Aalto University
School of Business

Bachelor's Programme in Information and Service Management

# Non-Conscious Data Collection

## A Critical Analysis of Risks and Public Perspectives

Bachelor's Thesis
Sofia Matomäki
Aalto University School of Business
Fall 2023

**Author** Sofia Matomäki

**Title of thesis** Non-Conscious Data Collection

**Degree** Bachelor's degree

**Degree programme** Information and Service Management

**Thesis advisor(s)** Tomi Seppälä

**Year of approval** 2023 **Number of pages** 27+7 **Language** English

**Abstract**

This literature review explores the issues and risks in non-conscious data collection and evaluates people's attitudes towards it. In the modern world, data is one of the most valuable resources, yet studies focused on the potential negative implications of the new data-driven technologies are lacking. Therefore, this thesis conducts a comprehensive literature review to identify and assess risks in non-conscious data collection technologies that are most relevant and referenced in current literature. Accordingly, the most prominent risks are related to privacy issues with personal data, bias in algorithms creating inequality, and the difficulties in creating adequate legislation. Subsequently, the thesis will explore existing studies about people's attitudes towards non-conscious data collection and examine the most significant socio-demographic determinants of those attitudes. Therefore, despite socio-demographic factors such as age, gender, and economic status affecting the attitudes people have towards data collection technologies, this thesis argues how these approaches can be explained by varying external factors such as prior experiences with similar technologies.

**Keywords** non-conscious data collection, emotional AI, artificial intelligence, big data, surveillance capitalism, technology acceptance

# Table of Contents

# 1 Introduction

In recent years, people have commonly referred to data as the "new oil" (Stach, 2023). This observation stems from the idea of data being an equally important resource in the fourth industrial revolution as oil was in the technological revolution. The value of this precious data lies in the wealth of information it can provide. However, data is not a new tool in the history of humankind. In fact, people have been using data to track information for hundreds of years, whether it was for measuring how long a food item will last or for keeping records of people in a society (Patil & Bhosale, 2018).

However, before modern technology, people could mainly access information in written documents like books and newspapers. Contrarily, individuals today can quickly access an abundance of knowledge and information through the internet. Accordingly, this shift of information becoming more accessible and easier to obtain has proliferated an increased demand for more data. Subsequently, this transition has created a new information economy where technology companies have been able to take advantage of their ability to collect data and turn it into an immensely profitable business. (Schyff et al., 2020)

However, the emergence of the information economy has created a whole new era of capitalism where users not only consume the commodity but are also the source of it. For example, in the life cycle of social media, its users create content for other users to consume. At the same time, the company behind the media platform collects user data and sells it to other businesses like advertising companies. The corporations can then use the historical data to predict people's interests, personalities, and, most importantly, their future behaviour. With these predictions, companies can, for instance, accurately target advertisements to the right people at the correct times and maximise the probability that the customer will buy their product. (Schyff et al., 2020)

Nonetheless, collecting and utilising potential customers' personal data for business gains is not a new phenomenon. The first software for managing extensive databases were created in the 1970s when early data brokers started to collect and sell data sets in list formats. These lists could contain pieces of people's

personal information such as addresses, credit reports, and contact information. (Beauvisage & Mellet, 2020) The landscape of the data business has since undergone a revolution with the advent of social media, as it started generating vast quantities of information, leading to the emergence of the term "big data" (Patil & Bhosale, 2018).

Consequently, the emotional AI industry is relatively new, yet it is already worth 24 billion dollars. Moreover, the industry is growing at such a pace that it is expected to double in worth by 2024. Technologies that can interpret users' emotions are improving quickly, and their advanced features are already used for a variety of purposes. The technology is embedded in a myriad of modern products, such as new smart cars, children's toys, voice assistants, and security devices. (Mantello et al., 2023) Furthermore, many of the most established technology firms are developing their own emotional AI applications. These companies include Apple, Google, Microsoft, Facebook, NEC, and IBM. (McStay, 2020)

Nowadays, data is tightly intertwined with all significant science and business endeavours. Big data analytics for enhanced business performance is an extensively studied subject, with global company leaders keen to comprehend it to optimise their outcomes (Batistič & van der Laken, 2019). The utilisation of big data is sometimes even considered a necessity for businesses to survive in the future information economy (Batistič & van der Laken, 2019). New ways of collecting and analysing information are continuing to change the world we live in. Emerging technologies like artificial intelligence are slowly embedded in the lives of people and although most of the changes are for the good, it is essential to identify potential risks and stay mindful of them. Despite non-conscious data collection (hereafter referred to as NCDC) being an integral part of most people's lives, people do not seem educated or motivated enough to influence their own privacy. Recent studies suggest a new privacy paradox where particularly young people no longer desire privacy in the same way as before. (Adorjan & Ricciardelli, 2019)

Undoubtedly, the significance of data is presumed to persist at a high level in the future. Accordingly, artificial intelligence applications like emotional AI will

ensure that the demand for data is perpetuated and even increased. Regardless of the topicality of the subject, academic research surrounding this problem is still limited. More specifically, literature is yet to explore the potential negative implications of NCDC practices combined with people's attitudes towards it.

Therefore, the objective of this thesis is not to create a dystopian outlook of the future of technology, nor is it to advise people not to use such technologies. Instead, the objective is to discover and point out potential risks and issues to encourage proactive measures and ensure everyone can enjoy the benefits of new data technologies safely without unnecessary inequality and injustice. In line with this objective, the thesis will conduct a comprehensive literature review to address the following research questions:

> Q1: What potential risks are associated with non-conscious data collection technologies?
>
> Q2: What are people's attitudes toward non-conscious data collection, and which socio-demographic factors influence these attitudes?

The structure of this thesis will be as follows. The second section introduces the most relevant risks and issues related to NCDC. Given the multitude of potential implications of new technology, this thesis narrows its focus to risks most frequently cited in the literature: the loss of privacy, algorithmic bias, and legal issues. The third section explores attitudes towards NCDC technologies. First, the thesis will introduce the most relevant theoretical frameworks in the field of technology acceptance. After that, the thesis will review relevant literature regarding people's attitudes towards NCDC and identify the most significant socio-demographic determinants of these attitudes. Subsequently, in the fourth section, the findings of this thesis will be discussed and aligned with the introduced theoretical frameworks, drawing connections with the reviewed empirical studies. Finally, the concluding section will summarise the key findings and insights from this thesis, providing a comprehensive overview of the research.

# 2 Conceptual frameworks

This section discusses the definitions and explanations of the central concepts and terms that are used in this thesis. Firstly, in this thesis, NCDC refers to the collection of information that is done without the subject's full attention. Businesses or other organisations may conduct this data collection, for example, in the background of websites and applications. Accordingly, this collected data includes personal data as well as less explicit pieces of information. (Schyff et al., 2020)

Accordingly, it is necessary to understand what personal data means in the context of this thesis. In the European Union's General Data Protection Regulation (GDPR) personal data is defined as:

> "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." (Regulation (EU) 2016/679 (General Data Protection Regulation), 2016)

When the data that businesses collect from their users is addressed, the discussion is usually focused on sensitive and personal data concerning financial records or contact information. However, while it is widely understood how important it is to protect this type of data from being misused, a different kind of personal data is often left unprotected: emotional data. Accordingly, this form of data includes the movements of facial muscles, voice tone, heart rate, and other information that can entail the subject's emotional state. The data can be stored in various forms, such as pictures, videos, text, or recordings. (McStay, 2020)

Subsequently, emotional AI is a form of technology that uses artificial intelligence to collect and analyse emotional data to predict emotions. Emotional AI algorithms use different sorts of available data to create a sophisticated prediction of someone's personality, interests, feelings, and even thoughts. (Mantello et al., 2023) For instance, Apple has a feature on its mobile phones that lets the user

send messages in the form of an animated character, “Animoji”. The Animoji works as a voice message that has the added feature of depicting the sender’s facial expressions. The Animoji works through a system called TrueDepth that is embedded in all Apple phones with a Face ID unlocking system. TrueDebth uses a combination of floodlights, infrared cameras, front cameras, dot projectors, proximity sensors, ambient light sensors, speakers, and microphones to read the user’s facial data. Therefore, Apple’s Animoji is an example of emotional AI that collects and utilises emotional data. (Gremsl & Hödl, 2022)

Lastly, the phenomenon where individuals, despite possessing sufficient information about privacy and expressing concerns regarding privacy issues, paradoxically refrain from taking actions to safeguard their personal information is called the “privacy paradox”. Accordingly, the privacy paradox conveys the apparent discrepancy between individuals’ expressed concerns about privacy and their actual online behaviours. Despite a growing awareness of privacy issues and the potential risks associated with online activities, people often engage in behaviours that compromise their privacy, such as sharing personal information on social media platforms or using services that collect extensive data. Hence, this paradox suggests that while individuals may express concerns about their privacy, they may not consistently act in ways that align with these concerns. Factors that studies have used to explain the reasons behind the privacy paradox include the convenience and perceived benefits of digital services, a lack of awareness regarding the extent of data collection, and a trade-off mentality. Essentially, the users are willingly exchanging personal information for the convenience or functionality offered by digital platforms. (Adorjan & Ricciardelli, 2019)

# 3 Risks of Non-Conscious Collection of Behavioural Data

The previous section of this thesis demonstrated the relevance of data collection practices for data-driven algorithms and artificial intelligence. Accordingly, a reality currently shaped by big data and algorithms is already in existence and is poised to endure well into the future. Importantly, new technologies bring the potential for a better world in many ways for some people, while for others, they can bring more inequality and reduce living standards. Therefore, it is vital to predict and assess the potential risks regarding technological improvement to be able to prevent them as much as possible. Hence, this section introduce and assess studies concerning the risks of implementing data and algorithms for different purposes in businesses and societies.

As data has become an indispensable resource for today's society, businesses and governments have created increasingly invasive ways to gain valuable information about people and their lives. A vast amount of this personal data is collected digitally via personal devices and in the background of social media platforms and websites (Schyff et al., 2020). The collected data ranges from explicit information such as the user's liked posts, demographic data, and internet searches (Schwab et al., 2011). Moreover, it includes less prominent data like the user's voice tone, writing style, and how they move their cursor (Ho et al., 2022). It is important to note that discreet NCDC is often done without explicit consent from the user (Schyff et al., 2020).

A report by the World Economic Forum (WEF, 2011) titled "Personal Data: The Emergence of a New Asset Class" emphasised that a comprehensive and reliable data infrastructure is a prerequisite for realising all potential gains. According to the report, the foundational element of this infrastructure should revolve around an individual's capacity to govern and derive benefits from their own data, discouraging unbridled NCDC practices that primarily favour companies and jeopardise individual gains (Schwab et al., 2011). Therefore, the current infrastructure does not support the protection of individual rights and poses multiple risks which this thesis will subsequently study in further detail.

## 3.1 Lost Privacy

While the capitalistic economy is the main driver behind the information economy and data monetisation, reasons and uses for data retention go far beyond targeted advertising (Andrew et al., 2023). For instance, in 2015, the Cambridge Analytica incident demonstrated the power of social media data when the third-party software company was able to predict people's voting behaviour before the 2016 United States presidential elections. The software development company Cambridge Analytica mined the data of 50 million Facebook users and successfully identified the voters who were not adamant in their political views and, therefore could still be influenced before the election. The company then proceeded to utilise the information and guide the uncertain voters to cast their vote for the candidate that Cambridge Analytica wanted to win the election. (Cadwalladr & Graham-Harrison, 2018)

Accordingly, enhancing public safety by adopting more comprehensive data surveillance practices aligns with the interests of most people. For example, until recently, the European Union and most of its member states have had a positive stance towards encryption technologies and supported their development (van Daalen, 2023). However, despite their previous support for encryption, the European Commission has now proposed a law requiring communications app providers to monitor even encrypted private communication (Birrer et al., 2023). The change in attitude towards privacy through encryption can also be seen outside the EU, with countries such as the United States and the United Kingdom investing heavily in projects that aim to weaken the rigid encryption technologies and combat the relevant laws (van Daalen, 2023).

One of the projects that has weakened the secrecy of personal data is the PRISM surveillance program developed in 2007. The program was devised to counteract terrorism through data surveillance, which authorised the U.S. government to request private user data from companies. (Schyff et al., 2020) A former head of the American National Security Agency (NSA) demonstrated the implications of data used for surveillance purposes by stating that the NSA utilises metadata in warfare strategies (Birrer et al., 2023). Hence, while the idea behind creating such a program is just, it also demonstrates the potential implications in the case of a

misinterpretation of data or an imperfection in the algorithms. Notably, this thesis does not aim to critique increased surveillance practices but instead aims to urge decision-makers to ensure that they consider various implicit perspectives when developing influential technologies.

However, the United Kingdom and the United States are not the only countries using data technologies and emotional AI to transform their societies. Technology under the brand name "Vibraimage" can decipher emotional data from video footage of a person and predict their emotional and mental state from the data. The technology measures even the most minuscule changes in expression and calculates their most probable feelings and even personality traits. Furthermore, despite insufficient evidence proving the accuracy of the technology, it is already widely employed worldwide (Wright, 2023). For instance, the technology is used in Russia at major airports to detect suspicious travellers and the Russian State Atomic Energy Corporation monitors employees working with high-risk substances such as used nuclear fuel and nuclear waste (Minkin, 2019). Moreover, in Japan the technology is also used on employers working at a nuclear plant as well as for security purposes at substantial events and theme parks. In addition, the technology was also used for security at the 2014 olympics in Russia, the 2018 olympics in South-Korea, and the 2018 FIFA World Cup in Russia. (Wright, 2023)

Furthermore, Wakefield (2021) claims that the Chinese government is using emotion recognition systems to control and restrict the lives of Uyghur Muslims, a religious minority in China. According to BBC's sources, people belonging to the minority are being forced to subject to digital scans and put under excessive surveillance through a government mobile application that constantly collects data of their location (Wakefield, 2021). Although injustice towards the Uyghur minority in China is known, weather they are being controlled through algorithms and data collection has not been conclusively proven (Dwyer, 2005). Regardless, it is evident that advanced and privacy-intrusive technologies pose considerable potential harm, especially when put into the wrong hands.

While the European Union is developing increasingly stringent legislation to control big data collection, the Chinese government has adopted a starkly

contrasting approach. In 2014, China started developing a social credit system that places Chinese citizens under extensive monitoring. (Aho & Duffield, 2020) The system allows the Chinese government to collect ample quantities of their citizens' data. The collected data is input into the system that uses algorithms to calculate a social credit score for each citizen and company. (Xu et al., 2022) The people and companies that receive a low credit score are essentially shunned and punished (Aho & Duffield, 2020). The severity of the penalties varies and may for instance include being denied access to public transport, specific schools, specific government jobs, or being denied bank loans. In addition, the names of the low-scoring citizens are sometimes published on government websites or physical billboards. (Xu et al., 2022)

China is a large country with a population of nearly one and a half billion people (Worldometer, n.d.). Partly due to its size, turbulent history, and authoritarian governance structure, the country has struggled with an undeveloped juridical system that has led to corruption and trust issues towards legal contracts. Combatting these issues is amongst the reasons why the social credit system was established. The notion of creating a safe and harmonized society is noble, but the realities of such a regime may not be as clear-cut. Many have criticized the system for enabling the government to tamper with the country's inner politics. Any people associated with opposing political parties or political activists are deliberately given low social scores and therefore blacklisted from entering many functions of society. In so doing, any criticism towards the government is effectively forbidden and the freedom of speech is suppressed. (Xu et al., 2022)

This form of Orwellian surveillance capitalism is already becoming a reality in China. Meanwhile, A. G. Scherer et al., (2023) proposes an alternative representation of a dystopian future where the critical maturity of human intelligence is lost alongside the loss of freedoms. According to their theory, the development of artificial intelligence replacing humans in more and more decision making is slowly making the ability of intellectual judgement redundant.

Accordingly, algorithms are already grouping people according to their perceived interests and personalities and using those assumptions to show the most suitable advertisements, news, and other content (Schyff et al., 2020). The

reasoning for the algorithms to work in such a manner is to maximize engagement and user experience to essentially show people what they assume they want to see rather than the most objective truth (Montag & Elhai, 2023). In other words, people are made to see content that already fits their world views and associate only with the people that share those same views (A. G. Scherer et al., 2023). Consequently, individuals tend to refrain from revising their perspectives in response to newly acquired information, instead perpetuating established viewpoints regardless of their accuracy. (A. G. Scherer et al., 2023) Zuboff (2015) further elaborates the theory of lost human maturity in a theoretical model of society that she calls "surveillance capitalism". Surveillance capitalism at its core is a world order where human life is reduced into the commodity of data collection and everything and everyone is controlled by a few large corporations and the government (Zuboff, 2015).

## 3.2 Algorithmic Bias

One significant concern in Emotional AI tools is the debatable science they are based on (Mantello et al., 2023). Accordingly, modern science is still lacking a consensus on the nature of human emotions, thus trying to quantify it into computable data is undoubtedly unreliable. (Mantello et al., 2023) Scientists have differing opinions on whether emotions are learned, if their development depends on surroundings, or if they are built into the biological human makeup (Ho et al., 2022). Moreover, tools created for deciphering emotions are primarily based on Paul Ekman's theory of the "universality of emotions" (Mantello et al., 2023). The often-sighted theory claims that all humans share certain core emotions: anger, fear, disgust, contempt, sadness, happiness, and surprise. These core emotions are innate for all humans regardless of culture or norms. Ekman further states that the seven universal emotions are physically expressed with the same cues in every culture and individual. (Ekman & Friesen, 1987) However, modern science has frequently called into question the validity of Ekman's theory, and evidence contradicting it has been found (K. R. Scherer et al., 2011). Nonetheless, given that a vast amount of the data-driven emotional AI technologies is aimed at people who experience and display emotions in the Western way, the technologies may not be accurate for everyone.

Accordingly, the fact that most emotion-sensing algorithms are based on Western beliefs and standards implies that they carry many Western biases (Mantello et al., 2023). For example, studies have found that facial recognition technologies are significantly less accurate when dealing with women or people with non-western features such as dark skin. Studies have found the same discrepancies in voice recognition technologies, which have more difficulties in understanding high-pitched voices and people with other accents than standard American or English. (Waelen & Wieczorek, 2022)

Hence, the discriminatory imperfections derived from the inequalities in our culture and society are transferred to AI models when they are programmed. The AI algorithms are often trained with historical data that is inherently biased due to our prejudiced society. Correspondingly, if the bias in the training data set is not controlled for, the AI model will follow the data and as a result learn to be biased. (Waelen & Wieczorek, 2022) Moreover, the more these types of imperfect technologies are implemented in society, the more they will affect people's lives in a negative way. Example of this include the algorithmic systems used in the United States as decision-making tools within the criminal legal system. Even though the systems were put in place partly to ensure objectivity and solve the issue of racism and classism, the data that fuels the algorithms is inherently biased due to it being a product of human actions and thoughts. In this example, the data is created by the police and people that choose which crimes to report and which people to arrest. If these people make systematic errors, such as false assumptions based on racist ideologies, the data becomes biased, and consequently, the algorithms perpetuate this bias. (Southerland, 2021)

## 3.3 Legal Considerations

Data retention and emotional AI have proven challenging to regulate on a national and international level. One major issue in establishing comprehensive law frameworks around these subjects is the varying views amongst different cultures on what constitutes sufficient data privacy. The issues of cultural differences related to privacy have appeared in international companies adopting new technologies to monitor the performance of their employees. For instance,

Amazon and IBM employees in Japan have raised arguments against the company's AI-driven performance metrics and wage assessment. Although the companies' practices align with Japanese labour laws, unions have raised a complaint that they violate traditional values and the norm of trusting employees. (Mantello et al., 2023)

The countries belonging to the European Union have a strict and extensive set of legislation for protecting their citizens' data compared to most other countries. In addition, some Western countries like Canada, Australia, and New Zealand have tightened their data protection regime and introduced new regulation measures. However, the reforms may not follow the changed attitudes of their citizens, but rather be ways of ensuring continued trade with the EU. (Bellman et al., 2004)

Unions and governmental agencies have created legislation like the General Data Protection Regulation (GDPR) to protect people's personal data. The effectiveness of the regulations, however, is not certain. Research suggests that the efficacy of GDPR relies mainly on the user's own actions. The privacy contracts people need to accept when using an application or website are made deliberately complicated and difficult to read. Hence, the complex privacy statements not only require an excessive amount of time to read through but also require knowledge on the subject that most people simply do not have. Furthermore, since privacy policies are constantly updated and modified by companies, users are less inclined or wholly incapable of keeping track of how their data is being used by different companies. Therefore, the mandate for websites and applications to provide a privacy policy and obtain the user's consent does not guarantee that the user acquires the tools necessary to manage their own data. (Schyff et al., 2020)

Another shortcoming of the current data protection legislation is the insufficient definition of personal data. Emotional data is not generally considered personal data when it has undergone anonymisation techniques because in most circumstances, personal data is strictly defined by the ability to identify a natural person from it (Gremsl & Hödl, 2022; European Union, n.d.). However, the definition is flawed as identifying individuals by combining different data sets is possible and even easy (Gremsl & Hödl, 2022). Furthermore, gaining people's data

through different applications has proven possible in numerous cases like the Cambridge Analytica -case (Symeonidis et al., 2018).

The European Union has proposed a new law to control the use of the ever-evolving artificial intelligence technology. If implemented, the Artificial Intelligence Act (AIA) would forbid the creation of social scoring systems, such as the one used in China. In addition, AIA would restrict the use of "high-risk applications", including the AI-powered CV-evaluating tools companies use to rank job applications. (Artificial Intelligence Act, 2021)

The increasingly strict regulations within the EU, EEA, and Switzerland are already impacting businesses. A recent example of this is the technology giant Meta's new model. Meta is infamous for its data breach incidents, yet the company has recently been forced to update its data privacy protocols due to the changing laws in Europe. (e.g., Symeonidis et al., n.d.; Cadwalladr & Graham-Harrison, 2018) Users within the countries that have implemented the new regulations are now offered a choice between continuing to use Meta's apps (e.g., Facebook and Instagram) for free and letting the company collect their data and use it for targeted advertising or paying a monthly fee to exclude their data from advertising use. (Meta, 2023)

Artificial intelligence is revolutionizing most aspects of people's lives, and NCDC is no exception. Already, decision-makers and lawmakers are struggling to keep up and monitor the ever-advancing technologies, and the pace at which they evolve is not predicted to get any slower. Moreover, Gremsl & Hödl (2022) found that legislation around new categories of data, such as emotional data, is currently inadequate.

# 4 Attitudes Towards Non-Conscious Data Collection

The popularity and prevalence of new Artificial Intelligence applications is on the rise, and the further the technology advances, the more it affects the lives of individuals. Although NCDC may pose risks for everyone, some people do not seem as alarmed as others.

Studies about people's attitudes towards the new AI technologies have started to emerge, but the subject is still relatively unknown, and the results are not coherent. Furthermore, most studies and theories rely on a rational privacy calculus that leaves irrational factors out. According to the privacy calculus, individuals weigh the potential benefits of providing personal data, such as improved services, personalized experiences, or access to certain features, against the potential drawbacks, such as loss of privacy, the risk of data misuse, or security concerns. Factors such as the perceived value of the service, trust in the entity collecting the data, the sensitivity of the information, and the perceived control over personal data influence this decision-making process. (Fernandes & Pereira, 2021)

This section of the thesis will review studies about the people's attitudes towards NCDC. First, the thesis will present the most relevant theories in the field of technological acceptance. Subsequently, empirical studies on people's attitudes and behaviour towards technologies and data collection will be reviewed and discussed.

## 4.1 Theoretical Frameworks

In the past, people's opinions and feelings towards new emerging technologies have been studied through various theories and theoretical frameworks. A simple cost-benefit calculation is usually used to explain people's attitudes towards emerging technologies. However, more complex theories have recently emerged that consider variables such as the user's socio-demographic background. This section will explain three relevant technology acceptance theories, which are necessary to understand the socio-demographic determinants of attitude towards behavioural data retention discussed later in the thesis.

### 4.1.1 Technology Acceptance Model

The most sighted theory in the field is Fred D. Davis' (1989) theory of perceived usefulness and perceived ease of use in the Technology Acceptance Model. Davis theorised that whether a new technology is accepted and taken into use by people depends on two key elements. The theory quantifies the subjective measure of acceptance of a new technology using two variables: perceived usefulness and perceived ease of use (Davis & Ann Arbor, 1989). Davis' theory focuses on technologies used in the workplace.

In the theoretical framework, the perceived usefulness is measured by the extent to which individuals anticipate that the technology will enhance their job performance, leading to increased job rewards. Perceived usefulness impacts the individual's attitude towards using and the behavioural intention to use the new technology as seen from Figure 1. The second key variable, perceived ease of use, is defined by the assumed amount of effort using and learning the new technology requires. Perceived ease of use in turn, affects the perceived usefulness and attitude towards using the technology (Figure 1). (Davis & Ann Arbor, 1989)

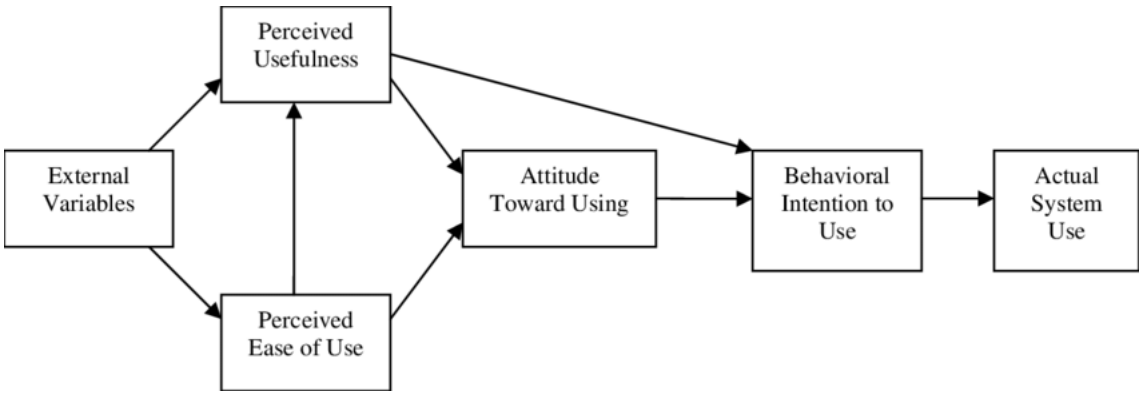


**Figure 1: Technology Acceptance Model variables illustrated by** Miller & Khera, 2010.

While the Technology Acceptance Model explains attitudes to some extent, it fails to consider cultural and social factors that vary among people and affect their behaviour differently (Ho et al., 2022). Nontheless, the narrow scope of the model

is explained by its focus on technology acceptance in a work environment. In the updated version of the technology acceptance model (TAM2), more variables are included, such as the social influence around the user (Venkatesh & Davis, 2000).

### 4.1.2 Unified Theory of Acceptance and Use of Technology

Another frequently sighted theory in the field of technology acceptance is the Unified Theory of Acceptance and Use of Technology (UTAUT) by Venkatesh et al. (2003). Similarly to the Technology Acceptance Model, the UTAUT was also limited to technology in the workplace. However, Venkatesh et al. have since expanded the UTAUT to format the UTAUT2 that can be applied to commercial consumer technologies. (Venkatesh et al., 2012)

The UTAUT2 defines four key indicators of technology acceptance: performance expectancy, effort expectancy, social influence and facilitating conditions. Performance and effort expectancy are defined similarly to perceived usefulness and perceived ease of use in Davis' model. Social influence refers to the user's close contacts (e.g., family or friends) likeliness to recommend using the technology. These three variables contribute to the behavioural intention to use the technology, which, combined with facilitating conditions, defines the actual use of technology. (Venkatesh et al., 2012)

The main modification from UTAUT to UTAUT2 is incorporating three new factors: hedonic motivations, habits, and price as seen from Figure 2. Hedonic motivations are the enjoyment of using the new technology, which has become relevant with recent technologies that revolve around entertainment. (Venkatesh et al., 2012) In addition to deliberate decisions, according to research non-conscious factors like habits significantly affect the use of technologies (Fernandes & Pereira, 2021). Costs, on the other hand, become significant when the UTAUT is adapted for consumer technologies because, unlike in the work environment, users must pay for any costs themselves (Venkatesh & Morris, 2000).

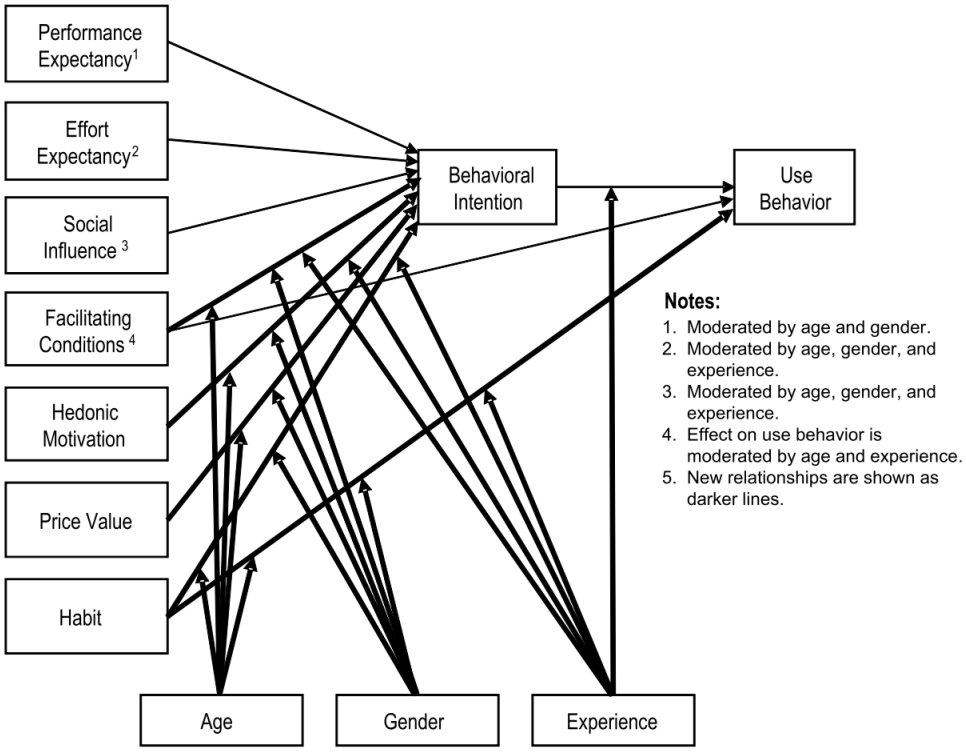


**Figure 2: UTAUT2 variables illustrated by** (Venkatesh & Davis, 2000)

### 4.1.3 Diffusion of Innovations Theory

One of the most classic and influential theories explaining people's acceptance of innovations is Everett Rogers' Diffusion of Innovations theory originally published in 1962 (Sahin, 2006). The theory provides a comprehensive framework for understanding how new ideas, products, or technologies are adopted and spread through social systems. It has been influential in various fields including political science, public health, economics, and education. Though the development of such technologies as AI was still in its infancy when Rogers formulated the theory, it is still relevant and fits the purpose of this essay (Haenlein & Kaplan, 2019). The theory is often used when studying specifically the acceptance of new technologies. Rogers uses the terms 'innovation' and 'technology' as synonyms in his paper, as most innovations include technological advancements (Sahin, 2006).

The four central components in the theory are time, innovation, communication channels, and social systems. The Diffusion of Innovations Theory first categorizes individuals into distinct adopter groups based on their likelihood to embrace the innovation at different stages. The five adopter groups are innovators, early adopters, early majority, late majority, and laggards. Rogers defines the adopter groups as members of a social system that vary in their aptitude to adopt an innovation. Time is central in this part of the theory as the adopter groups go through the diffusion of innovation at different paces. (Everett M. Rogers, 1995)

Aligning with the previously explained theoretical frameworks, central to this theory are the perceived attributes of innovations. However, Rogers specifies more variables, including the technology's relative advantage, compatibility with existing norms, complexity, trialability, and observability. Relative advantage refers to the new technology's superiority to the technology it replaces. Compatibility with existing norms is the level at which it aligns with previous experiences and the needs of the future. Complexity is similar to the perceived ease of use in TAM and the effort expectancy in UTAUT and UTAUT2. Trialability depicts how much the technology can be tested and modified before full approval. Finally, observability is the degree to which people can view the use of the technology. For example, new software is difficult to see physically and, therefore, has a lower degree of observability than a machine (Everett M. Rogers, 1995). However, in the present context, social media has made the use of a certain type of software more visible (e.g., mobile applications); hence, the nature of Roberts' observability has somewhat evolved.

Finally, the theory also highlights the role of communication channels and the broader social environment in influencing the rate and pattern of adoption. Communication channels signify the sources from which the individual receives information about the innovation. The information can be received through either interpersonal communication or mass media, and the origin of the message may be an individual or an institution. The social system encompasses norms, values, and communication networks and, according to Rogers' theory, significantly influences the diffusion of innovations. The theory acknowledges

that societal context is crucial in shaping individuals' attitudes and behaviours toward adopting new ideas or technologies. (Everett M. Rogers, 1995)

There are multiple well-established theories in the field of technology acceptance. However, for the purposes of this thesis, only the three theories mentioned above are introduced.

## 4.2 Socio-Demographic Determinants of Attitude Towards Behavioural Data Retention

While previous academic research on people's acceptance of new technologies has not emphasized socio-demographic factors, recent studies dedicated to exploring these aspects have emerged in the past few years. The reason for the recent interest in this subject may stem from its newfound relevancy due to artificial intelligence merging human life with technology in an unprecedented manner. This section will review and compare scientific findings about the socio-demographic factors determining how an individual feels about NCDC.

### 4.2.1 Gender

While most studies have found gender to be a significant factor in determining how an individual responds to new technology and NCDC, the findings are not coherent and conflicting evidence exists. For instance, Ho et al. (2022) finds male gender to be a predictable factor for a positive attitude towards NCDC. Moreover, being male was the most reliable factor in predicting the attitude towards non-conscious data collection done by the private sector. Notably, they also find other variables that relate to a privileged position in society, like higher income and higher level of education, to predict a positive attitude. (Ho et al., 2022) The evidence for gender having a significant effect, however, is not coherent across all studies. For example, Fernandes & Pereira (2021) conversely found the recipient's gender not to significantly affect willingness to disclose personal information online.

Furthermore, Park (2015) studied the difference between men and women when managing data privacy online. Park (2015) found that the main difference is that

men tend to report higher levels of self-efficacy in the technical matters of data protection. The findings are in line with the technology acceptance model and the unified theory of acceptance and technology use, which both suggest that a higher level of confidence in the required technical skills can lead to a better-perceived ease of use and, respectively, lower expectancy of complexity (Davis & Ann Arbor, 1989;Venkatesh et al., 2016).

There are many possible reasons for this gender imbalance in confidence towards the technicalities of online privacy. For instance, men still disproportionately dominate the tech industry and STEM (science, technology, engineering, and math) education (Ho et al., 2022). Consequently, technological skills are viewed as masculine, and therefore, men and boys are more inclined to get educated or educate themselves in the matter (Smith et al., 2013). Furthermore, Park (2015) found the differences in men and women depend on the respondent's age and marital status. In their study, the difference between the two genders was amplified in younger individuals due to young men reporting the highest self-efficacy levels, whereas, for women, age was not as significant of a factor. Moreover, being married entailed lower confidence in one's technical skills for women, while on the other hand it seemed to have no significant effect on men (Park, 2015). Notably, men (particularly those not belonging to any minority) experience less algorithmic bias and are thus less prone to notice the shortcomings in the technology (Waelen & Wieczorek, 2022).

Venkatesh & Morris (2000) studied the effect of gender in Davis' technology acceptance model. Accordingly, they found differences in how women and men implement the use of new technologies. More specifically, they found differences in what each of the two genders prioritize when evaluating technology. According to their results, men value perceived usefulness significantly more than perceived ease of use or subjective norms. On the other hand, women put more emphasis on the two latter mentioned factors when evaluating the technology. This could stem from men being more interested in merely maximising productivity while women tend to take a more holistic approach. (Venkatesh & Morris, 2000)

### 4.2.2 Age

All the studies included in this literature review have noted age as a variable to be controlled for. As noted earlier, certain studies have identified age as a consistent factor influencing individuals' technical proficiency in managing their privacy. Especially young men tend to report high self-efficacy in technological skills. (Park, 2015)

Moreover, Miltgen & Peyrat-Guillard (2014) also found young people to be more confident in their knowledge and skills to manage data. Young people, especially ages between 19 and 24, were also found less worried about privacy risks. Instead, they presented a false belief in the law protecting them more frequently than older age groups did. In contrast, middle-aged people were found to have the most negative attitudes towards data disclosure. (Miltgen & Peyrat-Guillard, 2014)

Regardless of young people being less worried, they do not display more recklessness online than older generations. Instead, Miltgen & Peyrat-Guillard (2014) found younger generations to be more cautious about their data on the internet. For instance, according to the study, young people are more likely to provide false personal information to websites when creating accounts. (Miltgen & Peyrat-Guillard, 2014)

Younger people seem to be more knowledgeable about the risks as well as the technicalities of data collection and online privacy (Miltgen & Peyrat-Guillard, 2014; Paine et al., 2007). Conversely, however, it seems that when the age gets low enough, the dynamics shift. Paine et al. (2007) found that under 20-year-olds are significantly less likely to be worried about data privacy than those over 20 years old. However, the study included respondents as young as 12 years old who cannot be expected to be as aware of privacy risks as those that are adults. (Paine et al., 2007). Nevertheless, it is important to note that in the USA, 65% of children aged 10-13 used the internet already in 2001 and are therefore susceptible to the same risks as their adult counterparts (Youn, 2005).

When studying people's concerns for risks online, Paine et al. (2007) found age to be a more reliable predictor than the reported number of hours spent on the internet, or the years spent using the internet. The older the recipient, the more

likely they were worried about their data privacy. Nevertheless, Paine et. al. found the concern for privacy issues to reduce when the individual gains more years of experience with the internet. On the other hand, age was not found a statistically significant predictor of action taken to protect one's privacy. Notably, the second and third most frequent answer for the reasons of the recipients' concerns online were spam and spyware, only bypassed by the concern for viruses. (Paine et al., 2007)

### 4.2.3 Income and Education

Studies have been relatively consistent in their findings about income and education affecting one's outlook on new technologies and NCDC. Ho et al. (2022) explain their findings of people with a higher level of income being more positive towards NCDC with the simple fact that those people are also the ones who can afford to benefit from the technology.

Interestingly, in their study on university students, Ho et al. (2022) find that having business as a major is a predictor of accepting data collection, particularly when conducted by the private sector. According to Ho et al. (2022) the findings may be explained by business students prioritizing productivity and financial result of companies more than students majoring in other subjects.

### 4.2.4 Culture and Religion

Data protection protocols vary highly around the world and therefore studying cultural differences in people's attitudes toward them is interesting. For example, Milberg et al. (2000) and Bellman et al. (2004) find cultural differences to be significant when predicting privacy concerns of people. The extent and nature of the influence are however not found consistent when comparing the two studies. Both studies used Geert Hofstede's esteemed theory of cultural values to compare countries (Milberg et al., 2000; Bellman et al., 2004). The studies sorted countries based on four of Hofstede's variables: power distance, individualism, masculinity, and uncertainty avoidance (Hofstede, 1984).

Bellman et al. (2004) found that people from countries with a high ranking of individuality are more accepting of data collection and are therefore less

worried about privacy concerns. This finding is consistent with most research but contradicts the findings of Milberg et al. (2000). The central characteristics of an individualistic culture include a strong emphasis on personal autonomy, self-expression, and individual achievement (Hofstede, 1984). In such cultures, there is a prevailing belief in the importance of personal goals and aspirations, with individuals encouraged to pursue their own interests and fulfil their unique potential. On the other hand, in collectivist cultures the emphasis is on group cohesion, interdependence, and cooperation rather than on individual autonomy and personal achievement. (Glazer, 2014) In collectivist cultures one's reputation is important; thus, privacy may be valued to avoid scandals and loss of face. In addition, people from individualistic countries may view managing privacy as everyone's own responsibility whereas collectivist cultures may be more inclined to see it as a collective effort and not necessarily the individual's own job. (Miltgen & Peyrat-Guillard, 2014)

Both Bellman et al. (2004) and Milberg et al. (2000) found that people were more likely to want stricter privacy laws implemented if they were from countries with an already high-level of privacy regulation. However, consumers were more concerned about privacy concerns related to online transactions if their country had no set privacy regulations (Bellman et al., 2004).

# 5 Discussion

The objective of this thesis was to evaluate the risks that are related to non-conscious data collection technologies and explore how people feel about them. Both issues were studied by conducting a comprehensive literature review and comparing existing research around the subject. In this section the findings of this thesis will be discussed and compared.

It has become clear that data is a valuable currency in the world we now live in. New data-driven technologies are revolutionizing everything from social relationships to medicine and surveillance. First and foremost, technology should be seen as an opportunity to solve difficult issues like climate change and improve and even save human lives. For example, companies can utilise data to create more personalised and overall better products and services for their clients, healthcare providers and scientists can develop better medicine, and governments can ensure safer and smoother lives for their citizens (Schwab et al., 2011). However, it is also clear that new technologies uphold the potential to be harmful for a vast amount of people. Technology is advancing at such speeds that if it is not properly prepared for, it can lead to unwanted consequences that may be difficult to reverse.

Firstly, the technology is at risk of perpetuating inequality and injustice that already exists in the world. For instance, this thesis found that most of the algorithms that exist today have been found to be flawed with discriminatory features against minorities and minoritized groups. Consequently, the more these flawed technologies are implemented in everyday actions, the more they will start to affect the lives of the people they discriminate against. The fact that face and voice recognition software do not work equally well with all faces and voices hardly seems like an urgent problem at the moment since the technology is mostly found in less than vital voice assistants and face ID-systems. However, when the same technology becomes part of medical care or safety, the underlying biases will start to matter more. From this point of view, it is not surprising that women and minorities are found to have a less positive outlooks on data collection and these technologies.

In addition to algorithmic bias making the everyday systems inequal, data as a valuable currency may further increase economic inequality. Accordingly, the very legislation created to protect people's data may inadvertently be driving the increased gap between the wealthy and the poor. Using Meta as a current example, the stringent laws in the EU, EAA and Switzerland have forced the company to change their policies surrounding user data collection. Now people are seemingly given a choice about their data; paying for their data to be protected or continuing to use the applications for free in exchange of Meta getting their data. This depicts the new era of capitalism and the information economy: data has become a currency that people can sell to receive benefits like the use of a social media platform. One might argue that this is simply how capitalism, and the market economy works and is therefore right. However, if other companies continue to adopt the same sort of systems, data privacy might soon become a privilege that only the rich can afford. Not only is that in conflict with the Charter of Fundamental Rights of the European Union, but it could further increase bias in our societies (Charter of Fundamental Rights Of The European Union, 2000). If people of higher economic status can essentially buy their data out from datasets, less wealthy people become oversaturated in the datasets. Furthermore, as established in the US' criminal justice algorithms, biased data creates biased algorithms, and the effects can be detrimental to those who the bias works against.

Therefore, this thesis depicts that there are still looming issues in the way data is handled and used. The problems seem to lie both in the users' behaviour, specifically their lack of knowledge or pure indifference, as well as the companies operating models. Issues such as bias in algorithms or cultural differences may not be prominent to all demographics and therefore go unnoticed through the technologies' design processes. This is one of the reasons why diversity is an important and beneficial feature for all disciplines. Working data infrastructure, legislation and the education of people is necessary to ensure all people can enjoy the benefits of new data technologies.

# 6 Conclusion

This thesis has studied the potential negative effects of data collection and the technologies used for it. The existing research on this subject is still not absolute in its findings and for some questions there remain differing opinions amongst scholars. Nevertheless, this literature review formed a comprehensive overview of the research findings and current knowledge.

Firstly, the thesis identified the most prominent issues related to non-conscious data collection technologies based on current studies. The problems were divided into three categories based on how they occur: privacy related issues, biased algorithms and data, and current legislation. The literature review found that issues are two-sided and may be caused by misuse of data or unintentional accidents. Unintentional mistakes in the algorithms are often caused by overlooking some cultural and social aspects. Furthermore, current legislation is not comprehensive enough to guide businesses towards fair and just data processes.

Secondly, the thesis introduced three of the most relevant theoretical frameworks in the field of technology acceptance: the Technology Acceptance Model (Davis & Ann Arbor, 1989), the Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2012), and the Diffusion of Innovations Model (Sahin, 2006). Subsequently, empirical research papers about peoples' attitudes towards non-conscious data collection were examined with an emphasis on finding socio-demographic determinants for peoples' opinions. To answer the second research question, this thesis concludes that people's attitudes towards data collection vary from optimism to fear. Although the findings on which factors determine a person's attitude are not entirely consistent, some patterns seem to exist. The most significant factors behind peoples' attitudes were found to be gender, age, economic status, and cultural background. Most of the empirical results seemed to be in line with the acceptance theories. Accordingly, a conclusion can be made that a multitude of factors affect someone's thoughts about data collection and socio-demographic background is just one of them.

Nevertheless, to reach more specific and conclusive results, further studies on this subject are required. The findings of this thesis are limited to existing studies. Although the studies used as reference are credible, it is possible that they include some sampling bias as accurate representation of the global population in survey studies is difficult. A natural progression for this thesis would be to conduct a survey-study that specifically examines the reasons behind people's attitudes towards NCDC. Furthermore, this thesis identified risks of NCDC from existing literature and discussed hypotheses for the connection between them and people's attitudes. How people's knowledge of these risks affects their opinions of NCDC remains an interesting topic for future research.

# References


Adorjan, M., & Ricciardelli, R. (2019). A New Privacy Paradox? Youth Agentic Practices of Privacy Management Despite "Nothing to Hide" Online. *Canadian Review of Sociology*, *56*(1), 8–29. https://doi.org/10.1111/cars.12227

Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, *49*(2), 187–212. https://doi.org/10.1080/03085147.2019.1690275

Andrew, J., Baker, M., & Huang, C. (2023). Data breaches in the age of surveillance capitalism: Do disclosures have a new role to play? *Critical Perspectives on Accounting*, *90*. https://doi.org/10.1016/j.cpa.2021.102396

Batistič, S., & van der Laken, P. (2019). History, Evolution and Future of Big Data and Analytics: A Bibliometric Analysis of Its Relationship to Performance in Organizations. *British Journal of Management*, *30*(2), 229–251. https://doi.org/10.1111/1467-8551.12340

Beauvisage, T., & Mellet, K. (2020). *Assetization : turning things into assets in technoscientific capitalism*. The MIT Press.

Bellman, S., Johnson, E. J., Kobrin, S. J., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *Information Society*, *20*(5), 313–324. https://doi.org/10.1080/01972240490507956

Birrer, A., He, D., & Just, N. (2023). The state is watching you—A cross-national comparison of data retention in Europe. *Telecommunications Policy*, *47*(4). https://doi.org/10.1016/j.telpol.2023.102542

Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Davis, F. D., & Ann Arbor. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 319–340.

Dwyer, A. M. (2005). *The Xinjiang Conflict: Uyghur Identity, Language Policy, and Political Discourse.* https://scholarspace.manoa.hawaii.edu/server/api/core/bitstreams/ee963095-13e7-4c6d-9f95-d9ddf9f3be36/content

Ekman, P., & Friesen, W. V. (1987). Universals and Cultural Differences in the Judgments of Facial Expressions of Emotion. *Journal of Personality and Social Psychology*, *53*(4), 712–717.

Artificial Intelligence Act, (2021). https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.pdf

Charter Of Fundamental Rights Of The European Union, (2000). https://www.europarl.europa.eu/charter/pdf/text_en.pdf

Regulation (EU) 2016/679 (General Data Protection Regulation), (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Everett M. Rogers. (1995). *Diffusion of Innovations* (4th ed.). The Free Press.

Fernandes, T., & Pereira, N. (2021). Revisiting the privacy calculus: Why are consumers (really) willing to disclose personal data online? *Telematics and Informatics*, *65*. https://doi.org/10.1016/j.tele.2021.101717

Glazer, S. (2014). The Role of Culture in Decision Making. *Cutter IT Journal*, *27*(9), 23–29.

Gremsl, T., & Hödl, E. (2022). Emotional AI: Legal and ethical challenges. *Information Polity*, *27*(2), 163–174. https://doi.org/10.3233/IP-211529

Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, *61*(4), 5–14. https://doi.org/10.1177/0008125619864925

Ho, M. T., Mantello, P., Ghotbi, N., Nguyen, M. H., Nguyen, H. K. T., & Vuong, Q. H. (2022). Rethinking technological acceptance in the age of emotional AI: Surveying Gen Z (Zoomer) attitudes toward non-conscious data collection. *Technology in Society*, *70*. https://doi.org/10.1016/j.techsoc.2022.102011

Hofstede, G. (1984). *Culture's consequences: International differences in work-related values* (Vol. 5).

Mantello, P., Ho, M. T., Nguyen, M. H., & Vuong, Q. H. (2023). Machines that feel: behavioral determinants of attitude towards affect recognition technology—upgrading technology acceptance theory with the mindsponge model. *Humanities and Social Sciences Communications*, *10*(1). https://doi.org/10.1057/s41599-023-01837-1

McStay, A. (2020). Emotional AI, soft biometrics and the surveillance of emotional life: An unusual consensus on privacy. *Big Data and Society*, *7*(1). https://doi.org/10.1177/2053951720904386

Meta. (2023, October 30). *Facebook and Instagram to Offer Subscription for No Ads in Europe*. https://about.fb.com/news/2023/10/facebook-and-instagram-to-offer-subscription-for-no-ads-in-europe/

Milberg, S. J., Smith, • H Jeff, Burke, S. J., & Graduate, B. (2000). Information Privacy: Corporate Management and National Regulation. *Organization Science*, *11*(1), 35–57.

Miller, J., & Khera, O. (2010). Digital Library Adoption and the Technology Acceptance Model: A Cross-Country Analysis. *Electronic Journal of Information Systems in Developing Countries*, *40*(1), 1–19. https://doi.org/10.1002/j.1681-4835.2010.tb00288.x

Miltgen, C. L., & 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), 103–125. https://doi.org/10.1057/ejis.2013.17ï

Minkin, V. (2019). *The Vibraimage Technology. Conference Proceedings (English Edition) The 2nd International Open Science Conference. Modern Psychophysiology*. (V. Minkin, A. Bobrov, V. Sedin, & E. Miroshnik, Eds.). ELSYS Corp. https://doi.org/10.25696/ELSYS.B.EN.VIC.2019

Montag, C., & Elhai, J. D. (2023). On Social Media Design, (Online-)Time Well-spent and Addictive Behaviors in the Age of Surveillance Capitalism. In *Current Addiction Reports* (Vol. 10, Issue 3, pp. 610–616). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/s40429-023-00494-3

Paine, C., Reips, U. D., Stieger, S., Joinson, A., & Buchanan, T. (2007). Internet users' perceptions of 'privacy concerns' and 'privacy actions'. *International Journal of*

*Human Computer Studies*, *65*(6), 526–536. https://doi.org/10.1016/j.ijhcs.2006.12.001

Park, Y. J. (2015). Do men and women differ in privacy? Gendered privacy and (in)equality in the Internet. *Computers in Human Behavior*, *50*, 252–258. https://doi.org/10.1016/j.chb.2015.04.011

Patil, P. C., & Bhosale, A. (2018). Big data analytics. *Open Access Journal of Science*, *2*(5). https://doi.org/10.15406/oajs.2018.02.00095

Sahin, I. (2006). Detailed Review of Rogers' Diffusion of Innovations Theory and Educational Technology-Related Studies Based on Rogers' Theory. *The Turkish Online Journal of Educational Technology*, *5*(2), 1303–6521.

Scherer, A. G., Neesham, C., Schoeneborn, D., & Scholz, M. (2023). Guest Editors' Introduction: New Challenges to the Enlightenment: How Twenty-First-Century Sociotechnological Systems Facilitate Organized Immaturity and How to Counteract It. *Business Ethics Quarterly*, *33*(3), 409–439. https://doi.org/10.1017/beq.2023.7

Scherer, K. R., Clark-Polner, E., & Mortillaro, M. (2011). In the eye of the beholder? Universality and cultural specificity in the expression and perception of emotion. *International Journal of Psychology*, *46*(6), 401–435. https://doi.org/10.1080/00207594.2011.626049

Schwab, K., Marcus, A., Oyola, J., Hoffman, W., & Luzi, M. (2011). *Personal Data: The Emergence of a New Asset Class*. https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

Schyff, K. van der, Flowerday, S., & Furnell, S. (2020). Duplicitous social media and data surveillance: An evaluation of privacy risk. *Computers and Security*, *94*. https://doi.org/10.1016/j.cose.2020.101822

Smith, J. L., Lewis, K. L., Hawthorne, L., & Hodges, S. D. (2013). When Trying Hard Isn't Natural: Women's Belonging With and Motivation for Male-Dominated STEM Fields As a Function of Effort Expenditure Concerns. *Personality and Social Psychology Bulletin*, *39*(2), 131–143. https://doi.org/10.1177/0146167212468332

Southerland, V. M. (2021). The Intersection of Race and Algorithmic Tools in the Criminal Legal System. *Maryland Law Review*, *80*.

Stach, C. (2023). Data Is the New Oil–Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration. *Future Internet*, *15*(2). https://doi.org/10.3390/fi15020071

Symeonidis, I., Biczók, G., Shirazi, F., Soì, C. P., Schroers, J., & Preneel, B. (2018). Collateral damage of Facebook third-party applications: a comprehensive study. *Computers & Security*, *77*, 179–208.

van Daalen, O. L. (2023). The right to encryption: Privacy as preventing unlawful access. *Computer Law and Security Review*, *49*. https://doi.org/10.1016/j.clsr.2023.105804

Venkatesh, V., & Davis, F. D. (2000). Theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Venkatesh, V., & Morris, M. G. (2000). Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior 1. *MIS Quarterly*, *24*(1), 115–139.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology 1. *MIS Quarterly*, *36*, 157–178.

Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified Theory of Acceptance and Use of Technology: A Synthesis and the Road Ahead. *Journal of the Association for Information Systems* , *17*, 328–376.

Waelen, R., & Wieczorek, M. (2022). The Struggle for AI's Recognition: Understanding the Normative Implications of Gender Bias in AI with Honneth's Theory of Recognition. *Philosophy and Technology*, *35*(2). https://doi.org/10.1007/s13347-022-00548-w

Wakefield, J. (2021, May 26). AI emotion-detection software tested on Uyghurs. *BBC News*. https://www.bbc.com/news/technology-57101248

Worldometer. (n.d.). *China population (live)*. Retrieved 21 December 2023, from https://www.worldometers.info/world-population/china-population/

Wright, J. (2023). Suspect AI: Vibraimage, Emotion Recognition Technology, and Algorithmic Opacity. *Science, Technology and Society*, 468–487. https://doi.org/10.1177/09717218211003411

Xu, X., Kostka, G., & Cao, X. (2022). Information Control and Public Support for Social Credit Systems in China. *Journal of Politics*, *84*(4), 2230–2245. https://doi.org/10.1086/718358

Youn, S. (2005). Teenagers' Perceptions of Online Privacy and Coping Behaviors: A Risk-Benefit Appraisal Approach. *Journal of Broadcasting & Electronic Media*, *49*(1), 86–110.

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. https://doi.org/10.1057/jit.2015.5