# Privacy Regulations' Effect on Consumer Behavior Online

A Theoretical and Behavioral Economic Review

Frida Standal Bjørnstad

**Master's thesis**

This thesis is submitted to complete the degree

**Master's degree in economics**

University of Bergen, Institute of Economics

June 2023


UNIVERSITETET I BERGEN

# Acknowledgments

Firstly, I would like to thank my supervisor, Eeva Mauring. I would not have been able to write this thesis without your help and expertise. I would also like to thank my friends at the Institute of Economics, for all the great conversations and discussions through my years at UiB. A special thanks to Sarah-Angelina and Jørgen for their help with proofreading and feedback. Lastly, I would like to thank my mom and dad for all their support throughout my years of studying.

# Abstract

In May 2018 the General Data Protection Regulation came into effect. A regulation based on transparency, consent, and limits of service. The regulation gives consumers more ownership of their own personal data and companies are required to protect the data they collect, in addition to informing their consumers of why and how they use the data.

In this thesis, I investigate how these privacy regulations, mainly the General Data Protection Regulation has affected consumer behavior online. Through a literature review of empirical, theoretical and behavioral papers I find that there is some effect of the regulation but there are also behavioral aspects such as nudging and biases that affect the users' privacy choices. The thesis also looks at a model of rationality and presents a numeric example of how optimism bias, present bias and status quo bias may affect consumers' choices when presented with cookie banners. The privacy paradox also plays a part throughout the thesis to explain where the main problem lies.

The thesis concludes that privacy regulations do not affect consumer behavior severely and discusses if biases and nudging can be a reason for the unchanged behavior. However, even though the General Data Protection Regulation is a step in the right direction, as it targets companies to protect consumers, the authorities need to examine possible measures on how to further protect consumers interests. Especially, regarding nudging and the privacy paradox.

# Table of contents

# 1 Introduction

In this thesis I wish to investigate what effects privacy regulations have had on consumer behavior. Firstly, I present the purpose and the motivation behind the theme, then explain my research question. Further, in chapter 2 I define some of the terminology that will be used throughout the thesis. I then present some statistics that motivate the research question. Chapter 4 is a literature review, of theoretical, empirical, and behavioral papers on the subject. In chapter 5 I present a model of rationality in privacy decision making, followed by a discussion and a numeric example based on the model. Lastly, I discuss the research question and conclude.

## *1.1 Purpose and Motivation*

The motivation for the thesis is rooted in the notion that personal data and information have become valuable commodities in the online marketplace. As the saying goes:

> "if the product is free, you are the product." (Lynskey, 2016).

The saying reflects the present economic value of personal data and the market for it in the online world. This suggests that consumers can use their personal information as a form of payment. This intriguing concept is of great interest and relevance, given the limited amount of research that currently exists on the topic. While most existing literature examines the changes brought about by the General Data Protection Regulation, further referred to as the GDPR, this thesis seeks to offer a more nuanced understanding of the regulations from a behavioral economics' perspective.

In traditional economics, people are often assumed to behave rationally and make optimal decisions in every situation. However, people's decision-making is often influenced by a range of cognitive and behavioral biases. Thus, this thesis will take a more behavioral approach to analyze the GDPR and try to understand how and why it has been effective or not.

The following analysis aims to shed light on behavioral aspects such as social bias, nudging, and overconfidence, to mention a few. By using these theories and a model on rationality in

privacy decision-making, I aim to explain some of the results from empirical papers and provide examples of how these behavioral concepts work. Ultimately, the thesis aims to provide insights into the effectiveness of privacy regulations, its limitations, and their function in practice.

## *1.2 Research Question*

Through the thesis I try to answer the following question:

*How have privacy regulations affected consumer behavior online?*

With my research I hope to determine whether the new privacy regulations, focusing on the GDPR, have affected consumer behavior in the online market, and if so in what direction. I intend to investigate the underlying factors that may explain any observed changes, or lack thereof in consumer behavior, such as consumer awareness and perception of privacy risks, trust in online platforms and attitudes towards sharing personal information online. I aim to provide a more comprehensive understanding of the impact of privacy regulations on consumer behavior and to shed light on potential avenues for improving the effectiveness of these regulations.

Throughout the thesis, there is an underlying assumption that consumers would prefer that their personal data is protected.

# 2 Definitions

In this chapter I define and explain the most important definitions used throughout the thesis. Firstly, I define what personal data is, I vary between using "personal data" and "personal information" throughout, however, the definitions have the same essence; therefore, I only define one in this chapter. Further, I explain cookies, and then the General Data Protection Regulation. It is important to state that this thesis focuses on the consent part of the regulation, and the definition is therefore influenced by that. Lastly, I shortly explain information externalities, nudging and the privacy paradox.

## *2.1 Personal Data*

Personal data is an economic good which is of great value for organizations and companies. The European Commission (2022) define Personal data as "…any information that relates to an identified or identifiable living individual." Different pieces of information that together may lead to the identification of a specific individual are also considered personal data. The same goes for all data that has been de-identified, encrypted, or pseudonymized, but can be used to re-identify a person. For personal data to be rendered as anonymous and to be truly anonymized, the anonymization must be irreversible.

Examples of personal data are as common as one's name and surname, health data, home address and ID-card numbers. Additionally, someone's e-mail, IP-address, geo-location, cookie ID and online behavior is also considered personal data. The GDPR protects personal data regardless of the technology used to process the data. The regulation is technology neutral and applies to both manual and automated processing (European Commission, 2022).

## *2.2 Cookies*

Cookies allow small pieces of data or files created by a web application to be stored on a web browser. These files can contain information on user authentication, or user activity, such as login credentials, website preferences, and browsing history. The purpose of cookies is to enhance the user experience by allowing websites to remember user preferences and settings, enable personalized content and advertisements, and track the user's behavior for analytics and marketing purposes. "On top of their original goal of providing stateful navigation, nowadays cookies are routinely used to track users *across* different websites, most often for advertising and analytics" (Sanchez-Rola et al., 2019, p. 341). This is mainly possible due to the fact that the websites often have third-party domains, that set uniquely identifiable cookies on the individual computer to track them across different websites. (Sanchez-Rola et al., 2019).

Cookies can both be *session-based*, which means that they are deleted when the user closes their browser, or *persistent*, which means that they remain on the user's device until they expire or are manually deleted. While cookies can be useful for improving a website's functionality, they can also raise privacy concerns as they may collect and store personal data without the user's consent.

## *2.3 General Data Protection Regulation*

In May 2018, the GDPR was enforced by the European Union. The GDPR is a law that sets mandatory rules for organizations and companies regarding the usage of personal data in a privacy-friendly way, where personal data follows the definition given in 2.1 (GDPRSummary, 2022).

The GDPR is founded on three principles: transparency, consent, and limits to service. Transparency dictates the consumers legal right to know how their personal data is utilized and shared. Consent requires companies to obtain user consent to use and process their data. Finally, limits to service dictate that companies cannot engage in price or quality discrimination based on a user's choice to share their personal data. This prevents companies from penalizing users for denying consent (Argenziano & Bonatti, 2021).

The GDPR establishes obligations for companies and provides rights to users, representing a significant practical implication of the law. One notable difference between the GDPR and previous data privacy laws is that the GDPR does not only apply for companies based in the EU, but it also applies if the company is based outside of the EU if they offer services to users located in the EU (European Commission, 2023). The most noticeable impact of the GDPR for users is probably the prevalence of cookie pop-ups that require users to decide whether to accept a sites' cookies or not.

In this thesis, I investigate the consent portion of the law, where the EU mandates that consent must be freely given, specific, informed, and unambiguous. Consent requests must be clearly distinguishable from other matters and presented in clear and plain language. Users have the right to withdraw previously given consent, and companies must maintain documentary evidence of consent (Wolford, 2023).

## *2.4 Information Externalities*

An externality is defined as "a cost or benefit caused by a producer that is not financially incurred or received by that producer." (Kenton, 2022). An externality can be negative and positive and may originate from both the production and the consumption of a good or service (Kenton, 2022).

In this thesis, information externalities often refers to "negative privacy externalities" (Choi et al., 2019, p. 115). The concept is based on the premise that some individual's decisions to share their personal information may allow the data controller to know more about other users, even if they did not consent directly. The externality arises because of (dis)utility for those who chose to not share their personal data, they may still be affected by those who did (Choi et al., 2019).

## *2.5 Nudging*

According to Thaler and Sunstein (2008, p. 6) a nudge is

*"Any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives. To count as a mere nudge, the intervention must be easy and cheap to avoid. Nudges are not mandates. Putting the fruit at eye level counts as a nudge. Banning junk food does not."*

To be clear, the GDPR is not a nudge since it is a regulation, but cookie design, especially if the choices are set as a default, can be described as nudging.

## *2.6 Privacy Paradox*

The privacy paradox refers to the inconsistency between privacy attitude and privacy behavior. People state that they wish to protect their personal information online, but when they are surfing the web, they do not act accordingly (Gerber et al., 2018).

# 3 Motivating Statistics

In this chapter I examine some statistics from Eurostat on privacy and protection of personal information and personal data. I also look at data on trust, security and privacy concerning the use of smartphones. I have chosen to look at the European Union as a whole, and therefore review the collected statistics on the 27 countries as a combined entity (excluding the United Kingdom as they left the EU in 2020). The datasets are of interest since they contain values from both before and after the implementation of the GDPR.

| **Privacy and protection of personal information and personal data** | **2015** | **2016** | **2020** | **2021** |
|---|---|---|---|---|
| a. Individuals who know that cookies can be used to trace movements of people on the internet | 51.46 | 58.17 | 69.08 | 71.60 |
| b. Individuals manage access to personal data on the internet: read privacy policy statements before providing personal data | --- | 29.21 | 39.58 | 34.63 |
| c. Individuals use anti-tracking software (software that limits the ability to track their activities on the internet) | --- | 13.86 | 17.06 | 18.72 |
| d. Individuals have ever changed the settings in their internet browser to prevent or limit cookies on any of their devices | 27.09 | 27.90 | 31.90 | 31.75 |

*Table 3.1: Data from Eurostat on privacy and protection of personal information and personal data in the 27 EU countries, where the results are presented in percent (Eurostat, 2023a, 2023b).*

The table 3.1 shows that the awareness of cookie tracking increased from before the implementation of GDPR, to after. It increased by approximately 13%, however the increase in changed settings to prevent cookies is only 4%. Why the respective 9% have not taken any measures to protect themselves is an interesting question, and what I wish to examine further.

An almost 10% increase in people reading privacy policy statements is also an interesting find. One could assume that this is because the statements have, through the GDPR, been required to be for the users, so one answer to this might be that the accessibility has increased. However, the same variable decreased from 2020 to 2021.

Further, I study some statistics concerning the use of smartphones.

| **Trust, security and privacy - Smartphones** | **2018**[1] | **2020** |
|---|---|---|
| e. Individuals at least once restricted or refused access to personal data, when using or installing an app on the smartphone | 43.40 | 51.86 |
| f. Individuals never restricted or refused access to personal data, when using or installing an app on the smartphone | 18.18 | 18.10 |
| g. Individuals didn't know it was possible to restrict or refuse access to personal data, when using or installing an app on the smartphone | 5.47 | 5.90 |

*Table 3.2: Data from Eurostat on Trust, security and privacy – Smartphones in the 27 EU countries, where the results are presented in percent (Eurostat, 2023c, 2023d).*

Row 3.2.e indicates an approximate 8.5% rise in individuals who have declined or restricted access to their personal data on their phone at least once. An interesting observation can be seen in f., where the percentage of people who have never restricted data access is almost the same from 2018 till 2020. The same can be seen for individuals that did not know it was possible to do so. These numbers are low to begin with, so there may of course be reasons for the observations, for example that there are survey participants who have other people that install their phone apps for them. Dark numbers could also be a factor.

[1] The data is from the first quarter of 2018, so before the implementation of the GDPR in May 2018.

The discovered statistics are intriguing and provide a drive for the research question as they reveal patterns in user behavior that could potentially be attributed to the impact of GDPR. Unfortunately, they are not able to serve as anything else than motivation for the rest of the thesis, as there is not enough data to conduct an analysis and find any statistically significant correlations. Nevertheless, it is an interesting find. Especially, that an awareness of cookies does not necessarily correlate with the actions of protection which one might suggest.

# 4 Literature Review

The chapter aims to provide a comprehensive literature review of privacy regulations and theirs impact on consumer behavior in the online market. The review encompasses various studies that explore the economic implications of the regulations and the role of consumer behavior in shaping the market of personal data. The chapter begins with theoretical papers that incorporate privacy regulations into theoretical models. Subsequently, empirical papers are examined. Additionally, the chapter includes three behavioral economic papers that provide insights into the actual behavior of consumers online. Lastly, I will discuss and summarize the literature.

## *4.1 Theoretical Papers*

### *4.1.1 The Economics of Privacy (Acquisti et al., 2016)*

This paper mainly serves as an overall view of what research is already conducted on privacy, and to get a basic understanding of what privacy economics is.

The researchers explore the concept of privacy from an economic standpoint. The paper examines the costs and benefits of privacy in both online and offline worlds, as well as the factors that influence an individual's privacy decisions.

Acquisti et.al. (2016) begin by discussing the various ways in which personal information is collected and used by businesses and governments. They note that while many people may be willing to trade some of their personal information for access to certain services or benefits, they may not fully understand the potential risks involved in doing so.

Further, the paper studies the costs and benefits of privacy economics. They note that privacy can be viewed as a form of property right and, as such, individuals should be compensated for giving up their personal information. One can argue that that there are benefits of sharing one's personal information, such as targeted advertising, price discrimination, and more personalized service.

The authors also discuss the concept of "privacy nudges", which can either be designed to encourage individuals to make more privacy-preserving decisions or in a less ethical way, to encourage individuals to share more personal information. One goal for privacy regulations is to encourage online companies to design their privacy decision settings in a way that avoids nudging the consumers in a particular direction. This is discussed and investigated more in detail later, in light of the GDPR's effectiveness and precision in formulating the regulations.
Furthermore, the paper examines the factors that influence the individual's decisions about privacy. The authors note that the decisions are often influenced by a variety of factors, such as the perceived benefits of sharing personal information, social norms, and trust in the entities collecting the information (Acquisti et al., 2016, p. 446).

Overall, *The Economics of Privacy* provides a comprehensive overview of the economic factors at play in the realm of privacy. The paper highlights the need for greater understanding of these components to better protect individuals' privacy rights while still enabling the benefits that can come from sharing personal information.

### *4.1.2 Privacy in Electronic Commerce and the Economics of Immediate Gratification (Acquisti, 2004)*

The primary focus of the papers is introducing a model that addresses rational decision-making considering immediate gratification. The author applies "… lessons from the research on behavioral economics to understand the individual decision-making process concerning privacy in electronic commerce." (Acquisti, 2004, p. 21). It modulates this using a model of rationality in privacy decision-making, which I explore in chapter 5.

The paper also delves into various psychological distortions such as self-control problems, hyperbolic discounting, and present bias. It highlights how they contradict the traditional economic assumption of a fully rational economic agent, which is used as a foundation for the discussion. The conclusion drawn is that merely providing more information and awareness in a self-regulative environment is insufficient to safeguard individual privacy.

The perspectives above are interesting as the GDPR relies on informed consent from the consumers. Acquisti (2004) presents examples of measures that could be executed to

sufficiently protect one's data in an even more secure manner than what the GDPR requires, such as using email encryption software. However, the model and the idea can translate to the GDPR as it relies on individuals "making an effort" and desire to protect their data.

The paper also discusses other aspects of rationality and psychological distortions, such as incomplete information. It highlights that the involved parties in a transaction may not have the same information, which is a challenge the GDPR addresses with its rule that all information websites collect from users must be accessible to them.

Furthermore, the paper touches on the subject of this eventually, stating that even if an individual had access to complete information and could appropriately compute it, they may still find it difficult to follow the rational strategy (Acquisti, 2004). The paper also addresses bounded rationality, which refers to the inability to calculate and compare the magnitudes of payoffs associated with different strategies that individuals may choose in privacy-sensitive situations. Traditional economic theory assumes that the agent is both rational and has unbounded computational power to process information.

Lastly, the paper explores the possibility of optimism bias, which is connected to immediate gratification. Optimism bias occurs when the agent believes their risks are lower than those of others under similar conditions. The paper concludes that individuals perhaps should not be trusted to make decisions in their best interest when it comes to privacy and self-regulation. Even in the presence of complete information and awareness, they may not be trusted to work for the same reason.

### *4.1.3 Privacy and Personal Data Collection with Information Externalities (Choi et al., 2019).*

This paper provides a theoretical model of privacy in a monopoly, more specifically a social planner monopoly. In this model, the data collection requires consumers' consent, and the consumers are fully aware of the consequences of such consent.

They touch on issues relating to companies, example wise Google, having large amounts of data about single individuals, and through this knowing "all" about you over different

platforms. The authors mention other examples such as Facebook, where one's friends can define your sexuality and that your genetics' tests' information can predict information about others with similar dispositions among the same racial or ethnic category.

They discuss the aforementioned element further using the standard adverse selection mechanism: in sum, the extensive information companies get from another can be combined with the basic information they have on you. With the use of big data and artificial intelligence algorithms, companies can calculate more information about you based on other consumers.

With the use of information externalities, the authors set up a monopoly model. One of the main drivers in their model is the information externality effect of data collection on non-users of the service. They study the social optimum and the monopolist's optimal choice. For the thesis the most interesting part is part 7 where they implement different aspects of privacy regulations. They study opt-in consent with and without price discrimination.

The paper concludes that even when consumers are fully aware of the consequences of consent, they would still opt in. Their model "… shows that the market equilibrium is characterized by an excessive collection of personal information and the resulting loss of privacy compared to the social optimum" (Choi et al., 2019, p. 122). And they conclude that this may be the reason the current privacy regulation framework of informed consent may be ineffective to address the privacy concerns in the data broker industry. They also have a model for a market with small independent websites, where they test the same propositions and still get the same result as in the monopoly model. Their results indicate that even with regulations, and the consumers that are fully aware of the consequences of consent and there is no cost connected to do the informed choice, there still is an equilibrium where the customers consent, regardless of the regulations. This is if the individual is affected by strong negative information externalities, even a costless reading of the terms and conditions and a perfect understanding, the externalities still have an immense effect (Choi et al., 2019).

## *4.2 Empirical Papers*

### *4.2.1 Regulating Privacy Online: The early impact of the GDPR on European web traffic & E-commerce Outcomes (Goldberg et al., 2019)*

In this article, the authors empirically examine the impact of the GDPR on European web traffic and E-commerce sales using web analytics data from a set of 1508 companies that use Adobe Analytics platform. With the use of a difference-in-difference[2] approach, they show that both the recorded pageviews and recorded revenues fall by about 10% for EU users after the regulations were enforced.

Privacy regulations increase the companies' cost of collecting their customer data, which indicates that matching users to relevant ads and products is more costly. Therefore, under the GDPR companies may choose to collect less web analytics data or find that fewer users consent to their data being collected. Crucially in their study, the authors differentiate the users by location and arrival point so that they can identify the European users and the marketing channels that push them to the websites.

In their study the authors do not find evidence of the user selection post-GDPR, whether this is due to users changing their preferences for sites after GDPR or that the only recorded data is from the users that do consent, is not stated. But the GDPR does increase the marginal cost of collecting and using individual data. The GDPR also increases the legal risk associated with e-mail and online display advertising as both rely on personal data in the form of cookies or e-mail lists.

Companies differ in how and when they comply with the GDPR. Therefore, it could be many explanations for the results of the analysis. However the mechanisms suggest different policy ramifications, such as "…reducing the share of data recorded may be the more intended policy goal than reducing total web outcome." (Goldberg et al., 2019, p. 7). The total web outcome consists of various metrics that are related to web traffic and e-commerce performance, such as

[2] "The difference-in-differences method is a quasi-experimental approach that compares the changes in outcomes over time between a population enrolled in a program (the treatment group) and a population that is not (the comparison group)." (The World Bank, 2023).

changes in advertising, website visits and online sales. What the GDPR wishes to do is minimize the data the websites collect of the consumers, and that they consent to giving it away.

They conclude that their analysis provides some evidence that the results are not driven by direct changes in user behavior. The authors suggest that more research is needed to quantify the benefit to users of these privacy laws, in order to get a better understanding of these tradeoffs. One indicator for this is the cited number regarding opt-in, which are seemingly similar pre- and post-GDPR. This may suggest that the GDPR does not deliver that much value to most users. Also, the legislators should consider how and why companies are using user information more explicitly in their legislations to better address these asymmetries (Goldberg et al., 2019).

### *4.2.2 The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR (Aridor et al., 2020)*

Aridor, Che and Salz study the effect of the GDPR on the companies' ability to collect consumer data, accrue revenue via online advertising, identify consumers over time and predict behavior. The latter is what I am mainly interested in.

The paper discusses how the GDPR has affected the ability of companies to predict consumer behavior. The authors suggest three main reasons for the changes in predictive ability. Firstly, the GDPR has significantly reduced the overall amount of available data. Secondly, the remaining consumers, that is consumers that have consented to give away their information, have a longer data history and they are therefore more traceable. And thirdly, the GDPR may reveal a correlation between consumer behavior and the length of consumer histories that were previously hidden.

The authors perform a difference-in-difference analysis with data from the online travel industry. They find a 12.5% drop in the intermediary observed consumers as a result of the informed consent requirement of the GDPR. The study provides evidence of a pattern consistent with their hypothesis, indicating that privacy-conscious consumers tend to substitute away from less efficient privacy protection measures to actively opting out of certain privacy practices.

Their results highlight the externalities that consumer privacy decisions have on both companies and other consumers.

The study implies that consumers who switch privacy protection methods might unknowingly make themselves more trackable and predictable for the companies with whom they share their data. This is potentially beneficial for the companies in question. If the enhanced identifiability compensates for the reduction in available data due to opt-outs, then there are possible advantages, such as more targeted advertising, for companies utilizing consumer data. The welfare of consumers who choose to opt in depends on how the companies utilize their data. If the data is employed to offer personalized advertising and customized services that cater to their needs, these consumers benefit from the regulations, even if they did not explicitly consider these externalities when opting in. However, if said data is exploited to extract consumer surplus, such as personalized pricing, these externalities could negatively impact them.

Their results reveal insight into how an individual's privacy choices, particularly the means by which they adopt to safeguard their privacy, can have implications for the broader economy, including other consumers. They conclude that the clear winners of the implementation of the GDPR are the privacy-concerned consumers, but the impacts, both positive and negative, on others, are less clear.

### *4.2.3 Can I Opt Out Yet? GDPR and the Global Illusion of Cookie Control (Sanchez-Rola et al., 2019)*

The paper conducts research where they evaluate the tracking performed on 2,000 high-traffic websites, from both in and out of the EU. Their study finds that the majority of the cookie banners fail to comply with GDPR's requirements.

The authors identify several issues concerning the current state of cookie consent mechanisms, including the prevalence of dark patterns[3] that manipulate users into consenting to cookies, the lack of granular consent options, and the difficulty in withdrawing consent once given. These issues undermine the GDPR's goal of giving users control over their personal data.

[3] Also known as "deceptive patterns" it is defined as "a user interface that has been carefully crafted to trick users into doing things" (Wikipedia, 2023a).

The authors analyze both the information provided to users and the actual tracking methods implemented via cookies. They discover that the GDPR has had an impact on the behavior of websites worldwide, both directly and indirectly. However, despite these changes, they find that tracking remains ubiquitous. The study shows that over 90% of the websites in their dataset used cookies that could identify users, and many websites provided misleading information, making it almost impossible for users to avoid being tracked.

Further, the authors found that few sites provided an easy way to opt out; less than 4% of the websites presented the user with a clear “reject” option or a cookie setting dialog straight away (Sanchez-Rola et al., 2019, p. 344).

In conclusion, the paper highlights the shortcomings of current cookie consent mechanisms, even though the regulation has had a global reach. They find that tracking is still ubiquitous and present in more than 90% of websites, even those in the EU (Sanchez-Rola et al., 2019, p. 350).

## *4.3 Behavioral Papers*

### *4.3.1 (Un)informed Consent: Studying GDPR Consent Notices in the Field (Utz et al., 2019)*

The authors conduct an experiment on a German website to investigate the influence of graphical user interface on consent notices. They conduct three experiments. I am mainly interested in the second experiment *Number of Choices, natural presentation vs. nudging*.

Previous work, such as Thaler & Sunstein's (2008) show that design and architecture of choice can heavily influence individual's decisions. The question is if it also has been shown successful in improving user privacy? In practice it is most often used to make users share more information (Utz et al., 2019, p. 977). The websites often have an interest in the users agreeing to share their data, so they have incentives to nudge them in that direction. The experiment presents its users with five options, "no option", "confirmation", "binary", "categories" and "vendors". Every category, except the "no option" one has both a nudging and non-nudging design.

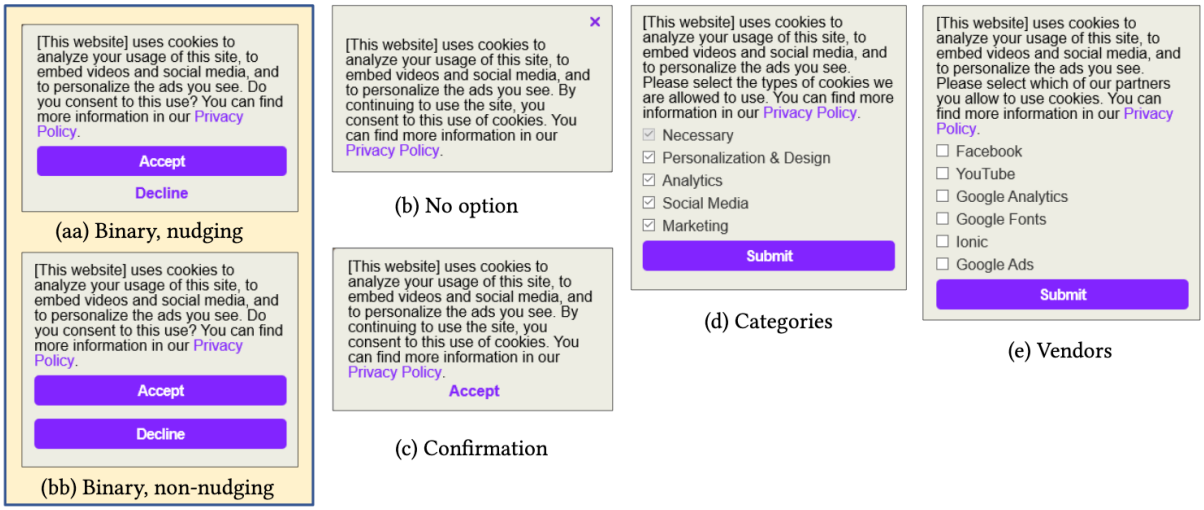


*Figure 1: Cookie consent notices that were used in the study with different choice mechanisms and nudging: (a) is a binary notice in two designs, one nudging with different colored buttons (aa) and one non-nudging with buttons in same color (bb). (b) is the no option notice where there is no nudging. (c) is the confirmation only notice (here represented with only the no-nudging design) In the nudging design the "Accept" button would be highlighted as in (aa). (d) is a category-based notice with pre-checked checkboxes (this is the nudging design). (e) is a vendor-based notice with the non-nudging design of unchecked checkboxes (Utz et al., 2019, p. 978).*

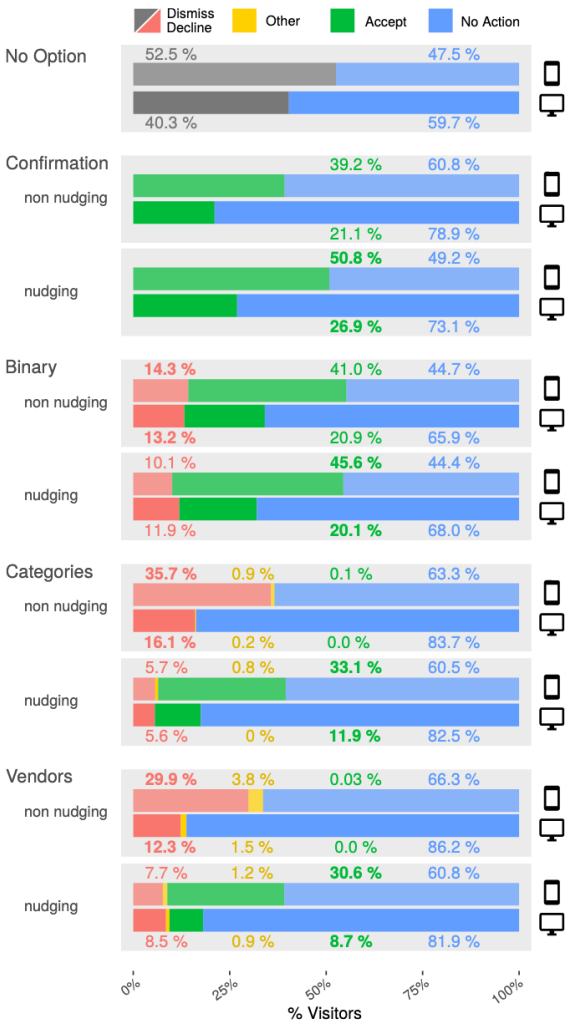


*Figure 2: Visitors' consent choices from the experiment conducted in the paper. "Accept" / "Decline" indicates that all of the options were declined or accepted. "Other" includes those individuals who accepted/declined to only some options. The bold figures indicate the default options (Utz et al., 2019, p. 981).*

Figure 2 summarizes the experiment's results. "The experiment revealed a strong impact of nudges and pre-selections." (Utz et al., 2019, p. 981). The effect was the most pronounced for category- and vendor-based notices, where the checkboxes were pre-checked in the nudging condition, but not in the privacy-by-default conditions.

One interesting find, as one can see from figure 2, was that more participants accepted cookies in both binary conditions, where they had the opportunity to reject or accept, than in the non-nudging confirmation condition, where they could only accept or ignore the notification.

The result of the experiment shows that pre-selection and nudges had a high impact on user's consent decisions. "It also underlines that the GDPR's data protection by default requirement,

if properly enforced, could ensure that consent notices collect explicit consent" (Utz et al., 2019, p. 982).

They conclude that their results further indicate that the GDPR's principles of data protection by default and purpose-based consent would require websites to use consent notices that lead to less than 0.1% of users actively consenting to the use of third-party cookies (Utz et al., 2019, p. 981).

### *4.3.2 E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior (Spiekermann et al., 2001)*

The authors conduct an experiment where they observe the participants during an online shopping trip. The participants filled out a survey disclosing their privacy preferences before and after their shopping trip. Many of the participants stated that privacy is important to them. However, regardless of the results from the experiment most participants did not live up to their self-reported privacy preferences. This is often referred to as the privacy paradox.

Their findings indicate that current approaches to protect online users such as the EU data protection regulation or P3P[4], may encounter challenges in their effectiveness. This is because they operate under the assumption that individuals are not only privacy conscious but will also act in accordance to their privacy preferences (Spiekermann et al., 2001, p. 1).

Lastly, they conclude that the disclosure of personal information remained unaffected by varying privacy statements, and interestingly the mention of EU regulation appeared to create a false sense of security. The results implies that individuals highly value communicative e-commerce environments[5] and tend to overlook privacy concerns once they are actively on the web (Spiekermann et al., 2001).

[4] Platform for Privacy Preferences Project is an obsolete protocol allowing websites to declare their intended use of information they collect about web browser users (Wikipedia, 2023b).
[5] An online platform where effective communication takes place between the seller and customers. The seller utilizes various communication tools to accommodate what different customers prefers. Such as chatbots, chat support and customer reviews to communicate and engage with their customers (Khurana, 2019).

### *4.3.3 Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online (Acquisti et al., 2018)*

The paper is a literature review on assisting individuals' privacy and security choices, including different methods where the users are nudged to certain choices. Here they also mention rationality models, and comment that a traditional rationality model glosses over several factors that affect the privacy and security choices consumers are faced with (Acquisti et al., 2018). Chapter 5 expands on this topic using the model from the paper in 4.1.2.

The paper further discusses how heuristics and bounded rationality can affect the consumers' choices. It investigates different cognitive and behavioral biases. Some of these are also mentioned in the paper from 4.1.2. I will now go through some of the other ways to nudge, since they will be used to discuss the model.

Firstly, there is "anchoring". Which entails that the users consider a point of reference for their situation and make their decisions based on that. For example, if you know that other people accept all cookies, this is your point of reference, and therefore you might choose to do so yourself, as it is the norm.

Secondly, there is "loss aversion". Which shows, contrary to traditional economic theory, that we as humans do not derive as much utility from a gain as we do from a loss. Prospect theory[6] notes that if an individual is faced with an equal opportunity of gains and losses, one would choose gains, since losses cause a greater emotional impact than gains. This theory also illustrates how people's willingness to pay (WTP) and willingness to accept (WTA) are not equal. While individuals would not be willing to pay for services that would help them protect their privacy online or pay a small sum to get their personal data back. They would accept payment for their personal information and data. Surveys show that people expect a larger payment for the latter. This shows that there is a great difference between a situation where the individuals feel like they own their data, and it is theirs to give, compared to a situation where they feel as if the data is already "lost".

[6] First introduced by Kahneman and Tversky (1979).

Thirdly, optimism bias and overconfidence are discussed. To summarize, optimism bias is "an underestimation of the chances that one might be subject to a negative event." (Acquisti et al., 2018, p. 9). Overconfidence is "an overestimation of one's accuracy of one's own judgement, resulting in excessive confidence in them." (Acquisti et al., 2018, p. 9).

The last cognitive bias the paper mentions is status quo bias, which "refers to individuals' affinity for default choices." (Acquisti et al., 2018, p. 10).

Lastly, the paper discusses how these different nudges are utilized, both to make the users share more, but also how one can design them to help the decision-making process. It concludes with that "the traditional economic view of individuals engaging in privacy calculus, rationally trading off costs and benefits of their actions, has been complemented by a more behaviorally grounded analysis of the heuristics and biases that may also influence behavior, and not always for the better." (Acquisti et al., 2018, p. 32).

## *4.5 Summary and Discussion of the Literature*

This chapter examines different papers related to the research question, although some are more directly relevant than others, as the GDPR's recent implementation limits the number of papers that are directly applicable. Thus, some incorporated papers are older, but nonetheless investigate privacy regulations, just not necessarily the GDPR.

My literature review reveals that privacy is an important theme, and especially the means of protecting it. One important point to mention is that even though many of the papers are from before the implementation of GDPR, they do still shed light on complications due to privacy regulations in general and general consumer behavior when faced with privacy questions.

A repeating theme in most of the articles is that privacy regulations have some effect on consumer and user behavior. However, their results and findings differ. The theoretical papers provide an overview of how privacy is connected to economics and an overview of the subject. The papers discussed in 4.1.2 and 4.1.3 both discuss the problems arising from asymmetries in information, where consumers unlikeliness of having full information may impact their decision. They decide to opt in on sharing their data. All the papers in this section in some way

touch on the subject of traditional economic theory which assumes individuals' rationality and that they act accordingly.

The section on empirical papers also gives an overview of important findings. Two of them directly examine the effect of the GDPR on different markets yielding comparable outcomes, however, somewhat vague results. The authors attribute this to the GDPR being a relatively new regulation, and a longer timeline is required to see more specified results. One similarity between the articles in sections 4.2.1 and 4.2.2 is that all research portrays the same tendency, privacy regulations have had some effect, especially for people that already are cautious in sharing their information online. However, the last empirical paper that is presented is quite interesting since it states that the presented choices concerning privacy online are of little consequence because they show that companies still tack cookies on consumers that explicitly opt out.

The last category of papers explores the more behavioral economic view of privacy and privacy regulations. These papers help in building an understanding of the more behavioral aspects of people's decisions making. In article 4.3.1 they investigate cookie design and find that even when the GDPR is implemented, companies can nudge their users to choose to accept and effectively give up their information through different cookie designs. The article presented in 4.3.2, even though it is old, gives a perspective and insight on how people's intentions and actions do not always align, which is the privacy paradox. The last paper in this section does not directly correlate with the GDPR, but rather describes different behavioral economic concepts.

I will now discuss some of the elements presented in the literature. In 4.1.1 it is mentioned that privacy regulations wish to encourage online companies to design their privacy decision settings to avoid nudging. The GDPR may not have necessarily accomplished this. The regulation focusses mainly on that the consumers should be able to give an informed consent, and that there should not be any discrimination regarding their choice. However, the regulations say little about how this choice should be presented. And as seen from the behavioral papers, the companies have means and ways to steer these choices.

Furthermore, I find that throughout most of the literature the authors conclude that privacy regulations do not have that much effect on the regular consumers. This observation can also

be seen and interpreted in the motivating statistics from chapter 3. If one assumes that the GDPR is the reason for the changes in the statistics, it correlates nicely with what the empirical and theoretical literature finds. It reads from the statistics that there is an increase in knowledge about cookies and what they track, but the increase in percentages of people that does something to change their tracking and cookies setting is much lower. This is similar to what some of the theoretical papers interpret, that even with full information and knowledge about that their data the individuals still choose to share. Both the statistics and the literature indicate that there is an asymmetric distribution between knowledge and action, which is also known as the privacy paradox.

To conclude, I have summarized and shortly discussed some elements from the literature. Remembering that some of the literature is pre-GDPR. The empirical papers look directly at its effects and conclude that there is little to no change in the consumers behavior as from what I have interpreted, except for privacy seeking individuals. The behavioral papers can potentially be interpreted as an answer to this, namely that the effect is small due to nudging and biases. The latter is seemingly backed by some of the statistics. However, more research is required.

# 5 A Model of Rationality in Privacy Decision Making

In this chapter I wish to present a more mathematical approach to the research question. To do so I use the model from the paper *Privacy in Electronic Commerce and the Economics of Immediate gratification* by Alessandro Acquisti (2004). Firstly, I go through and present the model. Secondly, I discuss the model's relevancy, some limitations with it, and how different biases could affect it. Lastly, I present a numeric example to substantiate the bias theories.

## *5.1 Disclaimer*

Chapter 5.2 serves as a presentation of the model from the paper, and consequently, it will bear some similarities with the paper. Therefore, while I have expressed the content in my own words, presenting a model inherently entails resemblances. However, I implement some of my own examples throughout.

## *5.2 Presentation of the Model*

In the paper Acquisti concludes in the first section that "… simply providing more information and awareness in a self-regulative environment is not sufficient to protect individual privacy" (2004, p. 22). This shows that even with informed consent, regulations that make all information available to the consumer do not necessarily have the effect that was assumed when the regulations were made.

The aim of the model is to investigate the fundamental assumptions about personal behavior and its contribution to the hypothesis that exist in traditional economics of complete rationality in decision making related to privacy.

$$\max_{d} U_t = \delta\Big(v_E(a), p^d(a)\Big) + \gamma\Big(v_E(t), p^d(t)\Big) - c_t^d \quad (1)$$

Equation (1) is the traditional economical decision process of an idealized rational economic agent faced with a privacy trade-off when completing a certain transaction.

$\delta$ and $\gamma$ are unspecified functional parameters that describe the weighted relations between the expected payoffs from a set of events $v$ and the associated probabilities of the occurrence of those said events, which is represented by $p$.

$t$ represents the transaction, and $U$ is the utility of completing the transaction $t$. It is important to note that the transaction $t$ can be any action (not necessarily a monetary operation) where there is a possibility that personal information can be exposed.

The utility of completing the transaction $t$ equals some function of the expected payoff $v_E(a)$ from keeping or [not] certain information private during the transaction. The probability of keeping or [not keeping] the information private when using technology $d$ is $p^d(a)$ or $[1 - p^d(a)]$.

$v_E(t)$ is the function for expected payoff from completing or [not completing] the transaction and possibly revealing personal information. The probability of completing or [not completing] the transaction with a certain technology $d$ is $p^d(t)$ or $[1 - p^d(t)]$; minus the cost of using the technology $d$: $c_t^d$.

Acquisti mentions that "In traditional economic theory, the agent is assumed to have both rationality and unbounded 'computational' power to process information" (2004, p. 24). Bounded rationality affects equation (1), more specifically the cognitive cost involved in trying to calculate the best strategy may be so high that the consumer rather opts for simple heuristics (Acquisti, 2004, p. 24).

When faced with privacy sensitive decisions, the consumer hardly ever has all the necessary information for a fully informed choice. This is what the GDPR intends to prevent through the informed choice regulation. The regulation forces the companies to disclose what information they collect and why, so that the consumers have the opportunity to read and make an informed choice regarding sharing their data. The companies are also obliged to have the collected data available to share with the consumer if asked.

Now I switch away from the rational individual model and implements a variable of future time $T$.

$$U_t = \sum_{\tau=t}^{T} \delta^T u_\tau \quad (2)$$

Equation (2) demonstrates that the cumulative utility $U$ at time $t$ is the sum of all utilities from the present moment until a future time $T$, where δ is the discount factor, ranging from 0 to 1. When δ equals 0, the individual heavily discounts the notion that utility from future periods has any value in the present. This differs from equation (1), which represented a one period decision. Equation (2) looks at when the consumer executes a transaction in a sequence from time t to T.

I now modify the traditional model of utility discounting which considers the possibility of time inconsistency of preferences. The equation yields the following:

$$U_t(u_t, u_{t+1}, \dots, u_T) = \delta^t u_t + \beta \sum_{\tau=t+1}^{T} \delta^\tau u_\tau \quad (3)$$

Equation (3) presents the time-inconsistency of preferences. $\beta$ is parameter of an individual's tendency to gratify herself immediately (a form of time-inconsistent preferences). When $\beta$ equals 1, the equation represents the traditional economic model. Whenever it is less than 1, there is time-inconsistency and self-control bias.

Self-control bias can be explained by the following example. You are at the store on a Monday, and you decide to buy chocolate, you tell yourself that you will save it for the weekend. Yet later that day the chocolate looks delicious, and you decide to eat it now rather than later since you want it now, and it will give you instant gratification.

According to experimental studies, humans tend to delay unpleasant activities and engage excessively in pleasurable ones, even if it results in decreased utility in the future (Acquisti, 2004, p. 25). This tendency may explain why consumers often choose to share their information without much thought when accepting cookies. Although the terms and conditions are in some way presented, consumers may opt for the immediate gratification of browsing and using the website rather than taking the time to make an informed decision about sharing their information. For example, if you're looking for a specific product online, you might click on the first link that appears, only to be prompted to accept cookies or go through the time-consuming process of turning off all the options in the "other options" menu. In such cases, consumers may prioritize the immediate gratification of finding the product and using the website, over protecting their privacy. This is an interesting find, and something I come back to later in chapter 5.3 and 5.4.

Subjects who were surveyed at time $t = 0$ regarding their attitudes towards privacy risks may consider the costs of protecting their privacy at a later time, $t = s$. These are compared to potential costs of privacy intrusions at an even more distant time, $t = s + n$. The options available to them at the time of the survey are expressed in equation (4).

$$\min_{wrt\ x} DU_0 = \beta \left[ \left( E\left(c_{s,p}\right)\delta^s x \right) + \left( E\left(c_{s+n,i}\right)\delta^{s+n}(1-x) \right) \right] \quad (4)$$

Equation (4) features a dummy variable, x, which takes the value of 0 or 1 and indicating an individual's choice between two costs. If $x = 1$, the individual chooses to face the expected cost of protecting themselves at time s, $E(c_{s,p})$, while if $x = 0$, they opt for the expected cost of privacy intrusions later, $E(c_{s+n,i})$.

The individual's objective is to minimize the disutility, DU, of these costs with respect to $x$. It is assumed that the individual discounts the two future events with uniform discount factors. even though they represent different time-periods. The individual concludes that investing in protection oneself is worthy for certain values of the parameters (Acquisti, 2004).

$$E(c_{s,p})\delta^s < E(c_{s+n,i})\delta^{s+n} \quad (5)$$

Equation (5): Tells us that that if the expected discounted cost now is lower than the expected discounted future cost, the individual chooses to complete the transaction and consume now.

Now I examine the scenario as the moment t=s arrives, wherein a tangible price must be paid to acquire a certain level of protection (such as encrypting all emails to safeguard against future intrusions). At this point, the individual's perception of the situation may shift considerably:

$$\min_{wrt\ x} DU_s = \delta\left[E(c_{s,p})x + \beta E(c_{n,i})\delta^n(1-x)\right] \quad (6)$$

Equation (6): Note that the equation remains unchanged (especially the individual's perceived risks), except for the time parameter. However, the value of $\beta$, which indicates the level of self-control issues, may influence the individual's decision. When $\beta$ is less than 1, the individual is likely to opt not to protect themselves when faced with the perceptible cost of doing so. This scenario occurs under the following condition:

$$\delta E(c_{s,p}) > \beta E(c_{n,i})\delta^n \quad (7)$$

It should be noted that under certain circumstances where $\beta < 1$, both inequalities (5) and (7) may be simultaneously met. See appendix A for numeric calculations.

At the time of survey, the individual expressed a genuine intention to protect themselves against privacy intrusions in the future. However, when confronted with the need to take action to safeguard their privacy in the present moment, the individual may choose to forego protection and take the risk of a privacy intrusion. This observation aligns with the privacy paradox, as evidenced in the literature, where consumers exhibit varying degrees of discounting between the two periods.

Finally, it is important to acknowledge that the model considers the perceived cost rather than the actual cost, as the real cost is unknown, and it is not asserted that the individual is aware of it.

## *5.3 Discussion of the Model*

In this part I discuss how immediate gratification and other psychological distortions can relate to the GDPR, and more specifically how cookie designs can nudge the consumers in a direction that makes them not protect their privacy. I also discuss some aspects of the model and its relevancy and present some limitations.

One interesting and important part of the model is to look at the time parameter, and people's willingness to protect their data in the future, but then when the problem arises in the present when they are not as interested and often opt to not "pay the price" for protection. This is the privacy paradox, that has been discussed earlier. The model and some of the literature that has been reviewed earlier shows that the GDPR not necessarily has had the expected effect. The model also illustrates the importance of time and the individuals discounting of their future, in the survey example. And shows through function (4) – (7) how the discount factor and time-inconsistency affect the original answer when the future arrives.

Further, it is mentioned in the model that we as humans, when presented with choices, tend to not have all the information. Which the GDPR tries to prevent. The regulation states that the users should have access to all the information needed to perform an informed choice. However, experience has shown that it sometimes can take a lot of work to locate this information, which can be seen as a cost for the consumers. If one includes the possibility of present bias, optimism

bias and status quo bias in the decision-making process, the consumer may just blindly accept, hoping and assuming that their data is not used in any mischievous ways.

The main factor, which distances the model from a traditional economic model is $\beta$. Acquisti shows how this element can affect and change an individual's choices, based on how much he or she is affected by immediate gratification. In chapter 5.4 I will present a numeric example showing how different biases, namely optimism bias, present bias and status quo bias can affect privacy choices when presented with cookies. Then investigate how these biases affect both $\beta$ and $\delta$ and thereby affect the consumers privacy decision-making.

### *5.3.1 Limitations*

It is important to mention that there are some limitations to the model. Most importantly, that it focuses on an individual level. When primarily examining the individual decision-making process, the model fails to consider social or contextual influences. In reality, privacy decision-making can be influenced by social norms, cultural factors and other contextual factors that extend beyond individual choices. The model also has a limited scope since it only focuses on the trade-offs between privacy and immediate gratification in electronic commerce. While this narrative is valuable, it may fail to capture the full range of factors and motivations that influence the individuals' decisions in other situations. The fact that the model only investigates the actions of one agent, is not optimal.

One thing that could elevate the model with more updated scenarios, is to implement another agent, namely the companies. Extending the model to include another agent enables it to account for nudging, as the literature has shown the potential effect this can have on the consumers privacy choice. Implementing this in future studies may be of value.

Despite this, I think the model is representative for answering questions concerning privacy choices. It investigates the aspect of human rationality in decision-making, or lack thereof, as well as the effect of time on the matter. It also portrays how individuals' intentions and action not always correlate when a time-parameter is included.

## *5.4 A Numeric Example*

The numeric example is presented to show how elements from the model can be applied to show how people act when presented with privacy choices, with two scenarios.

In the first one the individual is presented with a non-nudging cookie. With one "Accept" button and one "Reject" button (further referred to as "A or R"). The second scenario presents a nudging cookie. With one "Accept" button and one "Other Options" button, which takes you to another site where you must manually turn of all the additional cookies (further referred to as "A or O").

I look at these scenarios simultaneously, where the individual is affected by different biases, mainly optimism bias, present bias, and status quo bias, as these are the main focus onward.

Firstly, I need to establish numbers for the example. As precise values for the costs and benefits are unavailable, I will instead provide some illustrative numbers.

$$Expected\ benefit\ of\ accepting:\ E(b_A) = 15$$

$$Expected\ benefit\ of\ rejecting: E(b_R) = 10 = E(c_T)$$

The expected benefit of rejecting ($E(b_R)$) equals the expected future cost ($E(c_T)$). This means that $E(b_R)$ also is affected by the variables $\delta$ and $\beta$, while $E(b_A)$ is not.

When accepting cookies there is a 10% probability that the individual would have to pay a cost in the future, for example identity theft. I expect this cost to be 100 and therefore we multiply the future cost by 0.1 to calculate the effect on the individual today. If the individual rejects, the future cost equals 0 and the probability also equals 0, but the expected benefit equals the 10 the individual could have lost if accepting, namely $E(b_R) = E(c_T)$.

$$Expected\ future\ cost\ when\ accepting: E(c_T|A) = 0.1 * 100 = 10$$

$$Expected\ future\ cost\ when\ rejecting:\ E(c_T|R) = 0$$

Further I assume the expected cost for today for the two scenarios. The expected cost for today is 0 in "A or R", since there is no extra cost for rejecting rather than accepting. In the "A or O" scenario the expected cost is 5, representing the loss of time where the individual could browse the website.

$Expected\ cost\ today\ when\ there\ is\ an\ Accept\ and\ Reject\ button:$

$E(c_t|A|AorR) = 0 = E(c_t|R|AorR)$

$Expected\ cost\ today\ when\ there\ is\ an\ Accept\ and\ Other\ button\ and\ you\ Accept:$

$E(c_t|A|AorO) = 0$

$Expected\ cost\ today\ when\ there\ is\ an\ Accept\ and\ Other\ button\ and\ you\ Reject:$

$E(c_t|R|AorO) = 5$

### *5.4.1 A Theoretically Rational Individual*

As the individual is a utility maximizing rational individual, $\delta$ and $\beta$ are assumed to both equal 1. And from the numbers we will get these results.

| | $Accept: E(b_A) - E(c_t) - \beta E(c_T)\delta$ | $Reject: \beta E(b_R)\delta - E(c_t) + \beta E(c_T)\delta$ |
|---|---|---|
| *A or R* | $15 - 0 - 10 = 5$ | $10 - 0 + 0 = \mathbf{10}$ |
| *A or O* | $15 - 0 - 10 = \mathbf{5}$ | $10 - 5 + 0 = \mathbf{5}$ |

According to the calculations above a theoretically rational individual chooses to reject cookies in the "A or R" scenario and is indifferent between rejecting and accepting in the "A or O" scenario.

### *5.4.2 Optimism Bias*

I begin with investigating optimism bias, which was defined in 4.3.3 as "an underestimation of the chances that one might be subject to a negative event" (Acquisti et al., 2018, p. 9). A person

that is optimism biased, can also be referred to as overconfident, is under the impression that the probability of something bad happening to them is much lower than for it to happen to someone else. For example, identity theft.

In the model one could assume that if an individual is affected by this, it would reduce δ, since the future expected cost of their choice of sharing their data is not as large as everyone else's. One could argue that this bias would affect the 10% probability, but the probability for it to happen is still the same. It is just as likely as before that the individual is affected by this cost. What has changed is the individual's perception of this probability, therefore the discount factor is reduced. Since it is assumed that the expected benefit when rejecting is equal to the expected future cost, δ affects this too. When reducing δ from the original 1 to 0.5 and $\beta$ equals 1, the results are as following:

| | $Accept: E(b_A) - E(c_t) - \beta E(c_T)\delta$ | $Reject: \beta E(b_R)\delta - E(c_t) + \beta E(c_T)\delta$ |
|---|---|---|
| *A or R* | $15 - 0 - (10 * 0.5) = \mathbf{10}$ | $(10 * 0.5) - 0 + 0 = 5$ |
| *A or O* | $15 - 0 - (10 * 0.5) = \mathbf{10}$ | $(10 * 0.5) - 5 + 0 = 0$ |

According to the table above, an individual influenced by optimism bias tends to discount the expected future cost. Resulting in a preference to accept in both scenarios. This bias leads the individual to perceive the expected future cost as significantly lower than its actual value. Thus, giving a shift from the rational individual situation from reject in "A or R" to accept and from indifference in "A or O" to accept.

### *5.4.3 Present Bias*

The next calculation demonstrates the effect of present bias. Being present biased means that you discount future rewards more heavily compared to someone that is not affected by present bias. A present biased person prefers immediate gratification, which is also what the model investigated. Present bias affects $\beta$, since the individual wishes to gratify themselves immediately. Here I set $\beta = 0.2$, and $\delta = 1$.

| | $Accept: E(b_A) - E(c_t) - \beta E(c_T)\delta$ | $Reject: \beta E(b_R)\delta - E(c_t) + \beta E(c_T)\delta$ |
|---|---|---|
| *A or R* | $15 - 0 - (0.2 * 10) = \mathbf{13}$ | $(10 * 0.2) - 0 + 0 = 2$ |
| *A or O* | $15 - 0 - (0.2 * 10) = \mathbf{13}$ | $(10 * 0.2) - 5 + 0 = -3$ |

Present bias indicates that the individual would in both scenarios accept the cookies. Since it is what gives him most utility. In this example the "A or O" scenario even gives the individual negative utility if he rejects.

### *5.4.4 Status Quo Bias*

Lastly there is status quo bias. This bias implicates a preference for the individual to maintain its current situation, and he or she chooses to not look for alternatives to deal with their personal information, since they wish for things to stay the same (Acquisti & Grossklags, 2007, p. 395).

Therefore, it does not matter as much what utility the different choices and scenarios gives, the individual's original preference is more important. One could assume that for many individuals, accepting the default option is common, as it often represents the preexisting state before any choice was available. Nudging can additionally enhance the idea of what the default choice is.

To summarize, I have presented a numeric example to see if different biases can influence an individual's choice concerning privacy. The example shows that a rational individual would be the only one to reject. Individuals with optimism bias, and present bias would accept in both scenarios. Lastly, I presented status quo bias. Individuals affected by this bias do not necessarily care or think about the utility gained from the different choices, but rather value sticking to their default preferences. So, if they have always accepted cookies, they continue to do so and vice versa.

# 6 Discussion

In this chapter, I discuss the research question and analyze the effects of privacy regulations on both consumers and companies. The thesis mainly focusses on the impact of regulations on consumers; however, I also touch upon the effect of the regulations on companies to provide a more comprehensive discussion.

Chapter 3 presents motivating statistics that indicate that there is an increase in the awareness of cookies and privacy after the implementation of the GDPR in the European Union. This increase in awareness can be interpreted to have a positive effect on the number of people taking measures to protect their privacy, according to the statistics. Although, there is not necessarily a correlation between the statistics and the implementation of the regulations. The GDPR requires companies to be transparent about the collection, processing, and use of personal data. This is often presented to the consumers using cookies, which as mentioned earlier, can bear different designs to influence the consumer. Nevertheless, this transparency has the potential to increase consumers' trust in the online platforms and may lead to greater usage and engagement. Additionally, privacy regulations have improved data security by mandating the implementation of more robust data security measures, such as the encryption of user-data stored in the companies' databases.

On the other hand, the implementation of regulations may also have negative effects. Strict regulations may reduce access to information on the consumers, particularly for companies delivering personalized content and services, resulting in reduced access to information and services for consumers that either reject sharing their data, or only share the necessary data. There is also an assumed increased cost connected to the implementation of privacy regulations, such as compliance costs, which may be passed on to the consumers in the form of higher prices for products and services. Furthermore, regulations may discourage innovation by limiting the use of data for research and development. One industry which could be affected by this is the advertising industry, which relies heavily on the information and data of consumers.

The thesis's derivations have shown that companies have incentives for their consumers to give up their personal data. Even with the GDPR, companies can use nudging to obtain more information from consumers. The GDPR is vague about the design of cookie acceptance

banners, beyond that the users should be able to make an informed choice and it is not allowed to discriminate based on consumer's choice to opt in or opt out. The paper I presented in 4.3.1 stated that even without nudging people often choose to opt in. This is similar to what two of the theoretical papers, mainly 4.1.2 and 4.1.3, find with their theoretical models. One answer to this can be a sense of security for the consumers that have knowledge of the GDPR. They might feel more secure, and therefore not care that much about their choices since they feel their data is protected by the GDPR anyway. Consequently, with knowledge of behavioral economics and biases, the companies can take even more advantage of their consumers.

However, the GDPR has set standards and limitations on how companies collect, process and use personal information. Giving the consumers the opportunity to have more control over their data and ensuring that companies use their data only for the intended purposes. The GDPR has also made companies more accountable for their actions with sanctions if they do not follow the regulations. Additionally, the GDPR has increased transparency to make it easier for consumers to understand how their data is being used.

Although the literature and the model suggest that consumers do not always act rationally when presented with privacy protection choices, even if they state that they wish to protect their data, one can argue that regulations have been effective in setting restrictions on how companies handle the data they collect from users. However, one could also argue that there should be more regulations on how the interaction between companies and consumers are handled, as there still are many individuals who are not seemingly aware of privacy risks or choose to not take any action to protect their privacy.

Despite this, some of the literature state that the individual's choice does not really matter. The paper in 4.2.3 states that even when the individuals opt out there is still cookie tracking. Information externalities are also mentioned in a few of the papers and is the main operator in 4.1.3. With the help of big data and AI algorithms the companies can use the information they get from the individuals that do consent to sharing their data and help predict information about the other consumers by finding patterns in their behavior. This makes it less useful for the privacy concerned consumers to reject, since the companies can still find a reasonable amount of information on them.

All the papers do in some way, or another, conclude with similar remarks, that the regulations seemingly have not had any or only a small effect on consumers behavior. The model in chapter 5 also demonstrates similar results. However, as I have discussed in this chapter, the consumers are not the targets of the GDPR. The regulations are there to protect the consumers, although it applies to the companies. Nevertheless, based on the presented findings, one could question if the GDPR has accomplished its purpose, since there seems like there is little to no change in the data being shared. One explanation, which makes the regulations counterintuitive, is that the GDPR is perceived as too comfortable a safety net that consumers do not feel they need to do anything themselves to protect their own personal data, and therefore do not care to act on their rights.

# 7 Conclusion and Summary

In summary, this thesis aims to address and answer the research question of how privacy regulations, particularly the GDPR, have affected consumer behavior in the online markets.

Since the regulations are still relatively new, there is little research on the matter and difficult to see the total effect. Therefore, the thesis has taken a more behavioral economics approach to the question.

I have found that there is some impact on people's behavior. The privacy seeking consumers are the winners of these regulations, but for the regular consumer the web experience is quite similar as before. I have also discussed what effect the design of cookie banners and pop-ups have on the users and discussed different biases, such as, optimism bias, present bias and status quo bias. Self-control bias, immediate gratification and overconfidence has also been mentioned and discussed briefly. Further, the main biases have been illustrated to see how they can affect consumers choices and perception of privacy risk. It can be interpreted from the analysis that legislators have a difficult task in helping people to choose to protect their personal information, because of the privacy paradox.

To conclude, there are many factors that contribute to consumer behavior in the online markets. The implementation of privacy regulations such as the GDPR may not have had an immense effect on regular consumers' behavior, as humans are not always rational creatures. Behavioral aspects may explain why people still share personal information online. The privacy paradox suggests that many individuals claim to be concerned about their privacy, but do not act accordingly when presented with a choice to protect it. Furthermore, companies (as explained by the literature) still create quite specific profiles on consumers with minimal data, rendering the choice to opt out irrelevant.

Finally, it is important to mention that the GDPR primarily regulates the company side of websites, while its visible impact on consumer behavior remains limited, privacy regulations are still important and give the consumer more ownership and rights to see what the companies do with their data. With that said, I believe there is still room for improvement, especially with

more regulation of how cookie consent banners are designed and how to avoid nudging, to give the consumer a more equitable choice.

If the legislators were to enact additional regulations concerning the design of cookie banners, such as implementing a standardized design everyone must follow, it could prevent nudging. However, this could pose challenges as different companies may have divergent interpretations in this regard. Furthermore, an area of improvement could be in enhancing the accessibility of "terms and services" by implementing regulations that require them to be easier to understand to the average consumer.

Ultimately, an underlying question arises as to the distribution of responsibility between legislators and consumers. As personal information sharing and protection are matters of individual's choice, there is a limit to what legislators can do before intervening upon consumers' freedom of choice.

# 8 References


Acquisti, A. (2004). *Privacy in electronic commerce and the economics of immediate gratification* https://dx.doi.org/10.1145/988772.988777

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., Wang, Y., & Wilson, S. (2018). Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online. *ACM Computing Surveys*, *50*(3), 1-41. https://doi.org/10.1145/3054926

Acquisti, A., & Grossklags, J. (2007). What Can Behavioral Economics Teach Us about Privacy? In (pp. 385-400). Auerbach Publications. https://doi.org/10.1201/9781420052183-29

Acquisti, A., Taylor, C., & Wagman, L. (2016). The Economics of Privacy. *Journal of Economic Literature*, *54*(2), 442-492. https://doi.org/10.1257/jel.54.2.442

Argenziano, R., & Bonatti, A. (2021). Data linkages and privacy regulations. *Researchgate*, 53.

Aridor, G., Che, Y.-K., & Salz, T. (2020). *The economic consequences of data privacy regulation: Empirical evidence from GDPR*. National Bureau of Economic Research.

Choi, J. P., Jeon, D.-S., & Kim, B.-C. (2019). Privacy and personal data collection with information externalities. *Journal of Public Economics*, *173*, 113-124. https://doi.org/10.1016/j.jpubeco.2019.02.001

European Commission. (2022). *What is personal data?* Retrieved november 2022 from https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en

European Commission. (2023). *Who does the data protection law apply to?* Retrieved april 2023 from https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/who-does-data-protection-law-apply_en

Eurostat. (2023a). *Privacy and protection of personal data (2020 onwards)* Eurostat. https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PRV20__custom_5757034/default/table?lang=en

Eurostat. (2023b). *Privacy and protection of personal information (until 2016)* Eurostat. https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_PRV__custom_5757022/default/table?lang=en

Eurostat. (2023c). *Trust, security and privacy - Smartphones (2018)* Eurostat. https://ec.europa.eu/eurostat/databrowser/view/isoc_cisci_sp/default/table?lang=en

Eurostat. (2023d). *Trust, security and privacy - Smartphones (2020 onwards)* Eurostat. https://ec.europa.eu/eurostat/databrowser/view/ISOC_CISCI_SP20__custom_5388206/default/table?lang=en

GDPRSummary. (2022). *GDPR Summary*. Retrieved november 2022 from https://www.gdprsummary.com/gdpr-summary/

Gerber, N., Gerber, P., & Volkamer, M. (2018). Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behavior. *Computers & Security*, *77*, 226-261. https://doi.org/https://doi.org/10.1016/j.cose.2018.04.002.

Goldberg, S., Johnson, G., & Shriver, S. (2019). Regulating privacy online: The early impact of the GDPR on European web traffic & e-commerce outcomes. *Available at SSRN*, *3421731*.

Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis Of Decision Under Risk. *Econometrica*, *47*(2), 263-292. https://doi.org/https://doi.org/10.2307/1914185

Kenton, W. (2022). *Externality: What it means in economics, with positive and negative examples*. Retrieved november 2022 from https://www.investopedia.com/terms/e/externality.asp

Khurana, A. (2019, 08/16/2019). *Doing E-Commerce Communication Right*. liveaboutdotcom. Retrieved may 16 from https://www.liveabout.com/how-to-do-ecommerce-communication-right-1141640

Lynskey, O. (2016). *The foundations of EU data protection law*. Oxford University Press.

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P., Balzarotti, D., Bilge, L., Vervier, P.-A., & Santos, I. (2019). Can I Opt Out Yet? https://doi.org/10.1145/3321705.3329806

Spiekermann, S., Grossklags, J., & Berendt, B. (2001, 2001). *E-privacy in 2nd generation E-commerce* ACM conference on Electronic Commerce, https://dx.doi.org/10.1145/501158.501163

Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness.* Yale University Press.

The World Bank. (2023). *Difference-in-Difference*. Retrieved may 28 from https://dimewiki.worldbank.org/Difference-in-Differences

Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019, 2019). *(Un)informed Consent: Studying GDPR Consent Notices in the Filed* ACM SIGSAC Conference on Computer

and Communications Security, London, United Kingdom. https://dx.doi.org/10.1145/3319535.3354212

Wikipedia. (2023a, 05/08/2023). *Dark pattern*. wikipedia.org. Retrieved may 15 from https://en.wikipedia.org/wiki/Dark_pattern

Wikipedia. (2023b, 03/16/2023). *P3P*. wikipedia.org. Retrieved may 2 from https://en.wikipedia.org/wiki/P3P

Wolford, B. (2023). *What is GDPR, the EU's new data protection law?* Retrieved march 2023 from https://gdpr.eu/what-is-gdpr/

# Appendix

## *A: Calculation of Function (4)-(7) from the Model*

$$\min_{wrt\ x} DU_0 = \beta\left[\left(E\left(c_{s,p}\right)\delta^s x\right) + \left(E\left(c_{s+n,i}\right)\delta^{s+n}(1-x)\right)\right] \quad (4)$$

$$x = 1 : \min_{wrt\ x} DU_0 = 0.5\left[(5 * 1 * 1) + \left(10 * 1 * (1-1)\right)\right]$$

$$\min_{wrt\ x} DU_0 = 0.5[5 + 0]$$

$$\min_{wrt\ x} DU_0 = 2.5$$

$$x = 0 : \min_{wrt\ x} DU_0 = 0.5\left[(5 * 1 * 0) + \left(10 * 1 * (1-0)\right)\right]$$

$$\min_{wrt\ x} DU_0 = 0.5[0 + 10]$$

$$\min_{wrt\ x} DU_0 = 5$$

$$E\left(c_{s,p}\right)\delta^s < E\left(c_{s+n,i}\right)\delta^{s+n} \quad (5)$$

$$5 * 1 \ < 10 * 1$$

$$5 < 10$$

$$\min_{wrt\ x} DU_s = \delta\left[E\left(c_{s,p}\right)x + \beta E\left(c_{n,i}\right)\delta^n(1-x)\right] \quad (6)$$

$$x = 1 : \min_{wrt\ x} DU_s = 1[5 * 1 + 0.5 * 10 * 0.5(1-1)]$$

$$\min_{wrt\ x} DU_s = 1[5 + 0]$$

$$\min_{wrt\ x} DU_s = 5$$

$$x = 0 : \min_{wrt\ x} DU_s = 1[5 * 0 + 0.5 * 10 * 0.5(1-0)]$$

$$\min_{wrt\ x} DU_s = 1[0 + 2.5]$$

$$\min_{wrt\ x} DU_s = 2.5$$

$$\delta E\left(c_{s,p}\right) > \ \beta E\left(c_{n,i}\right)\delta^n \quad (7)$$

$$1 * 5 > 0.5 * 10 * 0.5$$

$$5 > 2.5$$