TOR VERGATA
UNIVERSITY OF ROME

# Università degli Studi di Roma "Tor Vergata"

Facoltà di Economia

Laurea/Bachelor of Arts

**in**

# Global Governance

The data collection-trust trade-off:
Why current data collection practices are a risk to customer loyalty

Candidate: Cornelius Balle

Supervisor: Prof. Laura Brandimarte

*Academic Year*

*2020-2021*

# Table of Contents

# The data collection-trust trade-off

## Why current data collection practices are a risk to customer loyalty

**Abstract**: The collection of user information by online service providers has become a widespread and profitable business model for many companies and created a large market around targeted advertisement online. Simultaneously, this has increasingly raised concerns about users' privacy and security on the internet, due to a great lack of awareness on the consumer's side about the dynamics and purposes of these data collection practices. As the awareness is spreading and calls for privacy protection online are enlarging among internet users, online companies are increasingly becoming subject to public scrutiny of their obscure practices and face growing pressure to change their approach on collecting users' personal information. This paper discusses the findings of a survey-based experiment on potential trade-offs faced by websites due to their current practices to collect users' personal information, also including the related internet privacy concerns and privacy protection measures of internet users. It investigated whether online service providers would be better off to implement transparent and privacy protective website designs instead of manipulative designs (dark patterns) tricking users into disclosing their personal information. This paper proposes a series of arguments why companies should opt for more transparency and enhanced privacy protection of their users' personal information.

**Keywords**: data collection, data collection trade-off, dark patterns, internet privacy concerns, privacy protection.

### 1. Introduction

The emergence of the digital age in the last decades led to the ever-increasing interconnection of people and machines through the internet. The digital space has by now entered almost every person's home and private life, merging the physical and digital worlds of people. Many daily activities have been outsourced to the online world, e.g. communication, shopping, education, entertainment etc., which has become an inevitable part of most human's lives. As this change has brought about many positive impacts on the living standards, welfare and opportunities of modern societies, it has led people to share vast amounts of personal information with online platforms and service providers in order to make use of these new opportunities. Many of these services online are available free of

charge, with most online platforms and service providers deriving large shares of their profit from the collection, analysis and sale of their users' personal information to advertising and marketing companies. This has become a widespread business model in the world of internet firms and created an enormous background market around targeted advertisement online. These developments increasingly raised questions and concerns about the security and privacy of internet users taking in the way companies gather, process and handle their users' information. Many privacy scholars criticize the imbalance of power between the companies and their users created by a large lack of privacy awareness among people and great information disproportionalities between the two parties. The growing societal debate about the regulation of data collection and the protection of people's privacy online has put pressure on companies to create more transparent and alternative models, also being slowly enhanced by a growing amount of legislation on data collection online and privacy. However, few companies have yet to fundamentally change their approach on this topic and their relationship with their users. As privacy awareness is continuously spreading and demands for stricter privacy regulations are increasing in societies all around the world, online platforms and service providers might soon face even greater pressure to change their business models towards greater privacy protection, possibly soon becoming an economic advantage in a privacy-aware world. With consumers all around the world becoming increasingly knowledgeable about the privacy-invasive techniques applied by many websites trying to harvest their personal information, internet users become more frustrated and increasingly take action or use tools to protect their privacy. Many of these measures can be harmful to companies as they pollute their databases for example or damage their relationship with the customer even risking losing them. This paper aims to investigate the potential trade-offs companies might face through their current data collection practices often based on tricky website designs. Furthermore, this paper wants to suggest that the respective websites are potentially better off by implementing fair and transparent website designs that are based on default privacy protection and hence build better relationships with their users.

Therefore, a survey-based experiment was conducted. The first section measured privacy concerns of the participants through the IPC scale developed by Hong and Thong (2013). The second part researched whether the participants undertook measures or applied tools in order to protect their privacy online, also investigating the existence of a potential

privacy paradox in combination with section one. In the last part of the survey, the actual experiment on potential data collection trade-offs was conducted. Therefore, the participants were split into a control group and experimental group. Both groups were presented the same three websites, but saw different website designs. The experimental group saw the original version of the website containing a manipulative design (dark pattern) helping the website to collect user's data. The control group saw a modified version of the same website presenting a transparent design allowing users to understand their options and achieve their goal more easily. The results showed strong privacy concerns among the participants while being online, but low activity concerning measures to protect their privacy. Hence, the existence of the privacy paradox was affirmed. It was difficult to definitely determine data collection trade-offs through the methodology applied in section three of this study, especially if the companies had a strong market position and offered a unique service. However, one trade-off was found for a website offering a substitutable service, and furthermore, the results indicated the possibility of further trade-offs under certain conditions for the other two websites and allowed speculations and realistic outlooks for future developments.

## 2. Literature review

The following literature review aims to reflect the main research findings for each of the sections investigated in the study (discussed in section 3 and following).

### 2.1. Privacy, internet privacy concerns and their measurement

Privacy is an ambiguous concept that many scholars have been trying to define for a long time. Some of the definitions that have been put forward define privacy as the protection of the personal space of people and an inherent right to be left alone (Warren and Brandeis, 1890), privacy as part of human dignity, autonomy and essentially of human freedom (Schoeman, 1992), and the individual's ability to control how, when and the extent to which one wants personal information to be communicated to others (Westin, 1967). The latter definition by Alan Westin has been widely used in the literature and research field. Even though the definitions might appear different from one another, many scholars today acknowledge exactly this variety as an important feature of privacy and highlight the importance of viewing privacy always in its respective environment making its meaning

highly context dependent (Brown and Muchira, 2004; Solove, 2007, Acquisti, Taylor, and Wagman, 2015; Finn Brunton and Nissenbaum, 2016). What all definitions have in common is that the individual is required to manage and negotiate one's own boundaries of the private and public sphere (Altman, 1975; Acquisti, Taylor, Wagman, 2015). This balancing of what an individual wishes to be public and what to stay private, depending on one's priorities in a situation, is also known as "privacy calculus". An invasion of privacy is the unauthorized use, disclosure, or collection of personal information (Wang, Lee, and Wang, 1998). Since the arrival of the internet in modern society, privacy issues and concerns about privacy have received increasing attention and are considered among the most important social, ethical, political and legal matters of the information age (Milberg et al., 2000; Culnan and Bies, 2003).

The constant emergence and development of better technologies, e.g. Big Data, presents a two-sided situation to society, as such technologies bear great opportunities to increase societal welfare, but on the other hand continuously pose new challenges to the understanding of privacy and its adequate protection. While the daily and global collection and analysis of personal information can contribute to beneficial discoveries such as unexpected interactions between drugs and early warnings for epidemics (Dugas et al., 2012), the excessive collection, aggregation and distribution of personal user information by private companies for marketing and advertising purposes has become strongly criticized for its exploitation of internet users. Scholars and experts have especially emphasized the created asymmetric relationships between online companies and their customers consisting in a strong lack of knowledge and awareness by internet users about the purposes and consequences of disclosing their personal information. This imbalance leaves internet users vulnerable and results in difficulties for users to make informed decisions online, therefore putting in question the required explicit consent by users for companies to collect their personal information (Culnan and Williams, 2009; Acquisti, Taylor, Wagman, 2015; Brunton and Nissenbaum, 2016). Among the major problems identified in these developments, is what came to be known as the Mosaic Theory of Privacy (Martin, 2016) or Information externalities (Choi, Jeon and Kim, 2019). They describe the ability, through new advances in predictive technologies and through the merging of distinct data bases, to combine small pieces of user information from everyday life that seem to be unrelated initially, but when aggregated together into personal profiles of data subjects, reveal great

amounts of new information that the person did not explicitly disclose[1] (Martin, 2016; Acquisti, Taylor, Wagman, 2015; Brunton and Nissenbaum, 2016). Some have even claimed that the Social Contract Theory would require consumers to be granted control and proper information about the intended use of the data collected, and only then the collection of personal information by companies would be justified (Donaldson and Dunfee, 1994).

Recent decades witnessed the rise of a giant data market (estimated to be worth between $300bn. and $400bn.) where consumer data is collected, aggregated into personal profiles of each user. This data is then analysed and eventually sold and distributed between service providers working in the background being mainly data aggregators, -brokers and ad-networks . Many of the participating actors in this data "supply chain" (Martin, 2016) are invisible to the consumer (Tene and Polonetsky, 2012) generating major revenues for all participating companies at the cost of the consumer (Martin, 2016). Choi, Jeon and Kim (2019) show that the current practices and dynamics of the data brokerage markets can incentivize small-scale websites without initial intention to collect user information, to start collecting it.

With a growing awareness being spread globally, internet users have been found to have certain privacy expectations about the collection and usage of their personal information by companies while interacting with them online and when using smartphone apps (Shilton and Martin, 2013). Hartzog (2014) claims the existence of a confidentiality agreement (also Donaldson and Dunfee, 1994) between the two parties when users access websites, since they disclose information with a specific purpose in mind, and would have not accessed the website and provided their information without adequate trust in the website's practices and handling of their personal information. Hence, inadequate handling of user data would make that confidentiality agreement invalid.

A political attempt to rebalance the relationship between online platforms and their users was the introduction of privacy policies on the side of the companies, e.g. through recent legislation such as the GDPR in the European Union. In many regions of the world, online service providers now must explicitly ask for the user's consent to collect their information and explain the company's data collection and processing practices. This "notice

[1] See also, Jernigan and Mistree's (2009) experiment about predicting the sexual orientation of Facebook users, solely based on their Facebook friendship associations, who did not disclose this piece of information and Acquisti and Gross (2009) demonstrating that US citizens' Social Security Numbers could be predicted with a fairly high accuracy, by knowing a person's state and date of birth.

and consent" mechanism to protect users' online privacy better has been widely criticized (Martin, 2013; Nissenbaum, 2011; Schwartz and Solove, 2011; Calo, 2012; Solove, 2013) as insufficiently informing consumers of the practices for several reasons: (1) The privacy policies are often too sophisticated and long for the average internet user to understand (McDonald and Cranor, 2008)[2], (2) many consumers are myopic and prefer immediate free services over reading privacy policies of the provider[3], and (3) future costs of privacy loss are difficult to grasp for many users, as they appear intangible and nebulous to many (Choi, Jeon and Kim, 2019).

Defining and measuring internet privacy concerns (IPC) accurately has therefore been of interest for researchers for a long time. The majority of studies to date agree on IPC being a multidimensional construct influenced by many factors such as self-development of a person, environmental impact and interpersonal interaction (Hong and Thong, 2013). Based on previous definitions that described IPC as the degree of an internet user's concern about the collection practices and use of his personal information by websites (Malhotra et al., 2004; Son and Kim, 2008), Hong and Thong (2013) argued that there is a fundamental difference between an individual's perception of one's own concerns about the handling of personal information by websites and the user's expectations on how websites should handle personal information, hence being a dyadic and interactive relationship between a user and an online entity. They created an updated and more comprehensive conceptualization of IPC aiming to contribute to a better understanding of the matter by establishing clear terminology and measurement of IPC, that was missing in previous literature. They also aimed to provide a useful instrument for researchers to inquire further into the subject in the future, a crucial activity in the current times of ever-increasing and -improving internet technologies (Hong and Thong, 2013). Their scale was used in this study to evaluate participants' privacy concerns (more in section 3). However, despite the growing consensus on IPC measurement and terminology, privacy concerns must always be regarded as highly dynamic and context dependent in order to achieve a better understanding of individuals' attitudes towards information management (Culnan, 1993, Malhotra et al., 2004). A long standing issue in the

[2] McDonald and Cranor (2008) estimated an economic loss of $781 billion if Americans were to read every single word of privacy policies

[3] This observation is backed by research in psychology showing that people are more likely to rely on foreseeable and imaginable benefits and costs in their decision making process, while humans tend to ignore and underestimate factors that are relevant in the future (Loewenstein and Prelec 1992; Mischel, Ebbesen, and Raskoff Zeiss 1972)

conduct of privacy surveys is the "talk is cheap" problem, showing that consumers demand much higher privacy protection than they actually desire (Harper and Singleton, 2001) since it is fairly easy to demand high privacy protection from companies. The debate about an adequate measure for IPC is ongoing, with some scholars criticizing Hong and Thong's (2013) IPC scale for not including the *right to be forgotten* which they found to be a separate aspect distinct from the six defined categories of privacy concerns (Steinbart, Keith, and Babb, 2017).

Several institutions now conduct large-scale surveys on privacy concerns on a regular basis. Most of them are detecting a similar development in societies around the globe of increasing online privacy concerns and an increasing sense of lacking control by users over their personal information being collected and distributed. As a result, low trust levels can be widely observed by consumers towards companies in this matter (Anant et al., 2020). A survey by the Pew Research Center (Auxier et al., 2019) of over four thousand U.S. adults found that the majority of respondents believed that their personal information is less secure today than five years ago (70%), overall data collection by companies practices bring more risks than benefits (81% of respondents) and that it is impossible to go through daily life without being tracked by companies, online and offline, and by the government to some extent. Furthermore, 79% were concerned about how companies used their data, 59% have very little understanding of what companies do with their information, and 69% lack confidence in companies using their data in ways that the users are comfortable with. The survey furthermore found that 72% believe that most of their online-activity on the smartphone is tracked by advertisers, tech firms and other companies, and 69% believe that offline behavior, such as location and conversations, are tracked by companies strengthening the argument put forward by Draper and Turow (2019) of a widespread sense of normalcy concerning the surveillance of people through companies.[4] Concerning laws and regulations, almost two thirds of the respondents reported having very little understanding of them[5], but awareness seems to be growing according to a report by McKinsey in 2020 (Anant et al.,

[4] Other scholars call it "surveillance capitalism", a term that became widely popular through Shoshana Zuboff's bestselling book "*The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*" (2019).

[5] Other examples of studies with congruent findings are the Digital Society Index 2019: Human Needs in a Digital World." n.d. Oxford Economics. https://www.oxfordeconomics.com/recent-releases/digital-society-index-2019-human-needs-in-a-digital-world. and a study by Cisco on the Critical Role of Privacy Emerging from Global Pandemic. n.d. Newsroom.cisco.com. https://newsroom.cisco.com/press-release-content?articleId=2139315.

2020) showing that six in ten consumers in Europe are now aware that their data usage is regulated by national and European legislation, an increase from four in ten consumers in 2015.

In the light of these developments, Draper and Turow (2019) claim to observe a new phenomenon of "digital resignation" in society, what they describe as people's dissatisfaction with the prevailing surveillance online and the widespread belief that the monitoring and privacy violations online are unavoidable and inescapable. According to their definition and survey, 58% of respondents have resigned. They claim that companies want to discourage users from understanding privacy policies on purpose in order to create a feeling of normality about online surveillance practices making users indifferent to the policies and hence collect data they might have not received if the users were fully informed of the practices. Also Brunton and Nissenbaum (2016) criticized the narrative created around individuals' balancing of privacy and utility in using online services, in which the utility of online services is presented unproportionally positive and the role of privacy protection being downplayed oftentimes. Furthermore, they have emphasized the illusion of real opting out from the data stream, arguing that nowadays a strong necessity and dependence on digital services exists requiring being and interacting online in order to lead a normal life.

Another phenomenon often encountered by researchers in the field of online privacy and practices, is the so-called privacy paradox (Norberg, Horne, and Horne, 2007). The privacy paradox describes the observation that people are generally concerned about their privacy online, as demonstrated by the studies discussed above, but don't act according to these concerns. Often, people have been found to consciously give up on their privacy in return for desired services online, of which many are available at no cost in exchange for the user's personal information. The continuous observation of a privacy paradox by researchers might be further proof of the presence of Draper and Turow's (2019) "digital resignation" and the "fantasy of opting out" described by Brunton and Nissenbaum (2016), and vice versa influencing one another in a feedback loop. Both of the latter phenomena are further accentuated by the widespread implementation of new software tools by companies on their websites, such as web beacons, flash cookies and browser fingerprinting, that are invisible to the visitors of the websites and continuously track a user's activities across contexts, in some cases even though one cares about privacy and has taken necessary steps to protect oneself.

### 2.2. Privacy Enhancing Technologies (PETs)

Just like technological improvements in companies allow greater advances in commercial data collection and analysis, often being harmful to the consumers' privacy, they also increasingly take place on the side of the consumer for the protection of online privacy. This development can be observed in the growing variety and availability of tools to protect one's privacy online on the internet market and in app stores (Anant et al., 2020), also known as privacy enhancing technologies (PETs). Not only do they enhance privacy protection of users, but some also allow users to learn more about who learns what about them and gives them greater choice in their information disclosure (Hoffman, 2014). Due to the abovementioned abundance of tracking by companies on the internet, an increasing number of people, even though still small, resort to the application of PETs in order to avoid the tracking of their data trails. The 2020 McKinsey Report on *Consumer data protection and privacy*[6] claimed that one in ten internet users (three in ten in the US) use an ad-blocking software, globally used on 600 million devices, and incognito browsers being used by more than 40% of internet users. In their survey 41% of the respondents said they had their browser set to turn-off cookies, but only 14% respectively used encrypted communication services and services for anonymous browsing, both being among the most effective PETs. Besides software tools, there are certain practices one can adopt to enforce privacy, which the study also reported on: 64% cleared cookies and browser history regularly, 36% did not use a website because it asked for a name, 26% used a temporary username or email address, and 13% provided inaccurate personal information. As these numbers show, the awareness and application of PETs and privacy protective practices is yet small, but is expected to grow in the coming decades. Some technologies implemented by companies, still track consumers even though steps to prevent online profiling were taken (Ayenson et al., 2011). As noted by Acquisti, Taylor, Wagman (2015), such PETs can help to protect privacy, but require users to be aware of tracking, often not being the case since a lot of tracking practices and tools are hidden to the website visitor. Additionally, PETs require extra efforts of users in terms of knowledge of such technologies and know-how about their implementation, which might be even more difficult to achieve in large vulnerable parts of a population. They also add

[6] https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative

that the lack of regulation in the field has stimulated industry growth on both sides of the spectrum, privacy enhancing and -invasive technologies. These dynamics resemble an arms race for data and privacy.

Another approach for privacy protection has been greatly elaborated in Finn Brunton and Helen Nissenbaum's (2016) work *Obfuscation: A user's guide for privacy and protest*. They define obfuscation as the "deliberate addition of ambiguous, confusing, or misleading information to interfere with surveillance and data collection" (Brunton and Nissenbaum, 2016, p.1) and present a series of tools and techniques to be used by people in order to obfuscate data collection online and enhance their privacy. They also discuss the ethical issues, such as data waste and free-riding, raised by critics but claim that there is no ground for criticizing obfuscation practices as long as the practice is proportional. They claim that this proportionality is often present in the practice of obfuscation by an individual and justified as long as commercial data collection and processing practices do not present a greater public value than the protection of privacy. If so, they ask to what extent an individual can be forced into sacrificing himself for the public good. They conclude that in the current imbalance of information and power between companies and users, in which the latter did not have an equal footing in the setting-up process and do not have a realistic option of escape, it is a justifiable practice for the less powerful offering them a form of resistance, obscurity and dignity.

A counter side of protecting one's privacy online is that users who implement such measures might end up paying a "privacy cost" by being excluded from price-discrimination (Choi, Jeon and Kim, 2019), and individually targeted advertisements and offers by companies resulting from the disclosure of personal information.

### 2.3. Dark patterns

With the rise of the internet over the last decades, the spread of personal computers and mobile devices throughout society, and the accompanying increased access to the e-commerce market by consumers all over the world, a growing emphasis by online service providers was put on the design of their websites and smartphone applications through which they offer their services. More specifically, online service providers started focusing on the design of the user experience (UX) on their platforms. Website operators have recognized the vast potential of such designs to market, promote and sell their services and products,

and furthermore to collect valuable user data. This led to the increasing occurrence of unfair and unethical designs helping companies to achieve these goals. These designs were later called “dark patterns”, a notion first coined in 2010 by Harry Brignull, a UX designer with a doctoral degree in cognitive science. He described dark patterns as "a user interface carefully crafted to trick users into doing things they might not otherwise do [...] they are not mistakes, they are carefully crafted with a solid understanding of human psychology, and they do not have the user’s interests in mind."[7] He went on to create a website aiming to spread awareness about dark patterns and exposing companies that implement them on their websites in a “hall of shame”[8], also inspiring an online movement through social media posts and hashtags calling out companies for their unfair UX designs.

As elaborated by Bösch et al. (2016), the effectiveness of dark patterns can be explained based on findings in psychological research about different motivational levels underlying thinking and reasoning processes of two different cognitive systems: System 1 (low motivation) and 2 (high motivation) thinking processes. Dark patterns function well when internet users are in a system 1 thinking mode, with low motivation to put effort into thinking and reasoning processes and also not having the capacity to do so due to a lack of knowledge, ability and time. This is the case with privacy policies and cookie preferences, which users often encounter in a state of low motivation and low consciousness about their privacy attitudes. Additionally, Bösch et al. (2016) argue that the basic human need to belong to significant others (E. Tory Higgins, 2011), expressed in the participation in online social networks and interaction online in general, further drives humans to disregard their privacy concerns and to surrender to dark patterns. This again, is another proof of Brunton and Nissenbaum’s (2016) argument that it is basically impossible to avoid being online and almost required in modern society.

Marthur et. al (2019) have conducted a major study on the presence of dark patterns on internet shopping websites. They have built a tool crawling through over eleven thousand shopping websites and found that 11.1% of the websites contained a dark pattern with a higher likelihood of popular websites to have dark patterns implemented in their design. They additionally found 22 third parties providing the construction of shopping websites

[7] Brignull, Harry. 2013. “Dark patterns: Inside the Interfaces Designed to Trick You.” The Verge. August 29, 2013. https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you#:~:text=A%20dark%20pattern%20is%20a (accessed 26 May 2021).
[8] “Dark patterns.” 2019. Darkpatterns.org. 2019. https://www.darkpatterns.org/.

with the option of creating dark patterns in their services, of which two service providers openly promoted the possibility to implement “fake” tools in the websites they create for their customers. The researchers built a useful taxonomy about dark patterns in general by combining prior research and their own findings, placing them into seven broad categories and 15 types of dark patterns, and defining their characteristics and the cognitive bias they exploit for their effectiveness. They have suggested their crawler to be used in other instances, as it allows an easier discovery and measurement of dark patterns online, and further activity in the field will allow the construction and distribution of more efficient tools against dark patterns of which they claim many to be unlawful.

Luguri and Strahilevitz (2019) further investigated the effectiveness of dark patterns and found that the implementation of dark patterns on websites is very effective in steering consumers into actions they would have not taken if they would have encountered a more neutral interface. In their experiment, they tried to convince consumers to sign up for a dubious identity theft program and managed to demonstrate that a “mild” dark pattern already more than doubled the percentage of subscriptions and “aggressive” dark patterns almost quadrupled the subscriptions. They also found that the aggressive dark pattern created a powerful backlash among participants, whereas the mild version did not. The implementation of a mild dark pattern would therefore be already a very powerful tool for companies, since they could easily achieve considerable advantages by experimenting with user behavior through very small changes to the software. Additionally, less educated people were more likely to surrender to the dark patterns. They called for necessary regulation of companies in the implementation of dark patterns suggesting that many of them would be against US law.

In website designs there is never a complete guarantee that the designs are intended as they appear to the user, potentially being unintended errors or influenced by external constraints. However, Luguri and Strahilevitz (2019) claim that most companies do have large amounts of resources at their disposal, and therefore intend almost all designs on their websites. Also Bösch et al. (2016) show that there are many proposed strategies for implementing so-called privacy patterns or strategies for “privacy by design” e.g. general architectural building blocks known as “Privacy Design Strategies" (Hoepman, 2014), being widely available and perfectly known to website designers. Since the consideration and resulting implementation of any pattern is typically part of the architectural design process

of a website, it becomes obvious that dark patterns do not follow privacy strategies on purpose, but rather do the opposite by deceiving users and tricking them into surrendering their personal information. This simple analysis supports the claims that many online service providers intentionally pursue dark patterns and strategies in order to collect their consumers' valuable data of which they can profit largely on the data market.

As a growing number of people become aware of the deceptive and manipulative effects of dark patterns (Chivukula et al., 2019) scholars have emphasized the importance of raising awareness and regular provision of information about dark patterns to increase motivation of consumers to reassess their consent to website permissions (Almuhimedi et al., 2015; Bösch et al., 2016), and therefore strengthening consumers' privacy consciousness.

### 2.4. Privacy protection as an economic advantage

The literature on the importance of trust for successful business making in e-commerce is vast. The research in online marketing shows that trust is even more important online, due to the lack of physical interactions between the vendor and the customer. However, the literature on the relationship of consumers' privacy concerns, trust levels and their willingness to buy and interact with platforms online, is very diverse and produced different findings, due to the context dependency and ambiguity of privacy attitudes and concerns. Privacy concerns by consumers can severely damage their trust levels in a company, and similarly, low trust levels can lead to more privacy concerns of consumers (Brown and Muchira, 2004). Several studies have found that companies can build trust with their consumers by protecting their privacy adequately (Culnan and Armstrong, 1999; Nam, Song, Lee, and Park, 2006), and that building trust is crucial to reduce privacy concerns and improve the relationship between the company and the consumer (Milne and Boza, 1999; Brown and Muchira, 2004). Privacy concerns can also be reduced by giving users more control over their information (Culnan and Armstrong, 1999; Malhotra et al., 2004; Tucker, 2014). Nam, Song, Lee and Park (2006) provide a good review on the relationship between privacy concerns and customers' willingness to provide personal information, finding that consumer privacy concerns strongly depend on the trust in the e-vendor, and on the value provided by the website. Consumers with higher privacy concerns were found to have lower trust in websites' handling of their personal information and found it riskier to provide personal information to websites (Hong and Thong, 2013). On the other hand, privacy

concerns might be reduced or superseded if consumers experience a sufficient level of participation in their relationship with the company (Campbell, 1997; Brown Muchira, 2004) or experience benefits such as time saving or a wider selection while shopping (Phelps, Nowak, and Ferrell, 2000). In other words, privacy concerns can have impacts on consumers' interaction with companies online, but are not the only factor determining the relationship and user actions, but depend on many factors e.g. brand value and reputation.

The developments in the recent decades led consumers to have low trust levels in general towards companies' ways of handling their data and its protection, as found in the 2020 McKinsey report on *Consumer Data Protection and Privacy.* In the report, no industry achieved a trust rating of 50%.[9] Recent legislation such as the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Lei Geral de Proteção de Dados (LGPD) in Brazil, are regarded as the strictest policies in the world as they heavily regulate the collection and processing of user data. They also urged companies and other institutions to comply with the laws in order to avoid high fines for data breaches and non-compliance (up to 4% of a company's global revenue under the GDPR). Complying with data regulation laws offers many more advantages for companies, apart from the avoidance of fines, that are crucial in the field of economic competitiveness (Garber 2018). Increasingly, scholars and experts researching in the field of privacy and business argue that companies can earn an economic advantage over their competitors by adding strong privacy protection to their business value and thereby increasing customer confidence into the brand (Holmes, 2006; Hoffman, 2014; Garber, 2018; Anant et al., 2020), especially emphasizing the potential benefits lying in the adoption of opt-in systems. Companies with higher "privacy trust scores"[10] were found to have higher response rates to their marketing campaigns by customers and a one percent increase in the score led to significantly higher revenues (Holmes, 2006). Also the *2021 Data Privacy Benchmark Study* by Cisco found that investments into privacy are worthwhile for companies, with 75% of the organizations seeing significant business value in the mitigation of security losses, enhanced agility and innovation and improved operational efficiency, and more than a third of organizations harvested benefits worth at least twice their privacy investment.

[9] Healthcare and Financial services reached the highest level of trust with 44% each (https://www.mckinsey.com/business-functions/risk/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative)

[10] Developed by the Ponemon Institute (https://www.ponemon.org/)

Also the widespread practice of consumer tracking online for targeted advertisement is getting more attention in the research field, since the main justification by companies for this practice is the goal to improve tailored offers and customer experience. Acquisti, Taylor and Wagman (2015) provide an extensive review of research on the pros and cons of balancing the protection of consumers' privacy with data tracking practices by companies in their paper *The Economics of Privacy*. They present and review a lot of economic models and research arguments demonstrating that the collection of data by companies for personalization purposes, such as targeted advertisements, offers and price discrimination, often do not achieve the desired outcome by the company. Some examples are the strategic rejections of offers by consumers if they are aware of tracking practices, improved precision of user information leading to less items being purchased (Bergemann and Bonatti, 2015), higher prices due to targeted advertising (De Corniere and Nijs, 2014), consumer backlashes due to price discrimination (Anderson and Simester, 2010), counterproductive effects of targeted advertisement due to increased privacy concerns of customers (Tucker, 2014), and tracking of consumers being only profitable to merchants if it is actually used to provide better personalized services to the consumer (Acquisti and Varian, 2005). According to the authors, such effects suggest that firms possess few incentives to match users with products and might be better off without tracking practices and with committing to stricter privacy policies. On the other side, privacy regulations must be chosen and implemented well, as for example regulation that enforces opting-in systems may lead to the fostering of "natural monopolies" since consumers are more likely to give their consent to large firms rather than to less established ones (Campbell, Goldfarb, and Tucker, 2015). Also, privacy regulation can be beneficial in case of naive consumers but might backfire in situations where selective targeting would be of benefit to the consumer, but where firms decided to abstain from it due to the regulation (Hoffmann, Inderest, and Ottaviani, 2014). Companies can further profit by allowing customers to anonymize to some degree (Conitzer, Taylor, and Wagman, 2012) and from stricter privacy protection since they could charge higher prices if they have certain proof of their privacy implementation in the form of privacy certificates or seals (Mai, Menon, and Sarkar, 2010) and, furthermore, because consumers have been found to be willing to pay higher prices for goods sold by vendors with more protective privacy policies (Tsai et al., 2011).

The literature review of the four fields shows that privacy and its protection in the information age has attracted a lot of attention by researchers, experts and legislators in the last decades, as technology and the internet have become an integral part of every human's life. However, this can be considered just the beginning since technological progress and the accompanying hunger for data will likely further fuel the arms race for privacy for a long time. While the privacy expectations and adopted protection measures by users have been researched more extensively, the high context dependency still leaves many uncertainties yet to be researched. Contrarily, the potential for benefits of strong privacy protection strategies implemented by companies deserves and requires much more attention and is just at the beginning of its discoveries slowly gaining traction. The first findings and a growing movement advocating for stronger privacy protection already hint towards a lot of hidden capacity of the concept to be unlocked by companies and institutions. This study aims to contribute to clearing the blur about the benefits for companies and institutions choosing transparency and privacy protection strategies over greed for data and deception of their customers.

## 3. Survey

### 3.1. Survey description and methodology

This study aimed at investigating a potential trade-off encountered by online service providers with their current data collection practices. In the companies' pursuit to collect user information, the implementation of dark patterns is a widespread practice to manipulate user choices and collect user information more easily. This study investigated whether implementations of dark patterns can have an opposite effect for the respective service provider in making users reluctant to provide information and to engage with the provider in the future. These outcomes would be opposite to the companies' goal of collecting valuable user information, potentially even having worse effects with users obfuscating information by providing wrong data, or dropping the services provided by the company or institution.

The survey was structured in four parts. The first section contained questions about demographics asking survey participants for their gender, age, country of birth, education, and employment to get an overview about the participants and allowing an analysis of potential patterns in privacy concerns and practices among different societal groups.

Section two of the survey aimed at examining general online privacy concerns of the participants and their trust and risk beliefs while engaging with companies online. This was evaluated through the internet privacy concerns (IPC) scale developed by Hong and Thong (2013). The scale presented 18 statements from six different categories (three statements for each category) to the participants asking them to what extent they agree or disagree with the presented statement. The original IPC scale contains two versions for each statement, one measuring participants' privacy concerns for government websites and another for commercial websites. This study only measured participants' privacy concerns about commercial websites, since commercial websites are more likely to use dark patterns compared to government websites. The trusting and risk beliefs followed the IPC scale each containing four statements. The addressed IPC categories were collection, secondary usage, errors, improper access, control, awareness. *Collection* is the degree to which a person is concerned about the amount of individual-specific data possessed by websites. *Secondary usage* is the degree to which a person is concerned that personal information is collected by websites for one purpose but is used for another, secondary purpose without authorization from the individual. *Errors* is the degree to which a person is concerned that protections against deliberate and accidental errors in personal data collected by websites are inadequate. *Improper access* is the degree to which a person is concerned that personal information held by websites is readily available to people not properly authorized to view or work with the data. *Control* is the degree to which a person is concerned that one does not have adequate control over one's personal information held by websites. *Awareness* is the degree to which a person is concerned about one's awareness of information privacy practices by websites. *Trusting beliefs* measure the general level of trust internet users have while being online concerning the handling and usage of their personal information by websites, and concerning the promises made by websites and their predictability regarding the usage of personal information. *Risk beliefs* measure the general risk perception of internet users while being online concerning giving out personal information, the potential for loss of that information, and the uncertainty and unexpected problems related to giving personal information to commercial websites. For each statement the participants were asked to select their level of agreement from a seven-point Likert Scale ranging from strongly disagree to strongly agree. All participants were given all 26 statements. The order of the statements was randomized intending to create a sense of diversity among the statements and to prevent participants from

getting confused by potentially perceived similarities between statements from the same section.

After having examined the participants' general privacy concerns, the third section was dedicated to learn about the participants' active role in privacy protection online. The first question asked whether the participants were taking measures to prevent their data from being collected or whether they were using obfuscation techniques to prevent data collection. The provided options were: provide a non-identifying email-address, give a wrong email address, decide not to provide information, give up access to a product/service, switch provider, clear cookies regularly, clear browser history, and an open option for additional measures. The second question asked the participants whether they were using privacy enhancing technologies (PETs) to protect their privacy online. The provided tools were: Advertisement-blocker, automated random ad clicking, anti-tracking software, private search engines, privacy protective web browsers, VPN, encrypted email and messaging services, secure collaboration/ productivity platform, and an open option for additional software tools used by participants. For both questions, the participants were given a set of measures asking them to answer how frequently they make use of the measure on a five-point Likert scale ranging from never to always. The order of asking the participants first about their privacy concerns online and afterwards about their actual implementation of privacy protecting measures also allowed an analysis of the congruence of participants' convictions with their according actions concerning privacy protection, hence an analysis of a potential privacy paradox existing among the participants.

In the fourth and final section of the survey, the core experiment about the trade-off effect of dark patterns was conducted. The participants were successively confronted with the websites of three popular companies each containing a different type of dark pattern. The three companies' websites containing dark patterns were Ryanair, Amazon, and CNN. The occurring dark patterns were represented in the survey through screenshots of the original scenarios on the websites with red marks indicating the required steps to achieve an imagined goal reflecting a realistic scenario. The websites were chosen with the intention to increase familiarity and engagement of the participants since they are very likely to be known or have been used by the participants. For each of the scenarios, the participants were provided a short paragraph introducing them to the scenario they should imagine themselves being in, and which users have to go through also in reality, if they would wish to conduct the

following actions. After each scenario, the participants were asked a set of follow-up questions: (1) How intentional by the company did they believe the design to be, (2) whether they would comply with the action required, (3) whether they would engage with the company's website again for future services and (4) how upset the required action(s) made them. In order to allow a comparison of the effect of the dark pattern and a potential trade-off for the providers, a control group was set up. A randomizing-tool ensured that participants were equally distributed in the experimental and the control group. The control group received the same screenshots used in the experimental group but in a modified version removing the dark pattern. The recreated scenario for the control group allowed users to achieve the same imagined goal of the experimental group more directly and intended to reduce or completely remove the burden to achieve the goal. Only the follow-up question (1) about intentionality from was removed for the control group, because the modified scenarios did not display the intention to manipulate users against their will.

The first dark pattern was an automated newsletter subscription on the Ryanair website (Appendix 1). The participants were told that they would like to book a flight on the website, and the last page of the check-out contained a box showing up in which participants were automatically subscribed to the Ryanair newsletter. If they didn't wish to receive the newsletter, they had to opt-out. According to the terminology defined by Marthur et al. (2019) this dark pattern belongs to the category of *sneaking* and the subcategory *sneak into basket.* Sneaking is a category of dark patterns aiming to falsely represent user actions, also hiding or delaying information, to which the user would likely object, if that information was made available. "Sneak into basket*"* in particular, is a dark pattern adding a product or service to a customer's checkout basket without one's consent (in this case subscribing them to a newsletter). The website operator hopes that the customer will stick with the automatically added product or service thereby exploiting the default effect cognitive bias of people[11]. They declared such patterns to be "partially deceptive [...] and information hiding" (Marthur et al., 2019). For the control group, the box approving the newsletter subscription was left unchecked and the description was changed to asking the users to opt-in if they wished to subscribe to the newsletter.

[11] Acquisti, Taylor, and Wagman (2015) found that users are more likely to remain subscribed to targeted advertisement under a default option in which users must opt-out, compared to an opt-in approach with the default option being unsubscribed, based on a demonstration by Cialdini and Goldstein (2004) in the case of organ donations obtaining similar results. Also Luguri and Strahilevitz (2019) had a default selection in their experiment leading to a doubling of subscriptions

The second dark pattern presented to the participants was the process required to close a user account on the Amazon website (Appendix 2). The imagined scenario given to the participants was that they wanted to close their Amazon account. Therefore, they were led through the original process, requiring customers to undergo a series of eight steps, of which multiple can be considered as hidden and obscure. In the terminology of Marthur et al. (2019) this pattern belongs to the category of *obstruction*, under the subcategory of *hard to cancel* (*Roach motel* according to Brignull[12]). Such obstruction patterns aim to increase the difficulty of simple actions in order to deviate users from taking the action. A *hard to cancel* dark pattern allows an easy subscription to a service or membership, but requires a more difficult procedure to quit the service. Such a pattern is classified by the researchers as "restrictive [...] and information hiding" (Marthur et al., 2019). In the control group, the participants saw a direct link leading them to the account closing process in the "Account & Lists" drop down menu allowing them to directly proceed to the page for closing an account. An additional follow-up question was posed for this scenario, asking whether participants would avoid products or services offered by Amazon in the future.

The third scenario was a pop-up window on the CNN website containing the website's cookie policies (Appendix 3). The participants were told to imagine that they would want to turn-off all non-essential cookies. In the original scenario, the users could either choose to accept all cookies or manage their preferences by clicking on a smaller link below ("Manage cookies+"). The latter option led them into a small window with many similarly looking options to select cookie preferences. The window was provided and operated by the company One Trust. After scrolling down, users were required to open each cookie category individually with each one opening up an option allowing the user to "object to legitimate interest". A total of 16 clicks was needed to achieve the goal of objecting to all non-essential cookies.[13] Such cookie settings, although not defined by Marthur et al. (2019), fit into the category of obstruction (or "privacy zuckering"), since an action that is supposed to be simple is made harder in order to deviate the user from pursuing his intended action. In the scenario for the control group, the same goal of refusing all non-essential cookies was

[12] "Roach Motel - a Type of dark pattern." n.d. Www.darkpatterns.org. https://www.darkpatterns.org/types-of-dark-pattern/roach-motel, (accessed 26 May 2021)

[13] Ironically, the company offers on its own website (https://www.onetrust.com/) a very simple dyadic cookie option to decline or accept all cookies. Hence, the company seems to offer building such deceptive patterns for other companies.

achieved by simply having an option to “Decline All” next to the “Accept All” option on the pop-up window.

All questions were mandatory to be answered to achieve conformity, completeness, and comparability between participants. As the control group received modified screenshots of the websites, they were offered the option of viewing the original versions containing the dark patterns after they had gone through all scenarios, or could choose to directly end the survey. The intention of this option was to add an educational aspect for interested participants in order to spread awareness about the presence and workings of dark patterns on the internet.

The survey experiment was created on the experience management platform Qualtrics (www.qualtrics.com). The recruitment of participants for the survey took place via the private social networks of the researching student, distributing and sharing the access link to the survey via WhatsApp Messenger, Facebook, LinkedIn, and Instagram. Responses were collected from 19 May - 31 May 2021. The main group reached was the student network of the Global Governance course at the University of Rome Tor Vergata. Some of the researching student’s contacts forwarded the survey to their networks, including student networks at a Masters program in Nürnberg (Germany), India, students of the University of Arizona (USA), and the University of Otago (New Zealand). Further detail on the demographics will be presented in section 4.

## 4. Analysis of the results

### 4.1. Sample description

The sample consisted of 116 participants (n = 116) after removing incomplete responses of participants who did not answer all questions. All participants completed section one (demographics), two (IPC), and three (PETs), and for section four (website scenarios) the randomization tool assigned 59 respondents to the control group, and 57 participants to the experimental group. There were more females (54%) than males (44%) among the survey participants. The average age of the participants was rather low, with the largest share being 18-24 (67%) and 25-34 year olds (20%), as expected from the university environment in which the survey was mainly distributed. People from 28 different countries participated in the survey, with the largest shares coming from Germany (29%), Italy (21%), USA (10%), and India (8%). The question asking for education did not reveal a lot of specific information,

since it was misunderstood by many. The question was aimed to capture the completed education by the participants, but many selected either the degree they are currently in or the number of years they have accomplished to date in their ongoing studies, resulting in a skewed picture of the actual education the participants have received. However, since most contacts of the researching student who helped share the study shared it primarily into university or peer groups, it can be concluded that most participants have some university experience, either with a finished degree or still pursuing their studies. The following question on employment offered more support for this assumption. As expected, the largest share and about half of the participants were students (48%). Furthermore, many were employed full time (30%) and part time (8%), and some were unemployed looking for work (6%) and not looking for work (4%), of which many can be expected to have a university degree according to the results in the question on education.

| Gender | | | Age | | | Country | | | Education | | | Employment | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Total | % | | Total | % | | Total | % | | Total | % | | Total | % |
| Female | 63 | 54% | <18 | 1 | 1% | GER | 34 | 29% | Less than High school | 1 | 1% | Full time | 35 | 30% |
| Male | 51 | 44% | 18-24 | 78 | 67% | ITA | 24 | 21% | High school | 19 | 16% | Part time | 9 | 8% |
| N-B/Third. | 2 | 2% | 25-34 | 23 | 20% | USA | 12 | 10% | Some college | 13 | 11% | Unempl. looking for work | 7 | 6% |
| | | | 35-44 | 4 | 3% | IND | 9 | 8% | 2Y degree | 6 | 5% | Unempl. not looking for work | 5 | 4% |
| | | | 45-54 | 2 | 2% | BRA | 3 | 3% | 3Y degree | 33 | 28% | Retired | 3 | 3% |
| | | | 55-64 | 7 | 6% | NZ | 3 | 3% | 4Y degree | 17 | 15% | Student | 56 | 48% |
| | | | 65-74 | 1 | 1% | UK | 3 | 3% | Masters | 21 | 18% | Prefer not to say | 1 | 1% |
| | | | 75-84 | 0 | 0 | RWA | 3 | 3% | Professional degree | 3 | 3% | | | |
| | | | >85 | 0 | 0 | | | | Doctorate | 2 | 2% | | | |
| | | | | | | | | | Prefer not to say | 1 | 1% | | | |
| Total | 116 | 100% | | 116 | 100% | | 91* | 78%* | | 116 | 100% | | 116 | 100% |

*Only countries with more than 3 participants

**Table 1.** Demographics of the survey sample

The experimental and control group each consisted of similar demographics. The control group had an even balance of male and female participants (49% each), whereas the experimental group consisted of more females (60%) than males (39%). In the experimental group, participants were slightly older but 84% were between 18-34 years old, and 90% in the control group. In both groups the largest share of participants came from Germany and Italy, although being higher in the control group (56%) than in the experimental group (44%). Also in employment the participants of both groups didn't differ a lot, with 74% in the experimental group being employed full time or students, and 83% in the control group, of which the experimental group had more full time employed participants (36%), and the

control group more students (60%). The data visualization and analysis was conducted through Microsoft Excel.

### 4.2. Internet privacy concerns and trusting- and risk beliefs

The survey investigated the general internet privacy concerns (IPC) of the participants by applying the IPC scale developed by Hong and Thong (2013) (Appendix 4). The scale measures the concerns in six categories: collection, secondary usage, errors, improper access, control, awareness. Additionally, two categories were added to measure the trust and risk beliefs participants have while engaging with websites online. The answer scale ranged from strongly disagree (1) to strongly agree (7), meaning that higher privacy concerns were expressed through higher values on the scale and vice versa for lower privacy concerns.

**Collection:** The survey found this category to be the strongest concern of participants with an average score of 5.85/7 and 74% agreeing or strongly agreeing to be concerned about the amount of individual-specific data possessed by websites.

**Secondary usage:** A similar high concern was found in this category, with a mean of 5.71/7 and almost two thirds (64%) of participants agreeing or strongly agreeing to be concerned that personal information is collected by websites for one purpose but is used for another secondary purpose without authorization from the individual.

**Errors:** Participants were less concerned about inadequate protections by websites against deliberate and accidental errors in personal data collected with an average score of 4.56/7 and only 35% agreeing or strongly agreeing to the respective statements. However, including participants that somewhat agreed, the share of concerned participants rose to 57%.

**Improper access:** In this category the mean was again higher (5.4/7) and 59% were concerned about personal information held by websites being readily available to people not properly authorized to view or work with the data.

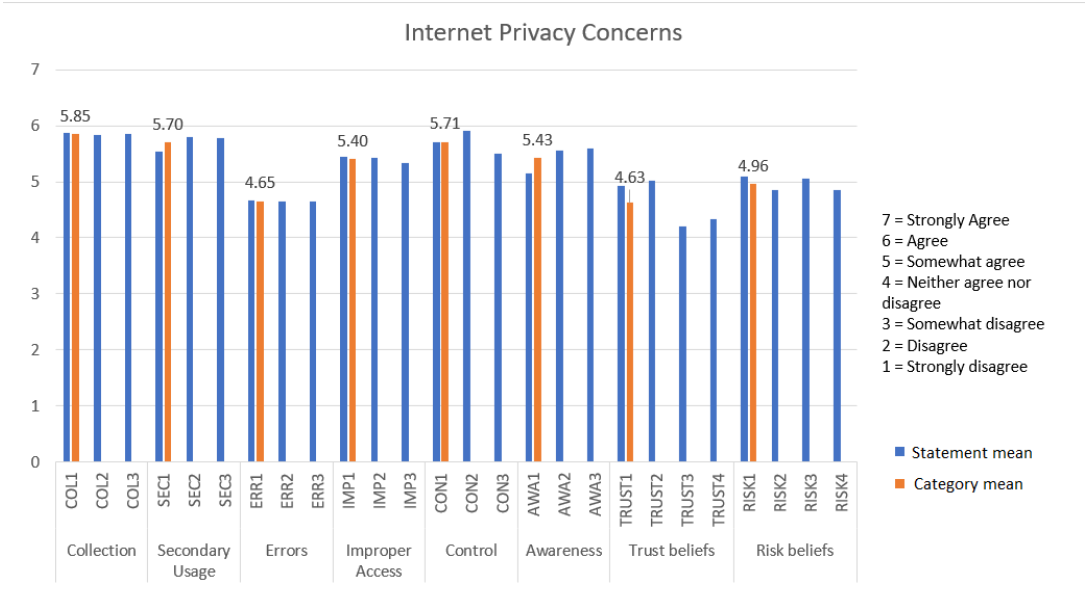
**Control:** Participants showed high concerns in the control category with a mean of 5.71/7 and two thirds (67%) being concerned that one does not have adequate control over one's personal information held by websites.

**Awareness:** This category describes the degree to which a person is concerned about one's awareness of information privacy practices by websites, being another area of considerable concern with a mean score of 5.43/7 and 55% agreeing or strongly agreeing to the concerns.

Overall, high privacy concerns were observed, with a total IPC mean of 5.46/7 and 80% at least somewhat agreeing with the concern statements and 59% even agreeing or strongly agreeing.

**Trusting beliefs**[14]: The survey indicated a certain lack of trust by the participants in the handling and usage of their personal information by websites, and concerning the promises made by websites and their predictability regarding the usage of personal information. Participants showed lower general trust into companies handling their personal information (4.93/7) and when asked whether they believe websites would keep the user's best interest in mind while dealing with their personal information (5.02/7), but were slightly more trusting about websites fulfilling their promises related to their personal information (4.21/7) and the websites' predictability and consistency regarding their personal information (4.34/7). The overall average was 4.63/7, with 56% at least somewhat disagreeing with the trusting statements (33% disagreed or strongly disagreed).

**Risk beliefs:** Participants showed higher risk beliefs concerning giving out personal information, the potential for loss of that information, and the uncertainty and unexpected problems related to giving personal information to commercial websites.




**Graph 1.** Internet privacy concerns of the participants

The average score was 4.96/7 and 68% somewhat agreeing with the risk statements provided (39% agreed or strongly agreed).

[14] Since the statements for the trusting beliefs were framed in a positive way, the answer scale was re-coded from (1 = Strongly Agree to 7 = Strongly disagree). Higher values indicated lower trust levels.

The overall mean score of IPC and trust and risk beliefs is 5.29/7 with 7 being the highest internet privacy concerns and the lowest trust levels. In total, 76% at least somewhat agreed to privacy concerns and risk statements, and somewhat disagreed with a general trustworthiness of websites. 53% even agreed or strongly agreed to privacy concerns and risk statements, and disagreed and strongly disagreed with the general trustworthiness of websites.

This result is also reflected by the investigation of correlations between the individual categories. Almost all IPC categories showed positive correlations ($r \geq 0.46$, most $r \geq 0.6$), meaning that participants having high concerns in one category were similarly concerned in another. *Error* showed the weakest correlations ($0.3 \leq r \leq 0.46$) to the other categories except one higher correlation with *improper access* ($r = 0.59$). Interestingly, low *trusting beliefs* did not correlate significantly to the high concerns in the other categories ($r \leq 0.15$). *Collection* correlated strongly with *secondary usage* ($r = 0.72$) and *control* ($r = 0.77$), *secondary usage* correlated strongly with *control* ($r = 0.74$), and also *awareness* and *risk beliefs* (0.71). The strongest correlation was found between *control* concerns and *awareness* concerns ($r = 0.81$), showing that both categories are closely related and people are similarly concerned about being in control over personal information held by websites, and being aware of a website's privacy practices. The *risk beliefs* of participants correlated very consistently with all IPC categories with $r \geq 0.63$ (except Error, $r = 0.41$).

| | *COL* | *SEC* | *ERR* | IMP | CON | AWA | TRU | RIS |
|---|---|---|---|---|---|---|---|---|
| **COL** | 1.00 | | | | | | | |
| **SEC** | 0.72 | 1.00 | | | | | | |
| **ERR** | 0.30 | 0.38 | 1.00 | | | | | |
| **IMP** | 0.46 | 0.60 | 0.59 | 1.00 | | | | |
| **CON** | 0.77 | 0.74 | 0.41 | 0.61 | 1.00 | | | |
| **AWA** | 0.64 | 0.62 | 0.46 | 0.61 | 0.81 | 1.00 | | |
| **TRU** | 0.15 | 0.15 | -0.02 | 0.10 | 0.12 | 0.05 | 1.00 | |
| **RIS** | 0.65 | 0.68 | 0.41 | 0.63 | 0.66 | 0.71 | 0.15 | 1.00 |

**Table 2.** Correlations within IPC

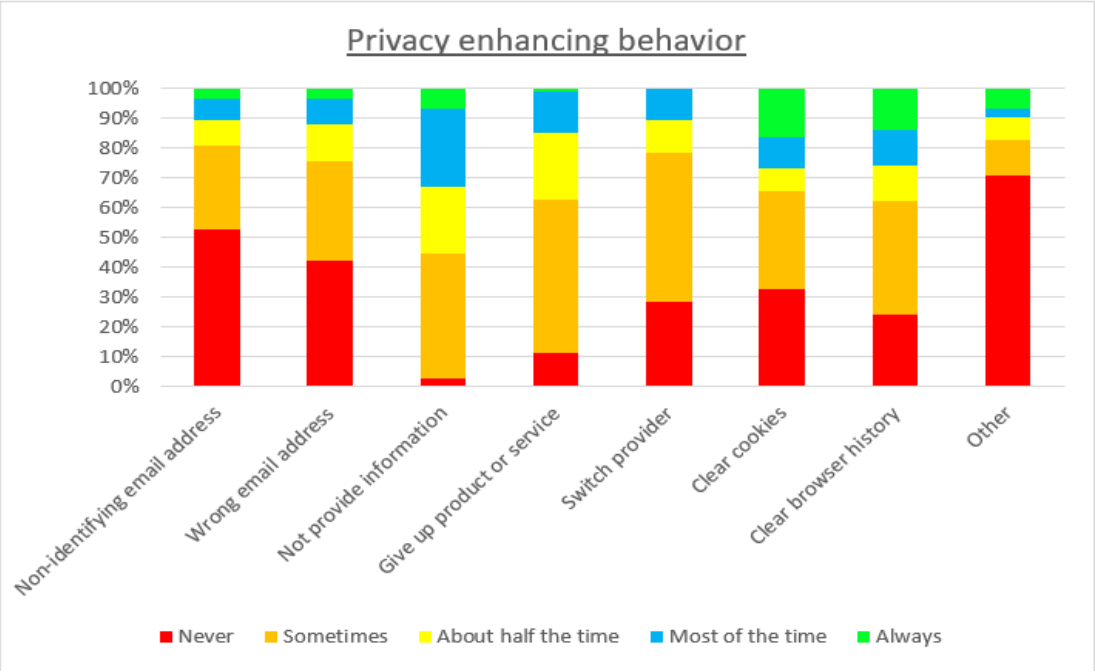
### 4.3. Privacy enhancing behavior and -technologies

After having analysed and found a high level of privacy concerns in the previous section, this part will evaluate whether the participants act accordingly to their privacy concerns with certain measures and tools to protect their privacy online. The participants

were provided a set of measures and tools and asked to provide how often they apply them (Never, sometimes, about half the time, most of the time, always).

### 4.3.1. Privacy enhancing behavior

Expecting a rather low level of privacy protection, due to the often observed privacy paradox, this survey did make some interesting and relevant findings concerning growing interest in privacy protection, especially among young people. The most impactful findings were that 97% of the participants said they would not provide information at least sometimes and 55% even about half the time. Also, 89% indicated to give up a product or service at least sometimes to protect their privacy or prevent their data from being collected by a provider. In the same frequency 72% said they would switch providers in such situations. Also the clearing of cookies and browser history was a common practice with 67% and 76% respectively saying to do it at least sometimes (every third did so at least half the time). About half of the participants (47%) indicated to use a non-identifying email address and 58% even said to provide a wrong email address at least sometimes. Further practices mentioned by the participants were giving wrong names and data, temporary self-destructing email addresses, selecting only necessary cookies, turning off the internet connection in shopping centers, and avoiding online services wherever possible. However, it must be noted that most participants applied most of the practices only sometimes, which indicates that a majority of their online behavior is still being tracked and gathered.




**Graph 2.** Privacy enhancing behavior of the participants

Nonetheless, these results show a widespread level of awareness of the possibilities to protect one's privacy and a certain willingness to apply them occasionally.

**Correlation with IPC**: A correlation matrix provided further insights on which participants were more likely to adopt certain privacy protective behavior. The decision not to provide information correlated somewhat with higher concerns in the IPC categories of *collection* (r = 0.35), *secondary usage* (r = 0.3) and *risk beliefs* (r = 0.3). Giving up a product or service correlated with concerns the categories of *collection* (r = 0.38), *control* (r = 0.33) and slightly higher with *risk beliefs* (r = 0.43). Participants that tended to switch providers if they did not feel their privacy sufficiently protected had slightly higher concerns in *collection* (r = 0.3) and *awareness* (r = 0.31). Providing a wrong email address correlated slightly with higher *risk beliefs* (r = 0.31).

| | *COL* | *SEC* | *ERR* | IMP | CON | AWA | TRU | RIS |
|---|---|---|---|---|---|---|---|---|
| Provide a non-identifying email address | 0.21 | 0.11 | -0.07 | -0.04 | 0.07 | 0.10 | -0.03 | 0.13 |
| Give a wrong email address | 0.17 | 0.26 | 0.06 | 0.19 | 0.15 | 0.23 | 0.17 | 0.31 |
| Decide not to provide information | 0.35 | 0.30 | 0.01 | 0.16 | 0.27 | 0.28 | 0.07 | 0.30 |
| Give up access to a product or service | 0.38 | 0.28 | 0.11 | 0.24 | 0.33 | 0.28 | 0.00 | 0.43 |
| Switch provider | 0.30 | 0.20 | 0.09 | 0.08 | 0.27 | 0.31 | 0.10 | 0.23 |
| Clear cookies regularly | 0.07 | 0.07 | 0.04 | 0.15 | 0.07 | 0.17 | 0.06 | 0.07 |
| Clear browser history | -0.01 | 0.00 | 0.07 | 0.21 | 0.09 | 0.14 | 0.06 | 0.08 |
| Other | 0.02 | 0.03 | -0.22 | -0.14 | -0.07 | 0.08 | 0.11 | 0.08 |

**Table 3.** Correlations between privacy enhancing behavior and IPC

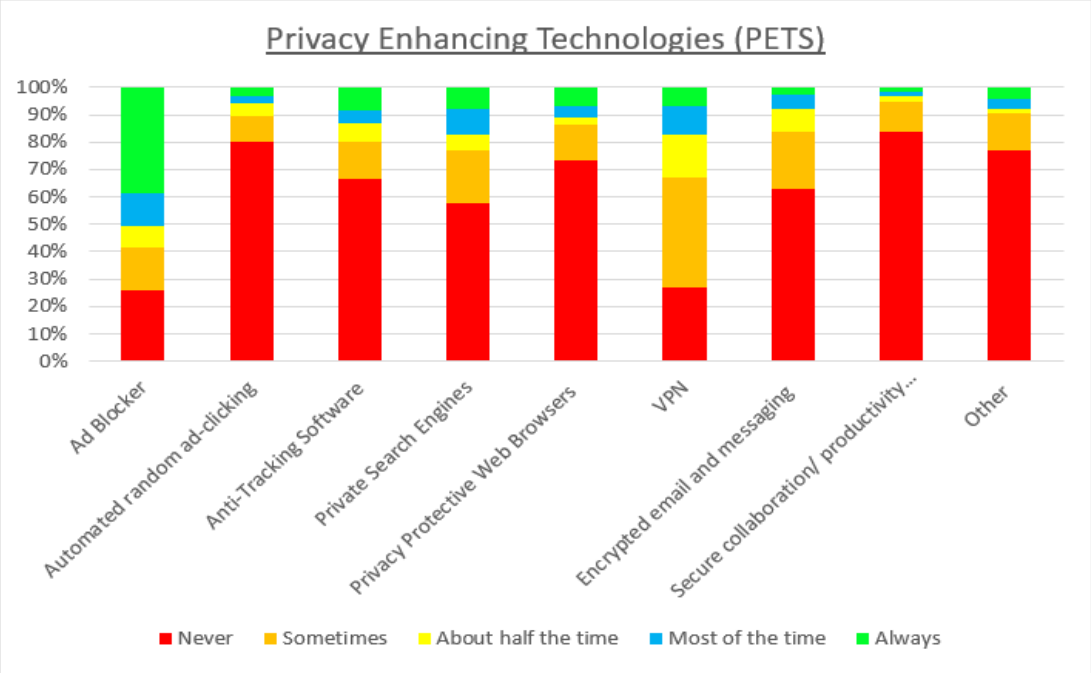
### 4.3.2. Privacy Enhancing Technologies (PETs)

The usage of PETs among survey participants was overall low with only a few finding a wider application. The most popular PET used by participants was the advertisement-blocker with 74% using it at least sometimes, 59% using it at least half the time and four out of ten participants (39%) always. Followed by virtual private networks (VPN) which 73% declared to use at least sometimes but only every third (33%) about half the time. Both tools' popularity is also supported by the fact that only 26% for ad-blockers and 27% for VPNs said they would never use them. The other tools in the list being applied at least sometimes

were private search engines (42%), encrypted email and messaging services (37%), anti-tracking software (34%), privacy protective web browsers (27%), automated random ad-clicking (20%) and secure collaboration platforms (16%).

A possible reason for the low usage of PETs could be the lack of knowledge required to understand the nature of data collection by websites, the risks it can pose to one's privacy online and how to address them appropriately through available PETs. Although many internet users believe to be helpless against their data being tracked and collected online, a further issue contributing to the low usage of PETs, even among people that want to protect their data, might be the perception of users that technological knowledge is required to apply some of them. However, if a PET becomes popular and easy to apply, as in the case of Ad-blockers and VPNs, they spread more quickly and demonstrate again a growing interest in privacy protection and a willingness to apply privacy protective tools. Furthermore, the popularity of the ad-blocker showed that many people do not wish to receive personalized ads or advertisements in general.

The analysis of the internet privacy concerns, trust- and risk beliefs, and privacy protective behavior online by the survey participants, proved once again the existence of a gap between privacy concerns and actions to protect one's privacy, the so-called privacy paradox. Although there are more and more individuals that prevent their personal information from reaching the websites, there are still major pools of personal data created




**Graph 3.** Privacy enhancing technologies used by the participants

by users every time they go online which are harvested by websites for profit day-by-day without the users' knowledge or explicit consent. Although the data did not clearly hint towards a closure of the paradox, it did allow room for speculation on the potentially growing interest of people to protect their privacy online. With adequate awareness campaigns and tools that are simple in their application, a more widespread movement on privacy protection might find more followers and users of PETs.

**Correlation with IPC:** There were no significant correlations between IPC of users and their usage of PETs, except a slight negative correlation between low *trust beliefs* and the usage of secure collaboration or productivity platforms ($r = -0.33$). A possible explanation could be that low trust levels towards websites degenerate the trust into proclaimed "secure" collaboration platforms or make users even more reluctant to use such platforms. However, this might also just be a random result since 84% of participants did say they never make use of them.

### 4.4. Website scenarios: Hypothesis and interpretation of results

In section four of the experiment (website scenarios) several effects of dark patterns used by websites to collect user data were investigated and measured. The participants of both groups, control and experimental, were given the same imaginary goal for each website and the same or similar[15] follow up questions. This allowed a comparison between the two different scenarios, with and without dark pattern, and the effect they had on the participants and their actions (see Section 3 for more details). Each follow up question gave rise to a null hypothesis ($H_0$) to be tested. The null hypotheses expected no difference between the mean of the control group and the experimental group. The hypotheses were then tested by subtracting the mean of the control group (M2) from the mean of the experimental group (M1) and conducting a student's t-test on the difference between M1 and M2 in order to test its statistical significance. The participants were asked to answer the follow-up questions on a five-point Likert Scale with 1 being the most positive outcome for the company and 5 being the most negative outcome for the company.

[15] Both questions were directed at the same goal but some questions required an adjusted wording for the questions to be logical, as the manipulation of the website in the control group changed the appearance of the scenario. See the footnotes of the questions for the adjustments.

### 4.4.1. Scenario 1: Ryanair

The Ryanair website contained a default newsletter subscription with an opt-out option if participants wished not to receive the newsletter, which was changed to an opt-in option for the control group. The follow-up questions asked to the participants were: (R1) How intentional of Ryanair do you think this selection is?[16], (R2) Would you opt out from the Ryanair newsletter?[17] (R3) Would you use the website again to book travel?[18], and (R4) How upset would you be after being automatically subscribed to the Ryanair newsletter?[19]

**R1. How intentional of Ryanair do you think this selection is?:** The mean for this question in the experimental group was a 4.6/5 (4 = Probably intentional, 5 = Definitely intentional). This score showed that people definitely believe companies to carefully think through and craft every design on their website, and not consider them to be accidents or unintended designs by the company.

**R2. Would you opt out to receive the Ryanair Newsletter?:** In the experimental group the mean was 4.16 (4 = Probably yes, 5 = Definitely yes) and in the control group the mean was 4.78 (4 = Probably not opt-in, 5 = Definitely not opt-in).

$$\mathbf{H_0(R2) : M1 - M2 = 0}$$

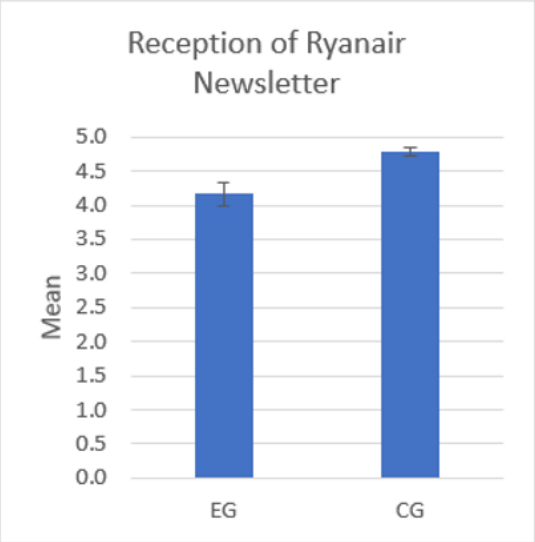
$$\mathbf{H_1(R2) : M1 - M2 \neq 0}$$

$$\mathbf{R2: 4.16 - 4.78 = - 0.62 \neq 0,\ p < 0.05}$$

The results show that participants in the control group were more likely to not opt-in for the newsletter, than people opting-out in the experimental group. In other words, participants in the control group were significantly less willing to receive a newsletter than in the experimental group. This allowed a rejection of the null hypothesis $H_0$(R2) proving the effectiveness of the dark pattern in making more people subscribe to the newsletter than under neutral conditions. It showed again why many companies are incentivized to implement dark patterns on their websites as they allow them to collect more customer data. This optimizes benefits for Ryanair since they can use the data for their marketing strategies, but contrarily clashes with the desires of the customers that do not want to provide their data

[16] Scale from 1 = Definitely not intentional, to 5 = Definitely intentional. This question was only asked to the experimental group as explained in chapter 3.
[17] Scale from 1 = Definitely Not to 5 = Definitely Yes, and question adjusted for Control group to: Would you opt in to receive the Ryanair newsletter?
[18] V. sup.
[19] Scale from 1 = Not at all upset, to 5 = Extremely upset, and question adjusted for the control group to: How upset would you be after being offered to opt in to the Ryanair newsletter?

to receive the newsletter. Although, also in the experimental group many people did not want to receive the newsletter and chose to opt-out (Mean: 4.16/5) the willingness to not receive a newsletter was even higher in the control group (Mean: 4.78/5). For Ryanair to be better off by not collecting data through the implementation of the default subscription, the mean in the experimental group should have been higher than the mean in the control group. This also proved the default effect cognitive bias of people and its successful exploitation by companies through implementing dark patterns with pre-selected options that Marthur et al. (2019) already observed and described in their paper. The high means in both groups could also be interpreted as a general unpopularity of email newsletters among people or being a result of participants' personal interest while visiting the Ryanair website e.g. people only use the website because they want to find cheap flights occasionally, but don't want to receive any further information from Ryanair in particular.




| | EG | CG |
|---|---|---|
| Mean | 4.16 | 4.78 |
| SD | 1.21 | 0.45 |
| SE | 0.16 | 0.06 |

**Graph 4.** Would you opt out to receive the Ryan air newsletter?

**R3. Would you use the website again to book travel?**: The mean in the experimental group was 2.54 and the mean in the control group was 2.85 (2 = Probably yes, 3 = Might or might not).

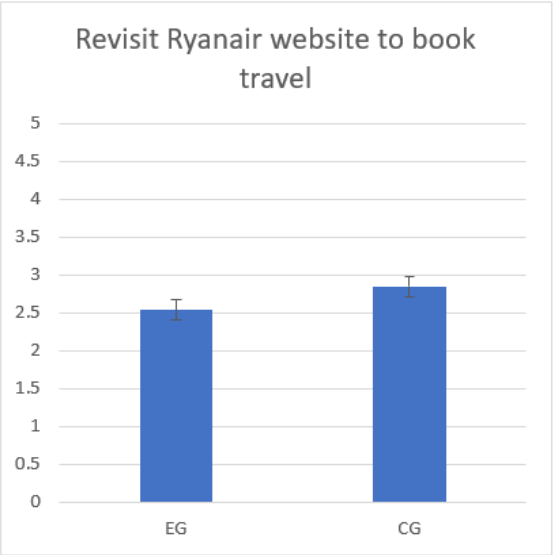
$$\mathbf{H_0(R3) = M1 - M2 = 0}$$

$$\mathbf{H_1(R3) = M1 - M2 \neq 0}$$

$$\mathbf{R3: 2.54 - 2.85 = -0.31 \neq 0,\ p > 0.05}$$

Participants in the experimental group were found to be slightly less determined to use the Ryanair website again to book travel than participants in the control group. The t-test did not prove this difference to be significant, and therefore the null hypothesis $H_0$(R2)

failed to be rejected. However, the tendency was again opposite to the expectations of the research, with the control group having a stronger tendency to not use the website again than the experimental group which encountered the dark pattern. A possible explanation for these results might be the nature of the website and the utility it carries for
the participants. As it's a popular website for cheap travel, many people might prioritize the utility it has for them, over their privacy concerns. Hence, even if they were upset about encountering a dark pattern on the Ryanair website, it was not enough to affect their usage of the website due to the benefits it carries for the users. As the difference between the groups was insignificant, the slightly higher result in the control group, might be a random fluctuation caused by e.g. the control group containing more determined Ryanair users than in the experimental group.




| | EG | CG |
|---|---|---|
| Mean | 2.54 | 2.85 |
| SD | 1.04 | 1.02 |
| SE | 0.14 | 0.13 |

**Graph 5.** Would you use the website again to book travel?

**R4. How upset would you be after being automatically subscribed to the Ryanair newsletter?**: The mean in the experimental group was 3.63 and in the control group 2.47 (1 = Not at all upset, 5 = Extremely upset).

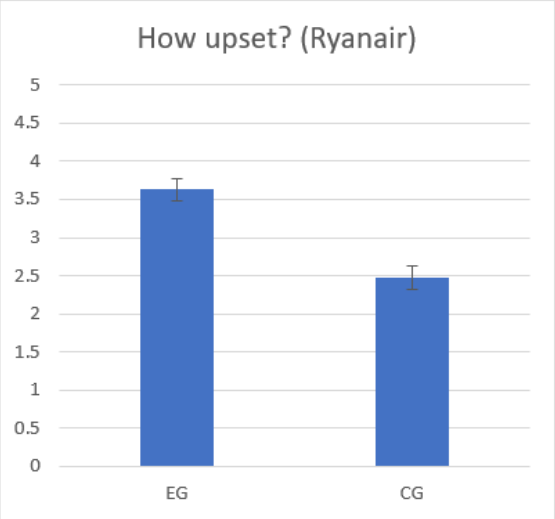
$$\mathbf{H_0(R4) = M1 - M2 = 0}$$

$$\mathbf{H_1(R4) = M1 - M2 \neq 0}$$

$$\mathbf{R4: 3.63 - 2.47 = 1.16 \neq 0,\ p < 0.05}$$

Participants in the experimental group were found to be significantly more upset by the default subscription than participants in the control group who were given the option to

opt-in for a subscription. Therefore, $H_0$(R4) was rejected, affirming users' discontent with dark patterns used to collect their personal information.




| | EG | CG |
|---|---|---|
| Mean | 3.63 | 2.47 |
| SD | 1.07 | 1.21 |
| SE | 0.14 | 0.16 |

**Graph 6.** How upset would you be after being automatically subscribed to the Ryanair newsletter?

**Interpretation of the results for Ryanair**: It must be concluded that Ryanair is very likely not facing a negative trade-off through its current data collection practices on its website. The results rather affirmed the effectiveness of the default subscription for the newsletter in the check-out process, as the high unpopularity of newsletters (R2) would leave fewer people to subscribe to the newsletter through an opt-in mechanism, and the dark pattern effectively increases the number of subscriptions by exploiting people's tendency to stick with default selections. Users' discontent with newsletters in general and the dark pattern in particular was not enough to result in negative consequences for the company. However, the results did allow some possible scenarios to be imagined in which Ryanair could face a negative trade-off. R1 showed a high belief of customers in the intentionality of the design, and R4 demonstrated that the dark pattern did create a higher level of discontent among participants than if they would have been given the choice of a subscription. As both groups pended between "probably yes" and "might or might not" concerning whether to use the website again (R3), in combination with R1 and R4, negative news about the company or the emergence of a competitor with equal services and less privacy invasive or more privacy protective designs could make customers switch from Ryanair to a competitor.

### 4.4.2. Scenario 2: Amazon

The participants were led through the process of closing one's Amazon account. It required a number of hidden and obscure actions to be taken in order to complete the account

closure. The control group was shown a scenario allowing them to close their account in a simple and direct procedure. The follow-up questions posed to the participants were: (A1) How intentional of Amazon do you think this process is?, (A2) Would you go through the process of closing your Amazon account, if you didn't need your account anymore?, (A3) Would you reopen an account knowing about the closing process?, (A4) How upset would you be after going through the process of closing your account?, and (A5) Would you avoid products or services offered by Amazon in the future?

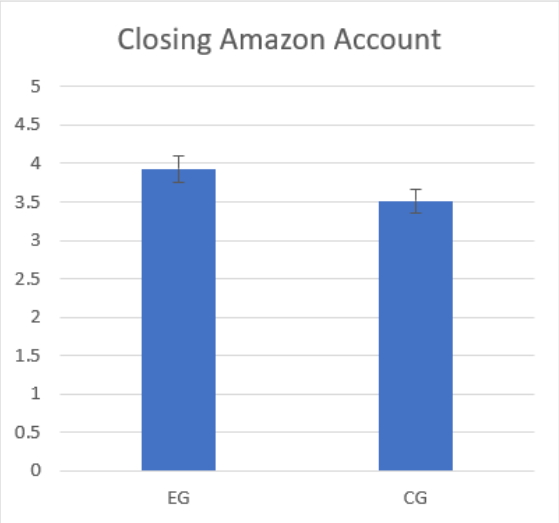
**A1. How intentional of Amazon do you think this process is?:** Similar to R1, participants strongly believed the procedure to be intended by Amazon with an even higher mean of 4.77/5 (4 = Probably intentional, 5 = Definitely intentional).

**A2. Would you go through the process of closing your Amazon account if you didn't need it anymore?:** The mean for the experimental group was 3.93 and the mean for the control group was 3.51 (3 = Might or might not, 4 = Probably yes)

$$\mathbf{H_0(A2): M1 - M2 = 0}$$

$$\mathbf{H_1(A2): M1 - M2 \neq 0}$$

$$\mathbf{A2: 3.93 - 3.51 = 0.42 \neq 0,\ p > 0.05}$$




| | EG | CG |
|---|---|---|
| Mean | 3.93 | 3.51 |
| SD | 1.28 | 1.16 |
| SE | 0.17 | 0.15 |

**Graph 7.** Would you go through the process of closing your Amazon account?

The results showed that people in the experimental group had a tendency to be more likely to close their Amazon account if they didn't need it anymore compared to participants in the control group, but the student's t-test only had a marginal significance of $p < 0.1$ (for the one-tailed t-test it was $p < 0.05$). Hence, we failed to reject the null hypothesis $H_0$(A2) as there was no significant difference between people who faced a simpler and more obvious

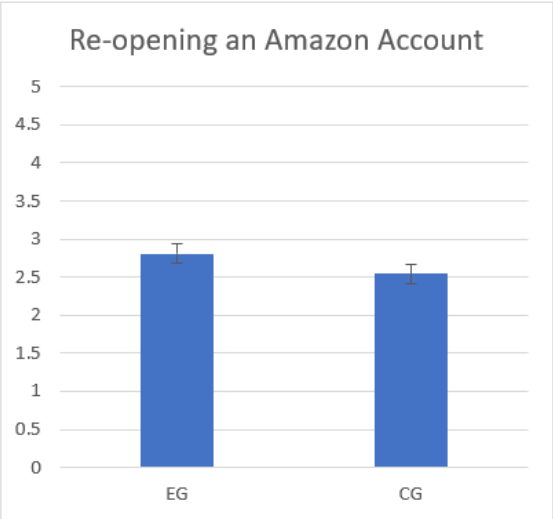
way to close their account and the participants who experienced the dark pattern. However, the marginal significance allowed some speculation on the implemented dark pattern by Amazon. Future experiments that avoid the limitations of this study and create more realistic scenarios might be able to find significant results. Following the tendency, the design seemed to have a negative effect on the participants' perception of the website, and determined participants in the experimental group slightly more to close their account, than participants in the control group. An interesting aspect to be considered in this result is that participants might have only learned about the complexity of the closing process through participating in this survey, and were not aware of it before. A different result might have been obtained if participants had been asked if they would consider closing their Amazon account in general, without knowing about the nature of the closing process.

**A3. Would you reopen an account knowing about the closing process?:** The mean in the experimental group was 2.81 and in the control group 2.54 (2 = Probably yes, 3 = Might or might not).

**$H_0$(A3): M1 - M2 = 0**

**$H_1$(A3): M1 - M2 ≠ 0**

**A3: 2.81 - 2.54 = 0.27 ≠ 0, p > 0.05**




| | EG | CG |
|---|---|---|
| Mean | 2.81 | 2.54 |
| SD | 1.00 | 1.03 |
| SE | 0.13 | 0.13 |

**Graph 8.** Would you reopen an account knowing about the closing process?

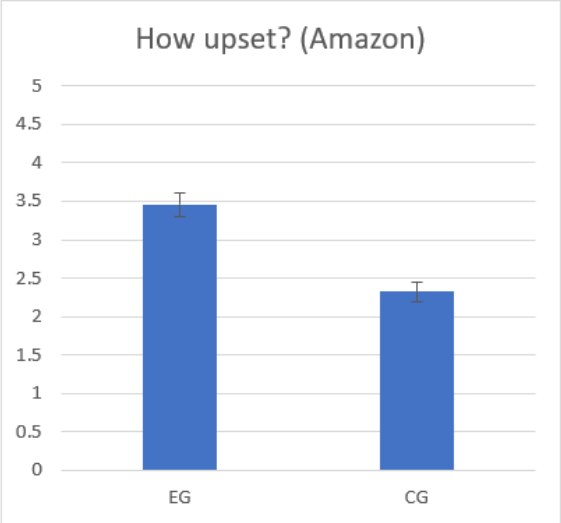
There was no statistically significant difference between participants in the experimental and the control group and therefore we failed to reject the null hypothesis $H_0$(A3). However, there was a slight tendency in this sample for participants that experienced the dark pattern to be more sceptical about reopening an account.

**A4. How upset would you be after going through the process of closing your account?:** The mean in the experimental group was 3.46 and in the control group 2.32 (1 = Not at all upset, 5 = Extremely upset).

**$H_0$(A4): M1 - M2 = 0**

**$H_1$(A4): M1 - M2 ≠ 0**

**A4: 3.46 - 2.32 = 1.14 ≠ 0, p < 0.05**




| | EG | CG |
|---|---|---|
| Mean | 3.46 | 2.32 |
| SD | 1.19 | 1.00 |
| SE | 0.16 | 0.13 |

**Graph 9.** How upset would you be after going through the process of closing your account?

The results indicate that the *hard to cancel* dark pattern did have a significant negative impact on participants' emotions, compared to participants facing a much simpler process to cancel one's account. The t-test indicated a rejection of the null-hypothesis $H_0$(A4).

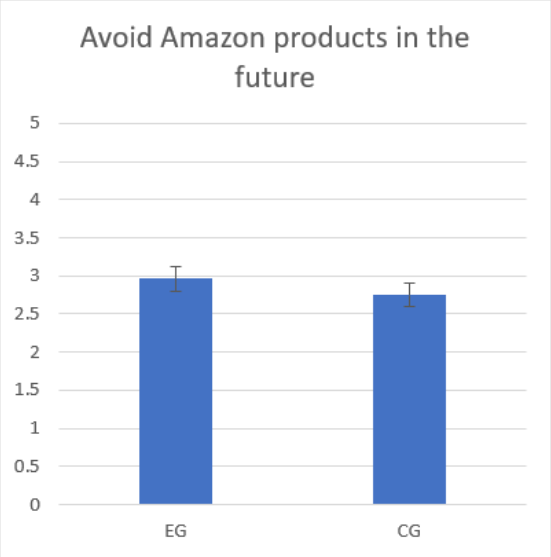
**A5. Would you avoid products or services offered by Amazon in the future?:** The mean in the experimental group was 2.96 and in the control group 2.75 (2 = Probably not, 3 = Might or might not).

**$H_0$(A5): M1 - M2 = 0**

**$H_1$(A5): M1 - M2 ≠ 0**

**A3: 2.96 - 2.75 = 0.21 ≠ 0, p > 0.05**

Both groups averaged between "Probably not" and "Might or Might not", with a tendency towards the latter, especially in the experimental group. The t-test did not prove this difference to be significant and hence we failed to reject the null hypothesis $H_0$(A5).




| | EG | CG |
|---|---|---|
| Mean | 2.96 | 2.75 |
| SD | 1.20 | 1.23 |
| SE | 0.16 | 0.16 |

**Graph 10.** Would you avoid products or services offered by Amazon in the future?

**Interpretation of the results for Amazon:** Even though Amazon is making it harder for customers to close their accounts, making them more reluctant to the closure if they fail in the process and eventually resulting in the accounts staying active, the company does not seem to face a negative trade-off therethrough. Similar to the Ryanair example, the utility and convenience Amazon brings to its users trumps the negative impacts of such practices by the company indicated by the investigations on whether users would re-open an account (A3) or avoid Amazon products/services in the future (A5). However, also in this example, some interesting scenarios could be laid out. Since the four comparisons (A2-A5) all showed a slight tendency in the experimental group towards less confidence in their engagement with the website, being a more negative impact for the company, the significant results in A2 (Closing the account) and A4 (Upsetness) did allow some speculation. In A2, more people in the experimental group were determined to close their account after having gone through the dark pattern. Under the assumption that the clearly negative experience of the dark pattern (A4) enhanced the participants' determination to close their account, Amazon could potentially face a more negative impact through its practice, if internet users increasingly learn and become aware of dark patterns online as propagated by Brignull (2013) and Bösch et al. (2016). Additionally, it could be argued that none of the means indicated a "blind following" of Amazon by consumers. Concerning reopening an account, the mean was between "probably yes" and "might or might not". Concerning closing the account, the mean was between "might or might not" and "probably yes" (tendency towards the latter) and concerning avoiding products in the future it was between "probably no" and

"might or might not" (tendency towards the latter). None of the means indicated a "definite" adherence to the company's services, showing that consumers reserve themselves open for other services and products depending on the circumstances. The high level of discontent of users with Amazon's dark pattern (A4) could cause a negative trade-off for the company in combination with negative news about its reputation, the emergence of competitors with a more transparent and fairer website design and/or increasing awareness of dark patterns among consumers.

#### 4.4.3. Scenario 3, CNN:

The participants in the experimental group were shown the pop-up cookie banner on the CNN website, and were led through the long and complex process required to opt out from all cookies. The control group saw the same banner, but containing a "Decline All" button to turn off all cookies. The follow-up questions asked to the participants were: (1) How intentional of CNN do you think this process is?, (2) Would you go through the process of selecting cookie preferences?[20], (3) Would you use the website again to read news?, and (4) How upset would you be after selecting the cookie preferences?

**C1. How intentional of CNN do you think this process is?:** As already observed in the Ryanair and Amazon example, also the CNN website was widely believed to have intentionally implemented the design for cookie preferences with a mean of 4.6/5 (4 = Probably intentional, 5 = Definitely intentional).

**C2. Would you go through the process of selecting cookie preferences?:** The mean in the experimental group was 2.63 and in the control group 4.15 (2 = Probably not, 3 = Might or might not, 4 = Probably yes).

$$\mathbf{H_0(C2): M1 - M2 = 0}$$

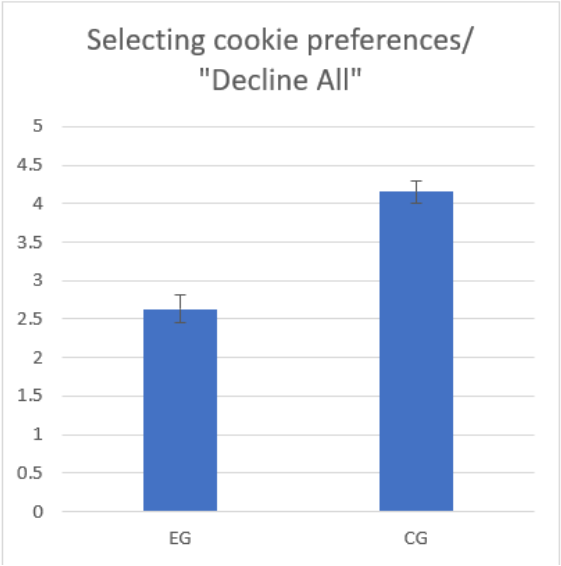
$$\mathbf{H_1(C2): M1 - M2 \neq 0}$$

$$\mathbf{C2: 2.63 - 4.15 = -1.52 \neq 0, p < 0.05}$$

The control group was found to be significantly more likely to turn-off all cookies, since it required them only one click, compared to the 16 hidden and obscure clicks in the experimental group. Similar to R2, the null hypothesis $H_0$(C2) was rejected demonstrating the effectiveness of dark patterns. Also there, the dark pattern exploits the default effect cognitive bias in making users reluctant to go through the process of turning off all cookies individually and accepting the default setting, allowing the website many tracing

[20] For the control group adjusted to: Would you select "Decline All" to turn off all the non-essential cookies?

opportunities. Another inference that can be made from this result is that many people do not want cookies to be turned on by default but would prefer to have them switched off. This is indicated by the mean of the control group 4.16 (4 = Probably yes) asking participants whether they would choose the “Decline All” option. Since many cookies aim at tracing users behaviour online, this could be seen as an affirmation of the widespread privacy concerns and the desire of many to not be traced online.




| | EG | CG |
|---|---|---|
| Mean | 2.63 | 4.15 |
| SD | 1.33 | 1.05 |
| SE | 0.18 | 0.14 |

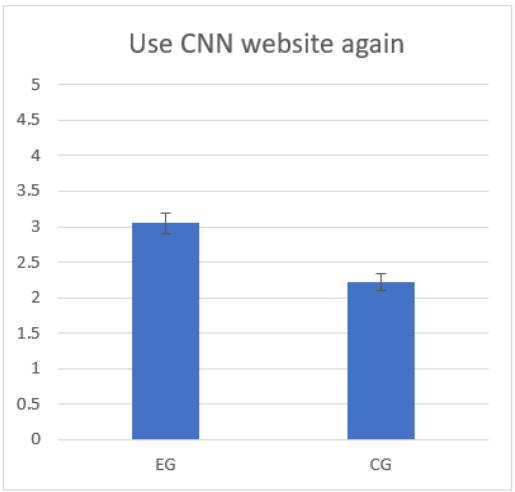
**Graph 11.** Would you go through the process of selecting cookie preferences?

**C3. Would you use the website again to read news?:** The mean in the experimental group was 3.05 and in the control group 2.22 (2 = Probably yes, 3 = Might or might not).

**$H_0$(C3): M1 - M2 = 0**

**$H_1$(C3): M1 - M2 ≠ 0**

**C3: 3.05 - 2.22 = 0.83 ≠ 0, p < 0.05**




| | EG | CG |
|---|---|---|
| Mean | 3.05 | 2.22 |
| SD | 1.10 | 0.92 |
| SE | 0.15 | 0.12 |

**Graph 12.** Would you use the website again to read news?

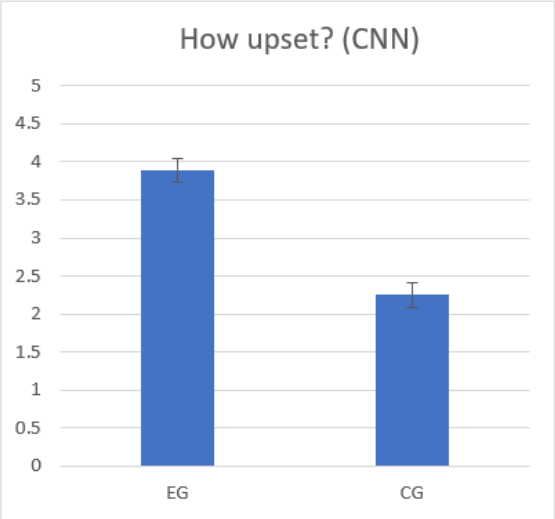
The null-hypothesis $H_0$(C3) was rejected. The participants in the experimental group were found to be significantly less determined to use the CNN website again after having faced the cookie selection process, compared to participants in the control group who could easily opt out from all cookies and hence showed a higher probability of using the website again.

**C4. How upset would you be after selecting the cookie preferences?:** The experimental group had a mean of 3.89 and the mean in the control group was 2.25 (1 = Not at all upset, 5 = Extremely upset).

$$\mathbf{H_0(C4): M1 - M2 = 0}$$

$$\mathbf{H_1(C4): M1 - M2 \neq 0}$$

$$\mathbf{C4: 3.89 - 2.25 = 1.64 \neq 0,\ p < 0.05}$$




| | EG | CG |
|---|---|---|
| Mean | 3.89 | 2.25 |
| SD | 1.10 | 1.23 |
| SE | 0.15 | 0.16 |

**Graph 13.** How upset would you be after selecting the cookie preferences?

Participants in the experimental group were significantly more upset by the cookie selection process than participants in the control group. The t-test allowed a rejection of the null hypothesis $H_0$(C4).

**Interpretation of the results for CNN:** All findings in the CNN scenario were significant and showed the website is facing a potential trade-off with its cookie selection mechanism. C2 demonstrated the general unpopularity of cookies among internet users with similar results being found by a recent analysis of the new opt-in function on iOS 14.5.[21] The update required apps to ask their users for permission to track them across apps and

[21] "Analytics Suggest 96% of Users Leave App Tracking Disabled in IOS 14.5." n.d. MacRumors. https://www.macrumors.com/2021/05/07/most-iphone-users-app-tracking-opt-out/.

websites through accessing the device's random advertising identifier. Only 4% of iPhone users in the US chose to activate the tracking meaning that 96% chose to keep the tracing off. C3 showed that the dark pattern implemented on the CNN website did have significant negative effects on the users' willingness to use the website again, as compared to a higher confidence of revisiting the website among users that received a simple mechanism to select their cookie preferences. It also made users significantly more upset than people in the control group (C4). Once again, it showed people's discontent with dark patterns if they become aware of them. It is probable that CNN loses some visitors on its website through the prominence of its design, but vice versa it can be shown that the provision of a simple and understandable choice mechanism for the selection of cookie preferences rather has a positive impact on the users' perception and relationship with the website, and creates confidence in visiting it again for its services. This could be an even more important learning from this study, since many of the other effects are more ambiguous and difficult to determine. A further aspect to explore would be the different nature of each website. Ryanair and Amazon offer products and services that customers can purchase and for which the customers specifically visit the websites. On the contrary, CNN does not sell anything, but offers its users to read news for free (no monetary compensation) and hence might be easier to substitute for the users. For such websites, the findings in scenario 3 might be of particular interest and help them create better relationships with more loyal customers.

**Correlation between the experimental group and IPC:**

| | | *COL* | *SEC* | *ERR* | *IMP* | *CON* | *AWA* | *TRU* | *RIS* |
|---|---|---|---|---|---|---|---|---|---|
| Ryanair | Intentionality | -0.10 | -0.02 | -0.29 | 0.00 | 0.01 | -0.06 | 0.31 | -0.17 |
| | Opt-out | 0.07 | 0.11 | -0.25 | -0.05 | -0.01 | -0.05 | 0.17 | 0.12 |
| | Use website again | 0.12 | 0.03 | 0.13 | 0.14 | -0.01 | 0.13 | 0.00 | 0.30 |
| | Upset | 0.35 | 0.31 | 0.08 | 0.17 | 0.34 | 0.41 | 0.27 | 0.34 |
| Amazon | Intentionality | -0.09 | -0.12 | -0.27 | -0.14 | -0.04 | -0.09 | 0.26 | -0.21 |
| | Close account | 0.07 | 0.23 | -0.03 | 0.19 | 0.18 | 0.19 | -0.07 | 0.05 |
| | Reopen account | 0.27 | 0.14 | 0.13 | 0.17 | 0.24 | 0.29 | 0.12 | 0.18 |
| | Upset | 0.38 | 0.35 | 0.06 | 0.13 | 0.25 | 0.21 | 0.28 | 0.22 |
| | Avoid products/ services | 0.28 | 0.22 | 0.21 | 0.20 | 0.22 | 0.10 | 0.10 | 0.13 |
| CNN | Intentionality | 0.10 | 0.29 | 0.15 | 0.50 | 0.13 | 0.19 | 0.16 | 0.27 |
| | Select cookies | 0.28 | 0.25 | 0.09 | 0.13 | 0.22 | 0.28 | 0.19 | 0.21 |
| | Use website again | 0.17 | 0.08 | 0.09 | 0.17 | 0.20 | 0.17 | 0.17 | 0.26 |
| | Upset | 0.23 | 0.34 | 0.15 | 0.38 | 0.26 | 0.23 | 0.41 | 0.34 |

**Table 4.** Correlations between IPC and experimental group

The question asking participants how upset they were about the respective dark patterns showed the most correlations with IPC categories for each website scenario. In the Ryanair example, participants with higher concerns in *collection* (r = 0.35), *secondary usage* (r = 0.31), *control* (r = 0.34), *risk beliefs* (r = 0.34) and even more in *awareness* (r = 0.41) showed a higher level of discontent with the default subscription to the Ryanair newsletter. For the Amazon dark pattern, participants with higher *collection* (r = 0.38) and *secondary usage* (r = 0.35) concerns were more upset about the closing procedure of the account. Similarly, in the CNN example slightly significant correlations existed between higher concerns in *secondary usage* (r = 0.34), *improper access* (r = 0.38), *risk beliefs* (r = 0.34) and slightly higher with low *trust beliefs* (r = 0.41). Low trust levels also slightly correlated with the belief of participants that Ryanair intended the default newsletter subscription on their website (r = 0.31). Also, higher *risk beliefs* were slightly correlated to participants being less likely to use the Ryanair website again (r = 0.3). The strongest correlation was detected between the IPC category *improper access* and the intentionality of the cookie selection process on the CNN websites (r = 0.5).

**Correlation between the control group and IPC:**

| | | COL | SEC | ERR | IMP | CON | AWA | TRU | RIS |
|---|---|---|---|---|---|---|---|---|---|
| Ryanair | Opt-out | 0.13 | 0.17 | 0.00 | 0.12 | 0.12 | 0.04 | 0.20 | 0.03 |
| | Use website again | 0.08 | 0.19 | 0.26 | 0.32 | 0.14 | 0.19 | -0.08 | 0.21 |
| | Upset | 0.23 | 0.14 | 0.30 | 0.41 | 0.23 | 0.22 | -0.09 | 0.36 |
| Amazon | Close account | 0.30 | 0.29 | 0.04 | 0.26 | 0.35 | 0.39 | 0.19 | 0.35 |
| | Reopen account | 0.12 | 0.10 | -0.11 | -0.10 | 0.00 | -0.08 | 0.26 | -0.03 |
| | Upset | 0.06 | 0.12 | 0.08 | 0.09 | 0.12 | 0.08 | 0.22 | 0.09 |
| | Avoid products/ services | 0.23 | 0.29 | 0.08 | 0.11 | 0.26 | 0.18 | 0.35 | 0.18 |
| CNN | Decline All | 0.34 | 0.40 | 0.08 | 0.31 | 0.32 | 0.35 | 0.29 | 0.27 |
| | Use website again | 0.06 | 0.01 | 0.05 | 0.03 | 0.15 | 0.15 | -0.09 | 0.14 |
| | Upset | 0.20 | 0.15 | 0.14 | 0.15 | 0.19 | 0.19 | -0.18 | 0.28 |

**Table 5.** Correlations between control group and IPC

In the control group, the question in the CNN scenario whether participants would chose to “Decline All” cookies with one click correlated with IPC in the categories *collection* (r = 0.34), *secondary usage* (r =0.4), *improper access* (r = 0.31), *control* (r = 0.32), and *awareness* (r = 0.35). It could be expected that people with higher privacy concerns would choose the one-click option to opt-out. Similarly, it was to be expected that people would close their Amazon account if the process was simpler and more transparent. This question

correlated with *collection* (r = 0.3), *control* (r = 0.35), *awareness* (r = 0.39), and *risk beliefs* (r = 0.35). Interestingly, some IPC categories, *errors* (r = 0.3), *improper access* (r = 0.41) and *risk beliefs* (r = 0.36) , correlated with higher discontent about the Ryanair newsletter, which in the control group was an opt-in (privacy protective) option. This could be a proof of the general aversion people have to newsletters, hence they don't even want newsletters to be offered to them at all. Other two slight correlations were between *improper access* and using the Ryanair website again (r = 0.32), and low *trust levels* and avoiding Amazon products or services in the future (r = 0.35). Since, there was no dark pattern that upset the participants largely, these might be general critics to the two platforms some people in the control group had.

# 5. Conclusion and outlook

## 5.1. Limitations to approach

The survey and the experiment had some limitations that could be further adjusted for future projects. Many of the IPC statements were perceived as similar or repetitive by many participants and some as too technically sophisticated which might have impacted participants' attention and concentration to answer each individual statement. Furthermore, the website scenarios in the experiment were hypothetical instead of consisting in real engagement of the participants with the website. The scenarios aimed at invoking familiar experiences in the participants, but thereby also posed the risk of not catching the participants' actual emotions, beliefs and behavior for the concerning situations. The results must therefore be understood as directions to interpret rather than representative behavior and attitudes of a population. Since the survey was mainly answered by young people and university students from several countries being disproportionately represented it did not draw a complete picture of one specific population. Lastly, since the survey was answered by many non-native English speakers, the English skills of some participants might have caused them problems in understanding some questions.

## 5.2. Directions

As this study and previous research has shown, there are considerable privacy concerns in the population, especially among young people, about their personal information being collected by online service providers. Alongside the emergence of the internet and

online technology in societies all around the world, the interest in the concept of privacy and privacy concerns received growing attention and produced a large amount of literature and research on the topics. This led to an increasing privacy-awareness among internet users to date and the continuous creation of several entities serving as watchdogs on privacy related issues. What has been once again confirmed by this study is the ongoing existence of the privacy paradox, as people still don't act according to their privacy concerns with adequate protection of their privacy by e.g. making use of privacy enhancing technologies (PETs). This study aimed to go a step beyond and contribute to further exploring whether online service providers face trade-offs through unfair data collection practices and the potential benefits for companies and online service providers in addressing the privacy concerns of their users adequately. It was demonstrated that companies with a unique service or product (Amazon and Ryanair) have a stronger and more loyal customer base and do not face a trade-off since they are less likely to be affected by negatively perceived data collection practices. In their case, customers prioritize the service or product over their privacy concerns. However, it must be noted that people did not blindly follow the companies but showed a potential willingness to switch providers. On the contrary, online service providers that did not offer a unique service (e.g. news broadcaster CNN) were negatively affected by their unfair website design for data collection purposes. Users that encountered the dark pattern on the pop-up window were less likely to return to the website compared to users that saw a simple-to-understand pop-up window. Thereby, the CNN website did face a trade-off in trying to collect the data of website visitors but scaring them away once they learned how the website tried to get hold of their data. CNN would have been likely better off by implementing a privacy design strategy, which proved to build a better relationship between the customer and the website by increasing their willingness to return to the website in this experiment. This finding becomes interesting in combination with research such as Acquisti, Taylor and Wagman (2015) who presented multiple examples that the often proclaimed goal by websites of targeted advertisement to improve customer experience is not optimal nor desired in many situations, neither for the websites nor for consumers. Since the selling of data is an important source of profits for many websites, some, such as CNN, might be better off to build good relationships through transparent practices and privacy design strategies, and find other strategies to profit from their more loyal customer base. As the research and literature on the potential benefits for companies and institutions of privacy design or

"privacy-by-design" strategies has yet to expand, also some recent examples from the tech world hint towards an unexploited potential. At the beginning of 2021, the messenger service WhatsApp announced new privacy policies, which according to the company would not change anything for private communications, but only for communications between businesses and their customers. However, this news created a major backlash for the company, potentially enhanced by previous negative privacy news and mistrust against the mother-company Facebook, and led the company not only to delay and revise the privacy policy update, but also made millions of WhatsApp users download competitive messenger services known for stronger privacy protection, e.g. Signal and Telegram (both achieved record downloads following the incident) with many of the users entirely abandoning WhatsApp and switching providers. Also Apple is known to distinguish itself from competitors in the big tech industry by advocating for strict privacy regulation and claiming to build privacy protective products itself. Although, it is debated how much better Apple actually is in terms of real privacy protection and to what extent the company's success can be attributed to its stands on privacy, the company has managed to shift market dynamics on the topic and trigger debates about privacy with big magnitude several times, e.g. with its announcement of the new iOS 14.5 in 2021, showing again how already the perception of a brand being more privacy protective can have a positive impact. However debated the reality may be, in fact many companies do rely on the brand for security and privacy reasons by e.g. only allowing iPhones as work phones. In general, the discussion on online privacy has grown and found a spot alongside the most relevant topics to be addressed in the coming decades. Although not elaborated in this paper, it has also vastly enlarged the amount of proposals for alternative business models based on privacy protection rather than the maximization of collecting users personal information, new responsibilities companies carry in the digital age, potential new legal rights for internet users and new perspectives on the ways we want to organize and structure the relationships between tech companies, the people and governments. Among all the uncertainties and research gaps to be filled in this topic, one thing is certain: the discussion around privacy and its issues has come to stay. Although this study had several limitations in its execution, it did deliver some interesting findings, especially regarding the fact that young people are the main actors and users of the internet. The growing interest and awareness of privacy concerns and problems with privacy, such as dark patterns, is likely to increase in the coming years. The future outlook and advice

following this investigation, must be that companies should not overhear and miss out on the privacy debate if they want to keep and enlarge their customer base and eventually stay competitive. Although a lot more research is needed in the field in order to fully understand the potential benefits companies and platforms can harvest from implementing strong privacy protection, privacy and its protection are likely to become highly cherished values in the increasingly digital society and following Joseph Schumpeter's principle of *creative destruction*, might soon make the difference in which companies consumers place their trust and hence for the companies' economic success.

## Bibliography/ References:


1) "Analytics Suggest 96% of Users Leave App Tracking Disabled in IOS 14.5." n.d. MacRumors.https://www.macrumors.com/2021/05/07/most-iphone-users-app-tracking-opt-out

2) "Cisco Study Reveals Critical Role of Privacy Emerging from Global Pandemic." n.d. Newsroom.cisco.com. https://newsroom.cisco.com/press-release-content?articleId=2139315.

3) "Digital Society Index 2019: Human Needs in a Digital World." n.d. Oxford Economics. https://www.oxfordeconomics.com/recent-releases/digital-society-index-2019-human-needs-in-a-digital-world

4) Acquisti, Alessandro, and Ralph Gross. "Predicting social security numbers from public data." *Proceedings of the National academy of sciences* 106, no. 27 (2009): 10975-10980.

5) Acquisti, Alessandro, Curtis R. Taylor, and Liad Wagman. 2015. "The Economics of Privacy." *SSRN Electronic Journal*.

6) Almuhimedi, Hazim, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, Lorrie Faith Cranor, and Yuvraj Agarwal. "Your location has been shared 5,398 times! A field study on mobile app privacy nudging." In *Proceedings of the 33rd annual ACM conference on human factors in computing systems*, pp. 787-796. 2015.

7) Altman, Irwin. "The environment and social behavior: privacy, personal space, territory, and crowding." (1975).

8) Anant, V., L. Donchak, J. Kaplan, and H. Soller. "The consumer-data opportunity and the privacy imperative." *McKinsey and Company. Retrieved July* 16 (2020): 2020.

9) Anderson, Eric T., and Duncan I. Simester. "Price stickiness and customer antagonism." *The quarterly journal of economics* 125, no. 2 (2010): 729-765.

10) Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar, and Erica Turner. 2019. "Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information." Pew Research Center: Internet, Science & Tech. November 15, 2019. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

11) Ayenson, Mika D., Dietrich James Wambach, Ashkan Soltani, Nathan Good, and Chris Jay Hoofnagle. "Flash cookies and privacy II: Now with HTML5 and ETag respawning." *Available at SSRN 1898390* (2011).

12) Bergemann, Dirk, and Alessandro Bonatti. "Selling cookies." *American Economic Journal: Microeconomics* 7, no. 3 (2015): 259-94.

13) Bösch, Christoph, Benjamin Erb, Frank Kargl, Henning Kopp, and Stefan Pfattheicher. 2016. "Tales from the Dark Side: Privacy Dark Strategies and Privacy dark patterns." *Proceedings on Privacy Enhancing Technologies* 2016 (4): 237–54.

14) Brignull, Harry. 2013. "dark patterns: Inside the Interfaces Designed to Trick You." The Verge. August 29, 2013. https://www.theverge.com/2013/8/29/4640308/dark-patterns-inside-the-interfaces-designed-to-trick-you#:~:text=A%20dark%20pattern%20is%20a.

15) Brown, Mark, and Rose Muchira. "Investigating the relationship between Internet privacy concerns and online purchase behavior." *Journal of Electronic Commerce Research* 5, no. 1 (2004): 62-70.

16) Calo, Ryan. "Against notice skepticism in privacy (and elsewhere)." *Notre Dame L. Rev.* 87 (2011): 1027.

*17) Campbell, Alexandra J. "Relationship marketing in consumer markets: A comparison of managerial and consumer attitudes about information privacy." Journal of Direct Marketing 11, no. 3 (1997): 44-57.*

18) Campbell, James, Avi Goldfarb, and Catherine Tucker. "Privacy regulation and market structure." *Journal of Economics & Management Strategy* 24, no. 1 (2015): 47-73.

19) *Changi Nam, Chanhoo Song, and Euehun Lee,Chan Ik Park (2006) ,"Consumers' Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online", in NA - Advances in Consumer Research Volume 33, eds. Connie Pechmann and Linda Price, Duluth, MN : Association for Consumer Research, Pages: 212-217.*

20) Chivukula, Shruthi Sai, Chris Watkins, Lucca McKay, and Colin M. Gray. "" Nothing Comes Before Profit" Asshole Design In the Wild." In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1-6. 2019.

21) Choi, Jay Pil, Doh-Shin Jeon, and Byung-Cheol Kim. 2019. "Privacy and Personal Data Collection with Information Externalities." *Journal of Public Economics* 173 (May): 113–24.

22) Cialdini, Robert B., and Noah J. Goldstein. 2004. "Social Influence: Compliance and Conformity." *Annual Review of Psychology* 55 (1): 591–621.

23) Culnan, Mary J. 1993. "'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes toward Secondary Information Use." *MIS Quarterly* 17 (3): 341.

24) Culnan, Mary J., and Cynthia Clark Williams. "How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches." *Mis Quarterly* (2009): 673-687.

*25) Culnan, Mary J., and Pamela K. Armstrong. "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation." Organization science 10, no. 1 (1999): 104-115.*

26) Culnan, Mary J., and Robert J. Bies. "Consumer privacy: Balancing economic and justice considerations." *Journal of social issues* 59, no. 2 (2003): 323-342.

27) De Corniere, Alexandre, and Romain De Nijs. "Online advertising and privacy." The RAND Journal of Economics 47, no. 1 (2016): 48-72.

28) Donaldson, Thomas, and Thomas W. Dunfee. "Toward a unified conception of business ethics: Integrative social contracts theory." *Academy of management review* 19, no. 2 (1994): 252-284.

29) Draper, Nora A, and Joseph Turow. 2019. "The Corporate Cultivation of Digital Resignation." New Media & Society 21 (8): 1824–39.

30) Dugas, Andrea F., Mehdi Jalalpour, Yulia Gel, Scott Levin, Fred Torcaso, Takeru Igusa, and Richard Rothman. 2013. "Influenza Forecasting with Google Flu Trends." *Online Journal of Public Health Informatics* 5 (1).

31) E. Tory Higgins. 2011. *Beyond Pleasure and Pain : How Motivation Works*. Oxford University Press -10-11.

32) Ferdinand David Schoeman. 1992. *Privacy and Social Freedom*. Cambridge University Press.

33) Finn Brunton, and Helen Nissenbaum. 2016. *Obfuscation : A User's Guide for Privacy and Protest*. Mit Press.

*34) Garber, Joe. 2018. "GDPR – Compliance Nightmare or Business Opportunity?" Computer Fraud & Security 2018 (6): 14–15.*

35) Harry Brignull, Marc Miquel, Jeremy Rosenberg, and James Offer. 2015. dark patterns - User Interfaces Designed to Trick People. http://darkpatterns.org/

36) Hartzog, Woodrow. "Reviving Implied Confidentiality." *Ind. LJ* 89 (2014): 763.

37) Hern, Alex. 2021. "WhatsApp Loses Millions of Users after Terms Update." The Guardian. January 24, 2021. https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update

38) Hoepman, Jaap-Henk. "Privacy design strategies." In *IFIP International Information Security Conference*, pp. 446-459. Springer, Berlin, Heidelberg, 2014.

*39) Hoffman, David. 2014. "Privacy Is a Business Opportunity." Harvard Business Review. April 18, 2014. https://hbr.org/2014/04/privacy-is-a-business-opportunity*

40) Hoffmann, Florian, Roman Inderst, and Marco Ottaviani. "Persuasion through selective disclosure: implications for marketing, campaigning, and privacy regulation." *Management Science* 66, no. 11 (2020): 4958-4979.

*41) Holmes, Allan. 2006. "The Profits in Customer Privacy." CIO. March 15, 2006. https://www.cio.com/article/2447333/the-profits-in-customer-privacy.html.*

42) Hong, Weiyin, and James Y. L. Thong. 2013. "Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies." *MIS Quarterly* 37 (1): 275–98.

43) Jernigan, Carter, and Behram F.T. Mistree. 2009. “Gaydar: Facebook Friendships Expose Sexual Orientation.” *First Monday* 14 (10).

44) Loewenstein, George, and Drazen Prelec. 1992. “Anomalies in Intertemporal Choice: Evidence and an Interpretation.” *The Quarterly Journal of Economics* 107 (2): 573–97.

45) Luguri, Jamie, and Lior Strahilevitz. 2019. “Shining a Light on dark patterns.” *SSRN Electronic Journal*.

46) Malhotra, Naresh K., Sung S. Kim, and James Agarwal. 2004. “Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model.” *Information Systems Research* 15 (4): 336–55.

47) Martin, Kirsten E. "Transaction costs, privacy, and trust: The laudable goals and ultimate failure of notice and choice to respect privacy online." *First Monday* 18, no. 12-2 (2013).

48) Martin, Kirsten. "Data aggregators, consumer data, and responsibility online: Who is tracking consumers online and should they stop?." *The Information Society* 32, no. 1 (2016): 51-63.

49) Mathur, Arunesh, Gunes Acar, Michael J. Friedman, Elena Lucherini, Jonathan Mayer, Marshini Chetty, and Arvind Narayanan. 2019. “dark patterns at Scale.” *Proceedings of the ACM on Human-Computer Interaction* 3 (CSCW): 1–32.

50) McDonald, Aleecia M., and Lorrie Faith Cranor. "The cost of reading privacy policies." Isjlp 4 (2008): 543.

51) McGee Patrick. 2021. “Apple Takes on the Internet: The Big Tech Battle over Privacy.” The Straits Times. May 4, 2021. https://www.straitstimes.com/opinion/apple-takes-on-the-internet-the-big-tech-battle-over-privacy.

52) Milberg, Sandra J., H. Jeff Smith, and Sandra J. Burke. "Information privacy: Corporate management and national regulation." *Organization science* 11, no. 1 (2000): 35-57.

53) Mischel, Walter, Ebbe B. Ebbesen, and Antonette Raskoff Zeiss. 1972. “Cognitive and Attentional Mechanisms in Delay of Gratification.” *Journal of Personality and Social Psychology* 21 (2): 204–18.

54) Nissenbaum, Helen. "A contextual approach to privacy online." *Daedalus* 140, no. 4 (2011): 32-48.

55) Nissenbaum, Helen. "Privacy as contextual integrity." *Wash. L. Rev.* 79 (2004): 119

56) NORBERG, PATRICIA A., DANIEL R. HORNE, and DAVID A. HORNE. 2007. “The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors.” *Journal of Consumer Affairs* 41 (1): 100–126.

*57) Phelps, Joseph, Glen Nowak, and Elizabeth Ferrell. 2000. “Privacy Concerns and Consumer Willingness to Provide Personal Information.” Journal of Public Policy & Marketing 19 (1): 27–41. https://doi.org/10.1509/jppm.19.1.27.16941.*

58) Shilton, Katie, and Kirsten E. Martin. "Mobile privacy expectations in context." TPRC, 2013.

59) Singleton, Solveig M., and James Harper. 2002. “With a Grain of Salt: What Consumer Privacy Surveys Don’t Tell Us.” *SSRN Electronic Journal*.

60) Solove, Daniel J. "Five myths about privacy." *The Washington Post* (2013).

61) Solove, Daniel J. "I've got nothing to hide and other misunderstandings of privacy." *San Diego L. Rev.* 44 (2007): 745.

62) Son, and Kim. 2008. “Internet Users’ Information Privacy-Protective Responses: A Taxonomy and a Nomological Model.” *MIS Quarterly* 32 (3): 503.

63) Steinbart, Paul, Mark Keith, and Jeffry Babb. 2017. “Measuring Privacy Concern and the Right to Be Forgotten.” *Proceedings of the 50th Hawaii International Conference on System Sciences (2017)*.

64) Tene, Omer, and Jules Polonetsky. "Big data for all: Privacy and user control in the age of analytics." *Nw. J. Tech. & Intell. Prop.* 11 (2012): xxvii.

65) Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti. "The effect of online privacy information on purchasing behavior: An experimental study." *Information systems research* 22, no. 2 (2011): 254-268.

*66) Tucker, Catherine E. "Social networks, personalized advertising, and privacy controls." Journal of marketing research 51, no. 5 (2014): 546-562.*

67) Wang, Huaiqing, Matthew KO Lee, and Chen Wang. "Consumer privacy concerns about Internet marketing." *Communications of the ACM* 41, no. 3 (1998): 63-70.

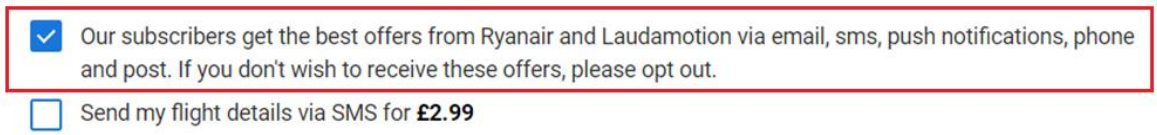
68) Warren, Samuel D., and Louis D. Brandeis. 1890. “The Right to Privacy.” *Harvard Law Review* 4 (5): 193–220.

69) Westin, Alan F. 1967. *Privacy and Freedom*. New York Atheneum.

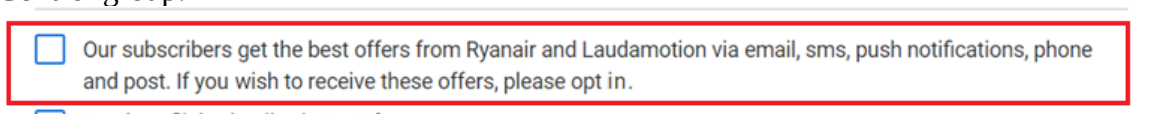
70) Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Publicaffairs.

## Appendix 1 - Ryanair

Experimental group:



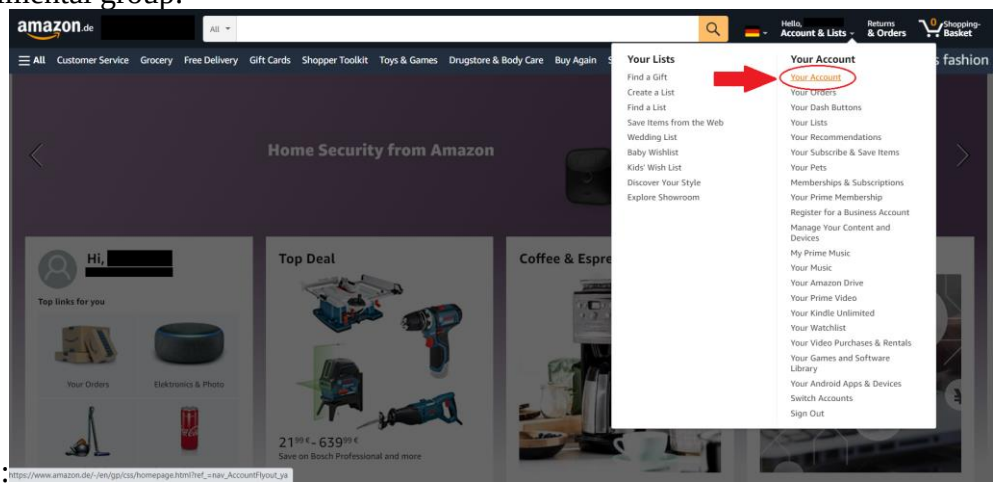

Control group:



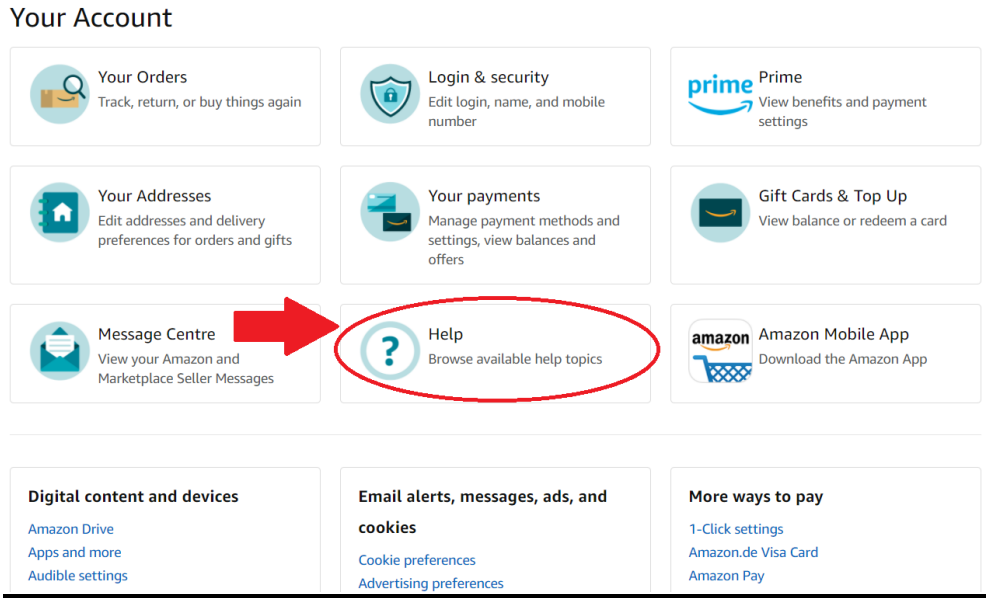

## Appendix 2 - Amazon

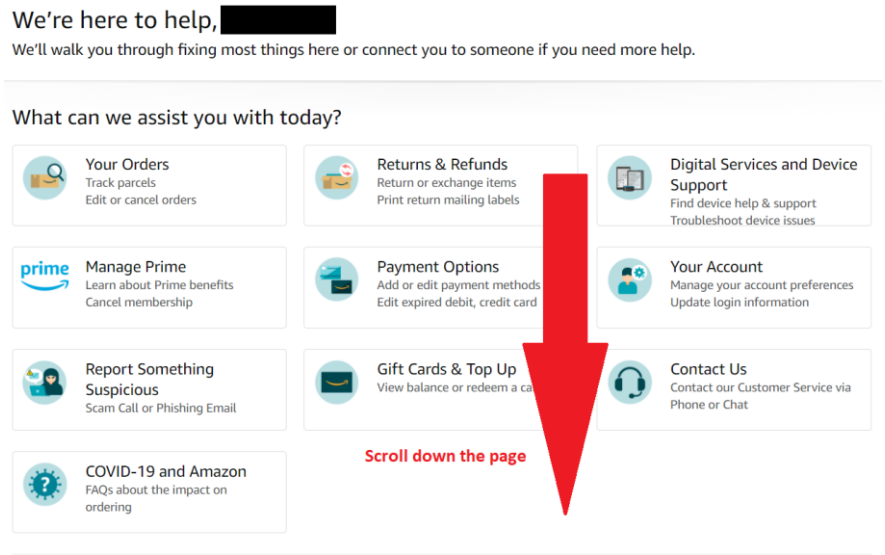
Experimental group:

Step 1:

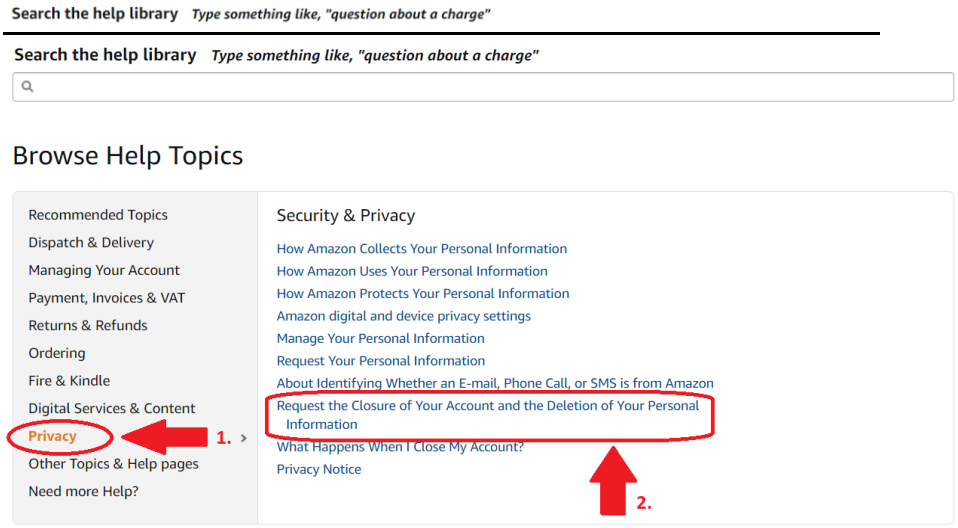



Step 2:

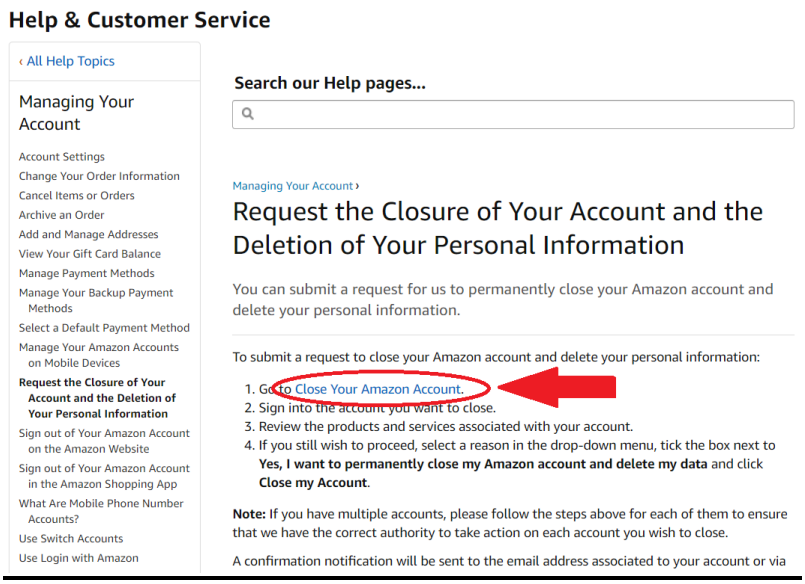





Step 3:

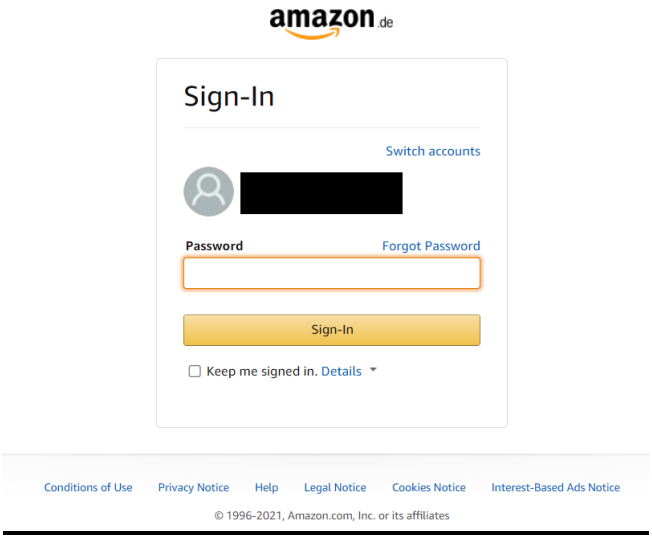



Step 4:

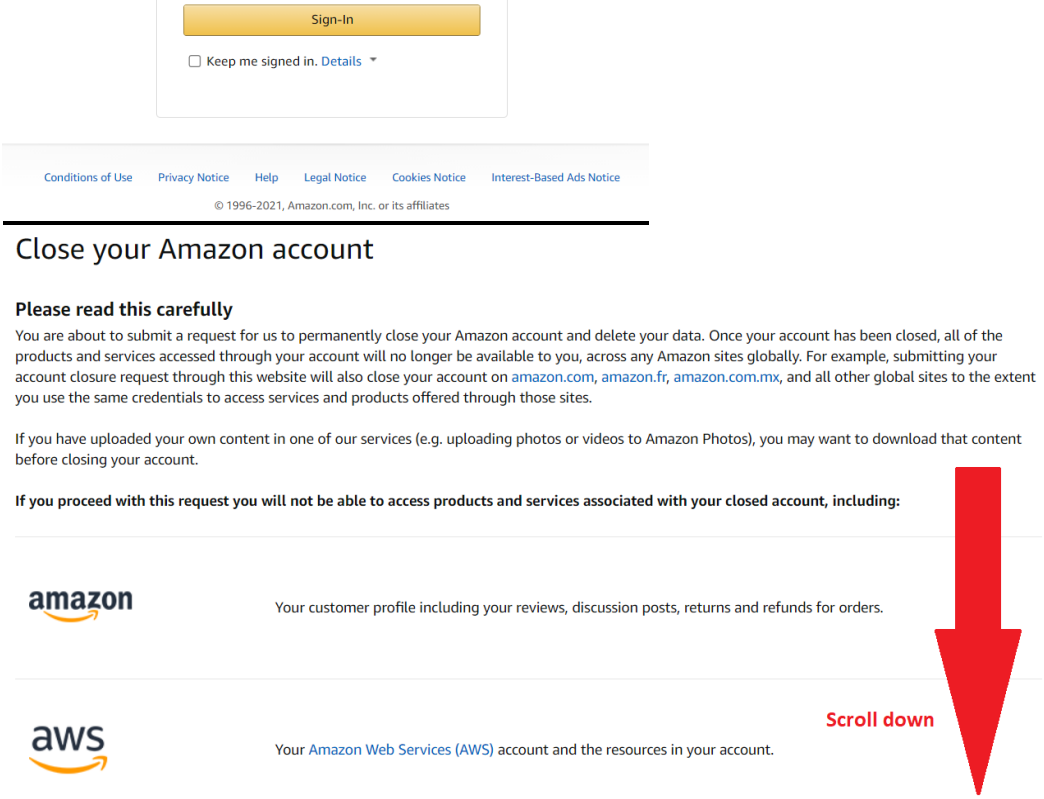




Step 5:

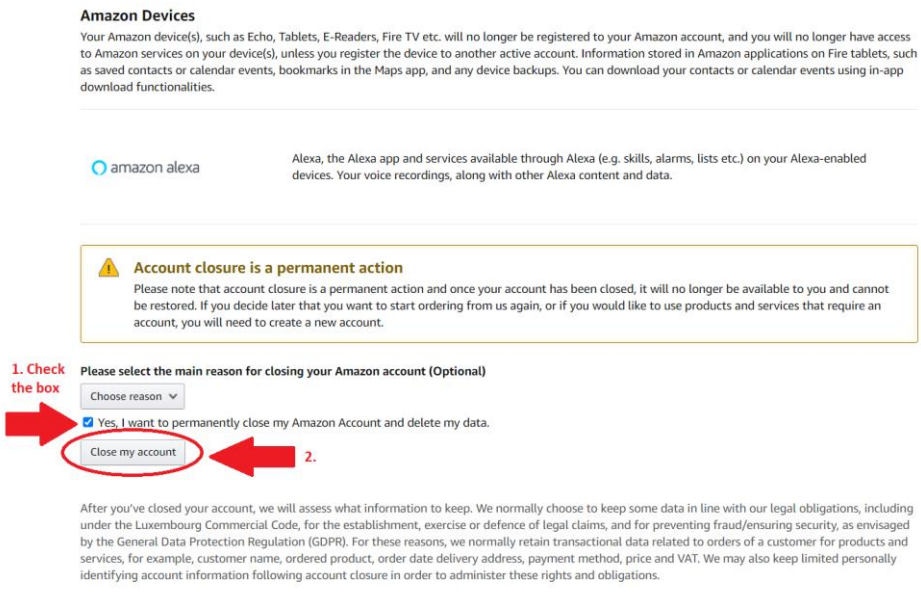
Step 6:




Step 7:

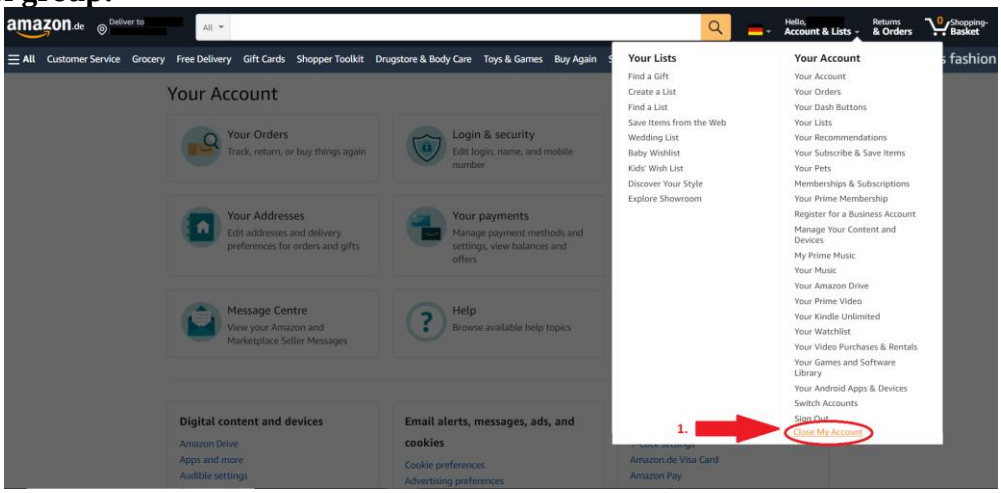


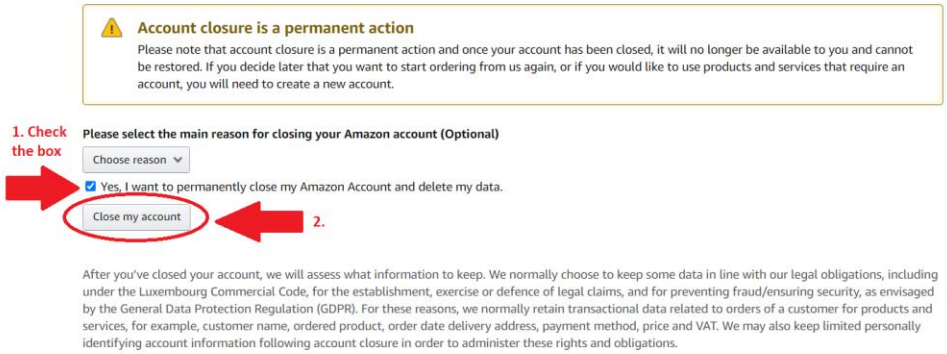

Step 8:



**Control group:**

Step 1:

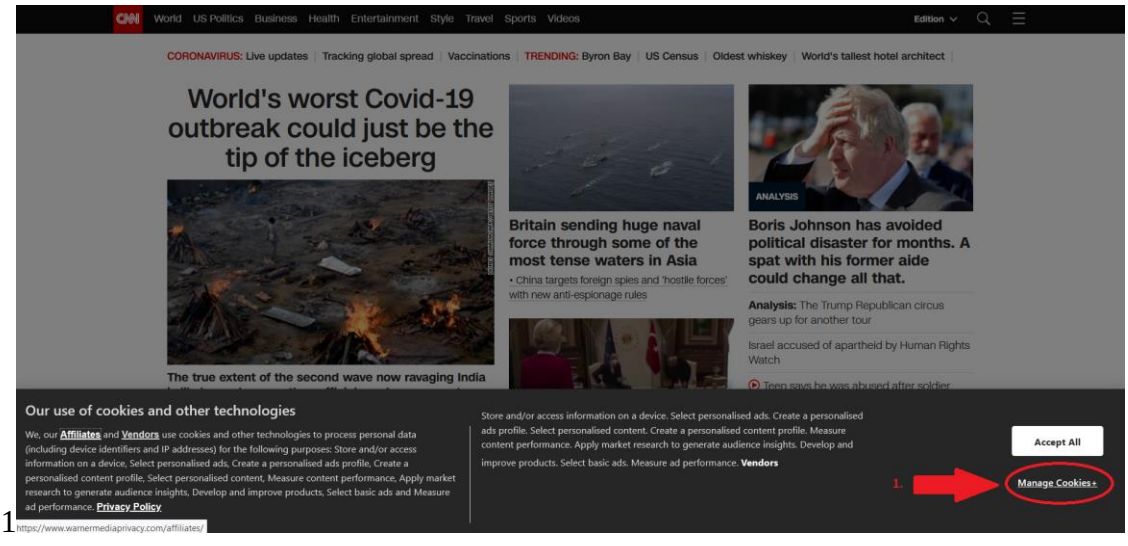


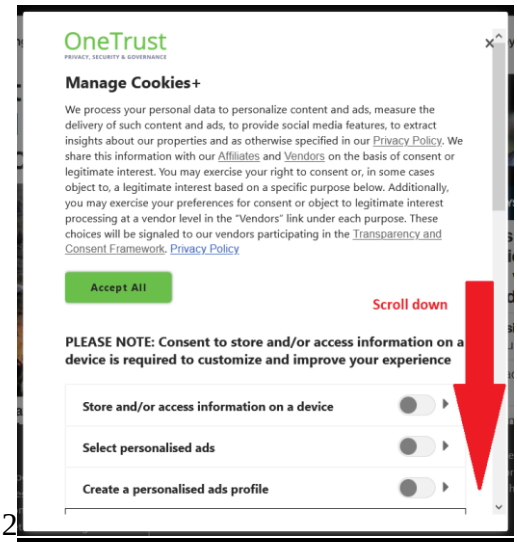

Step 2:

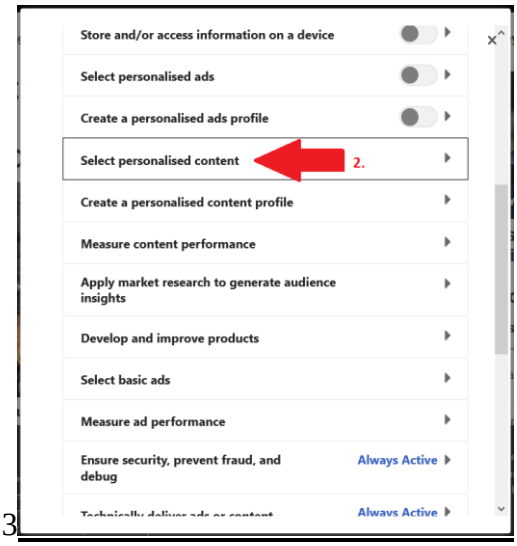
## Appendix 3 - CNN

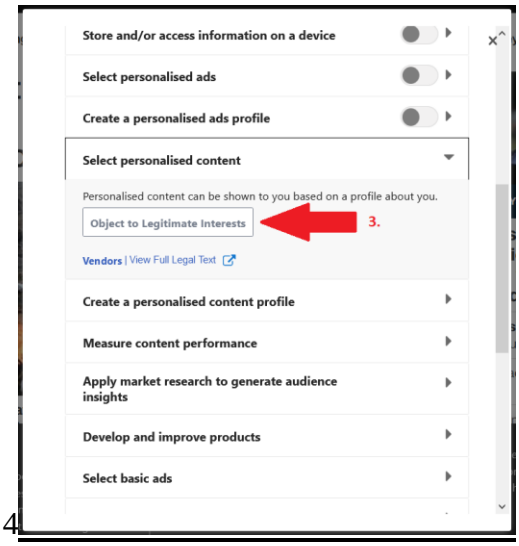
Experimental group:

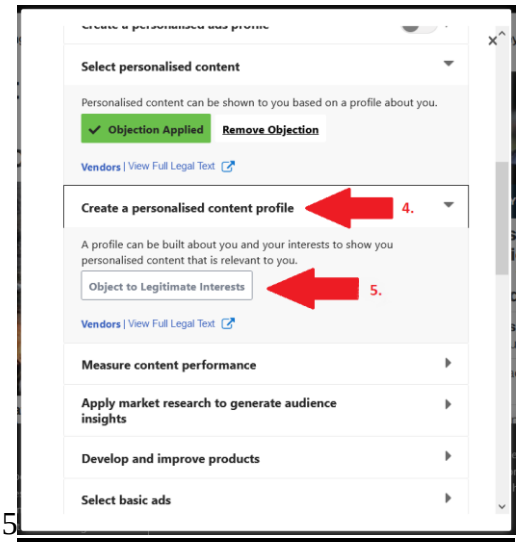


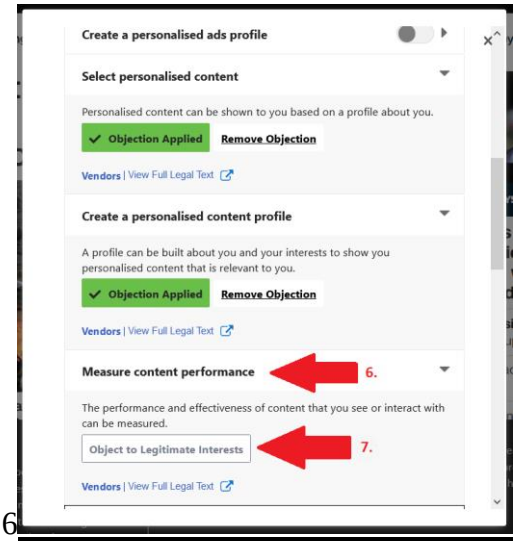

1

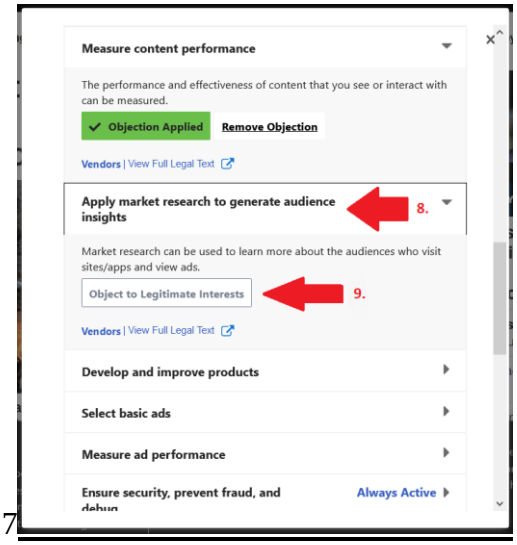

OneTrust
Manage Cookies+
We process your personal data to personalize content and ads, measure the delivery of such content and ads, to provide social media features, to extract insights about our properties and as otherwise specified in our Privacy Policy. We share this information with our Affiliates and Vendors on the basis of consent or legitimate interest. You may exercise your right to consent or, in some cases object to, a legitimate interest based on a specific purpose below. Additionally, you may exercise your preferences for consent or object to legitimate interest processing at a vendor level in the "Vendors" link under each purpose. These choices will be signaled to our vendors participating in the Transparency and Consent Framework. Privacy Policy
Accept All
Scroll down
PLEASE NOTE: Consent to store and/or access information on a device is required to customize and improve your experience
Store and/or access information on a device
Select personalised ads
Create a personalised ads profile
2


Store and/or access information on a device
Select personalised ads
Create a personalised ads profile
Select personalised content
2.
Create a personalised content profile
Measure content performance
Apply market research to generate audience insights
Develop and improve products
Select basic ads
Measure ad performance
Ensure security, prevent fraud, and debug
Always Active
3

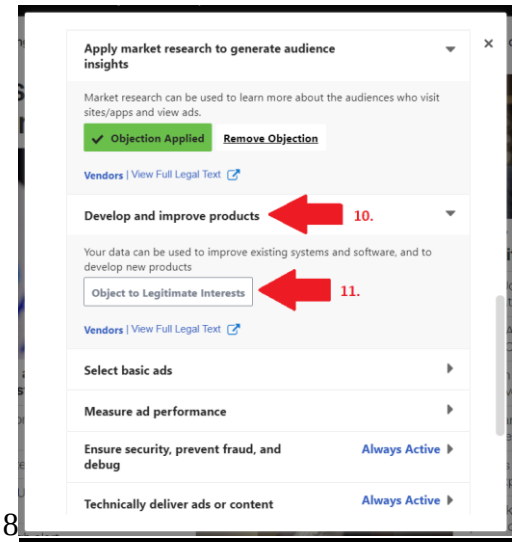

Store and/or access information on a device
Select personalised ads
Create a personalised ads profile
Select personalised content
Personalised content can be shown to you based on a profile about you.
Object to Legitimate Interests
3.
Vendors | View Full Legal Text
Create a personalised content profile
Measure content performance
Apply market research to generate audience insights
Develop and improve products
Select basic ads
4


Select personalised content
Personalised content can be shown to you based on a profile about you.
Objection Applied
Remove Objection
Vendors | View Full Legal Text
Create a personalised content profile
4.
A profile can be built about you and your interests to show you personalised content that is relevant to you.
Object to Legitimate Interests
5.
Vendors | View Full Legal Text
Measure content performance
Apply market research to generate audience insights
Develop and improve products
Select basic ads
5

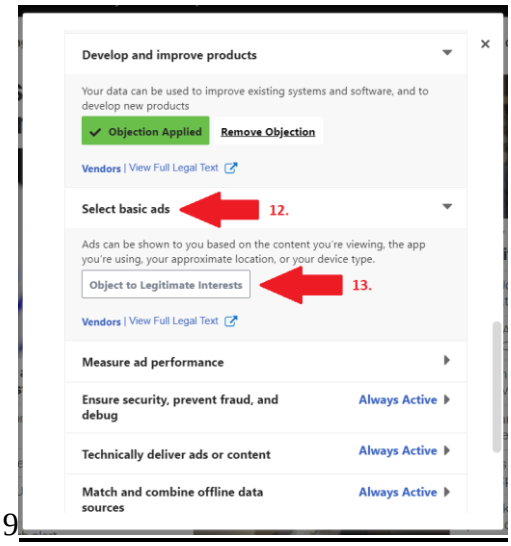

Create a personalised ads profile
Select personalised content
Personalised content can be shown to you based on a profile about you.
Objection Applied
Remove Objection
Vendors | View Full Legal Text
Create a personalised content profile
A profile can be built about you and your interests to show you personalised content that is relevant to you.
Objection Applied
Remove Objection
Vendors | View Full Legal Text
Measure content performance
6.
The performance and effectiveness of content that you see or interact with can be measured.
Object to Legitimate Interests
7.
Vendors | View Full Legal Text
6


Measure content performance
The performance and effectiveness of content that you see or interact with can be measured.
Objection Applied
Remove Objection
Vendors | View Full Legal Text
Apply market research to generate audience insights
8.
Market research can be used to learn more about the audiences who visit sites/apps and view ads.
Object to Legitimate Interests
9.
Vendors | View Full Legal Text
Develop and improve products
Select basic ads
Measure ad performance
Ensure security, prevent fraud, and debug
Always Active
7

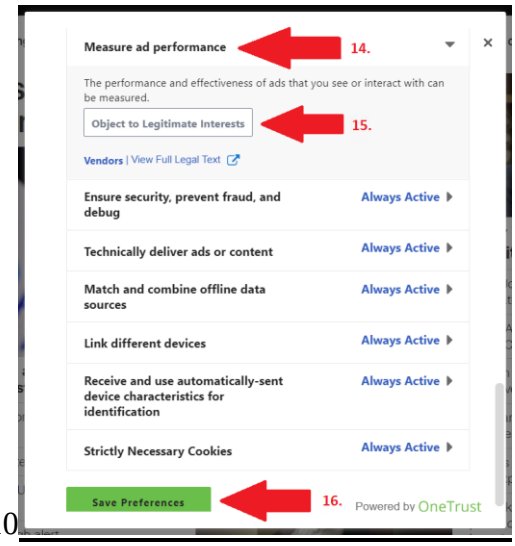
8




9

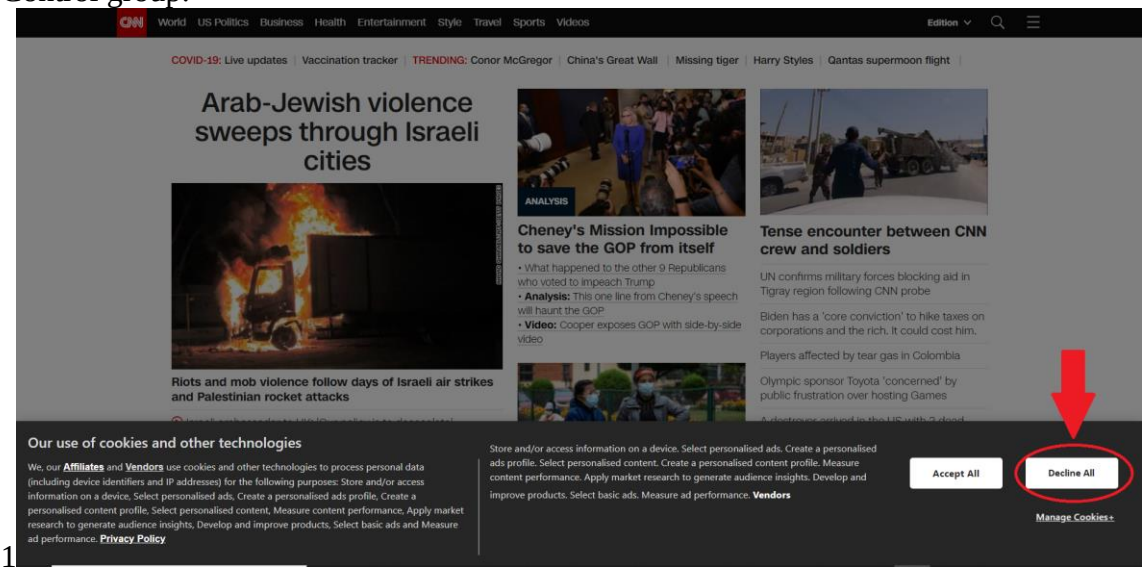



10




Control group:

1



## Appendix 4 - IPC scale and results

**IPC (Collection)**

1. It usually bothers me when commercial websites ask me for personal information.
2. When commercial websites ask me for personal information, I sometimes think twice before providing it.
3. I am concerned that commercial websites are collecting too much personal information about me.

**IPC (Secondary usage)**

4. I am concerned that when I give personal information to a commercial website for some reason, the website would use the information for other reasons.
5. I am concerned that commercial websites would sell my personal information in their computer databases to other companies.
6. I am concerned that commercial websites would share my personal information with other companies without my authorization

**IPC (Errors)**

7. I am concerned that commercial websites do not take enough steps to make sure that my personal information in their files is accurate.
8. I am concerned that commercial websites do not have adequate procedures to correct errors in my personal information.
9. I am concerned that commercial websites do not devote enough time and effort to verifying the accuracy of my personal information in their databases.

**IPC (Improper access)**

10. I am concerned that commercial website databases that contain my personal information are not protected from unauthorized access.
11. I am concerned that commercial websites do not devote enough time and effort to preventing unauthorized access to my personal information.
12. I am concerned that commercial websites do not take enough steps to make sure that unauthorized people cannot access my personal information in their computers.

**IPC (Control)**

13. It usually bothers me when I do not have control of personal information that I provide to commercial websites.
14. It usually bothers me when I do not have control or autonomy over decisions about how my personal information is collected, used, and shared by commercial websites.
15. I am concerned when control is lost or unwillingly reduced as a result of a marketing transaction with commercial websites.

**IPC (Awareness)**

16. I am concerned when a clear and conspicuous disclosure is not included in online privacy policies of commercial websites.
17. It usually bothers me when I am not aware or knowledgeable about how my personal information will be used by commercial websites.
18. It usually bothers me when commercial websites seeking my information online do not disclose the way the data are collected, processed, and used.

**Trusting beliefs**

19. Commercial websites in general would be trustworthy in handling my personal information.
20. Commercial websites would keep my best interests in mind when dealing with my personal information.
21. Commercial websites would fulfil their promises related to my personal information.
22. Commercial websites are in general predictable and consistent regarding the usage of my personal information.

**Risk beliefs**

23. In general, it would be risky to give my personal information to commercial websites.
24. There would be high potential for loss associated with giving my personal information to commercial websites.
25. There would be too much uncertainty associated with giving my personal information to commercial websites.
26. Providing commercial websites with my personal information would involve many unexpected problems

| IPC Category | Question | Mean | Category Mean |
|---|---|---|---|
| Collection | COL1 | 5.87 | 5.85 |
| | COL2 | 5.83 | |
| | COL3 | 5.85 | |
| Secondary Usage | SEC1 | 5.54 | 5.71 |
| | SEC2 | 5.79 | |
| | SEC3 | 5.78 | |
| Errors | ERR1 | 4.67 | 4.65 |
| | ERR2 | 4.65 | |
| | ERR3 | 4.64 | |
| Improper Access | IMP1 | 5.44 | 5.40 |
| | IMP2 | 5.42 | |
| | IMP3 | 5.34 | |
| Control | CON1 | 5.71 | 5.71 |
| | CON2 | 5.91 | |
| | CON3 | 5.50 | |
| Awareness | AWA1 | 5.14 | 5.43 |
| | AWA2 | 5.55 | |
| | AWA3 | 5.59 | |
| Trust beliefs | TRUST1 | 4.93 | 4.63 |
| | TRUST2 | 5.02 | |
| | TRUST3 | 4.21 | |
| | TRUST4 | 4.34 | |
| Risk beliefs | RISK1 | 5.09 | 4.96 |
| | RISK2 | 4.85 | |
| | RISK3 | 5.05 | |
| | RISK4 | 4.86 | |