical assumption is that participants that received a negative article on data privacy will be more willing to protect their data than participants that did receive a positive one.

3.1.1.2 Hypotheses

This experimental design investigates whether the news article influences the privacy context decision-making. It is expected that participants receiving the negative article are less likely to share personal information and more willing to pay a price to protect their data, than participants receiving the positive article.

H1 User’s privacy concerns and behavior will change according to the content of the news article they read

H2 Depending on the article participants receive they will be willing to pay a higher/ lower price to protect their data

Participants

To reach participants the experimental survey was shared via social media such as WhatsApp and LinkedIn. WhatsApp uses End-to-End encryption and LinkedIn is upholding GDPR standards (WhatsApp website, 2020) (LinkedIn website, 2020). However, the main reason to choose those two applications was that many swiss citizens

use them. The only information participants received was that I am working on my Bachelor Thesis concerning Data Privacy and Data Collection.

3.1.1.3 Expected outcomes

The survey experiment is designed to gain a better understanding of the Digital Privacy Paradox and how information on data privacy and data collection influences consumer behavior. The survey should answer the aforementioned hypothesis 1 and 2.

3.1.2 Survey Intro

"Hello:

You are invited to take part in this survey for my Bachelor Thesis. It will take approximately 10 minutes to complete the questionnaire.

Your survey responses will be strictly confidential and data from this research will be reported only in the aggregate. **If you do not want to answer a question, you can always choose the option: prefer not to say.**

Please **read the article** in the beginning of the survey, as the questions are related to it. Thank you very much for your time and support."

A lot of attention was paid to the wording of the survey. Next to the explanation of why this survey is being conducted, the amount of time it approximately will take to complete it, that participants received carefully chosen additional information.

First, in the intro part of the survey I claim that the information will be strictly confidential, and the data will only be used to aggregate. There is no intention to use the provided information for any other purposes than this study, but this is an online survey conducted on the https://www.questionpro.com/ website. As mentioned before, QuestionPro is claiming to be compliant with GDPR and CCPA. Additionally, the website is ISO 27001:2013 certified (questionpro website, 2020). However, the website is created by a third party, it is difficult to actually know what happens with the data collected on the website.

Second, in the first part of the survey relative sensitive questions to health and income are asked. As aforementioned, those questions purposefully touching on sensitive subject such as health and financial to analyze if the pervious perceived information has

an influence on how participants answer the first 15 personal questions. In the intro part of the survey experiment, it is emphasized that there is the possibility of not answering the questions and to choose the option “prefer not to say” instead. It is important that participants at the beginning of the survey are aware of that option.

Third, due to the nature of the survey experiment, it is very important that participants read the article in the beginning. That is why in the introduction of the survey the importance of reading the article before answering the questions is emphasized.

3.1.3 Questions organization

After the Intro, the first part of the survey is the article. The participants either receive an article that put emphases on the negative aspects of data collection or put emphases on the positive aspects. The very first question of the survey is about how the participants perceive the article. Does the article highlight the positive, neutral or negative aspects of data collection? The responses to this question will be up most important while analyzing data collected in the survey to answer questions such as if the perception of the article influence the survey answers.

Second part of the survey, the first three questions are general demographic questions sex, age range and what part in Switzerland the participants live. Information about the participants profile will relevant while analyzing the collected data. The questions 5 to 15 are questions about rather sensitive topics such as health, drugs, income and financial depth. This part is probably very different from what the participants expected, and it is supposed to make them feel uncomfortable. I am purposefully pushing the boundaries with what can be asked in a survey, and therefor also pushing the boundaries on what participants are willing to answer. It is expected that participants that are reading the negative article are more likely to choose the option “Prefer not to say”. The second part of the survey should be answering the hypothesis 1 :

H1 User’s privacy concerns and behavior will change according to the content of the news article they read

In the third part of the survey, participants are asked, if they felt comfortable answering the questions in the second part. It is expected that participants that have read the negative article are more aware of the question being unusual intrusive and are more likely to perceive the questions uncomfortable than participants that have read the positive article. In the next three questions, participants are asked about how much the

participants are willing to spent on data protection per year for the data provided in the survey, how much for their data on social media and how much for all their data online. As it might be difficult for participants to think about an amount, they are willing to spend and to make it easier to analyze the data, answer options from 0 CHF to maximum 150+CHF were created. The third part of the questions should answer the hypothesis 2:

H2 Depending on the article participants receive they will be willing to pay a higher/ lower price to protect their data

In the last part of the survey, participants have the option to fill in their contact information such as name, email and phone number. This part is clearly marked as optional. It is expected that most participants will not choose to add their contact information, but it will be interesting to see if participants that have read about the positive aspects of data collection are more likely to add additional personal information than participants that read the negative article.

3.1.4 Difficulties encountered

3.1.4.1 Read the article

It is curial to the survey experiment, that participants read the article before answering the questions. However, knowing that many of the participants want to complete the survey as quickly as possible and that some might be likely to skip reading the article in the beginning, it was critical to put emphasis on the importance of the article in the survey introduction. To further ensure that the articles will be read, relatively short and engaging articles were chosen to keep the participants interest. Additionally, both articles were shortened to 251 words respectively 281 words. To increase the participant's trust in the article given, it was important to choose articles from trustworthy sources and to add the source with a link to the original website at the bottom of the survey article page. Before launching the survey, I sent it to 6 test persons, asking for an in-depth feedback on the wording of the survey, the questions and especially if they have read and how they would categorize the articles. The test persons were asked questions such as was the article positive or negative, was it engaging, what they felt after reading it. The survey experiment was than adapted accordingly.

3.1.4.2 Finding the right online survey

It was more difficult than expected to find an online survey that was suitable for the purpose of the survey experiment. Most websites either have limitations on basic functions or are expensive to use. It was decided to go with the https://www.questionpro.com/ website. The website offered most functions free of charge and was easy to use. Further, QuestionPro is compliant with the EU General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Additionally, the website is ISO 27001:2013 certified. (questionpro website, 2020) Importantly, the questionpro-website does not have limitations on the amount of questions or responses per survey, the full articles could be added to the survey, the collected data can easily be exported and there are many additional options that make it easy to create an engaging survey. However, even though I was able to add both articles to the survey, the formatting of the articles automatically changed, which made them less appealing to read. This is an unfortunate issue, especially as it is likely that most participants will complete the survey on their smartphones. The small smart phone screen further emphasis the bad formatting and make the article harder to read (Screenshot of the survey article page in the appendix).

3.1.4.3 Bias

Many participants after completing the survey, were interested in the nature of the survey and why I was asking such intrusive questions. Despite participants knowing that I am writing about data privacy and data collection, they did not realize that it was expected for them to not wanting to answer the questions. They told me that they answered all the questions truthfully, because they wanted to help me with my bachelor thesis and thought that I needed the data. They thought, it would be beneficial for me to get honest and complete answers. Receiving this feedback in the early stages of the survey experiment was very important, as the survey experiment should be as representative as possible. Receiving the feedback in the early stages of the survey experiment, gave me the opportunity to target participants that did not know me personally. I asked people in my social circle to share the survey with their acquaintances, which made it harder to find enough participants, but should have made the survey more representative. However, the acquaintances still knew that they participated in the survey for a student's bachelor thesis. It is assumed that they were less critical evaluating what to share as they wanted to help the student to get enough data.

4. Results

4.1 Experimental Survey Analysis

Both parts of the experimental survey had a similar completion rate. The survey part containing the negative article (Negative Survey) had a rate of 38.61% in comparison to the survey part containing the positive article (Positive Survey) 37.93%. In total the experimental survey was completed by 72 participants. The positive article had a word count of 251 words and the negative article had a word count of 281 words. On average participants completed the Negative Survey in 8 minutes and the Positive Survey in 5 minutes. Previously it was estimated that the completion of the survey would take about 10 minutes.

4.1.1 Positive Survey

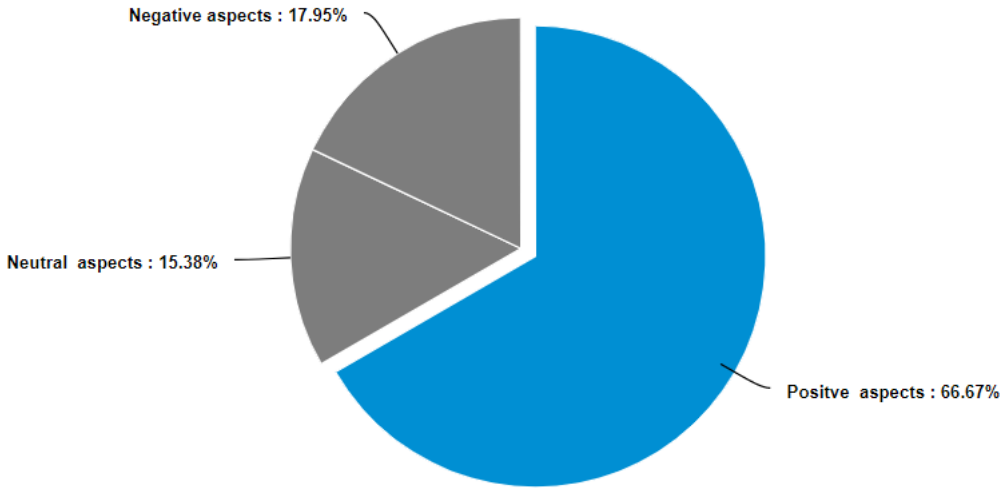
Table 1: Participant's Profile Positive Survey

Profile	Category	Number of Paricipants	% of Participants
Gender	Male	14	35.90%
	Female	**25**	**64.10%**
	Other	0	0.00%
	prefer not to say	0	0.00%
Age	0 - 18	0	0.00%
	18-24	16	41.03%
	25-34	**17**	**43.59%**
	35-44	3	7.69%
	45-54	2	5.13%
	55-64	0	0.00%
	64+	1	2.56%
	prefer not to say	0	0.00%
Canton	Canton GE	**18**	**46.15%**
	Canton VD	5	12.82%
	Canton BE	5	12.82%
	Canton NE	1	2.56%
	Canton FR	0	0.00%
	Other	9	23.08%
	Prefer not to say	1	2.56%
Total Priticipants			**39**

64.1% of the participants of the Positive Survey are women and 35.9% men. Most participants are between 25 – 34 years old 43.59%, followed by 18 – 24 years 41.03%,

35 – 44 years 7.69% and 45 – 54 years 5.13%. Most of the participants live in the canton of Geneva 46.2%, followed by other not mentioned regions 23.1%. A smaller amount of the participants lives in the cantons Vaud 12.82%, Bern 12.82% and Neuchatel 2.56%. Only one participant chose the option prefer not to say.

Figure 1 : Interpretation Positive Article



This group of participants was asked to read the article that highlights the positive aspects of data collection. 66.67% of the participants perceived the article to be drawing attention to the positive aspects. These participants average time to complete the survey was 6 minutes. 33.33% of the participants replied that they perceived the article as neutral or as negative. It is notable that those participants on average only spend 4 minutes to complete the survey. To complete the survey in such a short amount of time suggests, that some participants that categorized the article as either neutral or negative might have skipped the article in the beginning of the survey.

Table 2 : Prefer not to answer in percentage Positive Survey

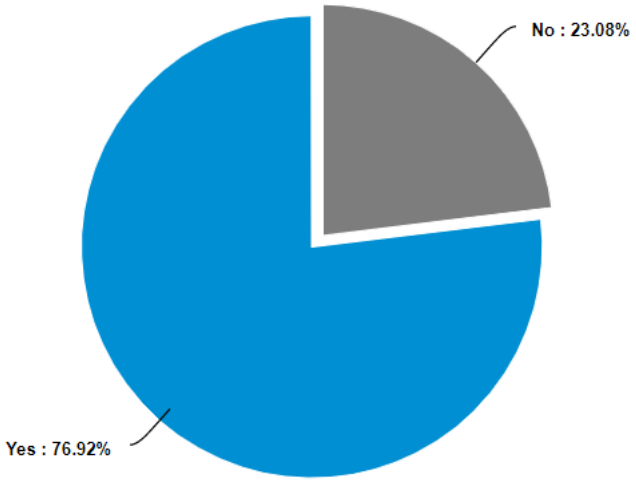
No	Question	Overall	Positive	Neuteral & Negative
1	Gender	0%	0%	0%
2	Age Range	0%	0%	0%
3	Canton	2.56%	3.85%	0%
4	Heatlh	0%	0%	0%
5	Chocolate	0%	0%	0%
6	Smoking	0%	0%	0%
7	Alcohol	0%	0%	0%
8	Drugs	0%	0%	0%
9	Cancer	7.69%	7.69%	7.69%
10	Mental Illness	10.26%	11.45%	7.69%
11	Time Online	2.56%	3.85%	0%
12	Income	20.51%	23.08%	15.38%
13	Support	17.95%	19.23%	15.38%
14	Spending	17.95%	19.23%	15.38%
15	Debt	20.51%	23.08%	15.38%

Overall 20.51% preferred not to answer the question about income and debt, 17.95% preferred not to answer the question about financial support and spending, 10.26% preferred not to answer the question about mental illness, 7.69 % preferred not to answer the question about cancer, 2.56% preferred not to answer the question about the area they live in and time spend online. This data shows that participants felt questions about financials more intrusive than question about health. This seems to be especially true for questions about monthly income and financial debt.

In comparison, out of the 66.67% of participants that perceived the article to be positive, 23.08% preferred not to answer the question about monthly income, financial debt, 19.23% preferred not to answer the question about financial support, weekly spending, 11.54% preferred not to answer the question about mental illness, 7.69% preferred not to answer the question about cancer and 3.85% preferred not to answer the question about the area they live in, time spent online.

Out of the 33.33%, 58.85% perceived the article as negative compared to 46.15% of participants who perceived the article as neutral. Out of the 33.33% of participants that perceived the article positive or neutral, 7.69% preferred not to answer the question about cancer, mental illness and 15.38% preferred not to answer the question about monthly income, financial support, weekly spending, financial debt.

Figure 2 Comfortable answering the questions Positive Survey



Overall 76.92% of the participants stated that they felt comfortable answering the question in the survey. The percentage distribution did not change for the group of participants that perceived the article as positive or for the group of participants that either perceived the article negative or neutral. The data collected shows that the interpretation of the article did not influence if the participants felt comfortable to answer the sensitive questions in part 2 of the survey experiment.

Table 3: Willingness to pay Positive Survey

		Overall		Positive		Negative & Neutral	
Question	CHF	Responses	percentage	Responses	percentage	Responses	percentage
Survey Data	0	**25**	**65.79%**	**16**	**64.00%**	**9**	**69.23%**
	10	4	10.53%	4	16.00%	0	0%
	30	5	13.16%	3	12.00%	2	15.38%
	50	2	5.26%	1	4.00%	1	7.69%
	100	0	0%	0	0%	0	0%
	150+	2	5.26%	1	4.00%	1	7.69%
Social Media	0	**15**	**39.50%**	**9**	**36.00%**	**6**	**46.15%**
	10	7	18.42%	6	24.00%	1	7.69%
	30	4	10.53%	2	8.00%	2	15.38%
	50	7	18.42%	6	24.00%	1	7.69%
	100	2	5.26%	1	4.00%	1	7.69%
	150+	3	7.89%	1	4.00%	2	15.38%
Data Online	0	8	21.05%	5	20.00%	**3**	**23.08%**
	10	**9**	**23.68%**	**6**	**24.00%**	**3**	**23.08%**
	30	3	7.89%	3	12.00%	0	0%
	50	7	18.42%	5	20.00%	2	15.38%
	100	5	13.16%	2	8.00%	**3**	**23.08%**
	150+	6	15.79%	4	16.00%	2	15.38%

Overall 34.21% of the participants are willing to pay a yearly fee to protect their data provided in the survey. 10.53% of the participants are willing to pay 10.- CHF,13.16% are willing to pay 30.- CHF, 5.26% are willing to pay 50.- CHF and 5.26% are willing to pay 150.- CHF or more. However, 65.79% of the participants are not willing to pay a yearly fee to protect their data provided in the survey. Overall 60.5% of the participants is willing to pay a yearly fee to protect their data on social media. 18.42% of the participants are willing to pay 10.- CHF, 10.53% are willing to pay 30.- CHF, 18.42% are willing to pay 50.- CHF, 5.26% are willing to pay 100 CHF and 7.89% are willing to pay 150.- CHF or more. 39.50% are not willing to pay a yearly fee to protect their data on social media. Overall 78.95% of the participants is willing to pay a yearly fee to protect all their data that's online. 23.68% are willing to pay 10.- CHF, 7.89% are willing to pay 30.- CHF, 18.42% are willing to pay 50.- CHF, 13.16% are willing to pay 100.- CHF and 15.79% are willing to pay 150.- CHF or more. 21.05% of the participants are not willing to pay a yearly fee to protect all their data online.

Out of the participants that perceived the article as positive 36% is willing to pay a price to protect their data provided in the survey, 64% is willing to pay a price to protect their data on social media and 64% is willing to pay a price to protect all their data online combined.

Out of the participants that perceived the article either neutral or negative 30.77% is willing to pay a price to protect their data provided in the survey, 53.85% is willing to pay a price to protect their data on social media and 76.92% is willing to pay a price to protect all their data online combined. The data collected suggest that the participants that categorized the article as positive in comparison to the participants that categorized the article as neutral or negative are more likely to be wanting to pay a price for the data collected in the survey and the data on social media, but that they are less likely to be wanting to pay a price for all their data online combined.

Table 4 : Optional Contact Information Positive Survey

Overall		Positive		Negative or Neutral	
Repsonses	Percentage	Repsonses	Percentage	Repsonses	Percentage
9	23.08%	7	26.92%	2	15.38%

Out of the 39 participants that completed the survey, 9 participants filled in the optional contact information which is 23.08% of the total participants. Of those 9 participants, 7 perceived the article as positive and 2 perceived the article as either negative or neutral. The data suggest that participants that perceived the article as positive are more likely to share their contact information.

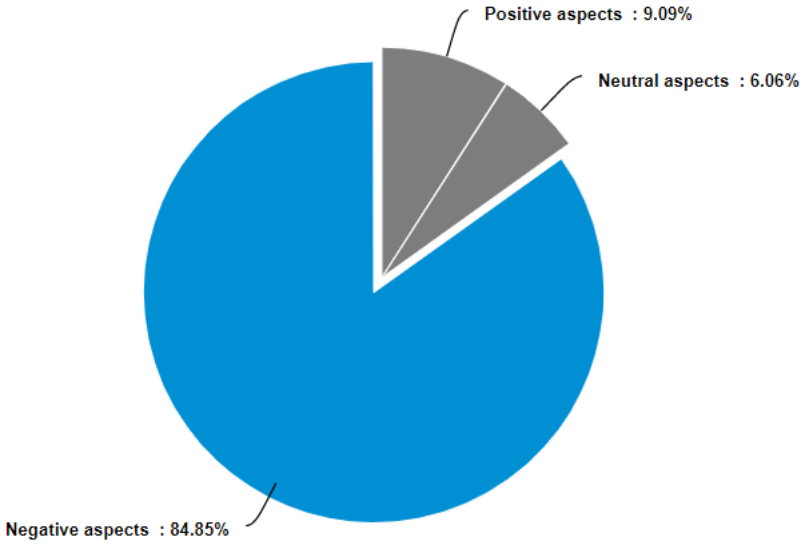
4.1.2 Negative Survey

Table 5: Participant's Profile Negative Survey

Profile	Category	Number of Paricipants	% of Participants
Gender	Male	10	30.30%
	Female	**20**	**60.61%**
	Other	1	3.03%
	prefer not to say	2	6.06%
Age	0 - 18	0	0.00%
	18-24	**15**	**45.45%**
	25-34	10	30.30%
	35-44	3	9.09%
	45-54	2	6.06%
	55-64	1	3.03%
	64+	0	0.00%
	prefer not to say	2	6.06%
Canton	Canton GE	**19**	**57.58%**
	Canton VD	4	12.12%
	Canton BE	5	15.15%
	Canton NE	0	0.00%
	Canton FR	0	0.00%
	Other	5	15.15%
	Prefer not to say	0	0.00%
Total Priticipants			**33**

In the Negative Survey the majority of participants are women 60.6%, in comparison to 30.3% men. 1 participant does not identify as male or female and 2 participants prefer to not reply to the question. Most participants are in the age group 18 – 24 years old 45,5%, followed by 25 – 34 years old 30.3% and 35 – 44 years old 9.1%. The majority as well lives in the canton of Geneva 57,6%, followed by the canton Bern 15,2% and the canton Vaud 12,1%. 15,2% are living in other areas.

Figure 3: Interpretation Negative Article



This group of participants was asked to read the article that highlights the negative aspects and problematics of data collection. 84.85% of the participants perceived the article to be drawing attention to the negative aspects. These participants average time to complete the survey was 9 minutes. 15.15% of the participants replied that they perceived the article as neutral or as positive. It is notable that those participants on average only spend 3 minutes to answer the survey. To complete the survey in such a short amount of time suggests, that some participants that perceived the article as neutral or positive might have skipped the article in the beginning of the survey.

Table 6 : Prefer not to answer in percentage Negative Survey

No	Question	Overall	Negative	Neuteral & Positive
1	Gender	6.06%	7.14%	0%
2	Age Range	6.06%	7.14%	0%
3	Canton	0%	0%	0%
4	Heatlh	3.03%	3.57%	0%
5	Chocolate	3.03%	3.57%	0%
6	Smoking	3.03%	3.57%	0%
7	Alcohol	6.06%	7.14%	0%
8	Drugs	6.06%	7.14%	0%
9	Cancer	12.12%	14.29%	0%
10	Mental Illness	12.12%	14.29%	0%
11	Time Online	6.06%	7.14%	0%
12	Income	15.15%	14.29%	20.00%
13	Support	18.18%	14.29%	40.00%
14	Spending	18.18%	17.86%	20.00%
15	Debt	18.18%	21.43%	0%

Overall 18.18% of the participants preferred not to answer the questions about financial support, weekly spending habits and financial debts. 15.15% preferred not to answer the question about monthly income. 6.06% preferred not to answer the questions about gender, age range, alcohol, drugs and time spent online. 3.03% preferred not to answer the questions about overall health, chocolate consumption and smoking. The data form the negative survey suggest that questions about financial are perceived more intrusive than questions about health. Especially the questions about financial support, weekly spending habits and debt.

Out of those 84.85% of participants that perceived the article to be negative, 21.43% preferred not to answer the question about financial debt. 17.86% preferred not to answer about weekly spending habits. 14.29% preferred not to answer the questions about cancer and mental illness in their family, monthly income, financial support. 7.14% preferred not to answer the questions about the area their gender, age range, the area they live in, alcohol, illegal drug consumption and time spend online. 3.57% preferred not to answer the questions about general health, chocolate consumption and smoking

habits. 57.14% stated that they felt comfortable answering the questions compared to 42.86% who did not.

Also, this is a much smaller sample set of participants. Therefore, percentage wise the weight of one participants answer is high. Out of the 15.15% that perceived the article positive or neutral, 20% preferred not to answer the question about the monthly income, weekly spending and financial debt. 40% preferred not to answer the question about the financial support. All the other questions were answered by all the participants. 100% of those participants stated they felt comfortable to answer the questions in the survey.

Table 7: Willingness to pay Negative Survey

		Overall		Negative		Positive & Neutral	
Question	CHF	Responses	percentage	Responses	percentage	Responses	percentage
Survey Data	0	**16**	**55.17%**	**12**	**50.00%**	**4**	**80.00%**
	10	3	10.34%	3	12.50%	0	0%
	30	4	13.79%	4	16.67%	0	0.00%
	50	3	10.34%	2	8.33%	1	20.00%
	100	2	6.90%	2	8.33%	0	0%
	150+	1	3.45%	1	4.17%	0	0.00%
Social Media	0	**13**	**44.83%**	**10**	**41.67%**	**3**	**60.00%**
	10	3	10.34%	3	12.50%	0	0.00%
	30	5	17.24%	5	20.83%	0	0.00%
	50	4	13.79%	3	12.50%	1	20.00%
	100	2	6.90%	2	8.33%	0	0.00%
	150+	2	6.90%	1	4.17%	1	20.00%
Data Online	0	**9**	**31.03%**	**6**	**25.00%**	**3**	**60.00%**
	10	3	10.34%	3	12.50%	0	0.00%
	30	3	10.34%	3	12.50%	0	0%
	50	4	13.79%	4	16.67%	0	0.00%
	100	4	13.79%	4	16.67%	0	0.00%
	150+	6	20.69%	4	16.67%	2	40.00%

Overall 44.83% of the participants are willing to pay a yearly fee to protect their data provided in the survey. 10.43% of the participants are willing to pay 10.- CHF,13.79% are willing to pay 30.- CHF, 10.43% are willing to pay 50.- CHF, 6.90% are willing to pay 100.- CHF and 3.45% are willing to pay 150.- CHF or more. However, 55.17% of the participants are not willing to pay a yearly fee to protect their data provided in the survey. Overall 55,17% of the participants is willing to pay a yearly fee to protect their data on social media. 10.34% of the participants are willing to pay 10.- CHF, 17.24% are willing

to pay 30.- CHF, 13.79% are willing to pay 50.- CHF, 6.90% are willing to pay 100 CHF and 6.90% are willing to pay 150.- CHF or more. 44.83% are not willing to pay a yearly fee to protect their data on social media. Overall 68.97% of the participants is willing to pay a yearly fee to protect all their data that's online. 10.34% are willing to pay 10.- CHF, 10.34% are willing to pay 30.- CHF, 13.79% are willing to pay 50.- CHF, 13.79% are willing to pay 100.- CHF and 20.69% are willing to pay 150.- CHF or more. 31.03% of the participants are not willing to pay a yearly fee to protect all their data online.

Out of the participants that perceived the article as negative, 50% is willing to pay a price to protect their data provided in the survey, 58.33% is willing to pay a price to protect their data on social media and 75% is willing to pay a price to protect all their data online combined.

Out of the participants that perceived their data as positive, 20% is willing to pay a price to protect the data provided in the survey, 40% to protect their data on social media and all their data online. Those data sets are more difficult to compare as the set of participants that perceived the article as neutral or negative is very small, but it seems that participants that have categorized the article as negative are more likely to pay a yearly fee to protect their data provided in the survey, their data on social media and all their data online than participants that categorized the article as neutral or negative.

Table 8 : Optional Contact Information Negative Survey

Overall		Negative		Positive or Neutral	
Repsonses	Percentage	Repsonses	Percentage	Repsonses	Percentage
7	21.21%	7	25.00%	0	0%

Out of the 33 participants that completed the survey, 7 participants filled in the optional contact information which is 21.21% of the total participants. Of those 7 participants, 7 perceived the article as negative. None of the participants that either perceived the article as positive or neutral filled in the optional contact information.

4.1.3 Hypotheses 1

H1 User's privacy concerns and behavior will change according to the content of the news article they read

As previously mentioned, the second part of the survey is containing next to 3 general demographic question rather sensitive questions about health, drug usage, income and financial debt. It was expected that participants that have read the negative article are more likely to choose the option prefer not to say avoiding to answer questions versus participants that have read the positive article. To eliminate the biases of different interpretation of the articles or responses of participants that have not read the article, only the results of participants that have correctly identified the negative article as negative or the positive article as positive are compared.

Table 9 : Comparison of "prefer not to answer" responses comparison Positive and Negative Survey

No	Question	Positive Survey	Negative Survey
1	Gender	0%	**7.14%**
2	Age Range	0%	**7.14%**
3	Canton	**3.85%**	0%
4	Heatlh	0%	**3.57%**
5	Chocolate	0%	**3.57%**
6	Smoking	0%	**3.57%**
7	Alcohol	0%	**7.14%**
8	Drugs	0%	**7.14%**
9	Cancer	7.69%	**14.29%**
10	Mental Illness	11.45%	**14.29%**
11	Time Online	3.85%	**7.14%**
12	Income	**23.08%**	14.29%
13	Support	**19.23%**	14.29%
14	Spending	**19.23%**	17.86%
15	Debt	**23.08%**	21.43%

The first three questions in the survey are about the demographic of the participants. 7.14% of the participants of the negative survey chose the option prefer not to answer for the question about gender and age range versus all participants of the positive survey chose to answer the question. The third demographic question about the canton 3.85% of the participants of the positive article chose the option not to answer versus all

participants of the negative survey answered. Out of the participants of the negative survey 3.57% chose the option prefer not to say for the questions 4,5 and 6, 7.14% for the questions 7 and 8. In comparison all participants of the positive article have answered the questions 4 to 8. 14.29% of the participants of the negative survey chose the option prefer not to say for the questions 9 and 10. 7.69% of the participants of the positive article chose the prefer not to say option for the question 9, 11.45% for the question 10. Out of the participants of the negative survey 14.29% chose the option prefer not to say for the questions 12 and 13, 17.86% for the question 14 and 21.43% for the question 15. In comparison out of the participants of the positive survey 23.08% chose the option prefer not to say for the questions 12 and 15, 19.23% for the questions 13 and 14.

Except for the question about the canton, until question 11 slightly more participants of the negative survey chose the option prefer not to say. However, more participants of the positive survey chose the option prefer not to say on the financial questions such as the questions about income, financial support, weekly spending habits and financial debt. Additionally, the positive article stresses the need to collect medical data in order to fight blood cancer. It was expected that participants of the positive survey are more willing to share medical information than participants of the negative survey. This is holds true for the question about cancer were only 7.69% of the participants of the positive survey chose the answer prefer not to say versus 14.29% of the participants of the negative survey. This does not hold true for the question about mental illness, which 11.45% of the participants of the positive survey chose not to answer versus 14.29% of the participants of the negative survey.

Table 10 : Contact Information Comparison Positive and Negative Survey

Positive		Negative	
Repsonses	Percentage	Repsonses	Percentage
7	26.92%	7	25.00%

In the last part of the survey participants had the option to leave their contact information such as name, email and phone number. This part was clearly indicated to be optional. It was expected that most participants will not choose to add their contact information, but that participants that read about the positive aspects of data collection are more likely to add additional personal information than participants that read the negative article. In

both surveys 7 participants added their contact information, which accounts for 26.92% of the positive survey and 25% of the negative survey. The data suggests that positive or negative information did not influence the participants to provide additional personal information.

Hypothesis 1 “User’s privacy concerns and behavior will change according to the content of the news article they read” could not be proven. It seems that the previously read information on data collection had very little influence on how the participants responded to the questions.

4.1.4 Hypotheses 2

H2 Depending on the article participants receive they will be willing to pay a higher/ lower price to protect their data

In the third part of the survey participants are asked, if they felt comfortable answering the sensitive questions in the second part of the survey and on a scale form 0.- CHF to 150.-+ CHF how much participants are willing to pay yearly in order to protect the data provided in the survey, their data on social media and all their data online. It was expected that participants that have read the negative article are more willing to pay a yearly fee to protect their data than participants that have read the positive article. To eliminate the bias of different interpretation of the articles or responses of participants that have not read the article, only the results of participants that have correctly identified the negative article as negative or the positive article as positive are compared.

Figure 4 : Positive Survey Comfortable Answering Questions in Part 2

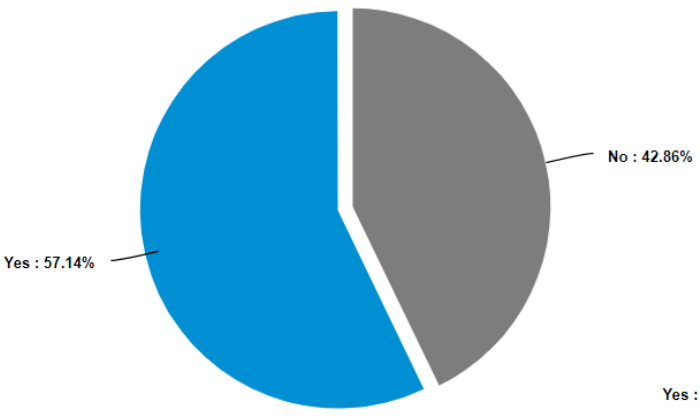
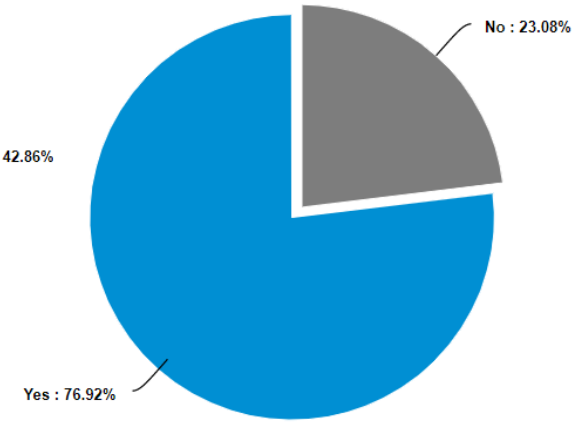


Figure 5 : Negative Survey Comfortable Answering Questions in Part 2



Despite the expectation than participants that have read the negative article are more aware of the question being unusual intrusive and are more likely to perceive the questions as uncomfortable than participants that have read the positive article, the collected data shows that in fact only 57.14% of the negative survey participants stated to be uncomfortable answering the questions versus 76.92% of the participants than of the positive survey. One could make the case, that participants of the negative survey did answer less of the sensitive questions and instead chose the option prefer not to say than participants of the positive survey, which could have led the negative survey participants to feel more comfortable. However, analyzing the second part of the survey, participants of the negative survey were not more likely to avoid answering the sensitive questions in the second part of the survey and thus, this is not a compelling argument.

Table 11 : Willingness to pay for data protection comparison Positive and Negative Survey

Question	Positive Survey	Negative Survey
Survey Data	36%	50%
Social Media	64%	58%
Data Online	80%	75%

I was expected that participants of the negative survey are more willing to pay a yearly fee to protect their data than participants of the positive survey. In the survey this theory holds only true for the data provided in the survey itself. 50% of the negative survey participants are willing to pay a price to protect their data versus 36% of the positive survey participants. Only 58% of the negative survey participants are willing to pay a yearly fee to protect their data on social media and 75% are willing to pay in order protect all their data online. In comparison 64% of the positive survey participants are willing to pay to protect their social media data and 80% of the positive survey participants are willing to protect all their data online.

Hypothesis 2 Depending on the article participants receive they will be willing to pay a higher/ lower price to protect their data, could not be proven. The data suggests that positive and negative information on data collection and data privacy have no influence on the willingness to pay a yearly fee in order to protect their data.

4.2 Interpretation of Results

Despite Hypothesis 1 and Hypothesis 2 being both very logical and seemingly easy to prove, they could not be proven to be correct. Additional information on data collection and privacy does not seem to influence participants behavior in terms of sharing personal information and participants do not seem to behave rational. As lengthy discussed in the literature review, the Digital Privacy Paradox does exist and is a complex phenomenon. Consumer behave paradoxically, being worried about data collection and data privacy but at the same time keep sharing personal information online. Instead of making rational choices, emotional factors play an important role in the paradoxical behavior and in risk evaluation. Assessing risks in an emotional manner is less than perfect and is subject to cognitive biases. It has been proven that those biases hold true even if they have previously been explained to the consumers. Consumer subconsciously downplay risks and threats, if an application or website is perceived in a positive way (menafn.com, 2018). This could be one explanation why the knowledge of a student writing about data collection and data privacy and the content of the article in the beginning of the survey, barley had an influence on the participants responses. The negative information about the risks of their personal data being collected online seemingly has hardly registered with the participants of the survey. It seems that many participants viewed a student conducting a survey for her Bachelor thesis in a positive manner, and therefore were willing to give up personal information to help the student collect enough data. Participants seem to not have reflected on the fact that by answering the survey their data is collected online. Viewing the survey in a positive light, lead participants to downplay potential risks and threats of disclosing sensitive personal information online.

Another explanation for the experimental survey results could be that emotional factors played a role in participants behavior and risk assessment. Since in recent years many scandals on data collection and invasion of privacy were highly publicized in the media, more consumers are aware of data collection and data privacy issues. Therefore, it is likely that many participants of the survey experiment already knew about the data collection and data privacy problematic. Switzerland is not a member of the EU or the EEA, therefor the implementation of the GDPR in 2018 did not directly impact Switzerland. However, the reform was still very important for Swiss business. Swiss businesses that have EU staff, customer or suppliers or conduct business activities within the EU need to uphold the GDPR (Andreas Knijpenga, 2020). Therefore, the implementation of GDPR lead to increased discussions about data collection, privacy

and security in Switzerland. Further, it is likely that many participants have used the internet and online applications for years, which could have led the participants to think that there is already such a huge amount of their personal data online and collected by companies, that sharing additional information will not make a difference anymore. Survey participants might have developed a feeling of apathy towards the collection of their personal data and did not care about sharing more personal information in the survey (Sarabia-Sánchez, Francisco-José; Aguado, Juan-Miguel; Martínez-Martínez, Inmaculada J., 2019) (Harry Readhead, 2020). An additional explanation for the survey participants behavior could be that a high anger of disgust at the cession of personal data does not necessarily lead to a change in privacy setting. This means that consumer that are stating intense emotions are not more likely to protect themselves from data collection than other consumers (Sarabia-Sánchez, Francisco-José; Aguado, Juan-Miguel; Martínez-Martínez, Inmaculada J., 2019). In the case of the survey experiment this could explain why participants that might felt disturbed by reading the negative article but are not more likely to share less of their personal information than participants that have read about the positive aspects of data collection.

As previously found in the literature review, trust could solve the Digital Privacy Paradox. If consumers have trust, they are willing to become vulnerable and to rely on the other party. If consumers trusted the Internet companies or enterprises concerning their data, the Digital Privacy Paradox would be resolved. Examples are “I trust a service because the benefits of trusting outweigh the costs” or “I trust a service because I feel I will not abuse my data or my trust (Christoph Lutz, PePe Strathoff, 2014)”. In the introductory part of the survey the statement is made that the survey response will be “strictly confidential”, which leads participants to believe their data is safe and that their anonymous. Additionally, the survey experiment was created by a student for her bachelor thesis, which is likely to seem trustworthy to most participants as most participants do not expect a student to abuse their personal data or trust. Despite the intrusive questions in the survey, many participants felt that their data was confidential, and they wanted to help a student. Participants were willing to complete the survey and to answer sensitive question because they trusted the student. Despite the paradoxical behavior of the participants and not being able to prove either one of the hypotheses, the results of the survey confirm the findings of the literature review.

5. Discussion and Recommendations

The Rational Choice Theory is suggesting that individual's make decisions reasonable and logical in order to create the greatest benefit or satisfaction (Susanne Barth, Menno D.T. de Jong 2017). However, to explain the online consumer behavior solely with the Rational Choice Theory is over simplified, insufficient and does not lead to a substantially better understanding. Additionally, the Rational Choice Approach is lacking the emotional and incorporated aspects of behavior. Online and offline, many actions are driven by irrational affective factors (Christoph Lutz, PePe Strathoff, 2014). The survey experiment results showed that additional information data collection and privacy does not influence the participants behavior in terms of sharing personal information and that survey participants behave irrational. The irrational online behavior is caused by faulty estimation of risks and potential threats (Christoph Lutz, PePe Strathoff, 2014). Risk assessment is influenced by small tangible or intangible rewards (Yong Jin Park, Scott W. Campbell, Nojin Kwak, 2012). Consumer tend to concentrate on the benefits instead of their stated concern or future risks. This holds true even if there is no actual relation between the benefits and the risks. Benefits such as personalization, convenience, economic benefits and social advantages are suppressing the risk perception and at the same time are emphasizing the benefit perception. Consumers might decide that the cost of reading the complex privacy policies outweighs the potential dangers and decide that the benefits of using the service outweighs any potential personal data abuse (Susanne Barth, Menno D.T. de Jong 2017).

Additionally, emotional factors are playing an important role in the paradoxical consumer behavior and heavily influence risk evaluation. Evaluation of risk in an emotional manner has many flaws and is subject to cognitive basis. If consumer perceive an application or an enterprise as positive, they subconsciously downplay the risks, the likelihood of threats and their potential impact. The opposite holds true if an application or an enterprise is viewed in a negative manner (menafn.com, 2018). Those findings were reflected in the survey experiments results. It seems that many survey participants viewed a student conducting a survey for her Bachelor thesis in a positive manner, and therefore were willing to give up personal information to help the student collect enough data. Survey participants seem to not have reflected on the fact that by answering the survey their data is collected online. Viewing the survey in a positive light, lead participants to downplay potential risks and threats of disclosing sensitive personal information online.

Especially amongst young consumer a feeling of apathy towards data privacy influences their behavior. Despite being aware of data harvesting and usage, many feel that already an enormous amount of their personal information has been collected and that the collection of additional personal information will not make a difference anymore. Many consumers feel like they have lost control over their personal data (Sarabia-Sánchez, Francisco-José; Aguado, Juan-Miguel; Martínez-Martínez, Inmaculada J., 2019). It is likely that many participants of the survey experiment have used the internet and online applications for years, which could have led the participants to think that there is already such a huge amount of their personal data online and collected by companies, that sharing additional information will not make a difference anymore.

Consumer regard social privacy concerns, which includes fears such as being stalked or bullied, as a more serious than institutional privacy concerns, which includes fears such as personal information being used for unwanted and unauthorized purposes. For instance, many Facebook users have very strong privacy settings for social privacy, but completely neglect the institutional aspects of privacy (Christoph Lutz, PePe Strathoff, 2014). Surprisingly, it has also been proven that consumer that state a high anger and disgust at the unauthorized cession of private data are not more likely than others to change their privacy settings (Sarabia-Sánchez, Francisco-José; Aguado, Juan-Miguel; Martínez-Martínez, Inmaculada J., 2019). Concerning the survey experiment, this could explain why participants that felt disturbed by reading the negative article are not more likely to share less of their personal information than participants that have read about the positive aspects of data collection.

The mean to resolve the paradox turned out to be trust. If consumers trust, they are willing to become vulnerable and to rely on the other party. The Digital Privacy Paradox would be solved. Due to the perceived anonymity online and the fact that consumers experiences are limited to their devices, trust becomes a critical factor for establishing growth online. Despite the low level of trust in tech giants and social media companies, consumers are still willing to provide them an enormous amount of personal information. The paradoxical consumer behavior does not encourage tech giants and social media companies to change their privacy policies, which leads the continuation of personal data collection, usage and selling. The willingness of consumer to keep sharing information does raise the question if privacy policies really need to change. Why should companies change their policies and governments enact new privacy protection laws, if consumer

choose convenience over data privacy? Why should the online trust problem be solved? What are the ethical and economic reasons that encourage change in data privacy policies?

5.1 Ethical reason

Data collection and usage creates many ethical dilemmas. Can the internet continue to be a medium that invites sharing personal information and encourages the freedom of expression, while at the same time it is becoming a tool of mass surveillance, either from corporate entities or from governments? Shocking scandals and revelations about invasion of privacy have been made public in recent years and raise many ethical questions. Those revelations raise questions about how much responsibility companies, tech giants and social media enterprises have, and to what extend they should harvest and use personal consumer information. The consumer behavior changing agency Cambridge Analytica was collecting voter's data from Facebook and other public available data sources in order to create voter user profiles. Those voter profiles where used to target and influence seemingly undecided voters with customized political advertisement in favor of the politician or political party they were hired by (Steve Andriole, 2019). The Cambridge Analytica scandal raises questions about how free democratic elections still are and how easily voters can be influenced online. Should political parties or politician have the right to hire so called behavior changing agencies or does it give them an unfair advantage over other candidates? Do tech giants and social media have the social responsibility to protect their users or should their main aim be the creation of profit for their shareholders? Should behavior changing agencies, political parties or social media enterprises be held accountable for invading voters' privacy?

In an article in early 2020, the New York Times published and investigative article about the facial recognition application Clearview AI and its groundbreaking new technology that surpasses every other previous facial recognition tool. The Clearview AI application has collected over 3 billion photos and has been used by multiple U.S police forces and the Canadian Law enforcement. This application is already in use, despite never have been tested by an independent party and automatically storing all the pictures uploaded. Seeing that the application has been used mainly by Law Enforcement, Clearview AI is able to collect a data base of people searched by the police. In an interview with the New York Times the founder of Clearview AI Ton-That has stated that despite high offers, he

is not planning on making his application public or selling it to “bad” governments. It is concerning that a CEO of such a powerful application can decide to whom he is selling and that citizens must trust him with his judgement of which government is a “bad” one. Additionally, it is highly possible that a copycat of the Clearview AI application emerges (New York Times, 2020) (The Daily, 2020). Those and many other similar revelations raise questions about what responsibilities governments have in protecting their citizens. Could it be ethically justified to use those or similar applications to reduce crime and to faster arrest criminals or is using this or similar application unjustifiable invasion of people’s privacy? Could it be that this or similar technology might lead to more citizens being arrested for crimes they have not committed? Can increased surveillance by the government be justified or does it limit citizens’ rights? Do governments have the responsibility to create up to date policies to protect their citizens, and if yes, how extensive should they be?

5.2 Economical reason

The mean to resolve the paradox turned out to be trust, because if consumers trusted online companies the Digital Privacy Paradox would then be solved (Christoph Lutz, PePe Strathoff, 2014). Despite consumer being worried about their personal data being harvested and misused, they make little to no changes to their behavior online, keep sharing personal information and keep using applications that have been proven to invade privacy (Spyros Kokolakis 2015). This raises the question, if tech giants or social media enterprises should change their data collection policies to better protect consumers personal information. Next to the ethical problematic of invading consumers privacy, a climate of distrust has been proven to not be a satisfying situation in the long run (Christoph Lutz, PePe Strathoff, 2014). Large scale studies have shown, that trust and social capital do have an economic impact and low trust levels cause lower economic growth. Societies with low trust levels craft public policy and do business to favor their own family, social class, tribe or other group. In those societies, consumer rather than seeking out investment with high returns, are choosing projects that are harder to be seized by others. Examples could be frauds or paying a government official to secure a lucrative deal. This leads to lower economic growth, more corruption, higher regulation and decreases trust levels further (Ana Swanson, 2016). Therefore, a more trustworthy environment might have a positive impact on the economy as whole. Trust is not an

isolated construct and functions with consumers privacy attitudes and behaviors (Christoph Lutz, PePe Strathoff, 2014). Conducting business online has become essential to many companies. However, handling business online is often overshadowed by consumers mistrust. The intangible nature of online services and the increased skepticism of consumers can make it difficult to acquire a sufficient number of new and loyal customers. Trust in the company has an even far greater importance on online purchase decision than the price level of the product or services offered. Consumer mistrust is generated by the lack of physical contact, which creates uncertainty, makes consumers feel vulnerable and can create a fear of fraud. Trust between consumer and a company can be describe as a lengthy process of convictions, attitudes and dispositions that requires the involvement of both parties (Anamaria-Catalina Radu, Mihai Cristian Orzan, 2016).

5.3 Creation of trust

Consumer worry that their basic rights and freedom might be infringed, while their trust in institutions and governments is declining (Bas Burger, 2020). Many of the scandals raise questions about the how far an enterprise or a government can go in collecting and surveilling consumers and the general public. Companies need to evaluate what their values are and what they are standing for. Despite the fact, that consumer do not change their online behavior and keep providing tech giants and social media companies with their personal data, the low trust levels do and will have a negative economic impact in the long run (Ana Swanson, 2016). This impact affects amongst others online service providers, which must operate in an environment of consumer mistrust (Anamaria-Catalina Radu, Mihai Cristian Orzan, 2016) (Nathan Fillion 2020). Further, it has been proven that in societies with overall low trust levels create public policies and handle business in favor of their own family, social class or tribe. This leads to a vicious cycle of negative externalities that decreases trust further and further. The decreasing level of trust has an even stronger negative economic impact, frauds and corruption tend to increase (Ana Swanson, 2016). An additional reason to rethink business online and to move to a more cooperate responsible strategy is that consumer expectations are changing. According to the World Economic Forum, in the past few years there has been a significant systemic shift towards purposeful business and responsible capitalism. Responsible capitalism is called stakeholder capitalism and means that instead of solely focusing on making profit for shareholders, corporations are oriented to serve any parties interested in or affected by their operations. This typically includes next to shareholders,

employees, customers, suppliers, communities and the environment. Younger generations tend to be less accepting to the business culture of making profit fast and creating shareholder value at any cost (Milton Cheng, 2020). According to the Edelman survey, three quarter of people globally believe that companies should act in a way which improves economic and social conditions. It has been reported that customers are more motivated to buy from brands that embody their value and beliefs as well as that that employees that work in high-trust companies have more energy at work, are 50% more productive and more engaged than employees in low trust companies. Facing the new reality, company boards need to reconsider what role their organization is playing in society to ensure long-term success (Bas Burger, 2020).

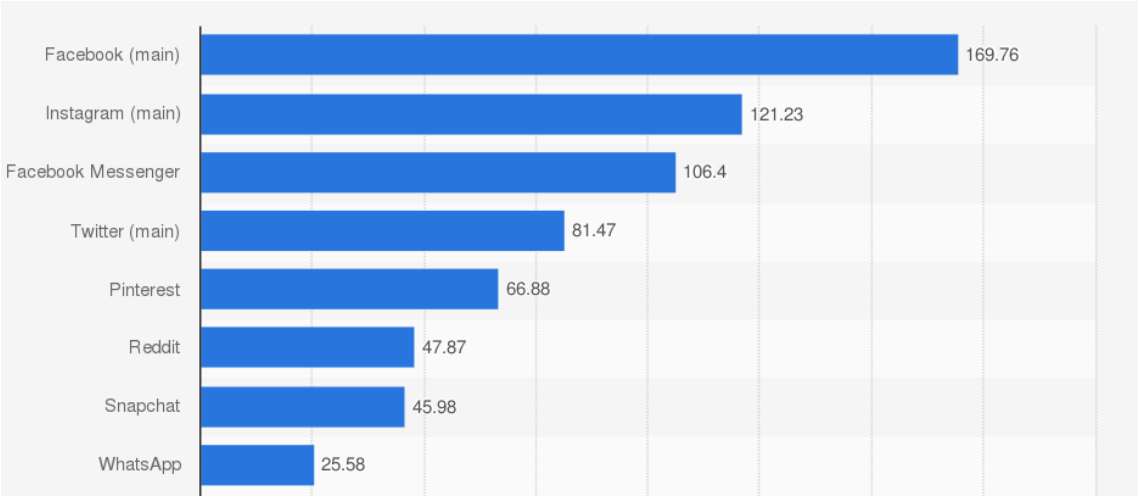
> *"The World Economic Forum is releasing a new Davos Manifest, which states that companies should play their fair share of taxes, show zero tolerance for corruption, uphold human rights throughout their global supply chains, and advocate for a competitive level playing field." (Klaus Schwab, Founder and Executive Chairman WEF, 2020)*

5.3.1 Social Media and Tech Giants

Many Tech companies have developed a multibillion-dollar business models with segmented advertising and managing ads to micro-segmented target groups. Instead of fighting for their privacy, many consumers do not change their privacy settings and accepted the terms and conditions without reading and keep providing their personal information in exchange for free services. Despite consumer being aware of and worried about their personal data being collected and misused, they keep using social media applications and tech giant's programs and devices. This holds true even if the company or the application has been involved in highly publicized scandals. One example is Facebook. In spite of being involved in numerous and very public scandals and being fined $5 billion by the American Federal Trade Commission over the violation's consumer privacy, consumer keep using their services (Enrique Dans, 2019) (Mary Meisenzahl 2019). After the Cambridge Analytica scandal broke in 2018, the outcry against Facebook was huge and the hashtag #deleteFacebook was trending on Twitter. However, most consumer either kept using the Facebook application and Facebook Messenger or switched to Facebook owned applications like Instagram (Menafn.com, 2018). The online consumer behavior implies that despite huge scandals, companies like

Facebook can continue with their business practices without making any substantial changes, while at the same time they are not losing users and keep making a horrendous profit (Julia Carrie Wong, 2019). Those conclusions do not give tech giants or social media companies incentives to change their policies and to protect consumers privacy. However, having a closer look at what happened in the Facebook case, Facebook was the biggest social media company in the US in 2019 and owned the three biggest applications Facebook, Instagram and Facebook Messenger as well as the widely used messenger application WhatsApp. It is highly possible that many consumers felt that they did not have another choice than to continue using one of Facebook's applications.

Table 12 : Most popular mobile social networking apps in the United States as of September 2019, by monthly users (in millions) - Statista



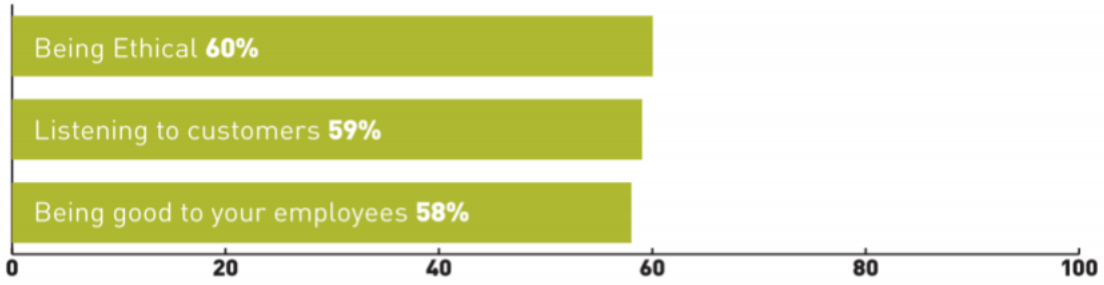
If there would have been other applications from companies that have a better reputation and are seemingly more trustworthy, it is likely that many consumers would have used an alternative application instead. In today's highly technological world it could be a unique selling point and a big advantage for a tech giant or a social media company to acknowledge cooperate social responsibility and to create or recreate consumer trust.

In addition, the EU implemented the General Data Protection Regulation (GDPR) law in 2018. The GDPR was forcing many companies worldwide to update their privacy regulations (Jennifer Lunn, 2019). Currently the European Union is working on a draft called the ePrivacy Regulation. The current draft focuses on rules for advertisers accessing consumer's electronic devices. The regulation would require that consumer provide consent before a company can access their device, which includes the reading and writing of cookies (Ari Levenfeld, 2019). In the United States 25 states have laws

that address data security practices of private sector entities (NCAL, 2019). Canada has introduced the Personal Information Protection and Electronic Documents Act (PIPEDA) by making user consent and transparency a top priority. The law includes ten fair information principles such as accountability, consent, accuracy and safeguards (Ari Levenfeld, 2019). It is likely that in the future more governments will implement similar or other data regulation privacy laws, which will make it more difficult for companies to store or collect user data (Jennifer Lunn, 2019). New stricter privacy laws will have an impact on how business can be conducted online and what standards online companies need to uphold.

According to Baker McKenzie the top three drivers for building trust between a company and consumer are being ethical, listening to customer and being good to one's employees (Milton Cheng, 2020).

Table 13 : Building Trust Drivers



By demonstrating strong values and expertise, company leaders can help to bring clarity and simplicity, giving consumer the tools to make informed decisions. Tech giants and social media companies do have the responsibility to work with governments and to help establishing policies that protect consumer. Global initiatives such as the Cybersecurity Tech Accord help foster international collaboration and to promote consumer safety online. Cybercrime has an increasingly high costs and international collaborations are the most effective way to combat it and strengthen the defenses of the global industry (Bas Burger, 2020).

5.3.1.1 Limitations of data proception laws and regulations

Since the 1960s and the expansion of information technology, business have been storing consumer data in data bases. Those data bases have been searched, cross-referenced and shared with other organizations. Growing public concern lead the German region in Hesse to pass the first data protection law in 1970. National laws emerged soon afterwards, and by January 2018 100 countries have adopted data protection laws. However, the sheer volume of data generated and the rapid development of technology, mean that existing data protection laws are soon outdated (Keys to Data protection, 2018). After four years of preparation the EU implemented GDPR in May 2018. So far GDPR has been the largest legislation of its kind and had effects extending beyond the EU boarder. The GDPR Article 83 states that noncompliance can be met with fines as high as 20'000'000 EUR or up to 4% of the total annual worldwide turnover of a company (Rob Sobers, 2020). However, GDPR's enforcement seems to be a big weak point. Regulators are taking a very long time to make a decision against or punish tech giants and only 231 fines and sanctions have been issued under the GDPR (Karlin Lillington, 2020). So far, Google is the only tech giant that received a slap on the wrist with a fine of 50mio EUR. The small nations Luxembourg and Ireland are tasked with the GDPR oversight of nearly all EU-operating tech multinationals. Due to the mix of low corporate tax rates and business-friendly regulation, multiple tech giants such as Google, Facebook, Microsoft and Twitter operate out of Ireland. This has created close relationships between Ireland and those tech giants, but also a strong degree of economic dependency (Nicholas Vinocur, 2019). Stand-alone national EU data-protection authorities (DPAs) seem not to be able to counter the staggering wealth and legal resources of the secretive tech corporations (Karlin Lillington, 2020). Surveys show that 39% of EU citizens are unaware what GDPR is. In addition, 53% of consumers globally state that even if they do read consent notices, they still do not understand how their data is being used (PR Newswire, 2019). The CMO Elie Kanaan of the digital advertising company Ogury said:

> *"The industry desperately needs to earn back consumers' trust, by granting them a clear and fair choice and gaining their explicit consent. That means consent notices must be in plain words, published in plain sight." (Elie Kanaan, CMO Ogury, 2019)*

71% mobile users state that they would share their data if they know exactly which data is being collected and how it will be used. This finding shows that consumers are willing to preserve a free internet as long as the exchange is fair and respected (PR Newswire, 2019).

5.3.1.2 Overview biggest Tech and Social Media Companies

Apple is one of the only Tech companies that has never actively engaged in the sale of advertising such as selling consumer information to third parties and instead focused on selling its own products and services. So far Apple has avoided privacy scandals and has become one the world's most valuable companies. Consumer seem to trust Apple when it comes to privacy (Enrique Dans, 2019).

In contrast most of Googles revenue stems from managing segmented advertising for consumer that use their search engine and from a huge network of programmatic advertising that auctions consumers profiles to the highest bidder each time the consumer visits a specific webpage (Enrique Dans, 2019). Ad auctions function similarly to normal auctions. They allow advertisers to state the price they are willing to pay for clicks on ads. Because the ad auction ranks advertisers based on their bids and Quality Score, it assigns the ad unit to the advertisers who value it the most. The winning ads are therefore from the advertisers who are willing to pay the most. Google uses a Quality Score to ensure good user experience (Google, 2020). For instance, if a consumer searches for a hotel in Rom, he then gets bombarded with advertisement about hotels or activities in Rom. Google has so far not been involved in personal data leaking scandals (Enrique Dans, 2019).

Amazon is monitoring all their consumers online shopping behavior in detail. A major part of Amazons revenue is generated by selling the collected information to advertising companies. So far Amazon managed not to be hit by a major privacy scandal. However, Amazon was accused of bugging consumers' homes with its domestic voice assistant device Alexa and of spying on consumer with its Ring Home security system (Enrique Dans, 2019).

Facebook has been the center of many highly publicized scandals, amongst it the Cambridge Analytica one, in which it became clear that the data of millions of Facebook users has been used to influence democratic elections. In 2019 Facebook was fined $5

billion by the American Federal Trade Commission over the violation's consumer privacy. In 2020 Facebook is still under fire for not fact checking political advertising. Facebook is a very unethical company that has been proven to have stolen consumer data, to have reached secret agreements about personal information collected, stored passwords and to have deceived consumers (Enrique Dans, 2019) (Mary Meisenzahl 2019).

5.3.1.3 Corporate Social Responsibility Measures

Knowledge and Control over own data

Sensitive consumer data is increasingly collected and used to predict consumer behavior and to create user profiles. User profiles will be increasingly used to influence voters or to make consequential decisions about consumers such as credit scoring or for making hiring decisions (privacy international, 2020).

There should be no creation of secret consumer profiles, which could limit consumers rights, freedom and opportunities. Instead online companies should give consumer full access to profiles created and give consumer the possibility to delete their data profile. Consumer should be informed if automated decision making is taking place, the conditions and have the right to redress it (privacy international, 2020). Consumers online privacy rights should include the right to dispute inaccuracy or error in the personal data, the right to request suspension, withdrawal, blocking, removal or destructions of personal data and the right to complain and be compensated for any damages sustained due to inaccurate, incomplete, outdated or unlawfully obtained data. To meet those rights, tech giants and social media companies need to have a procedure for inquiries and complaints that will specify how concerns and documents shall be received and acted upon (National Privacy Commission, 2017).

Control Over Intelligence

New technology and Artificial Intelligence such as smart devices or voice control made consumers activities and behavior increasingly traceable. Metadata and other forms of personal data are constantly created. This enormous amount of sensitive information collected, gives institutions with access to it unprecedented knowledge about individuals, groups, communities, markets and whole nations. In the future tech giants and social media companies will have greater insight into the world than powerful intelligence agencies (privacy international, 2020).

There should be more transparency and consumer should be informed about the data that is generated and who has access to their personal information. Emails, text messages or financial transitions, what does which provider and who has access to it? If possible, consumer should have the right to object data collection. In systems where this is not a possibility, their data should be anonym and the data collection minimized (privacy international, 2020). Additionally, tech giants and social media companies need to ensure that their IT staff, workforce and management are aware of their responsibilities. The collected data should be classified, in a way that both workers and the management can understand the difference and confidential data is clearly indicated as such. An important part of data security is to grant access to sensitive consumer data only to employees who need it and to keep monitoring employees' access. Regular data security audits will ensure that staff and management are complying with the various elements of the data security policies (Vijay Basani, 2016).

Data Protection

As more and more devices are connected at all times a massive amount of consumer data is collected. However, often devices or infrastructure are insecure and unsafe, which leads to a hazardous environment and leaves consumer vulnerable (privacy international, 2020).

Tech giants and social media companies must implement appropriate physical, technical and organizational measures for the protection of consumer data. Those security measures aim to maintain the availability, integrity and confidentiality of consumer data. The data needs to be protected against natural dangers such as accidental loss or destruction, but also against unlawful access, fraudulent misuse, unlawful destruction and contamination (National Privacy Commission, 2017). End-to-end encryption should be default for devices, networks and platforms for data in-transit or data at-rest. Data collection should be minimized across all devices and platforms. If less data is generated and processed, less data can be misused or breached. There should be increased open and transparent cybersecurity research, which identifies security and safety challenges. Cybersecurity should be considered a common good, which benefits the whole society (privacy international, 2020). In addition, tech giants and social media companies must develop and implement policies and procedures for the management of a personal data breach. This ensures the ability to take immediate and effective action in case of a data

breach. Further, there must be a periodical review of those policies and procedures as well as periodical reviews of the risk assessment and vulnerabilities of the network (National Privacy Commission, 2017).

5.3.2 E-Commerce and Online Service Providers

Due to the low level of trust in online, many e-commerce companies and online service providers have difficulties to gain enough customer. The intangible nature of online services and the increased skepticism of consumers can make it difficult to acquire enough new costumers. Consumer trusting the company has an even far greater importance on online purchase decision than the price level of the product or services offered (Anamaria-Catalina Radu, Mihai Cristian Orzan, 2016). In fact, 49% of people that abstain from shopping online state that they do so because of fears that range from cyber criminals to unscrupulous companies. Consumer mistrust is generated by the lack of physical contact, which creates uncertainty, makes consumers feel vulnerable and can create a fear of fraud (Nathan Fillion 2020). For online service providers the website is the acting mediator between the company and the consumer. The website therefore is heavily influencing consumers trust and purchase behavior. Thus, the online providers website quality is up most important. It is essential to provide consumers with the information needed and establishing a relationship between costumers and the company. The more familiar consumers are with the website and the more satisfaction is felt by previous purchases, the more trusting they become. Trust subsequently leads to more rapid purchase, fidelity and consumer loyalty (Anamaria-Catalina Radu, Mihai Cristian Orzan, 2016).

Increased Cybersecurity

Many consumers are worried about or even completely avoid online transaction due to the fear of their personal and payment information being stolen. To increase consumer trust in their business, companies should make sure to uphold the latest Payment Card Industry Data Security Standard (PCI-DSS) compliance requirements. By adhering to the standard, companies need to sufficiently secure cardholder data and reduce the likelihood of a data breach. On their website they can then display the official trust badges and seals. Those stamps represent the legitimacy from third-party organizations such as anti-virus software providers and payment gateways (Nathan Fillion, 2020).

Social proof

Consumer tend to trust each other more than online providers. Social proof such as testimonials form pervious buyers, honest product ratings and reviews, ability to share on social media or partnership with an influencer increase consumer trust. The more social proof the less hesitant customers are to finalize their purchase (Nathan Fillion, 2020).

Emotional Factors

Next to building trust with consumer by ensuring cybersecurity, it is important to connect with consumers on an emotional level. Online service provider should avoid portraying themselves or their brand as generic, anonymous or overly technical. The website should not solely offer manufacturer description, but also have its own brand voice, humanizing the website and giving the customer a glimpse of what the brand stands for (Nathan Fillion, 2020). Warby Parker is an American online glasses retailer and is very successful and known for establishing an emotional connection with its consumers. For instance, that's how they describe their own history on their website:

> *"Warby Parker was founded with a rebellious spirit and a lofty objective: to offer designer eyewear at a revolutionary price, while leading the way for socially conscious businesses.Every idea starts with a problem. Ours was simple: glasses are too expensive. We were students when one of us lost his glasses on a backpacking trip. The cost of replacing them was so high that he spent the first semester of grad school without them, squinting and complaining. (We don't recommend this.) The rest of us had similar experiences, and we were amazed at how hard it was to find a pair of great frames that didn't leave our wallets bare. Where were the options? (Warby Parker website, 2020) ..."*

6. Conclusion

Tech giants and social media companies have developed a multibillion-dollar business models with segmented advertising and managing ads to micro-segmented target groups (Enrique Dans, 2019). Doing business by invading consumers privacy does raise ethical questions and generated many highly publicized scandals. Revelations and scandals created new consumer awareness concerning privacy intrusion and misusage of personal data. However, the new gained awareness does not lead to a change in online consumer behavior and does have little influence on the success and profit of tech giants and social media companies (Spyros Kokolakis, 2015). Their continuous success and the barley changed online consumer behavior does not incentivize tech giants and social media companies to take action and to change their business models (Enrique Dans, 2019). However, next to the questionable ethics of making business by invading consumers privacy, the environment of mistrust does and will have an economic impact (Nathan Fillion 2020). Additionally, there has been a systemic shift of consumer expectations towards stakeholder capitalism. Younger generations tend to be less accepting to the business culture of making profit fast and creating shareholder value at any cost (Milton Cheng, 2020). The mean to resolve the paradox turned out to be trust, because if consumers trusted online companies the Digital Privacy Paradox would then be solved (Christoph Lutz, PePe Strathoff, 2014). Many tech giants and social media companies have been involved in privacy scandals, which led to a high level of mistrust online. According to Baker McKenzie the top three drivers for building trust between a business and consumer are being ethical, listening to customer and being good to one's employees (Milton Cheng, 2020). Being an ethical and socially responsible company can not only help to create or recreate consumer trust in the company, but it could be a huge advantage and a unique selling point. In addition, after four years of preparation the EU implemented GDPR in May 2018. So far GDPR has been the largest legislation of its kind and had effects extending beyond the EU boarder. The GDPR Article 83 states that noncompliance can be met with fines as high as 20'000'000 EUR or up to 4% of the total annual worldwide turnover of a company (Rob Sobers, 2020). Canada has introduced an updated version of in 2017 PIPEDA and the State of California has implemented California Privacy Act in 2018 (Ari Levenfeld, 2019). It is likely that in the near future more nations will implement updated stricter data privacy laws and regulations, that would have an impact on how business is conducted online.

6.1 Social Responsibility Measures for Tech Giants and Social Media companies

Knowledge and Control over own Data

No secret consumer profiles should be created. Consumer need to be given full access to all their profiles and have the possibility to delete them. Consumer should be informed if automated decision making is taking place and under which conditions (privacy international, 2020). Consumers online privacy rights should include the right to dispute inaccuracy or error in the personal data, the right to request suspension, withdrawal, blocking, removal or destructions of personal data and the right to complain and be compensated for any damages sustained due to inaccurate, incomplete, outdated or unlawfully obtained data. To meet those rights tech giants and social media need put the corresponding procedures for inquiries and complaints in place (National Privacy Commission, 2017).

Control Over Intelligence

Data collection needs to be transparent and consumer need to be given the knowledge on who has access to their personal information. If possible, consumer should have the right to object data collection. In systems where this is not a possibility, their data should be anonym and the data collection minimized (privacy international, 2020). Tech giants and social media companies need to ensure that their staff and management are aware of their responsibilities and the collected data is classified. The classifications need to be easy to understand and confidential data needs to be clearly indicated as such. Employees access to consumer data needs to be monitored and regular security audits need to be conducted to ensure compliance (Vijay Basani, 2016).

Data Protection

Tech giants and social media companies must implement appropriate physical, technical and organizational measures for the protection of consumer data. The data needs to be protected against natural dangers such as accidental loss or destruction, but also against unlawful access, fraudulent misuse, unlawful destruction and contamination (National Privacy Commission, 2017). The consumer information needs to be protected from access by third parties. End-to-end encryption should be default for devices, networks and platforms for data in-transit or data at-rest. Data collection should be minimized

across all devices and platforms. Cybersecurity should be considered a common good, which benefits the whole society (privacy international, 2020). Policies and procedures for the management of a data breach need to be implemented to ensure immediate and effective action. Policies, procedures, risk assessment and vulnerabilities of the network need to be reviewed on a regular basis (National Privacy Commission, 2017).

6.2 Creation of Trust E-Commerce and Online Service Providers

E-commerce and service providers a strongly impacted by the low consumer trust level online and many have difficulties to acquire enough customers. Consumers trusting a company has an even far greater importance on the online purchase decision than the price level of the product or services offered. Due to the intangible nature of doing business online, the company website is acting as a mediator between the company and the consumer. Consequently, the company websites quality is up most important, as it strongly influences consumer trust and purchase behavior. Trust leads to more rapid purchase, fidelity and consumer loyalty (Anamaria-Catalina Radu, Mihai Cristian Orzan, 2016) (Nathan Fillion 2020).

Increased Cybersecurity

Business need to make sure to uphold the latest Payment Card Industry Data Security Standard (PCI-DSS) compliance requirements. Displaying the official stamps and seals, represents the legitimacy from third-party organizations such as anti-virus software providers and payment gateways (Nathan Fillion, 2020).

Emotional Factors

An own brand voice, humanizing the website and giving the customer a glimpse of what the company stands for helps to increase consumer trust on an emotional level (Nathan Fillion, 2020).

Social proof

Social proof such as testimonials form pervious buyers, honest product ratings and reviews, ability to share on social media or partnership with an influencer increase consumer trust. The more social proof the less hesitant customers are to finalize their purchase (Nathan Fillion, 2020).

7. Bibliography

ANDRIOLE, Steve, 2019. Data Into Propaganda - Watch “The Great Hack” & Worry Way Beyond Cambridge Analytica. *Forbes* [online]. 21 August 2019. [Viewed 18 February 2020]. Available from: https://www.forbes.com/sites/steveandriole/2019/08/21/data-into-propaganda-watch-the-great-hack-worry-way-beyond-cambridge-analytica/

ANT, Adeane, 2019. Blue Whale: The truth behind an online “suicide challenge.” *BBC News* [online]. 13 January 2019. [Viewed 29 April 2020]. Available from: https://www.bbc.com/news/blogs-trending-46505722

ATHEY, Susan, CATALINI, Christian and TUCKER, Catherine, 2017. The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. . 6 January 2017. P. 34.

BARTH, Susanne and JONG, Menno D.T. de, 2017. The privacy paradox - Investigating discrepancies between expressed privacy concerns and actual online behavior â€“ A systematic literature review | Elsevier Enhanced Reader. [online]. 28 April 2017. [Viewed 16 April 2020]. Available from: https://reader.elsevier.com/reader/sd/pii/S0736585317302022?token=88EE2616843289C14048765742A19A3964E877D3BB417A724AD8599F8137CFFED00BD99B8E4B769A5CB5F5769E3D88B5

BAS, Burger, 2020. As technology advances, businesses need to be more trustworthy than ever. *World Economic Forum* [online]. 24 January 2020. [Viewed 4 May 2020]. Available from: https://www.weforum.org/agenda/2020/01/trust-in-technology-is-vital-heres-how-to-maintain-it/

BASANI, Vijay, 2016. 9 Important Elements to Corporate Data Security Policies that Protect Data Privacy. [online]. 5 October 2016. [Viewed 1 June 2020]. Available from: https://www.securitymagazine.com/articles/87113-important-elements-to-corporate-data-security-policies-that-protect-data-privacy

BERENDT, Bettina, GÜNTHER, Oliver and SPIEKERMANN, Sarah, 2005. Privacy in e-commerce: stated preferences vs. actual behavior. *Communications of the ACM*. 4 January 2005. Vol. 48, no. 4, p. 101–106. DOI 10.1145/1053291.1053295.

BERNERS-LEE, Tim, 2019. Opinion | I Invented the World Wide Web. Here’s How We Can Fix It. *The New York Times* [online]. 24 November 2019. [Viewed 31 May 2020]. Available from: https://www.nytimes.com/2019/11/24/opinion/world-wide-web.html

BISSON, David, 2020. 5 Ways Your Organization Can Ensure Improved Data Security. *The State of Security* [online]. 28 January 2020. [Viewed 1 June 2020]. Available from: https://www.tripwire.com/state-of-security/security-data-protection/5-ways-you-can-ensure-improved-data-security/

CARRRASCAL, Juan Pablo, CHERUBINI, Mauro, OLIVEIRA, Radrigo de, RIEDERER, Christoper and ERRAMILLI, Vijay, 2013. Your browsing behavior for a big mac | Proceedings of the 22nd international conference on World Wide Web. [online]. 5 January 2013. [Viewed 15 March 2020]. Available from: https://dl.acm.org/doi/10.1145/2488388.2488406

CERN, 2020a. A short history of the Web. [online]. 2020. [Viewed 31 May 2020]. Available from: https://home.cern/science/computing/birth-web/short-history-web

CERN, 2020b. The birth of the Web. [online]. 2020. [Viewed 31 May 2020]. Available from: https://home.cern/science/computing/birth-web

CHENG, Milton, 2020. Questions directors need to ask in the age of stakeholder capitalism. *World Economic Forum* [online]. 1 August 2020. [Viewed 1 May 2020]. Available from: https://www.weforum.org/agenda/2020/01/what-is-the-role-of-directors-in-the-age-of-stakeholder-capitalism/

CLAIMING HUMAN RIGHTS, 2008. Privacy - Definition. *Claiming Human Rights* [online]. 18 December 2008. [Viewed 16 March 2020]. Available from: http://www.claiminghumanrights.org/privacy_definition.html

CLEMENT, J., 2020. Top U.S. mobile social apps by users 2019. *Statista* [online]. 29 April 2020. [Viewed 4 May 2020]. Available from: https://www.statista.com/statistics/248074/most-popular-us-social-networking-apps-ranked-by-audience/

COHEN, Julie *E., What Is Privacy For*, [no date]. [online]. [Viewed 16 March 2020]. Available from: https://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf

CONSTINE, Josh, 2019. Facebook shares rise on strong Q3, users up 2% to 2.45B | TechCrunch. [online]. 30 October 2019. [Viewed 15 December 2019]. Available from: https://techcrunch.com/2019/10/30/facebook-earnings-q3-2019/

DENTZEL, Zaryn, 2013. How the Internet Has Changed Everyday Life. *OpenMind* [online]. 2013. [Viewed 31 January 2020]. Available from: https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/

FAUERBACH, Therese, 2017. Data Reigns in Today's Data Economy. *The Northridge Group* [online]. 21 December 2017. [Viewed 14 March 2020]. Available from: https://www.northridgegroup.com/blog/more-valuable-than-oil-data-reigns-in-todays-data-economy/

FILLION, Nathan, 2017. Why Trust Is So Important in Ecommerce - Thought Reach. [online]. 2017. [Viewed 2 May 2020]. Available from: http://thoughtreach.com/why-trust-is-so-important-in-ecommerce/

GIMPEL, Henner, KLEINDIENST, Dominikus and WALDMANN, Daniela, 2018. The disclosure of private data: measuring the privacy paradox in digital services. *Electronic Markets*. 11 January 2018. Vol. 28, no. 4, p. 475–490. DOI 10.1007/s12525-018-0303-8.

GLOBAL ENGLISH, 2018. How Facebook uses the "privacy paradox" to keep users sharing. *Global English (Middle East and North Africa Financial Network)* [online]. 15 April 2018. [Viewed 28 March 2020]. Available from: https://advance.lexis.com/document/?pdmfid=1516831&crid=e2a71e4e-da4e-414e-8fc7-bbfcb23d6a8e&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A5S4D-W5H1-JCNX-30XF-00000-00&pdcontentcomponentid=300986&pdteaserkey=sr1&pditab=allpods&ecomp=pp79k&earg=sr1&prid=73df54ab-f6e3-427c-9b4e-cab4ed58d184

GOOGLE, 2020. About the ad auction - AdSense Help. [online]. 2020. [Viewed 24 May 2020]. Available from: https://support.google.com/adsense/answer/160525?hl=en

GREENWALD, Glenn, MACASKILL, Ewen and POITRAS, Laura, 2013. Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian* [online]. 11 June 2013. [Viewed 20 May 2020]. Available from: https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

HILL, Kashmir, 2020. The Secretive Company That Might End Privacy as We Know It. *The New York Times* [online]. 18 January 2020. [Viewed 14 March 2020]. Available from: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

HUIZER, Erik, 2017. A Brave New World: How the Internet Affects Societies. *Internet Society* [online]. 5 November 2017. [Viewed 4 February 2020]. Available from: https://www.internetsociety.org/resources/doc/2017/a-brave-new-world-how-the-internet-affects-societies/

LILLINGTON, Karin, 2020. EU needs to rebuild GDPR after only two years in existence. [online]. 28 May 2020. [Viewed 31 May 2020]. Available from: https://advance.lexis.com/document/?pdmfid=1516831&crid=f99092cd-8b48-46c8-b2d1-c2dc73bf54fc&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A600T-7CJ1-JC8Y-8393-00000-00&pdcontentcomponentid=142626&pdteaserkey=sr1&pditab=allpods&ecomp=kb63k&earg=sr1&prid=1fe8de95-61e5-4e74-af9f-81e4973ae802

KNIJPENGA, Andreas, 2020. GDPR-Consequences for Swiss businesses. *Deloitte Switzerland* [online]. 2020. [Viewed 31 May 2020]. Available from: https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-consequences-for-swiss-businesses.html

KOKOLAKIS, Spyros, 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*. 1 January 2017. Vol. 64, p. 122–134. DOI 10.1016/j.cose.2015.07.002.

KOTLER, Philip and ARMSTRONG, Gary, 2018. *Principles of Marketing 17e*. 17. Pearson Education ©. ISBN ISBN 978-0-13-449251-3.

KÜBLER, Dorothea, NORMANN, Hans-Theo and BENNDORF, Volker, 2015. Privacy concerns, voluntary disclosure of information, and unraveling: An experiment - ScienceDirect. [online]. 4 January 2015. [Viewed 14 December 2019]. Available from: https://www.sciencedirect.com/science/article/pii/S0014292115000069

LEE, Chung Hun and CRANAGE, David A., 2011. Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel Web

sites. *Tourism Management*. 10 January 2011. Vol. 32, no. 5, p. 987–994. DOI 10.1016/j.tourman.2010.08.011.

LEETARU, Kalev, [no date]. As GDPR Turns One Is It A Success Or A Failure? *Forbes* [online]. [Viewed 31 May 2020]. Available from: https://www.forbes.com/sites/kalevleetaru/2019/05/06/as-gdpr-turns-one-is-it-a-success-or-a-failure/

LEVENFELD, Ari, [no date]. Quantcast BrandVoice: Data Protection Trends: What GDPR And Other Regulations Mean For 2019 And Beyond. *Forbes* [online]. [Viewed 31 May 2020]. Available from: https://www.forbes.com/sites/quantcast/2019/03/14/data-protection-trends-what-gdpr-and-other-regulations-mean-for-2019-and-beyond/

LUKÁCS, Adrienn, [no date]. WHAT IS PRIVACY? THE HISTORY AND DEFINITION OF PRIVACY. . [online] [Viewed 15 January 2020] Available from: http://publicatio.bibl.u-szeged.hu/10794/7/3188699.pdf

LUND, Jennifer, 2019. GDPR: What is It and How Does it Impact My Business? *CRM Blog: Articles, Tips and Strategies by SuperOffice* [online]. 21 November 2019. [Viewed 15 December 2019]. Available from: https://www.superoffice.com/blog/gdpr/

LUTZ, Christoph and STRATHOFF, Pepe, 2014. Privacy Concerns and Online Behavior Not so Paradoxical after All? Viewing the Privacy Paradox Through Different Theoretical Lenses. *SSRN Electronic Journal* [online]. 2014. [Viewed 20 November 2019]. DOI 10.2139/ssrn.2425132. Available from: http://www.ssrn.com/abstract=2425132

MASSE, Estelle, Two Years Under The EU GDPR , [online]. May 2020 [Viewed 31 May 2020]. Available from: https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf

MARREIROSA, Helia, VLASSOPOULOS, Mirco, SCHRAEFEL, M.C. and MICHAEL, Toni, 2017. “Now that you mention it”: A survey experiment on information, inattention and online privacy | Elsevier Enhanced Reader. [online]. 30 March 2017. [Viewed 14 December 2019]. Available from: https://reader.elsevier.com/reader/sd/pii/S0167268117300896?token=3B12F2988A86BFAD7FBC2C7155FD2EAD328753F0E31C9CCB3C85C68E9A4AD70D33FDE822DAE18BEA5053721708ABEC78

MCMENEMY, David, 2016. Rights to privacy and freedom of expression in public libraries: squaring the circle. . 15 August 2016. P. 9.

MEISENZAHL, Mary, 2019. The 11 biggest scandals Mark Zuckerberg faced over the last decade as he became one of the world's most powerful people. *Business Insider* [online]. 16 December 2019. [Viewed 3 May 2020]. Available from: https://www.businessinsider.com/mark-zuckerberg-scandals-last-decade-while-running-facebook-2019-12

NATIONAL PRIVACY COMMISSION, 2017. Creating a Privacy Manual. *National Privacy Commission* [online]. 20 March 2017. [Viewed 1 June 2020]. Available from: https://www.privacy.gov.ph/creating-a-privacy-manual/

NAUGHTON, John, 2019. The privacy paradox: why do people keep using tech firms that abuse their data? *The Guardian* [online]. 5 May 2019. [Viewed 15 December 2019]. Available from: https://www.theguardian.com/commentisfree/2019/may/05/privacy-paradox-why-do-people-keep-using-tech-firms-data-facebook-scandal

NCSL, 2019. Data Security Laws | Private Sector. [online]. 29 May 2019. [Viewed 31 May 2020]. Available from: https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx

NORBERG, Patrica A., HORNE, Daniel R. and HORNE, David A., 2007. The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors - NORBERG - 2007 - Journal of Consumer Affairs - Wiley Online Library. [online]. 3 June 2007. [Viewed 14 December 2019]. Available from: https://onlinelibrary.wiley.com/doi/full/10.1111/j.1745-6606.2006.00070.x

OCTAVIAN, Radu Anamaria-Catalina, ORZAN Mihai Cristian , DOBRESCU Andra Ileana, Arsene, 2016. The Importance of Trust and Privacy in Social Media. [online]. 30 June 2016. [Viewed 11 April 2020]. Available from: https://advance.lexis.com/document/?pdmfid=1516831&crid=9b4c77fd-d3ea-4462-b2ed-234b8378517a&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A5K4J-4G31-JD09-30YM-00000-00&pdcontentcomponentid=400927&pdteaserkey=sr1&pditab=allpods&ecomp=pp79k&earg=sr1&prid=caba85e9-9f36-479b-9276-99b0639a0acc

OGURY, [no date]. GDPR One Year On: Survey Findings Show Consumer Awareness with Data Use is Concerningly Low; - A staggering eight percent of consumers globally feel they have a better understanding of how companies use their data since GDPR's introduction. [online]. [Viewed 1 June 2020]. Available from: https://advance.lexis.com/document/?pdmfid=1516831&crid=5c958407-a134-4d08-ac15-b4e4b0de4bfe&pddocfullpath=%2Fshared%2Fdocument%2Fnews%2Furn%3AcontentItem%3A5W5X-5YN1-DXP3-R0CV-00000-00&pdcontentcomponentid=8054&pdteaserkey=sr4&pditab=allpods&ecomp=kb63k&earg=sr4&prid=c3c8c765-7677-4dcd-bfb6-7c54b333c175

PARK, Yong Jin, CAMPELL, Scott W. and KWAK, Nojin, 2012. Affect, cognition and reward: Predictors of privacy protection online. [online]. May 2012. [Viewed 12 April 2020]. Available from: https://reader.elsevier.com/reader/sd/pii/S0747563212000064?token=451920230C6F69CC90D632D68F8D00BF597AB57EC489C841AB235425B3F6EB604D560097140A0BD7E5690EBB7FD9A060

PAVEL, Valentina, 2019. We should know all our data and profiles | Privacy International. [online]. 17 July 2019. [Viewed 3 May 2020]. Available from: https://privacyinternational.org/taxonomy/term/488

PLESCH, Joachim and WOLFF, Irenaeus, 2018. Personal-Data Disclosure in a Field Experiment: Evidence on Explicit Prices, Political Attitudes, and Privacy Preferences. *Games*. 2018. Vol. 9, no. 2, p. 1–14. June 2018 [Viewed 1 February 2020]. Available from: https://search.proquest.com/econlit/docview/2160363530/E376636F36644619PQ/7

PRIVACY INTERNATIONAL CAMPAIGNS, 2017. What Is Privacy? *Privacy International* [online]. 23 October 2017. [Viewed 16 March 2020]. Available from: https://privacyinternational.org/explainer/56/what-privacy

PRIVACY INTERNATIONAL, 2020. GDPR - 2 years on. *Privacy International* [online]. 22 May 2020. [Viewed 31 May 2020]. Available from: http://privacyinternational.org/news-analysis/3842/gdpr-2-years

PRIVACY INTERNATIONAL, The Keys to Data Protection [online]. August 2018 [Viewed 31 May 2020]. Available from: https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf

READHEAD, Harry, 2020. The privacy paradox: How we got trapped in a data dystopia. *City AM*. 1; National. City AM Ltd, 18 February 2020. p. 18. [Viewed 28 March 2020]. Available from: http://global.factiva.com/redir/default.aspx?P=sa&an=CITYMO0020200218eg2i0001o&cat=a&ep=ASE

ROCHELANDET, Fabrice and TAI, Silvio H., 2016. Do privacy laws affect the location decisions of internet firms? Evidence for privacy havens. *European Journal of Law and Economics; New York*. 10 January 2016. Vol. 42, no. 2, p. 339–368. DOI http://dx.doi.org/10.1007/s10657-013-9428-6.

SARABIA-SÁNCHEZ, Francisco-José, AGUADO, Juan-Miguel and MARTÍNEZ-MARTÍNEZ, Inmaculada J., 2019. Privacy paradox in the mobile environment: The influence of the emotions. *El Profesional de la Información*. 3 December 2019. Vol. 28, no. 2, p. 1–11. DOI 10.3145/epi.2019.mar.12.

SAS, [no date]. Big Data: What it is and why it matters. [online]. [Viewed 12 February 2020]. Available from: https://www.sas.com/en_us/insights/big-data/what-is-big-data.html

SHARMA, Vijay K, 2019. Impact of internet on business. *KLIENT SOLUTECH* [online]. 16 January 2019. [Viewed 12 February 2020]. Available from: http://www.klientsolutech.com/impact-of-internet-on-business/

SOBERS, Rob, 2019. GDPR's Impact So Far: Must-Know Stats and Takeaways - Varonis. *Inside Out Security* [online]. 27 June 2019. [Viewed 31 May 2020]. Available from: https://www.varonis.com/blog/gdpr-effect-review/

STATISTA, 2019. Internet usage worldwide. *Statista* [online]. 25 June 2019. [Viewed 31 January 2020]. Available from: https://www.statista.com/study/12322/global-internet-usage-statista-dossier/

SWANSON, Ana, 2016. The economic impact of distrust. *World Economic Forum* [online]. 9 January 2016. [Viewed 1 May 2020]. Available from: https://www.weforum.org/agenda/2016/09/the-economic-impact-of-distrust/

TADDICKEN, Monika, 2014. The 'Privacy Paradox' in the Social Web: The Impact of Privacy Concerns, Individual Characteristics, and the Perceived Social Relevance on Different Forms of Self-Disclosure. *Journal of Computer-Mediated Communication*. 1 January 2014. Vol. 19, no. 2, p. 248–273. DOI 10.1111/jcc4.12052.

TEXAS A&M UNIVERSITY, 2015. The right to privacy in the digital age Definition of Privacy and its importance Privacy is the right to be free from. *Texas A&M University* [online]. 2015. [Viewed 15 April 2020]. Available from: https://www.coursehero.com/file/31608159/ochr-privacy-reportpdf/

THE GLOBAL GOALS, 2020. Privacy Policy. *The Global Goals* [online]. 2020. [Viewed 1 June 2020]. Available from: https://www.globalgoals.org/privacy-policy

The right to privacy in the digital age, [no date]. [online]. [Viewed 15 March 2020]. Available from: https://www.ifla.org/files/assets/faife/ochr_privacy_ifla.pdf

THE WORLD BANK GROUP, 2020. Connecting for Inclusion: Broadband Access for All. *World Bank* [online]. 2020. [Viewed 31 May 2020]. Available from: https://www.worldbank.org/en/topic/digitaldevelopment/brief/connecting-for-inclusion-broadband-access-for-all

THE WORLD ECONOMIC FORUM, Digital Transformation Initiative, [online]. May 2018 [Viewed 30 January 2020]. Available from: http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-executive-summary-20180510.pdf

TOOTHMAN, Jessika, 2008. What's the Difference Between the Internet and the World Wide Web? *HowStuffWorks* [online]. 9 July 2008. [Viewed 31 May 2020]. Available from: https://computer.howstuffworks.com/internet/basics/internet-versus-world-wide-web.htm

UNITED NATIONS, 2016. Human Rights. [online]. 30 August 2016. [Viewed 16 March 2020]. Available from: https://www.un.org/en/sections/issues-depth/human-rights/

Universal Declaration of Human Rights, [no date]. [online]. [Viewed 16 March 2020]. Available from: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

VINOCUR, Nicholas, 2019. 'We have a huge problem': European tech regulator despairs over lack of enforcement. *POLITICO* [online]. 27 December 2019. [Viewed 1 June 2020]. Available from: https://www.politico.com/news/2019/12/27/europe-gdpr-technology-regulation-089605

WARBY PARKER COMPANY, 2020. Warby Parker History. *Warby Parker* [online]. 2020. [Viewed 2 May 2020]. Available from: https://www.warbyparker.com

WIBSON, 2020. How Much Is >Your< Data Worth? At Least $240 per Year. Likely Much More. *Medium* [online]. 12 May 2020. [Viewed 2 June 2020]. Available from: https://medium.com/wibson/how-much-is-your-data-worth-at-least-240-per-year-likely-much-more-984e250c2ffa

WITTES, Benjamin and LIU, Jodie C, 2015. The privacy paradox: The privacy benefits of privacy threats. . 5 January 2015. P. 21. [Viewed 25 November 2019]. Available from: https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:5G1T-GS01-F03R-N36M-00000-00&context=1516831.

WITTES, Benjamin, 2015. The Privacy Paradox: The Privacy Benefits of Privacy Threats. *http://www.lawfareblog.com* [online]. 21 May 2015. [Viewed 25 November 2019]. Available from: https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:5G1T-GS01-F03R-N36M-00000-00&context=1516831.

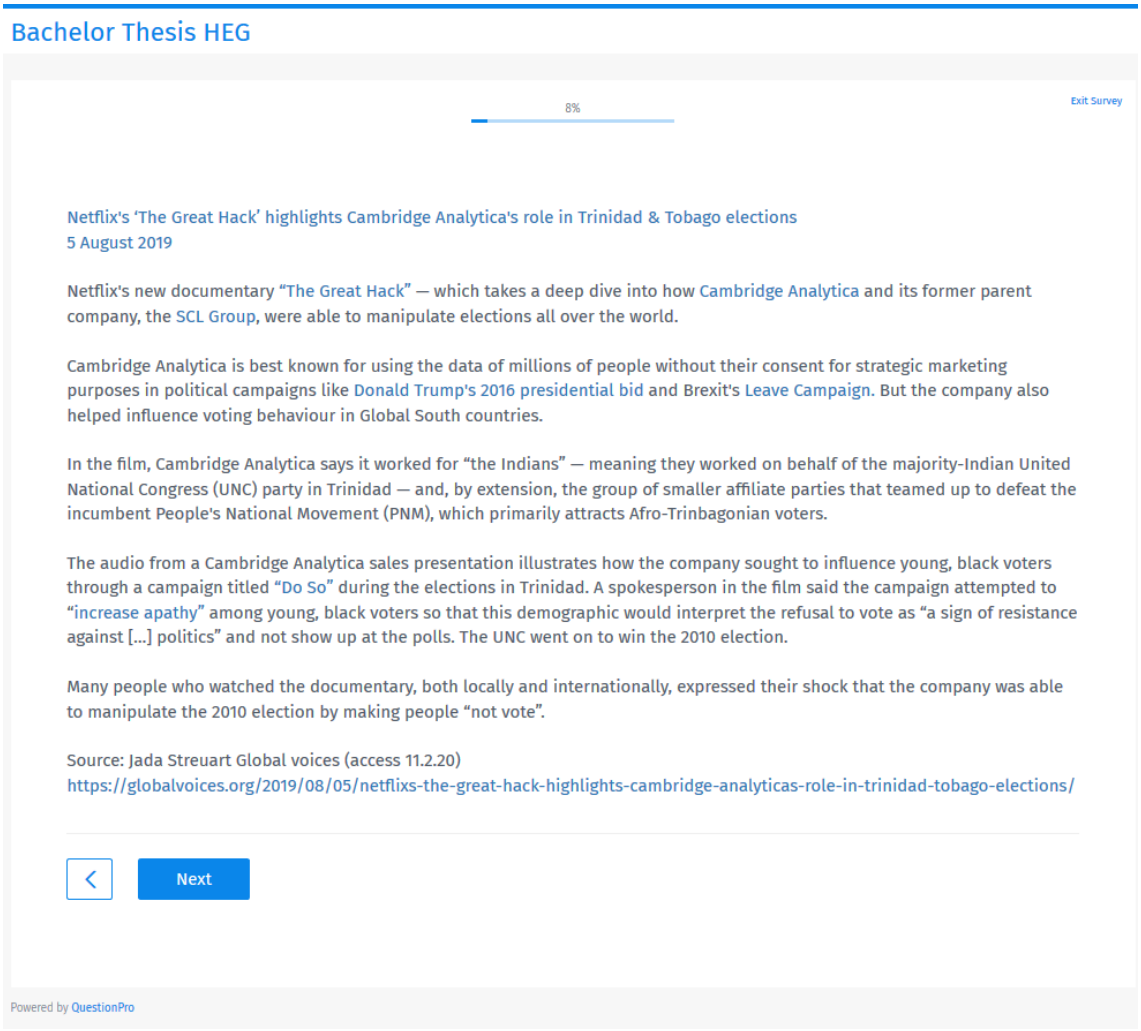
WITTES, Benjamin, 2017. The Privacy Paradox II: An Event at Brookings on Friday. *Lawfare* [online]. 1 October 2017. [Viewed 25 November 2019]. Available from: https://advance.lexis.com/api/document?collection=news&id=urn:contentItem:5MKS-53C1-F03R-N13M-00000-00&context=1516831

WONG, Julia Carrie, 2019. The Cambridge Analytica scandal changed the world – but it didn't change Facebook. *The Guardian* [online]. 18 March 2019. [Viewed 20 May 2020]. Available from: https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook

WORLD WIDE WEB FOUNDATION, 2020. Sir Tim Berners-Lee. *World Wide Web Foundation* [online]. 2020. [Viewed 31 May 2020]. Available from: https://webfoundation.org/about/sir-tim-berners-lee/

8. Appendix

Appendix 1: Screen shot of hard to read article in the survey



Appendix 2: Survey Questions

Q1: The previously read article looks at which aspects of data collection?

- Positive aspects
- Neutral aspects
- Negative aspects

Q2: You are:

- Male
- Female
- Other
- Prefer not to say

Q3: What's your age range?

- Younger than 18
- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 64+
- Prefer not to say

Q4: In what part of Switzerland do you live?

- Canton GE
- Canton VD
- Canton BE
- Canton NE
- Canton FR
- Other
- Prefer not to say

Q5: In general would you say that your health is

- Excellent
- Very good
- Good
- Fair
- Poor
- Prefer not to say

Q6: How often do you eat chocolate?

- Almost never

- Once a week
- 2-5 times a week
- Daily
- Multiple times a day
- Prefer not to say

Q7: How often do you smoke?

- Never
- Sometimes
- Regularly
- Often
- Prefer not to say

Q8: How often do you drink alcohol?

- Never
- Sometimes
- Regularly
- Often
- Prefer not to say

Q9: Do you take illegal drugs?

- Never
- Sometimes
- Regularly
- Often
- Prefer not to say

Q10: Do you have any history of cancer in your family?

- Yes
- No
- Never

Q11: Do you have any history of mental illness in your family?

- Yes
- No
- Never

Q12: How much time do you spent online per day?

- 0-30min
- 30-60min

- 60-90min
- 90-120min
- 120-150min
- 150min+
- Prefer not to say

Q13: What is your monthly income?

- 0-500 CHF
- 500-1000 CHF
- 1000-1500 CHF
- 1500-2000 CHF
- 2500 CHF+
- Prefer not to say

Q14: How much financial support do you receive?

- 0-500 CHF
- 500-1000 CHF
- 1000-1500 CHF
- 1500-2000 CHF
- 2500 CHF+
- Prefer not to say

Q15: How much money do you spend on a weekly basis?

- 0-500 CHF
- 500-1000 CHF
- 1000-1500 CHF
- 1500-2000 CHF
- 2500 CHF+
- Prefer not to say

Q16: How much financial debt do you have?

- 0-500 CHF
- 500-1000 CHF
- 1000-1500 CHF
- 1500-2000 CHF
- 2500 CHF+
- Prefer not to say

Q17: Did you feel comfortable answering the above questions?

- Yes
- No

Q18: How much are you willing to pay to protect your data provided in this survey for one year?

- 0 CHF
- 10 CHF
- 30 CHF
- 50 CHF
- 100 CHF
- 150+ CHF

Q19: How much would you be willing to pay to protect your data on social media (Facebook, Whatsapp, Instagram etc.) for one year?

- 0 CHF
- 10 CHF
- 30 CHF
- 50 CHF
- 100 CHF
- 150+ CHF

Q20: How much would you be willing to pay to protect all your data (browser history, google search history, history of products bought online etc.) for one year?

- 0 CHF
- 10 CHF
- 30 CHF
- 50 CHF
- 100 CHF
- 150+ CHF

Contact Information (optional)

- First Name
- Last Name
- Phone
- Email Address