Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technologies

Bachelor Thesis

Privacy Attitudes and Behaviour in Online Social Networks

Kalinina Elizaveta Alisa

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

BACHELOR THESIS ASSIGNMENT

Elizaveta Alisa Kalinina

Business Administration

Thesis title

Privacy Attitudes and Behavior in Online Social Networks

Objectives of thesis

The main objective of the thesis is to explore relationships between the privacy attitudes and actual behavior among online social network (OSN) users.

The partial objectives of the thesis are such as following:
- To create an up to date overview of definitions and theoretical models describing privacy concerns of OSN users;
- To conduct a survey among group of active users at a major OSN platform;
- To synthesize and discuss findings with other relevant studies in the field.

Methodology

The methodology of this thesis will be based on the literature review and quantitative methods of approach, such as a questionnaire survey and hypothesis testing. First of all, the literature study will be done. Secondly, the own research will be conducted in a form of survey, statistical analysis and interpretation. After the data is analyzed the statistical inference will be shown and the conclusion of the study will be formulated.

The proposed extent of the thesis

30 – 40 pages

Keywords

Privacy, online social networks, privacy perception, behaviour, personal data.

Recommended information sources

CHOI, Hanbyul; PARK, Jonghwa; JUNG, Yoonhyuk. The role of privacy fatigue in online privacy behavior. Computers in Human Behavior, 2018, 81: 42-51.

KOKOLAKIS, Spyros. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. Computers & security, 2017, 64: 122-134.

LIU, Yabing, et al. Analyzing facebook privacy settings: user expectations vs. reality. In: Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference. ACM, 2011. p. 61-70.

ZHANG, Chi, et al. Privacy and security for online social networks: challenges and opportunities. IEEE network, 2010, 24.4: 13-18.

ZHELEVA, Elena; TERZI, Evimaria; GETOOR, Lise. Privacy in social networks. Synthesis Lectures on Data Mining and Knowledge Discovery, 2012, 3.1: 1-85.

Expected date of thesis defence

2020/21 SS – FEM

The Bachelor Thesis Supervisor

Ing. Miloš Ulman, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 21. 7. 2020

Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 19. 10. 2020

Ing. Martin Pelikán, Ph.D.

Dean

Prague on 25. 02. 2021

Declaration

I declare that I have worked on my bachelor thesis titled "Privacy Attitudes and Behaviour in Online Social Networks" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the bachelor thesis, I declare that the thesis does not break copyrights of any their person.

In Prague on 14.03.2021 _____

Acknowledgement

I would like to thank Professor Mr. Milos Ulman for his advice and support during my work on this thesis.

Privacy Attitudes and Behaviour in Online Social Networks

Abstract

For the past few years, online social networks (OSNs) experienced ascending growth and have become a significant part of online activity. Online social networks give web users many new ways to socialize, communicate and share news about their life. In one way or another, almost every network like Facebook, Twitter, Instagram and YouTube keep important and personal information on users and their interactions, which raises a big consideration on privacy and security. Many surveys reveal that people in the computer age are concerned about their privacy on the internet. In spite of this, users are willing to trade their privacy for a comparatively small reward. In this paper, we analyze studies that provide evidence of differentiation attitudes and real behavior in OSNs.

Keywords: privacy, privacy paradox, personal data, online social networks.

Soukromí postoje a chování v online sociálních sítích

Abstrakt

Během posledních několika let zaznamenaly online sociální sítě (OSSs) vzestupný růst a staly se významnou součástí online aktivity. Online sociální sítě poskytují uživatelům webu mnoho nových způsobů, jak se stýkat, komunikovat a sdílet zprávy o svém životě. Facebook, Instagram a YouTube tak či onak uchovávají důležité a osobní informace o uživatelích a jejich interakcích, což vyvolává velký ohled na soukromí a bezpečnost. Mnoho průzkumů ukazuje, že lidé v počítačovém věku mají obavy o své soukromí na internetu. Navzdory tomu jsou uživatelé ochotní vyměnit své soukromí za poměrně malou odměnu. V tomto článku analyzujeme studie, které poskytují důkazy o diferenciačních postojích a skutečném chování v OSS.

Klíčová slova: soukromí, paradox soukromí, osobní údaje, online sociální sítě.

Table of content

List of tables

List of figures

1 Introduction

Privacy was the main concern for people from the ancient world up until the digital age. Nowadays privacy is included in human and legal rights all over the world and considered essential for the person. As nearly 3 billion people use OSNs, it has become very easy to obtain data from the individual. Firms and OSNs can broadcast an individual's secrets to anonymous recipients, who can use this information in different ways.

There are many surveys that indicate people reveal their personal information on social networks for a comparatively small reward. Once was conducted an experiment after which was found out that people value their online browsing history for only 7 Euros (Carrascal, Riederer, Erramilli, Cherubini, De Oliveira, 2013). Nevertheless, many surveys show that individuals are very concerned with gathering and using their private information. Pennsylvanian University in 2015 discovered that 91% of participants agree that personal data should not be traded for any type of discount. Also, 71% of subjects think that although stores give free wireless internet, it is unethical to monitor what people are looking for online (Turow, Hennessy, Draper 2015). In 2013 the Pew Research Center in its poll discovered that 86% of US participants try to stay private online by using encryption of emails and cookies (Rainie, Kiesler, Kang, 2013). They also found out that 74% of phone owners use the device for location information in real-time and 18% of those people use applications to show friends their current location (Zickuhr, 2012). This contradiction between privacy attitude and real behavior is called the "information privacy paradox" (privacy paradox). The term was first coined by Bedrick in 1998 (Kirtley, Writers, Bedrick, Lerner, Whitehead 1998) and can be found in numerous researches, studies, and surveys.

Privacy paradox and privacy problems have become a big obstacle for e-commerce, e-government and online social networks. E-commerce and OSNs are the biggest collectors of personal information, that is why many people still prefer traditional ways of communicating and shopping as they have to give a lot of personal details such as ID, credit card number and address when shopping online. Proving the existence of a privacy paradox would encourage OSNs and firms to collect more personal information.

After the introduction, the paper continues with presenting the objectives and methodology of the thesis. In section three will be done the literature review with the definitions of OSNs and privacy. Furthermore, some threats that people can face while

searching online and additionally privacy security will be presented. In section four the survey about the dichotomy between privacy attitudes and behavior will be organized. In section five the results of the questionnaire will be analyzed and shown with the discussion of the topic. Finally, in the sixth section, the conclusion of the paper will be conducted.

2 Objectives and Methodology

2.1 Objectives

The main objective of the thesis is to explore relationships between privacy attitudes and actual behavior among online social network (OSN) users. Another objective is to see if people are willing to disclose their personal information for money. This will be done with the creation of an up-to-date overview of the research on privacy concerns and behavior of OSN users. Also, to deliver empirical evidence, a survey among a group of active users will be conducted on an OSN platform. All the findings will be discussed and synthesized with the other findings in the field.

2.2 Methodology

The methodology of this thesis will be based on the literature review and quantitative methods of approach, such as a questionnaire survey and hypothesis testing. First of all, the literature study will be done. Secondly, the own research will be conducted in a form of a survey, statistical analysis and interpretation. After the data is analyzed the statistical inference will be shown and the conclusion of the study will be formulated.

3 Literature Review

3.1. Online Social Networks

In recent years the participation in OSNs has dramatically increased and went from an unknown phenomenon to a daily part of people's life. Communicating across big distances was a big concern for people from ancient history.

3.1.1. Background

The first communication method dates back to 500 B.C. It was very important for people to know what the other tribes were doing. The basic delivery system was by messengers. Later, people started to write letters, but the only problem with them was the long wait for the answer. That is why sometimes people used fire codes. They could be seen from far away and even could mean different messages. For example, one bonfire meant that enemies are coming, two bonfires that they are very close to, and four bonfires code was for emergencies. Centuries later, in 1792 was invented the new communication system, which was called the telegraph. Although the messages were very short, they could come far faster than a messenger on the horse (Coe L, 1993). The biggest inventions in communication at long distances were the telephone in 1890 and the radio in 1891. These technologies helped people to communicate instantly at any point in the world. Nowadays we still use these technologies in our daily life, the one difference is that the newest developments are much more complicated than the former ones.

In the 20th century, all technologies become to grow rapidly. After the first supercomputer in 1940, just in 20 years, the first network similar to nowadays the Internet was invented. The first Social Networking site was created in 1997, which led to a huge sensation in the world of technologies. From this moment more and more sites were created, which was the starting point of OSN's popularity.

3.1.2 What is OSN?

Generally speaking, OSNs are sites that help people to communicate in daily life. They have different purposes, from business communication to looking for aspirations. In spite of this, they have a basic feature, which is called a profile. This is an independent

page that represents real or “fake” users. Sometimes people make fake profiles in order to stay anonymous or appear the opposite of how they are. Users have to fill a small questionnaire that will represent themselves, their interests and hobbies. The majority of the websites ask users to add a profile photo and other sites encourage people to post more multimedia in profiles or modify them. (Dwyer, Hiltz, Passerini, 2007)

Nowadays, many businesses make a profile in OSNs to help them grow faster and make more profit from it. There are many categories of social media sites can be divided into, but the most popular are:

- Communication networks, where people can contact others or find new dates and friends (Facebook, Tinder, Twitter). If you are an influencer, they can also help your business in marketing, customer services and building new relationships.
- Media sharing networks, where people disclose or find some photos and videos (Instagram, YouTube, Snapchat). They are helpful with valuable audience engagement, business awareness and also marketing. If the influencer has nice pictures or videos on its page and trying hard to engage customers, the probability that customers will notice and choose them is more.
- Discussion and blogging forums. They were one of the first OSNs, where people shared opinions, discussed different points of view and shared new information (Reddit, Tumblr, Quora).
- Content Networks, which help people to find new inspirations and creative ideas. It helps to discover, share and save new content (Pinterest, Flipboard).
- Shopping networks, in which people can find new clothes or trends, follow brand’s shops and purchase new outfit (Etsy, Farfetch, Polyvore)
- Sharing networks, the main point of which is sell, trade and buy commodities or services (Uber, Airbnb and many other sites to find a dog sitter or a new cook home)

While in one OSN people are communicating with friends and relatives, on some websites people are not entitled to the relationship’s types at all, not by either user itself or the social site. Very often people are granted the possibility to have an exclusive relationship with people they do not even know on the OSN. Moreover, sometimes users are involved in the connection with the person without any further real relationships. That happens for example on YouTube, where people are subscribing to the person. They mainly like to watch their videos, but on the relationship level, subscribers understand they may not ever talk to that person not by either messaging or in real life (Elie Raad, 2013).

On Facebook, the users following each other are called “friends”, even though they may have met one time through friends and do not really know each other. Other social networks with their structure of relationship names can be seen in the following table:

Social Network Name	Focus	Relationships
Facebook	Communication	Friends
Instagram	Photo-sharing, blogging	Followers
YouTube	Video-sharing	Subscribers
Telegram	Communication, microblogging	Contacts communication, followers
Twitter	Microblogging	Followers

Table 1. Popular OSN and their purpose

Many people are using OSNs in their daily life basics. For Example, Facebook has 2.7 billion monthly engaged users, YouTube has 2 billion and Instagram has 1 billion. (McMullan, 2020) This brings us to the question if it is safe to have an OSN account and be involved with big corporations’ systems. In 2010 the founder of Facebook, Mark Zuckerberg said that with the invasion of social networks in our life, privacy could not be the social norm anymore (Johnson, 2014). Not many people liked that statement, as privacy was a big concern for people. The older people were very confused and frightened by the fact that their personal life would not be the same anymore. The young generation was taking this information more gently as some of them started using OSNs from the university or school times. In our time every twelve-year-old child has a profile in one or more social networks, where they post a lot of personal data on display. Nevertheless, there is still confusion between how people say they behave in OSNs and their real actions.

3.2. Privacy

Nowadays exist many definitions and concepts of the word ‘privacy’. Overall, it may be stated that privacy is a right to control the connection to somebody. The right of privacy is the most cultivated rights, moreover, it is preserved in law. Unfortunately, information privacy hasn’t achieved status like that yet.

Privacy is valuable for a person. It may differ depending on the country and species. Nevertheless, it is a basic human need to separate sometimes from society (Moore 2003).

3.2.1. Privacy definition

Before looking at the differences between privacy attitudes and behavior, the definition of privacy has to be stated. In the Cambridge dictionary, privacy characterizes as “someone’s right to keep their personal matters and relationships a secret”. There are three aspects of privacy: territorial privacy which can be recognized as the surrounding area of a person; the privacy of a person which gives protection to a person from misjudgment; and informational privacy, which states whether and how personal data can be gathered and used (Rosenberg, 1992) (Holvast, 1993). In this paper, we would study and discuss the third type of privacy

Informational privacy is very significant for the person, especially in the digital age. First research about information privacy dates back to the 1970s (Baker, 1972) and now it is still a popular topic to write and argue about. From that time many things have changed and if in 1970 computers just started to appear on markets, now we live in the computer world.

3.3. What data is gathered from OSN?

As people are sharing a vast majority of information online, companies can collect these pieces of information for their use. There was already been a big study, that gathered a lot of information and in which the author came up with the taxonomy of personal information (Schneier, 2010). In the end, he concluded 13 different types of information, which can be divided into two groups: service provider data type and user data types.

Service provider data types consist of the data that OSN is mainly responsible for. Even though the data is processed with the computers, sometimes the breaches of information happen and most of the time the people and especially individuals the user knows can be the cause of the problem. It includes 3 data types:

1. **Login data.** This is the first data that OSNs are gathering about an individual, which provides the identity of the user. It includes username, email address and passwords.
2. **Connection data** identifies the IP address, operating system and the location of the user. It helps OSN to acquire some information about the movement of the user, to de-anonymize some of them and connect it to already known unrelated data.

3. **Application data** includes card numbers, purchased items and statistics from users in online games. This type of data should be highly secured by the providers, as in the future it can lead to card frauds.

User data types are usually those for which the user is being responsible. OSNs are giving full freedom for people to create profiles and their social life on the sites, consequently, people are sharing there want they want and what they think is suitable for the particular network. These data types also divide into semantically specified, which gives the individual the opportunity to describe and express themselves; and semantically unspecified, which includes data that is predefined, but cannot be read by machines (for example photos). Semantically specified types are:

1. **Mandatory data** is a little set of data, which OSN are kindly asking to fill. It refers to the data users need to give, when registering for the first time. Common examples are the date of birth, hometown and some professional data.
2. **Extended profile data** helps users to describe some personality traits: favorite music, hobbies, education, interests and profile picture.
3. **Ratings/interests.** These are usually things, that bond OSN together, for example, people or groups users follow.
4. **Network data.** As people are coming to the social networks to communicate, the network data shows who the person follows, individuals' friends and followers.
5. **Contextual data** usually connects to already existing data, in order to give more information, including tagging features on the photos or adding the location to them.

Semantically unspecified types are:

6. **Private communication.** By the name of this data, it is very easy to understand what it stands for and usually, such type of data includes private conversations and video chats.
7. **Disclosed data** is all the information a person posts on the wall of the profile. It can be deleted only by the individual who owns the wall and depending on his settings, this data can only be seen to some group of people.
8. **Entrusted data** is comments or posts made on another person's wall. It can be deleted only by the user who posted it or the person who owns the wall.
9. **Incidental data** is usually sharing someone's post on the own wall. That way it becomes part of an individual's data.

10. **Disseminated data** is information that is being shared by an individual by other communication channels.

On the following figure are seen all of the data types mentioned above:

Source: https://www.researchgate.net/publication/269464322_Taxonomy_of_Social_Network_Data_Types

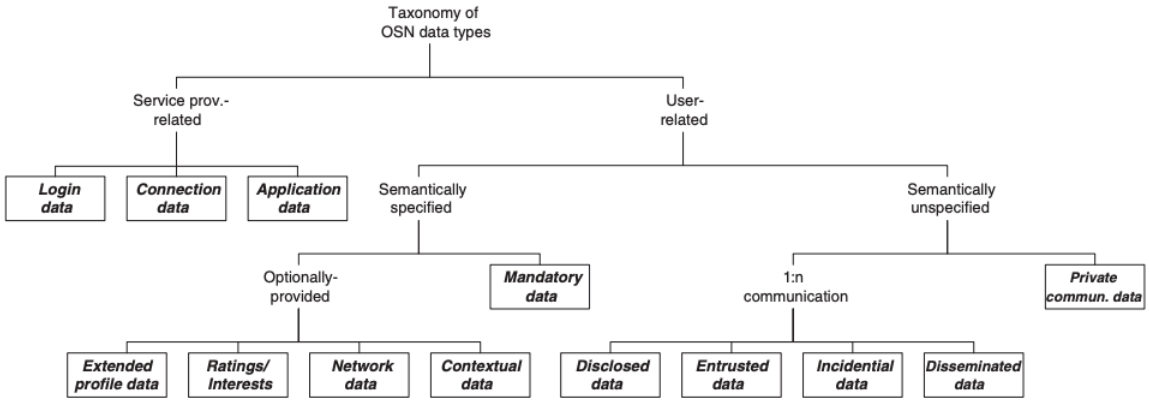


Figure 1. Data Types

3.4. Privacy and security

Generally, all the information mentioned above is gathered by OSNs and kept in their databases. For their maintenance and security is also responsible the social networks. Sometimes the users' private data is being exploited and sold to third parties for different purposes. A common example of it is when users are leaving a digital print in the OSNs and then their data is being analysed for profiling or advertising.

3.4.1. Threats

Because the vast majority of people using OSNs, the users may attract some attention from hackers and other privacy threats (Fire, 2014).

3.4.1.1. Classical threats

These types of threats have been known with the invention of the internet. Due to the spreading of OSNs, these attacks went viral. Usually, they try to expose personal information which has already been published by the users and their friends.

Malware is the short version of malicious software. Generally, it is an attack on someone's computer with the aim of accessing private content. The basic example of malware is stealing credential numbers and impersonating the user with it.

Phishing attacks are frauds, in which the attackers log into the OSN via fake or stolen identity and then inviting users' friends to click on the spam links in private messages.

Spam messages are those that people are not wanting to get. It can be posted on the walls of users or groups and messaged directly to the person. Usually, they consist of ads or links to phishing sites. They come from fake profiles, special spam applications or compromised accounts.

Cross-site scripting is an attack aimed at web-based applications, which gives the possibility to the intruder to enter some sensitive information, such as cookies and saving credit card numbers.

Internet Fraud also takes advantage of the people. They take advantage of users' profiles and then write to users' friends in order to ask them for a money transfer (Fire, 2014).

3.4.1.2. Modern threats

Mainly, those threats have a goal to obtain users' information or their friends.

Clickjacking is an attack, wherein the users are clicking on a link, which is not the same as what they intended. This type of threat mainly is used to spam on the user's wall.

De-Anonymization. It is widely used in the OSNs to log in with pseudonyms to protect one's data. Techniques of this type are using some methods, like cookies tracking and user group memberships to uncover the real identity of the individual.

Fake profiles are the most popular attacks, in which people create fake profiles and then spam from them to other users.

Identity clone attack is used to create a new fake profile but with credentials of another user's profile. It is used to collect information from that user's friends or do an online fraud

Cyberstalking is used to harass users with the aim to steal an identity, threat or monitor the individual.

3.4.1.3 Combination threats and threats targeting children

Combination threats are different types of threats merged together, which is used by attackers very often.

As for children, they also get classical and modern threats, but they are little and sometimes do not know some dangers in OSNs, that is why they become a very specific aim of attackers.

Online predators usually collect much personal information from the child, pretending it is a friend. Some of that relationship may end in kidnapping or rape when the child meets with the predator.

Risky Behaviours include talking to strangers, sometimes in a sexual way, sharing personal information and photos.

Cyberbullying is harassing the child I the OSNs with hurtful messages or even threats. Often it includes embarrassing pictures or videos of the individual.

It has been mentioned only a part of all the attacks, people can deal with in OSNs (Fire, 2014). The full list can be found in Figure 2.

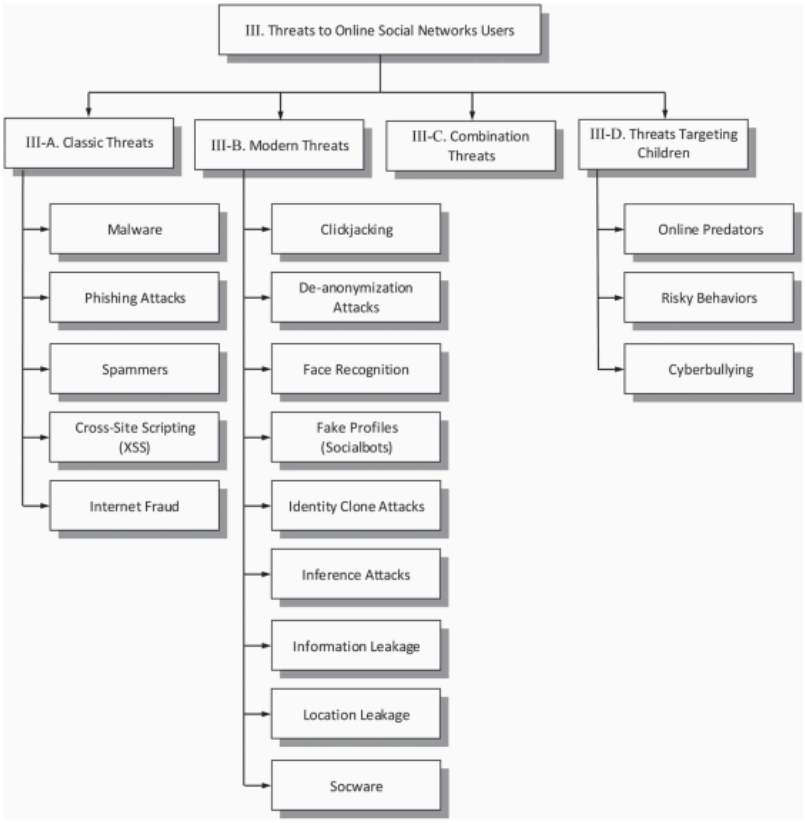


Figure 2. Data threats

3.5. Security by OSNs

With the attackers inventing new solutions to steal users' personal information, the OSNs are also making everything possible to protect it by creating safety measures. With

some of these techniques' users are dealing with every day, not even knowing about it (Fire, 2014).

An authentication mechanism is used to see whether a real person logs into the system, a robot, or a compromised account. These measures include CAPTCHA and multi-factor authentication, which asks a user not only a password, but a confirmation sent as a code on a mobile device.

Security and privacy settings are given by OSNs so a user can decide what personal information such as photos, posts and personal details they can hide from others.

Report users are mainly participants, that violated the policy of the network or harassed other people. Each profile has the button "report user" and if some people find another user guilty of the violation, they can complain.

Internet Security Solutions are given to OSNs by other companies, such as Kaspersky or AVG. Their software includes anti-virus and a firewall that secure OSN users against many threats.

Additionally, there are many pieces of advice that OSNs give their users to protect their profiles and data. Firstly, users should consider what information they share online. Online networks recommend deleting some extra information about their friends and family, and not using the full names when registering. Furthermore, hiding some personal data from unknown users by adjusting the settings and keeping some information for only close friends is a good decision. Another suggestion is to reject friend requests from strangers. If the user is unsure about that stranger, the information about his name or profile picture can be checked on the internet. Moreover, it is recommended to install security software and delete any installed third-party applications, as they collect a huge amount of personal data. And the last request is to doubt any online friends, the user never met and also check your children's OSN friends and profile.

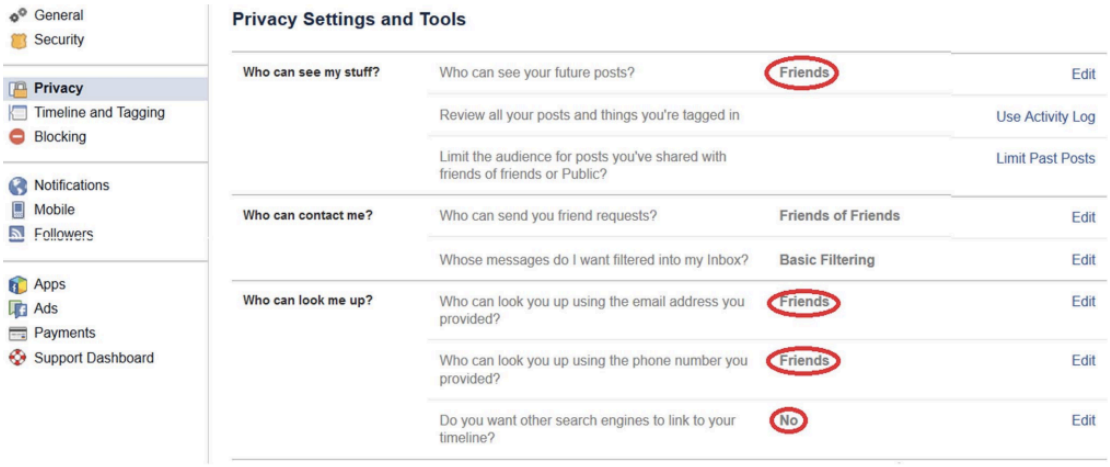


Figure 3. Recommended data settings

3.6. Security by government

As businesses and companies collect a vast amount of personal data, from the movies people watch to items which are bought online and other financial transactions. All the organizations' person interacts with, and sometimes the company's person doesn't even know, gathers tons of personal data of him. This data helps to analyse future behaviour and make some judgments. In the previews section we talked about how OSNs are trying to protect people, but there are some restrictions made on the government level.

3.6.1. GDPR

To help people protect their personal data, the government imposes new laws, like GDPR (General Data Protection Regulation). It is the strictest law, which was issued in the European Union and includes all the organisations around the world as long as they gather personal data in the EU. By the GDPR, companies and OSNs will pay big fines and get penalties if they violate specific security standards. The law consists of hundreds of pages of regulations, with the help of which Europe flashes the attitude on privacy for all organisations, including small and medium-sized enterprises (Wolford, 2021).

GDPR has seven core principles on how companies should behave, gathering personal data

- **Lawfulness, fairness and transparency**. It states that the processing of data should be fair, not questioning how the data is used. Companies should be clear with people about how they will use personal information.

- **Purpose limitation**. Organizations need to be clear for what purpose they need a person's data, that is why they need to record it in the documentation and privacy information for individuals.
- **Data minimisation**. Businesses must ensure they gather and process the exact amount of information they only need for specified purposes.
- **Accuracy**. Companies should control that personal data is correct and up to date.
- **Storage limitation**. Personal data have to be kept for no longer than it is necessary for the purpose of the company.
- **Integrity and confidentiality**. Organizations need to ensure that personal data is kept using appropriate security and confidentiality.
- **Accountability.** This principle requires companies to take the responsibilities for working with personal data and also for making sure all principles are followed.

3.6.1.1. Data Security

As GDPR is the main framework of data protection, it obligates the organisations to apply technical and organisational measures for data security. For technical measures, companies are being recommended to use two-factor authentication for accessing the system, which is used to process personal information. Furthermore, mobile phones are more likely to be stolen or lost, that's is why they need more care which is represented by encrypting all personal data, contained on the phone.

Organization measures include staff meetings, privacy data policy and the limitation of employees, who can access personal information. Additionally, in case of a breach, organizations are obligated to tell this information to people in 72 hours or otherwise they will be given penalties.

3.6.1.2. Cookie policy

Cookies usually are small pieces of personal data, which are stored in the computer browser. They are used to remember your account and your preferences on the website in order to help the person in the future to register and stay logged in. There are many types of cookies with different usage:

- **Strictly Necessary**. These cookies are used to perform essential and basic functions, such as allow users to perform account functions, authenticate users, who are already registered on the site and save items on the "cart".

- **Functionality**. This type of cookies saves one's preferences, such as location and language.
- **Analytics and Performance**. To improve the functions of websites, organizations need to know what people do on the site, for example, which pages they visit the most time
- **Advertising**. Companies usually put ads on their site and advertising cookies help them understand which ads are most likely to match the user's necessity. They track the details of the advertisements and also build user's profiles by showing products people have already seen. Furthermore, advertising cookies are set by trusted third-party networks
- **Security**. Special cookies, which are used to prevent security breaches.
- **Third-party**. These cookies are set by third parties to check the user's activity.

Cookies is the most popular way to gather personal data. That is why GDPR sets rules for using cookies. The website can only collect personal data after the user has given cookie consent. Usually, cookie consent is shown as the banners on the sites.

3.6.2. CCPA

California Consumer Privacy Act is a state law, which is similar to GDPR and it helps to enhance consumer protection for the residents of California. With the Act, citizens have the right to check what type of personal data is being gathered about them, check if this data is being sold and to whom. Furthermore, the consumer can ask the company to delete personal information about that consumer and sue the company if the rules are violated.

CCPA affects all companies that have annual revenue of more than $25 million and companies, which keep personal data on more than 50,000 people or companies that have at least half of their earnings made by selling personal data. Moreover, companies don't have to be located in California or the United States to fall under the law (Gilbert, 2020).

With so high digital interaction with companies, people sometimes do not realise what amount of personal data they leave behind. CCPA is protecting not only the basic consumer's data, for example, age, email address and name, but all the data entered in the computer, such as credit cards, demographics, geolocation data, biometric information and other identifiable data. Although this data is used in advertising, it can get into the wrong

hands, that is why consumers need the protection act and businesses need to follow the obligations.

3.7. Privacy paradox

It can be seen that people disclose a big amount of personal data on social networks or give the information while shopping online. On the other hand, many people care about their private information and say that they value this information a lot and would never share it. This dilemma is called the privacy paradox.

Many scientists believe that the privacy paradox is real, while others strongly deny its existence. In this paper, the two sides of the dilemma will be analyzed, and we will decide what occurs to be true believing.

3.7.1 Evidence showing privacy attitudes are different from privacy behaviour

There are many studies that conclude people do not care about their personal data and at the same time many types of research indicating that people hardly protect it. One of them is the experiment by Beresford (Beresford, Kübler, Preibusch, Sören,2012) in which participants were put into a situation where they have to purchase a DVD in one of two different online shops. The first shop was required to give more delicate information, such as income and birth date. At the same time, the other shop urged participants to answer only about their favorite color and year of birth. Apart from that, the shops were exactly the same. When the price equal in both stores, the sales were also identical. Nevertheless, when the first store reduced the price to one Euro, nearly all the participants chose the cheaper shop, in spite of the fact it asked for more delicate information.

Another experiment was organized in which was revealed with the help of a browser plugin how online users worth their personal information. Firstly, the plugin gathered information about the user's behavior. 168 users downloaded the plugin on their computer, and they have been monitored for two weeks in order to extract different personal information. There were popups with different questions on which participants should answer. Questions were framed as the auction, meaning that people could put a specific price on each question or do not participate in the particular question at all. Questions were mainly about privacy, for example: "What is the minimum price you would accept for

sharing your age, gender, address and salary to the private company?" The results show a relatively low appraisal of their personal data. Offline personal data, which was mentioned above, such as age, gender and economic status was evaluated by 25 Euros. For the online browsing activity participants gave only 7 Euros. The higher valuation was for online interactions at 12 Euros, but for shopping information was only 5 Euros (Carrascal, Riederer, Erramilli, Cherubini, De Oliveira, 2013).

In the series of interviews and an experiment was concluded that people intentionally share their personal information. As the participants confided, despite their deep concerns and risk, they get a good benefit from sharing (Lee, 2013).

On the other hand, Huberman conducted an experiment in which he put on the action weight and age. Doing so he wanted to find out how people value their personal information by converting it into money. At the end of the experiment, he conducted that the average price for age was $57.56 and $74.06 for weight. The experiment showed that the weight price was higher. As participants said, revealing weight information was more embarrassing than age. Additionally, younger people were more willing to display their age information (Huberman, Adar, Fine, 2005).

Egelman (Egelman, Felt, Wagner, 2012) also supervised an experiment in which participants had to choose between different shopping applications. A quarter of the participants decided to pay $1.50 over the given price of $0.49. Although the price was small, some people valued their personal information more than others.

In the experiment by Hann (Hann, Hui, Lee, Png, 2007) 268 participants faced a trade-off situation in which they had to choose between incomplete privacy protection and bonuses like promotions. Participants estimated the improper access to personal data and secondary use of information was worth between $30.49 and $44.6.

3.7.2 Evidence showing privacy attitudes and privacy behaviour are related

The studies above were referred to the fact that there is a dichotomy between privacy attitudes and real behavior. However, there can be found many types of research doubting the existence of the privacy paradox. In fact, when given a choice, people tend to choose an online store, which best protects their personal information. Furthermore, some individuals are willing to pay a premium for personal data to be safe (Tsai, Cranor, Egelman, Acquisti, 2011).

Common assumption says that with the digital age, young people do not try to protect personal data. Nevertheless, many studies deny this fact. The young generation is more careful, responsible and confident than adults. That is why their misuse of data is highly unlikely. They also register in OSN with pseudonyms and give false information in the registration fields (Miltgen, Peyrat-Guillard 2014). Moreover, it is suggested that OSN users try to share only part of private information to maintain the balance between being too disclose and too private (Skjetne 2010).

When the young generation tends to disclose private information, it usually happens with the need for popularity. And on the contrary, closing the access to the profile and denying friend requests happen because of a low trust level (Christofides, Muise, Desmarais 2009).

Moreover, it has been analyzed, that young people are more likely to protect their private information. Almost 95% of teenagers, aged 14-17 have read or modified privacy settings. In the contrast, only 32.5% of elderly people have done these actions. Also, people who have higher education and earn more money are likely to check their settings, followed by employed and single ones (Blank, Bolsover, Dubois 2014).

One study discovered that 54% of people decided not to download the app, which requests a lot of personal data, which they did not want to share. 30% of the subjects uninstalled the app, which they downloaded earlier because they found out it was collecting their private information. Also, 32% of participants clear their online history on the smartphone (Boyles 2012).

Furthermore, it has been discovered that people tend to share personal data in order to gain the benefit or intangible reward. It may seem that it is irresponsible, but before giving the information, OSN users weigh the losses and benefits and share the information only when the benefit of sharing overweight the expected risks (Debatin, 2009).

One more study conducts a series of experiments in which behavior and intentions are altered once again (Sun, Willemsen, Knijnenburg 2020). In the first experiment. people were asked to answer some questions about the Internet of things devices, particularly Smart Assistant, Smart washing machine and Smart Camera. The results show that people are more likely to share their personal data to the company's server rather than to third-party. The IoT devices also influence the decision of sharing. Participants are more disclosed to share their washing machine data than Smart Assistant, and less likely to share Smart Camera data. Nevertheless, in the experiment, it was found out that people are

actually less likely to share their personal data in the situation where they were asked to take part in actual behavior rather than in disclosing intentions. Furthermore, the benefit dominance can predict a person's behavior. When people are about to make a decision concerning privacy and benefits, they will first think if the benefit of sharing the information will be worth it.

3.7.3 Explanation

The research on the differences between private attitudes and real behaviour has shown contradictory results. Various researchers suggested the existence of a privacy paradox. On the other hand, other studies show that privacy attitudes and behaviour in OSN are in relation. In this section, we will explain why the contradiction happens.

First of all, many studies are based on the monetary experiments, for example in the experiment, where participants valued their browsing history for 7 Euros (Carrascal, Riederer, Erramilli, Cherubini, De Oliveira 2013) or the one in which was conducted that average price for age was $57.56 (Huberman, Adar, Fine 2005) The interpolations of these studies can be different at least in two ways. Some can think that 7 Euros is a very high price for that information, others will think it is inappropriately low. Nevertheless, the study shows that people care about their personal data, even with the valuating it only for 7 Euros.

Secondly, there are many types of personal data, for example, age, location, weight, browsing history and they all are evaluated differently. That is why we cannot compare various types of data with each other. In addition, there are multiple types of privacy attitudes, for example, concerns about social threats, like bullying or stalking; and concerns about organizational threats, such as marketing and reuse of personal data (Krasnova, Günther, Spiekermann, Koroleva 2009).

Thirdly, many studies are based on surveys, which can be appropriate for examining attitudes, but not for the studies with the real behavior, especially irregular or infrequent, because it is not easy to report such behavior accurately (Staddon, 2013). That is why experiments are more suitable, but they affect the quality of results being generalizable. As an example, we can compare two monetary experiments that were mentioned before. It was estimated that the price for age was on average $57.56 (Huberman, Adar, Fine 2005) and the average price for age, salary, address and gender were 25 Euros (Carrascal, Riederer,

Erramilli, Cherubini, De Oliveira 2013). Although the experiments consisted of a reverse second price auction, their samples and sittings were different.

Moreover, the environment of the experiment is very important. Sometimes people do not behave the same way in the experiment as do you at home, even if we give them false information and they would not suspect the experiment is about privacy.

3.7.4. Country differences

One more point to be taken into consideration is that studies are done in different countries and the results of these studies can also vary. Culture is a collective thinking mind, and it distinguishes people from different cultural groups. It also affects people's behavior and thinking (Hofstede 2011). Schomakers (Schomakers, Lidynia, Müllmann, Ziefle 2019) in the study compared how information sensitive are people in Germany, Brazil and the US. After the experiment, it was found out that all data types can be divided into three main groups: highly sensitive data (credit cards, passwords, financial account number), medium sensitive data (phone number, address, GPS location) and less sensitive data (email address, weight, hair color). Comparing the countries' responses, US citizens were more sensitive about their personal information, than Germans and the least sensitive were Brazilians. Furthermore, US and German samples were nearly alike, but the Brazilian sample varied a lot. These countries have many cultural differences, and, in this study, it was conducted that nationality plays a big role in the sensitivity analysis and additionally, the data protection policy impacts the results.

4 Practical Part

4.1 Method

The vast majority of researchers tried to test and explain the privacy paradox. Unfortunately, the existing results are contradictory and not explained properly. In the practical part an empirical questionnaire will be conducted, and two main questions of the paper will be studied:

- Is there a differentiation between attitudes and behavior in OSN?
- Would people disclose their personal information for money?

4.1.1 The survey

The survey was published in the Facebook groups and Instagram posts, which mainly attracted the target group of the research, which included the young generation, mainly high school graduates, college graduates or people with an undergraduate degree. The survey was available for two weeks for everyone and gathered 100 responses. The sample was created by the convenience sampling method. Mainly, the principle of the method, is gathering the data of people who are conveniently available to participate on the internet. The first people to give an answer source, will be included in the research. Generally, it means that participants can be found wherever it is convenient. This method has many advantages, as the data can be found easily and inexpensive. Also, it is easy to do the sample like that and analyse it. Furthermore, the sample was not targeted on the specific country region. It was mainly distributed to students from the EU and Russia.

The survey was implemented in Google Forms and consists of three parts, which include 9 questions. The first part includes demographic characteristics (age, gender, and education level). In the second part, participants are asked about their attitudes, when using OSNs and what pieces of information are sensitive to them (email, date of birth, age, weight and height, political views). The third part is mainly about behaviour of participants. They were given a choice when registering in the new OSN, what pieces of information from the list they would disclose and if they would disclose it for $20.

4.2. Descriptive statistics

From the survey can be obtained many data from the participants. As it was already mentioned, the survey was taken by 100 respondents, all of them passed the quiz completely. Out of all the respondents, 62% are female and 38% male (Figure 4). The majority of the respondents have an undergraduate degree or college degree, which is 65% and another 35% only completed high school (Figure 5). The majority of the participants are in the age of 21-23, which includes 43%, another 38% are between 18 and 20 years old and the last group with 19% has people over 23 years (Figure 6).

Figure 4. Gender percentage

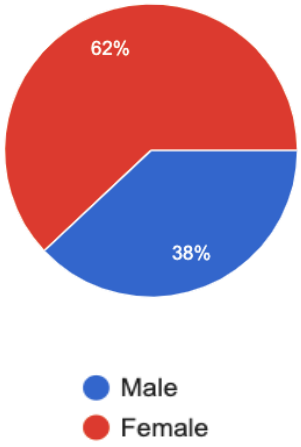


Figure 5.Education percentage.

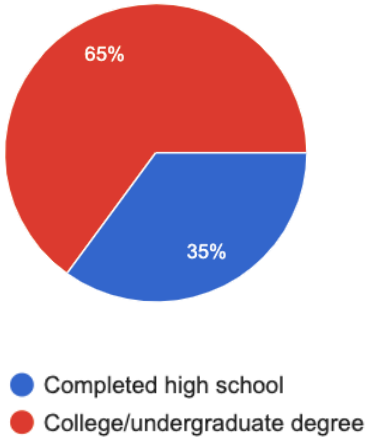
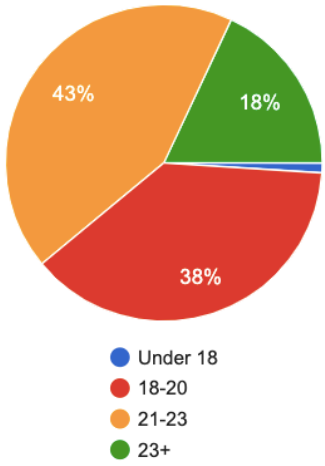


Figure 6. Age percentage



4.2.1. Privacy attitudes toward personal data

Of all the participants, nearly a half of them spend more than 6 hours on the internet per day, and another 43% spend from 3 to 6 hours. Only one in ten participants said they only use the internet for 1-3 hours a day (Figure 7). Furthermore, when sharing something online, only a minority (7%) would share their personal data with close friends, almost a quarter (23%) with everybody on the network, 30% of participants to all of the friends and the majority, which is 40% would share some personal information for close friends and some information for everybody (Figure 8)

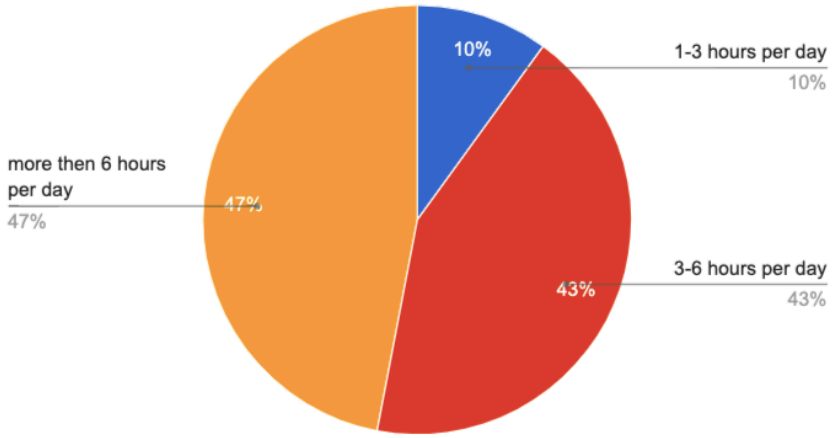


Figure 7. Hourly usage of the Internet

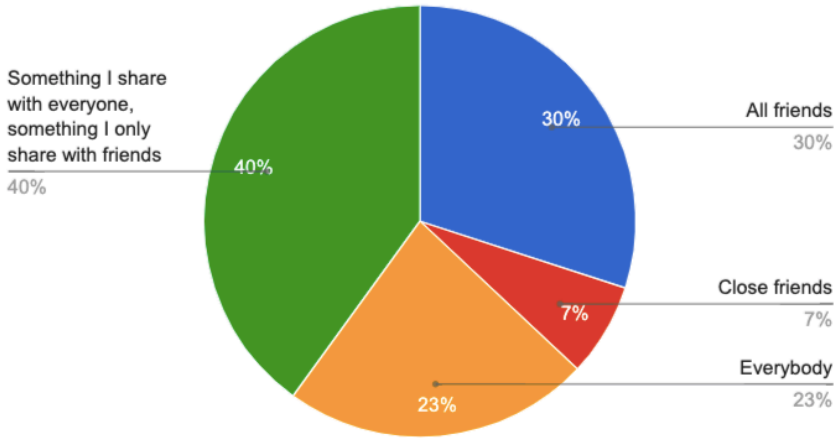


Figure 8. To whom participants disclose personal data?

Another question is about how often participants check their privacy settings in online social networks. The minority of 1% said daily, another 3% voted for weekly, but the majority split into 2 nearly even parts. 45% check the privacy settings monthly and another half of the respondents honestly answered that they never do it (Figure 9).

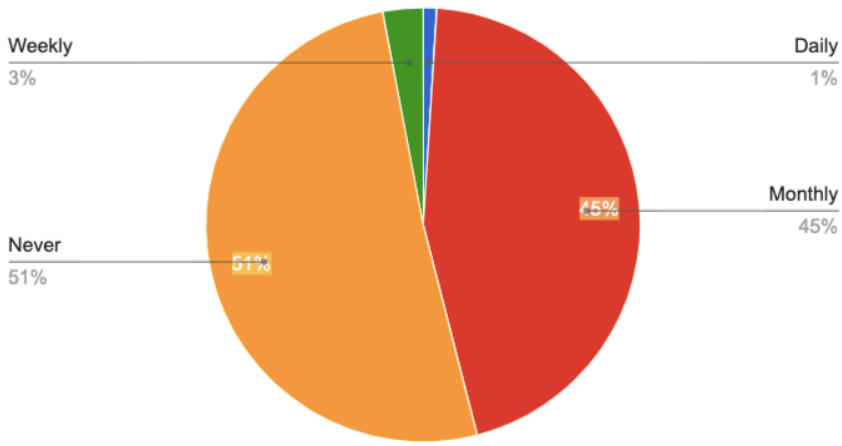


Figure 9. How rarely people check OSN settings?

4.2.2. Privacy behaviour in OSN

When participants were asked how they really felt about their personal data, the results started to vary.

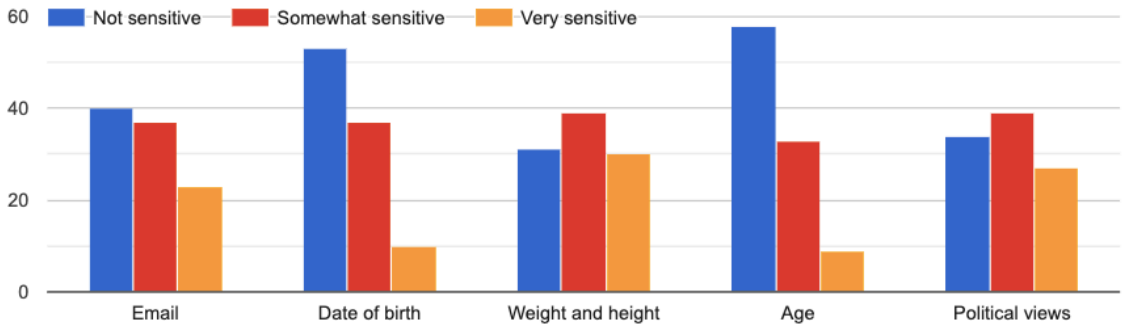


Figure 10. How sensitive are people to these pieces of information?

According to Figure 10, the graph was not distributed evenly. As the less sensitive piece of information participants chose age (58%) and date of birth (53%) and most sensitive weight with the height and political views with 30% and 27% respectively. These two positions also took a leader spot at “somewhat sensitive”.

In another question the participants were asked if they would share personal information in the new OSN. The full answers can be found in Figure 11. Most of them would disclose email, date of birth and age. Only a small part of participants would keep them. Nevertheless, a big amount of individuals would not share the weight with height and political views and only half of each group would disclose these pieces (Figure 11).

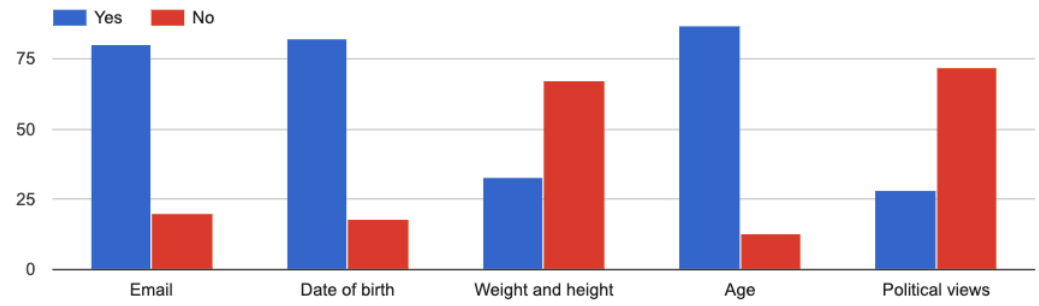


Figure 11. Would people share these pieces of information in OSN?

The last question in the survey was about money and precisely if people would sell their pieces of information, if they were given $20. It can be clearly seen that Figures 11 and 12 are again varying with only two pieces of personal information. Email, date of birth and age are not changing a lot, but some of the participants would totally sell their weight and height, what cannot be said about political views. The votes are divided into two nearly equal parts, with half of the people voting for selling their political views and another part for not selling.

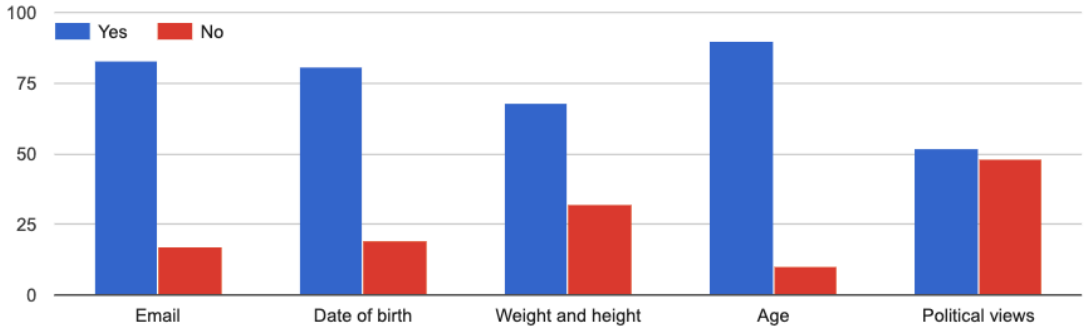


Figure 12. If participants were given money, would they share personal information?

In the next part, the last three graphs will be analysed in detail with the hypothesis testing, so it can be seen completely how the attitudes and behaviour differ in the study.

In the survey, last three questions included non-numerical answers and for the statistical analysis these values had to be converted. After the transformation, all the answers which included “Very sensitive” became number 1, which is supposed to match the setting “No” in another question; and “Not sensitive” or “Somewhat sensitive” number 2, matching “Yes”.

The descriptive statistics analysis was conducted for the last questions of the survey. Mainly it was given only two numbers (“1”- sensitive, “2”- not sensitive) and the

descriptive statistical results vary between them. As it can be seen in Table 2, which gives us the analysis of the 7th question in the survey ("How sensitive are you to these pieces of information?") participants did not show any particular sensitivity to the pieces of information, as the mean number is mostly close to the number 2, rather than 1. The standard deviation varied in most of the data pieces for more than 0.4, which indicates a big spread of the data from the mean. With the help of variance, it can be seen, that the numbers are not set far from each other, which is logical, considering the fact, that there are only two numbers. Median and mode are identical, as the number 2 appears more times, than number 1.

Name	Mean	Standard Deviation	Median	N	Variance	Mode
Email	1.77	0.4229526	2	100	0.1788889	2
Date of birth	1.9	0.3015113	2	100	0.0909091	2
Weight and height	1.7	0.4605662	2	100	0.2121212	2
Age	1.91	0.2876235	2	100	0.0827273	2
Political views	1.73	0.4461960	2	100	0.1990909	2

Table 2. How sensitive are people to their data?

Table 3 represents the analysis of the question 8 ("Would you disclose these pieces of information in the new OSN?"). The numbers are starting to change a little as three out of five pieces of personal information (email, date of birth, age) would be disclosed by the majority of the people, when registering to the new OSN, as the mean is fluctuating near 1.8. And two out of five pieces of data (weight, height and political views) people would not share, as the mean is near number 1.3. The standard deviation and variance are almost the same as in table 5, but median and mode differ. Two out of five pieces have number 1, which can conclude, that this information is very private and sensitive for people.

Name	Mean	Standard Deviation	Median	N	Variance	Mode
Email	1.8	0.4020151	2	100	0.1616162	2
Date of birth	1.82	0.3861229	2	100	0.1490909	2
Weight and height	1.3	0.4725819	1	100	0.2233333	1
Age	1.87	0.3379977	2	100	0.1142424	2
Political views	1.28	0.4512609	1	100	0.2036364	1

Table 3. Would you disclose these pieces of personal data in new OSN?

In Table 4, the results of descriptive statistics can be seen. It is the last question in the survey and its aim was to see if people are willing to give their information up for money. The mean number is mainly high (1.83, 1.81 and 1.9 for email, date of birth and age respectively). And as people answered, they would not disclose weight, height and political views in the previous question, in this table it can be seen that half of the participants would sell it (mean 1.6 for weight and height; 1.52 for political views). The standard deviation numbers are less, which means that the numbers also became less spread out. Median and mode also have the identical number 2 in each raw, which can mean the majority of people are more willing to disclose personal data for money.

Name	Mean	Standard Deviation	Median	N	Variance	Mode
Email	1.8300000	0.3775252	2	100	0.1425253	2
Date of birth	1.8100000	0.3942772	2	100	0.1554545	2
Weight and height	1.6000000	0.4688262	2	100	0.2197980	2
Age	1.9000000	0.3015113	2	100	0.0909091	2
Political views	1.5200000	0.5200000	2	100	0.2521212	2

Table 4. Would you disclose these pieces of information for money?

4.3. Normality test

Usually, in statistics, normality tests are used to figure if the sample has a normal distribution or not. It shows how frequently the values are appearing. Also, it is an important step, as it helps to decide what statistical data analysis to use on the data. The most common way to do it is the histogram. In Figure 1, on the left, can be seen a normal

distribution, which characterizes with the typical curve line. The data on the right picture is distributed with a little deviation of the line but still, it has a bell curve. On the right picture the data has another shape of the distribution, which tells us it is not a normal distribution.

Source: https://towardsdatascience.com/6-ways-to-test-for-a-normal-distribution-which-one-to-use-9dcf47d8fa93

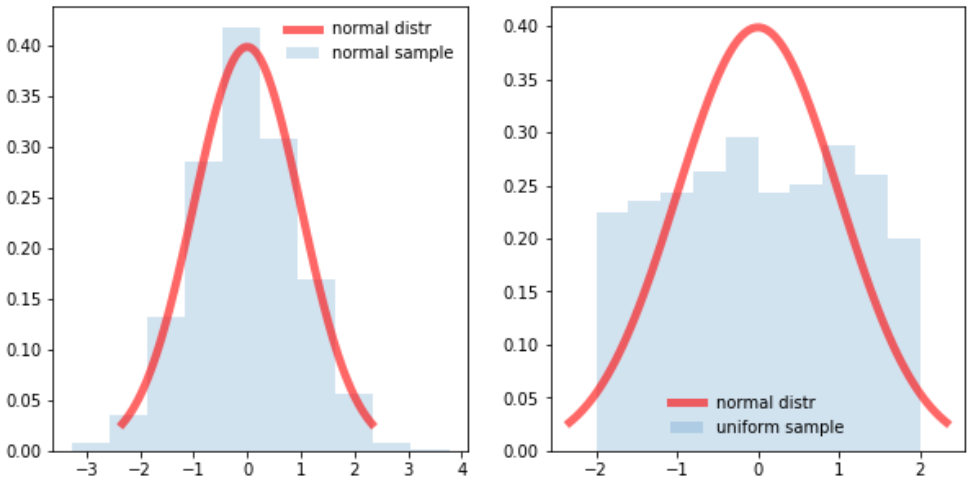


Figure 9. Normal and not normal distribution

The data of this study cannot be distributed normally. In each of the questions, there are only 2 answers (1 and 2), that is why there is no way the data can be distributed in a bell shape, so it cannot be called normal. That can relate to all of the numerical data in the study. In Figure 10 the histograms can be seen. They were made on the samples of data from the study. The histogram on the left represents the question: "How sensitive are you to disclose email?". And histogram on the right represents the question: "Would you disclose your email for $20?"

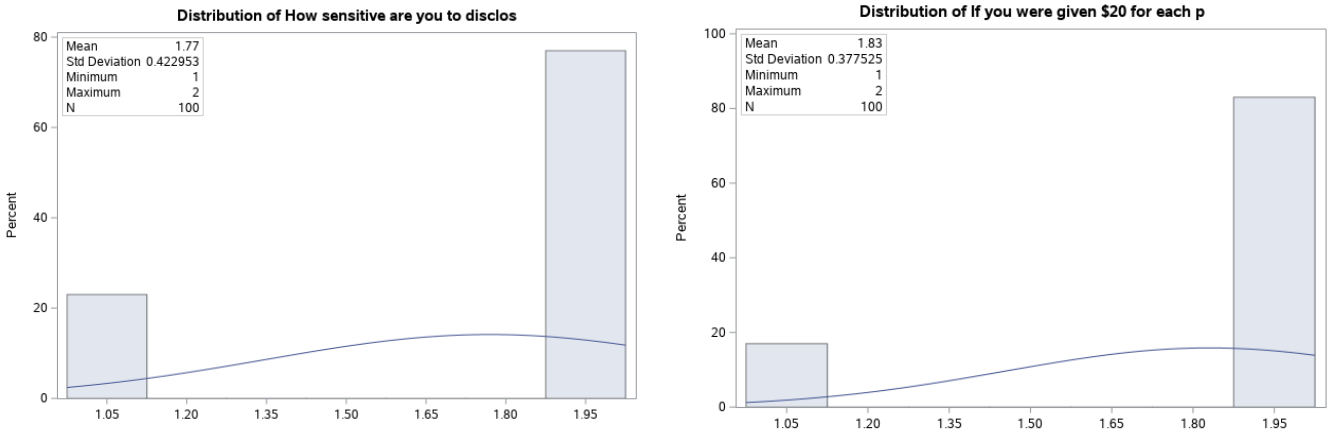


Figure 10. Histograms based on the study data.

4.4. Hypothesis testing

Although people claim, they are concerned with their personal information being shared, some evidence shows that their behaviour diverges from the intentions. That is the main question of this research and to will be put on the test in the first position. The helping tool for the test will be hypothesis testing and the null hypothesis is stated as follows:

H0: Participants will not disclose some pieces of personal data, even though they find these pieces not sensitive.

H1: Participants will disclose some pieces of personal information, even though they find these pieces sensitive.

The literature review covered many studies, which concluded the willingness to disclose more personal information when given money for it. The second research question of the study relates to this topic. After the survey results, it can be compared with the previous studies in order to see if the results match.

H0: Participants are not willing to share personal data for money.

H1: Participants are willing to share personal data for money.

4.4.1 First testing

To test the dichotomy, the chi-square test was run, comparing two answers in the different questions. The first study was about comparison of the questions 7 ("How sensitive are you toward the five pieces of information: email, date of birth, age, weight and height, political views.") and 8 ("A new online social network is launching, and part of the network is doing research into the student's market. When registering in that network, would you provide this information?"). The answers can be seen in the following table:

Data	P-value
Email	0.009
Date of Birth	0.2978
Weight and height	<0.0001
Age	0.38885
Political views	0.0222

Table 5. Differentiation between attitudes and behavior

Given the significance level of 0.05, it can be clearly seen that the p-value of email (0.009), weight, height (<0.0001) and political views (0.0222) are less than significance level, which leads to the decision, that null hypothesis has to be rejected. On the other hand,

date of birth (0.2978) and age (0.38885) exceed the significance level, which means the null hypothesis is accepted. Given these facts, it can be conducted that the participants will disclose email, weight and height and political views, but they will not share their age and date of birth in the new OSN.

4.4.2 Second testing

In the second study, we compared the questions 7 ("How sensitive are you toward the five pieces of information: email, date of birth, age, weight and height, political views.") and 9 ("If you were given $20 for each piece of information, would you share it?") with the aim to see if individuals would trade their data for money even though it is sensitive for them.

Data	P-value
Email	0.0001
Date of Birth	<0.0001
Weight and height	<0.0001
Age	0.2001
Political views	1.8785

Table 6. Will people share personal data for money?

From table 6, it can be declared that three out of five pieces of personal data people would disclose for money, including email (0.0001), date of birth (<0.0001) and weight with height (<0.0001), as their p-values are less than significant level, which leads to rejecting the null hypothesis. Nevertheless, the age and political views people would not share as the null hypothesis is acceptable due to the p-values exceeding the significance level (0.2001 and 1.8785 for age and political views respectively)

5. Results and Discussion

5.1. Descriptive statistics

From the descriptive statistics, it can be declared, that most people are spending a lot of time on the internet per day (Figure 7). It can be argued that many of them may work using the internet, but as the survey was taken among young people, which are mainly students, the majority of them do not work, which leads to the conclusion that they spend their time watching videos or communicating with friends. They also share a lot of personal information with friends on social networks (Figure 8), which means they do not care about privacy and additionally, Figure 9 only confirms that fact, as the majority of them do not check their privacy settings.

Moreover, we found that the most sensitive pieces of information were weight with height and political views. Participants also would not like to share them in the OSNs. It also can be proved by the descriptive statistics and especially the mean numbers (weight and height had 1.3 mean and political views 1.28 in table 3)

5.2 Hypothesis testing results

In the thesis, it was empirically analysed the dichotomy between privacy attitudes and privacy behaviour to conclude if the privacy paradox exists or it is just a myth. The study represented the young generation of participants from Europe and Russia. The hypothesis testing including chi-square tests were made to find the p-value of the compared questions and on its base reject or accept the null hypothesis. In the first testing, we found out that people would disclose email, weight with height and political views, when registering to the new OSN, even though they found these pieces of information sensitive. Nevertheless, participants would not share age and date of birth. In the second testing, participants would reveal email, date of birth and weight with hight, if they are given money for it. But they would not disclose age and political views.

5.3 Discussion

The purpose of the studies was to confirm or deny the particular behaviour in OSNs that has been already witnessed in other papers. However, while we tried to provide realistic and honest results, the findings can differ from the real opinions. Firstly, the study that was presented by the author had only five pieces of personal information and it can

tell not so many conclusions, as in the other papers with twenty pieces. Furthermore, the study was targeted at a particular age group, in order to see what the young generation think about privacy and the answers from the other studies may vary in particular because of the age groups differences. Additionally, as many studies try to provide a realistic environment for the experiment, the privacy paradox is still a very contextual spectacle, that is why it is hard to say if individuals are answering the questions the way they really feel.

5.3.1 Privacy paradox

There can be made two conclusions, based on the studies presented in the paper. The first conclusion that can be made after the analysis, is that people would disclose some personal information regardless of the fact, that some pieces of information are sensitive to them. In the literature review, we covered many scientific papers which concluded in the experiments either the fact that people care about personal data (Tsai, Cranor, Egelman, Acquisti, 2011) or they do not care at all (Lee, 2013). In our experiment, three out of five pieces of information were disclosed (email, weight with height and political views), which leads us to the fact that the privacy paradox exists. However, there are still two out of five pieces of information that people find sensitive and will not share (age and date of birth). This can only conclude that sometimes individuals will share their data without even thinking, but from time to time they will keep some of it out of the internet.

The second conclusion mainly suggests that individuals are more likely to share their data when they see benefit from it, in our study the benefit was money. From the previous studies in this paper, we see that people are more sensitive to political views, weight and height, but for the money, they would not give only political views with the age. According to the study of Carrascal et al (2013), which was presented in the literature review earlier, the participants would also give 7 Euros for the browsing history and 5 Euros for the shopping information. Furthermore, Huberman conducted an experiment in which he put on the action weight and age and conducted that the average price for age was $57.56 and $74.06 for weight. By comparing the studies, it can be said that all information has a price and people are willing to sell it, sometimes even for a little amount of money.

By these two conclusions, it cannot be decided that either privacy paradox exists, or it is the tale, that some people write about to scare others. It can only be assured, that people have different opinions and there are situations, in which individuals would disclose some of their data and there are also other situations in which people would not give it up even for money.

6 Conclusion

The main objective of the thesis was to explore the relationships between attitudes and behaviour and try to confirm or deny the existence of the privacy paradox. To study the privacy relationships, we conducted a questionnaire and, on its base, summarised the analysis. Firstly, the percentage analysis was made, then the descriptive statistics was written with the normality test. Afterwards, the hypothesis testing was conducted. By doing chi-square tests, we found the p-values and with its help, the null hypothesis could either be accepted or rejected. Two questions were compared in order to analyse the participants' behaviour and see if individuals would disclose their personal data in the new OSN.

The partial goal of the study was to see if people would trade their personal information for money. That study also included hypothesis with chi-square testing. By covering a vast majority of different papers and studies, looking at many studies, a particular decision on either confirm or deny the dichotomy between privacy attitudes and behaviour cannot be done. The studies of that problem date back on twenty and even thirty years and yet, new studies are also coming every year. That is a very large topic for discussion in many countries in the world and maybe with even more studies coming up and engaging people into the topic, some of them may rethink the choices they make about personal data and start treating it more carefully. One more point to be taken into the consideration is that OSN's, companies and cites are taking the responsibilities of user's information and maybe if users will be taking more attention to how their data is treated and who has accesses to it, they would not share it as much as they do now.

As the relationships between behaviour and attitudes in OSN and through the whole internet is such a big topic, we can hope, that one day all the questions will be answered. A further possible research question that emerged after this thesis is maybe next studies should not be focused on what individuals think about their personal data and how they treat it, but how people make these decisions about disclosing personal data at the first place and why.

7 References

Ali, S., Islam, N., Rauf, A., Din, I.U., Guizani, M. and Rodrigues, J.J., 2018. Privacy and security issues in online social networks. *Future Internet*, *10*(12), p.114.

Beresford, A.R., Kübler, D. and Preibusch, S., 2012. Unwillingness to pay for privacy: A field experiment. *Economics letters*, *117*(1), pp.25-27.

Blank, G., Bolsover, G. and Dubois, E., 2014, August. A new privacy paradox: Young people and privacy on social network sites. In *Prepared for the Annual Meeting of the American Sociological Association* (Vol. 17).

Boyles, J.L., Smith, A. and Madden, M., 2012. Privacy and data management on mobile devices. *Pew Internet & American Life Project*, *4*.

Brandtzæg, P.B., Lüders, M. and Skjetne, J.H., 2010. Too many Facebook "friends"? Content sharing and sociability versus the need for privacy in social network sites. *Intl. Journal of Human–Computer Interaction*, *26*(11-12), pp.1006-1030.

Carrascal, J.P., Riederer, C., Erramilli, V., Cherubini, M. and de Oliveira, R., 2013, May. Your browsing behavior for a big mac: Economics of personal information online. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 189-200).

Christofides, E., Muise, A. and Desmarais, S., 2009. Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyberpsychology & behavior*, *12*(3), pp.341-345.

Coe, L., 2003. *The telegraph: A history of Morse's invention and its predecessors in the United States*. McFarland.

Debatin, B., Lovejoy, J. P., Horn, A. K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. Journal of Computer-Mediated Communication, 15(1), 83-108.

Dwyer, C., Hiltz, S. and Passerini, K., 2007. Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, p.339.

Egelman, S., Felt, A.P. and Wagner, D., 2013. Choice architecture and smartphone privacy: There'sa price for that. In *The economics of information security and privacy* (pp. 211-236). Springer, Berlin, Heidelberg.

Elie Raad, Richard Chbeir, Albert Dipanda. Discovering relationship types between users using profiles and shared photos in a social network. Multimedia Tools and Applications, Springer Verlag, 2013, Multimedia Tools and Applications, 64 (1), pp.141-170.

Fire, M., Goldschmidt, R. and Elovici, Y., 2014. Online social networks: threats and solutions. *IEEE Communications Surveys & Tutorials*, *16*(4), pp.2019-2036.

Gilbert, A., 2020. California Consumer Privacy Act (CCPA) Compliance Guide: Everything You Need to Know About the New Data Privacy Law.
From https://www.osano.com/articles/ccpa-guide

Hann, I.H., Hui, K.L., Lee, S.Y.T. and Png, I.P., 2007. Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems*, *24*(2), pp.13-42.

Hofstade, G., 2011. Dimensionalizing cultures: The Hoftade Moel in Context dalam Larry Samovat et al Intercultural Communication: A Reader. *Cengage Learning*.

Holvast, J. (1993), Vulnerability and Privacy: Are We on the Way to a Risk-Free Society? In: Proceedings of the IFIP-WG9.2 Conference, May 20–22, 1993, Namur, Belgium.

Huberman, B.A., Adar, E., and Fine, L.R. (2005). Valuating privacy. IEEE Security & Privacy, 3(5), 22-25.

Johnson, B., & Vegas, L. (2010, January 11). Privacy no longer a social norm, says Facebook founder. The Guardian. Retrieved 8 Jan, 2014 from https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Kane, M.K., 1975. Data Banks in a Free Society. By Alan F. Westin and Michael A. Baker. Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems.

Kirtley, J., Bedrick B., Lerner, B., Whitehead, B., 1988. Privacy Paradox in *The Reporters Committee for Freedom of the Press.*

Krasnova, H., Günther, O., Spiekermann, S. *et al.* Privacy concerns and identity in online social networks. *IDIS* **2,** 39–63 (2009).

Lee, H., Park, H. and Kim, J., 2013. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, *71*(9), pp.862-877.

Lee, H., Park, H. and Kim, J., 2013. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies*, *71*(9), pp.862-877.

Markos, E., Milne, G. R. and Peltier, J. W. (2017) 'Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil', Journal of Public Policy & Marketing, 36(1), pp. 79–96.

McMullan, K. (2020). Social media: Are we in control? Social media has swept across modern culture, but are we really in control? Behaviorist psychology says otherwise. ISSUU from https://issuu.com/europeanbusinessmagazine/docs/38_european_business_magazine_summer_2020/s/11050962

Miltgen, C.L. and Peyrat-Guillard, D., 2014. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. *European Journal of Information Systems*, *23*(2), pp.103-125.

Moore, A.D., 2003. Privacy: its meaning and value. *American Philosophical Quarterly*, *40*(3), pp.215-227.

NORBERG, PATRICIA A., et al. "The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors." *The Journal of Consumer Affairs*, vol. 41, no. 1, 2007, pp. 100–126.

Rosenberg, R. (1992), The social impact of computers. Academic Press Inc.

Schomakers, E.M., Lidynia, C., Müllmann, D. and Ziefle, M., 2019. Internet users' perceptions of information sensitivity–insights from germany. *International Journal of Information Management*, *46*, pp.142-150.

B. Schneier, "A Taxonomy of Social Networking Data," in *IEEE Security & Privacy*, vol. 8, no. 4, pp. 88-88, July-Aug. 2010

Staddon, J., Acquisti, A., and LeFevre, K. (2013), Self-reported social network behavior: Accuracy predictors and implications for the privacy paradox. In: Proceedings of the 2013 International Conference on Social Computing (SocialCom 2013), September 8-14, Washington, USA.

Sun, Q., Willemsen, M.C. and Knijnenburg, B.P., 2020. Unpacking the intention-behavior gap in privacy decision making for the internet of things (IoT) using aspect listing. *Computers & Security*, *97*, p.101924.

Tsai, J.Y., Egelman, S., Cranor, L. and Acquisti, A., 2011. The effect of online privacy information on purchasing behavior: An experimental study. *Information systems research*, *22*(2), pp.254-268.

Turow, J., Hennessy, M. and Draper, N., 2015. The tradeoff fallacy. *University of Pennsylvania*.

Wolford, B., 2021. What is GDPR, the EU's new data protection law? From https://gdpr.eu/what-is-gdpr/

Zickuhr, K., 2012. *Three-quarters of smartphone owners use location-based services*. Pew Internet & American Life Project.

Appendix

Survey Questions

1. What is your gender?
    - Male
    - Female
2. What is your level of education?
    - Completed high school
    - College/ undergraduate
3. Which age group describes you?
    - Under 18
    - 18-20
    - 21-23
    - 23+
4. What is your average Internet usage rate?
    - Less than 1 hour per day
    - 1-3 hours per day
    - 3-6 hours per day
    - 6 or more hours per day
5. When you post something in social media, who can see what you share?
    - Everybody
    - All friends
    - Close friend
    - Something I share with everyone, something I share only with my friends
6. How often do you check or change your privacy settings?
    - Never
    - Monthly
    - Weekly
    - Daily
7. How sensitive are you to disclose these pieces of personal information? (Email, Date of birth, Age, Weight and Height, Political views)
    - Not sensitive
    - Somewhat sensitive
    - Very sensitive
8. A new online social network is launching, and part of the network is doing research into the student's market. When registering in that network, would you provide this information? (Email, Date of birth, Age, Weight and Height, Political views)
    - Yes
    - No
9. I you were given 20$ for each piece of information, would you share it? (Email, Date of birth, Age, Weight and Height, Political views)
    - Yes
    - No