STOCKHOLM SCHOOL OF ECONOMICS
Department of Economics
5350 Master's thesis in economics
Academic year 2016–2017

THE PRIVACY PARADOX
ON ITS EXISTENCE AND COMPETING EXPLANATIONS

Bensam Solomon (22959)

Abstract: The privacy paradox is the observation that people's concern about protecting their personal information does not match their behavior in their willingness to divulge said information. Acquisti (2004) explains this dynamic inconsistency using a model where agents exhibit immediate gratification bias. In the literature, a consensus has developed around this preference-based explanation. Recently, Cofone (2015) presented a competing explanation that goes against the consensus that cognitive biases are the cause of the paradox. He argues that dynamically inconsistent behavior is rational in situations of uncertainty. While both a preference-based and uncertainty-based explanation predict the same behavior they have different implications for policy. The former would lend support to a more paternalistic policy approach, that limits data subjects' choice sets. Conversely, the latter promotes policy that gives citizens flexibility, but provides tools to deal with potential privacy violations ex-post. Being able to contribute to the academic literature and policy debate motivates this study's research question: *If the privacy paradox exists is a preference-based or an uncertainty-based explanation a better solution for it?* To answer the question, an experiment on 132 high school students was conducted. The results of this study provide evidence against the existence of the privacy paradox. This precludes us from testing the relative strengths of the two explanations.

Keywords: privacy, privacy paradox, dynamic inconsistency

JEL: D12, C91

Supervisor: Chloé LeCoq
Date submitted: May 15, 2017
Date examined: May 30, 2017
Discussant: Sebastian Dypbukt Källman
Examiner: Mark Sanctuary

Acknowledgements

I am thankful to my supervisor, Chloé LeCoq, for the interesting conversations, helpful comments and encouragement throughout the process. I am grateful to my classmates who were always willing to read my drafts and provide constructive feedback. Heartfelt thanks to the teachers at the International School of Stockholm Region (ISSR), Lars, Maria, Clara and Karl, who were kind enough to give part of their class for me to run my experiments. Thanks to the students at ISSR for their patience and willingness to take time to take participate in my experiment. I am immensely grateful to Professor MacCarthy for sparking my interest in privacy. A special thanks to Sona, for the insightful feedback, constant support and encouragement.

Table of Contents

1. Introduction

The advent of social media, the ubiquity of internet-connected devices, and advances in data analysis have heralded the age of Big Data. Big Data marks the confluence of three factors: the unprecedented massive scale collection of personal data from a myriad of sources, the ever declining cost of storing the data, and the advance in analytic tools that allow the making of useful inferences and predictions (The Federal Trade Comission, 2016). The benefits these developments have brought, from lower search costs and personalized services to breakthroughs in medicine and social planning are many (McAfee, et al., 2012). However, people have grown increasingly uneasy with the amount of personal information governments, organizations and corporations have access to and the risks to which this exposes them (Boyles, et al., 2012). A recent report by the Federal Trade Commission (FTC), the US agency tasked with privacy protection, outlines what these risks might be and the ways in which the current policy framework fails to adequately protect the interests of data subjects, i.e. the person or entity to whom the personal data relates (see (The Federal Trade Comission, 2016))

Part of this concern is driven by the uncertainty related to the threat of privacy violations. Acquisti (2010) identifies four types of potential costs from privacy violations. Immediate but intangible costs, such as the psychological discomfort from the feeling of being observed; immediate and tangible costs, for example improved price discrimination that lowers consumer surplus; indirect costs, namely behavioral targeting that exploits weaknesses (e.g. an addiction) and probabilistic costs, e.g. database breaches that may lead to identity theft. Acquisti (2010) finds that because of the uncertainty associated with and intangible nature of many costs, it has been difficult to estimate the cost of privacy violations at the individual level.

In light of these trends, researchers and observers alike have puzzled at people's continued willingness to share their personal information in various contexts in a way that seems at odds with their stated intentions. Several empirical studies have found evidence that participants' privacy concerns do not seem to predict their behavior, i.e. their willingness to disclose personal information (Spiekermann, et al., 2001; Norberg, et al., 2007). The *privacy paradox* was coined to describe this inconsistency (Brown, 2001). There is no consensus in the literature as to the existence of the paradox, with some empirical evidence against it (Tsai, et al., 2011; Wakefield, 2013). However, among those who maintain its existence, there had been a consensus as to the cause: cognitive biases. Acquisti (2004) presents the most sophisticated explanation based on

present bias (henceforth a *preference-based* explanation). An agent is said to exhibit present bias if they tend to overweight payoffs today relative payoffs in the future more than accounting for the time value of money would imply (Laibson, 1997). This leads to dynamically inconsistent behavior. In other words, in situations where the benefits from revealing personal information are imminent and the costs, i.e. a potential privacy violation, are delayed, a person who exhibits present bias might overweight the benefits and underweight the costs and divulge their personal information. In so doing, the person may act inconsistently with their previously stated intentions.

Recently, a competing, *uncertainty-based,* explanation for the privacy paradox has emereged. Sozou (1998) and Azfar (1999) independently show that with high levels of uncertainty, it is rational to be dynamically inconsistent. Cofone (2015) argues that this might be the case in privacy as well, that the privacy paradox might be rational due to the high uncertainty the privacy decision-making process entails. While both explanations, *preference* and *uncertainty-based,* predict the same behavior, they have different policy implications. The former would lend support to a paternalistic approach to privacy regulations. The latter would favor policies that give data subjects the support and flexibility to deal with uncertainty.

Up until now, these two competing explanations have not been empirically tested. The aim of this thesis is to address this. The research question of this this thesis is then: *If the privacy paradox exists is a preference-based or an uncertainty-based explanation a better solution for it?* The intended contribution of this thesis is threefold. Firstly, to provide further evidence for or against the existence of a privacy paradox. Secondly, this thesis presents, for the first time, an empirical test of two competing explanations for the paradox. Finally, this thesis intends to contribute to privacy policy by providing an economic foundation for understanding data subjects' privacy decisionmaking. Depending on whether datasubjects are behaving dynamically inconsistently or not, whether they are behaving rationally or not, the appropiate approach to policymaking varies significantly.

The rest of the paper is organized as follows. Section 2 provides a brief background of the history of privacy and an overview of privacy regulations in the EU and the US. Section 3 surveys the economic literature on privacy, with a focus on the privacy paradox. Section 4 details the method, including research design, of this study. Section 5 presents the results of the experiment. Section 6 discusses the results, and section 7 concludes.

2. Background

Privacy is multi-faceted and context-dependent. Some define it as the right to seclusion. Others would say it is the concealment of (potentially) socially useful information (Posner, 1977). A third widely-held view is that it is the fundament to human autonomy, individuality and integrity (Solove, 2002). To add to the complexity, it is a *highly contextual phenomenon* (Morando, et al., 2014). We expect different levels of privacy depending on where we are, who we are with and what we are doing. This applies within a culture but, even more so, across cultures (Whitman, 2004). Nonetheless, for the purposes of a purely economic analysis, that will be undertaken in this thesis, some of the complexity must be shed in favor of a narrow and operational concept that can more readily be applied.

Privacy, in its modern form, emerged as a distinct concept towards the end of the 19th century. In their seminal article, Samuel Warren, a prominent lawyer, and Louis Brandeis, lawyer and later Associate Justice of the Supreme Court of the US, outlined what they termed the "right to privacy" (Warren & Brandeis, 1890). Up until that point in history, this right was a subset of the right to private property. This was sufficient protection, as up until then, since any intrusion into a person's voluntary seclusion would have required trespassing on their private property. Technological developments at the time, namely affordable photo cameras, however, allowed for privacy intrusions without intruding on private property (Glancy, 1979). It was as a result that privacy emerged as a separate legal concept. Since then, the development of the concept of privacy, and the policies that protect it, have been inextricably linked to the development of technology (Wittes, 2011).

2.1 Privacy Policy in the Age of Big Data

One of the aims of this thesis is to contribute to the privacy policy debate. In order to do so, it is useful to understand the evolution and current state of privacy regulations in the EU and the US. The focus on these two jurisdictions is due to the fact that they have the most developed policy framework, and consequently receive most of the attention in the literature. Furthermore, they are similar enough to enable comparison, but different enough to justify juxtaposition. Just as the development of privacy as a concept has been inextricably linked to technology, so has government policy on privacy in the EU and the US. The advent of mainframe computing, in the mid 1960s, gave governments and businesses an unprecedented ability to collect and process data. This stoked fears among citizens of potential abuses of the system, and highlighted the lack of statutory protection of informational privacy. To address the dearth of a comprehensive

regulation, in the early 1970s, the Fair Information Practices (FIPs) were developed (Gellman, 2016). The FIPs are a set of principles that outline the best practices of handling personal information Though they have been codified in various ways, the most well-known version is the OECD's 1980 "Privacy Guidelines" (OECD, 2011, pp. 21-22). At the core of the framework is the principle of informed consent. The FIPs would underpin the wave of privacy laws that would come to be passed across Europe and in the US, e.g. the 1973 *Data Act* in Sweden, that would represent the first statutory protection of privacy (OECD, 2011).[1]

By the mid- to late 2000s, with the ubiquity of internet-connected devices, the advent of social media and other developments heralded the age of Big Data – technology once again tested the limits of regulation. Big Data is marked by the confluence of three factors: the unprecedented massive scale collection of personal data from a myriad of sources, the ever declining cost of storing the data and the analytic tools that allow the making of accurate inferences and predictions (The Federal Trade Comission, 2016). In principle, the FIPs require informed consent for every time data is collected and used (i.e. consent for each time it is used in a way that was not specifically consented to previously), while mandating full transparency throughout. This is at odds with the multi-use, data-hungry nature of Big Data-driven technologies such as social media. While it goes without saying that it has many potential benefits, the risks are also many. In a report, the Federal Trade Commission (FTC), the US agency tasked with privacy protection, outlines what these risks might be and the ways in which the current policy framework based on the FIPs fails to adequately protect the interests of data subjects (see Federal Trade Comission, The, 2016).

2.1.1 Comparative Privacy Policy: Pre-commitment vs. Flexibility

In the EU and the US respectively, policymakers have reacted to these new risks and the deficiencies in existing policies in different ways. The EU has stuck with the rights-based approach and further strengthened data subjects' protections under the FIP framework (MacCarthy, 2010; Gellman, 2016). Firms are precluded from certain kinds of practices, e.g. some forms of targeted advertising, price discrimination, even though in certain cases they might be beneficial to consumers overall, or at least to the most sophisticated among them (Goldfarb & Tucker, 2011). This can be due either to direct legislative ban or the indirect result

[1] The FIPs can be blamed for the hundreds-of-pages long terms of services people have to read (but seldom do) and agree to when sharing their personal information. And it is no surprises that no one reads them. One estimate puts the opportunity cost of reading them in the range of a quarter of a trillion dollars in the US alone (McDonald & Cranor, 2008).

of onerous costs disproportionately borne by firms. In practice, this amounts to restricting citizens' choice set to only those choices that are deemed to be safe enough.

Conversely, the same developments have pushed US regulators to increasingly favor a more utilitarian rather than a rights-based approach. The FIPs and the rights-based approach remain an important part of US privacy statutory policy. In practice, however, the FTC has moved towards a more flexible approach based on insights from economics (Beales & Muris, 2008). In their article, Beales, former director of the Bureau of Consumer Protection at the FTC, and Muris, former chairman of the FTC, argue that in dealing with the current privacy threats, FIPs are inadequate to protect consumers from the novel threats that have emerged. An example of a new threat, not addressed by the traditional FIPs, is that of negative privacy externalities, "where one person's decision to share information can adversely affect others who choose to remain silent" (MacCarthy, 2010, p. 3). Modern algorithms can be used to estimate personal information of an individual by using the personal information that others who are adjacent to that person, whether physically or virtually, have chosen to make available about themselves (for examples, see MacCarthy, 2010). FIPs cannot protect against this, as, at all times, only those who consented have shared their personal information, but this may result in harm for those who have not nonetheless. And, indeed, Beales and Buris argue that protecting data subjects from harm is more important than giving them consent over each use of their personal information. Their approach to policy does this by letting market forces shape privacy protections while protecting consumers from harm through strong tools for redress in the event of a harm. Consequently, instead of restricting the choice set, the approach gives consumers the ability to act freely, supplemented by tools to redress any unintended consequences. This is not to say that this approach is superior to the EU approach on all points. Freedom and flexibility come at the cost of robust protections, and there are cracks in the system that can be exploited. Carl Bennet, the political philosopher, argues that "the approach to making privacy policy in the US is reactive rather than anticipatory, incremental rather than comprehensive and fragmented rather than coherent. There may be a lot of laws but there is not much protection" (Solove, 2004, p. 71).

In summary, though both the EU and the US privacy regulations are built on the bedrock of the FIPs, recent developments have led to a divergence in their respective approaches to regulation. The EU has tended to double down providing what, in this thesis, will be called *pre-commitment technology*. Conversely, US policy has favored the provision of what will be called

flexibility technology in this thesis. Pre-commitment technology refers to the restriction of a data subject's choice set to pre-empt harm. Pre-commitment technology can be a policy, or a market product or service, that allows an individual to restrict his or her choice set now and at any point in the future. For example, most credit cards come with the functionality allowing the holder to restrict how and where the card can be used if the user has concerns about the risk of privacy violations in certain contexts, e.g. blocking the usage of the card online where there is a high risk of identity theft. The converse of pre-commitment technology is flexibility technology. This would allow someone to maintain as broad a choice set as possible now and at any point in the future. Thus, instead of a restriction on where a credit card might be used, one would be able to purchase insurance against identity theft. This keeps one's choice set as broad as possible, while providing a way to minimize the cost of potential privacy violations.

2.1.2 The Case for the Economics of Privacy

The question becomes then, which approach is best suited to deal with the novel challenges that we see today. As noted above, there are trade-offs for both. The EU's more paternalistic but rigid approach provides more robust protection, but has some significant flaws, e.g. weak protection against negative privacy externalities. On the other hand, the US approach is flexible enough to adapt to new challenges, but critics argue that the fragmented patchwork of laws and regulations is insufficient and provides inadequate protection in most cases. It is unlikely that any one approach will be better for both the EU and the US. Whitman (2004) argues that privacy policy differences reflect deep cultural differences between the EU and the US – privacy policy in the EU puts invididual dignity above all else, while US policy values liberty the most. Therefore, it is not wise to seek a one-size-fits all formula for optimal policy.

Regarldess of the optimal approach, it will have to be adapted to the cultural context, but there are some common elements to all policy making that economic analysis can contribute to. At the core of any policy is an, oftentimes implicit, assumption about how data subject's act. If people make decisions that do not optimize their own welfare (i.e. are prone to cognitive biases) or diminish social welfare, it would justify the pre-emptive restriction of their choice set. If, however, people do act rationally, maximizing their own welfare and not harming others, it would be hard to justify restricting their choice set. Rather, the optimal policy would be to provide them with tools to redress harms that might befall them from the actions of others. Thus, the view one takes or the assumption one makes about how people behave will determine what policy one adopts.

Here, economic analysis can contribute to a better understanding of the microfoundations of behavior in privacy-related contexts. Indeed, this is what has been lacking from privacy policymaking, according to James Cooper, former Deputy Director of the FTC, and Joshua Wright, current Commissioner at the FTC. In a chapter of a forthcoming book on privacy policy, Cooper and Wright (2017, Forthcoming, p. 2) bemoan the lack of an economic approach to privacy policy:

> *FTC reports are devoid of any economic analysis or empirical evidence, and instead are based almost solely on anecdotes and hypotheticals presented at workshops…It's not much of an exaggeration to say that privacy regulation today stands where antitrust regulation stood in the 1970s – rudderless and incoherent.*

This motivates the approach chosen by this thesis, and highlights the possible contributions to policy economics can make.

3. Literature Review

This section defines the scope of this thesis and surveys the economic literature on the privacy paradox. The first subsection gives an economic definition of privacy, including which specific aspects of privacy, that best matches the purposes of this study. The second extensively surveys the empirical literature on the privacy paradox, and the theoretical papers that present solutions to it. Finally, the third section concludes with intended contribution of this thesis.

3.1 Defining Privacy in Economics

Privacy is difficult to define precisely, as we discussed in the previous section. Acquisti, et al. (2016, p. 2) argue that "at its core, the economics of privacy concerns the trade-offs associated with the balancing of public and private spheres between individuals, organizations, and governments … primarily focused on [the] informational dimension." Although useful to set the boundaries of the field of privacy economics, this is an altogether too broad and imprecise definition to be useful as an operational one. For our purposes, a better definition is given by Jentzsch (2016, p. 33), "Privacy is … a relationship of asymmetric distribution of personal data between market players." The EU Data Protection Directive (European Union , 1995) defines personal data as:

> *Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.*

The economic argument for protecting privacy and the needs for privacy regulations is set forth in Posner's (1977) seminal paper on *The Right of Privacy*. Posner (1977, 1981) argued that society had no general interest in protecting privacy, which he defined as secrecy, as it could facilitate individuals gaining from the asymmetric distribution of information thereby reducing social welfare. Futhermore, to maximize economic efficiency, Posner (1977, p. 403) thought that the right to privacy should be restricted to "secret[s] that [are] a byproduct of socially productive activity…if [their] compelled disclosure would impair the incentives to engage in that activity." This was in contrast to the view of privacy at the time, and that continues to pervade certain strands of literature, that privacy was a fundamental right.

The literature distinguishes between three dimensions of privacy: *(i) territorial privacy*, i.e. protection of the physical area around a person, *(ii) privacy of person,* i.e. protection against undue interference, e.g. physical search *(iii) informational privacy*, i.e. control over the flow of personal information, e.g. how data is collected, stored and distributed (Rosenberg, 1992; Holvast, 1993; Kokolakis, 2017). In this thesis, the focus will be exclusively on informational privacy as this is what the privacy paradox relates to.

3.2 The Privacy Paradox

The *privacy paradox* was coined by Brown (2001) to denote the inconsistency between people's privacy concern or attitudes, on the one hand, and their privacy behavior, on the other hand (Norberg, et al., 2007). For example, Spikermann et al. (2001) conducted an experiment comparing participants' self-reported privacy preferences and their actual behavior in disclosing personal information, while shopping online, and found an inconsistency between the two. Participants were much more willing to disclose personal information online than their espoused preferences would have predicted. In response, some have argued that the privacy paradox does not exist. One reason might be that attitudes or concerns are expressed generically, while behaviors are specific and context-dependent (Fishbein & Azjen, 1975). Proponents of the, so-called, *privacy calculus* model, argue that data subjects frequently engage in the mental trade-offs of balancing privacy concerns and behaviors, through which they acquire an expertise in the exercise (Milberg, et al., 1995; Dinev & Hart, 2006). Consequently, data subjects will sometimes act to share their personal information and other times to protect it, according to what is optimal for the situation and context. Thus, they conclude that any inconsistency is an adaptation to the context a person finds themselves in rather than evidence of a paradox.

Empirical findings of specific inconsistency directly contradict these arguments against the existence of a privacy paradox. Initial evidence for the existence of a privacy paradox came from Spiekermann, et al. (2001), Acquisti & Grossklags (2005), and Norberg, et al. (2007). In a field experiment, Norberg, et al. (2007) elicited privacy intentions by asking subjects whether they would be willing to disclose certain types of personal information in different contexts, twelve weeks later a market researcher requested that information from subjects. Participants were willing to disclose more than their stated intentions. In Acquisti & Grossklags (2005), 89% of subjects said they were very or moderately concerned about protecting their privacy. However approximately a quarter then admitted that they had revealed their social security and/or phone numbers for discounts on services and goods. In the most complete study in this vein, Beresford, et al. (2012) conducted a field experiment that tested participants' willingness to disclose information for monetary reward. Subjects were asked to buy a DVD from two virtually identical, competing stores. To complete the purchase, one store, call it high privacy (HP) store, requested year of birth and favorite color; the other one, call it low privacy (LP) store, requested income and date of birth. When prices were the same, participants were equally likely to buy from each store. When the price was set 1 Euro lower in the LP store, the vast majority of subjects favored it versus the now more expensive HP store. The participants were asked to fill out a survey regarding privacy attitudes after the experiments, and three-quarters of them stated a strong interest in data protection and 95% indicated that they had a strong interest in protecting their personal information.

New technologies, such as social networking sites (SNSs), have received a great deal of attention in the literature on the privacy paradox. A number of survey-based studies find evidence of a privacy paradox. Tufekci (2008) surveys students' self-disclosure behavior in SNSs, and finds little to no relationship between stated privacy concerns and personal information disclosure behavior. A finding confirmed by similar studies (Reynolds, et al., 2011; Hughes-Roberts, 2013). Zafeiropoulou, et al. (2013) investigate attitudes and behavior regarding the protection of location data, a new type of personal information that is readily available due to the proliferation of mobile information technologies. Their survey show the existence of a privacy paradox. Finally, Oomen and Leenes (2008) find that privacy risk perception, i.e. the risk a person attaches to potential privacy violation, has little to no relation to the use of privacy enhancing technologies.

While there is substantial evidence that supports the existence of a privacy paradox, there are

also a number of studies whose findings suggests the contrary. In the context of commercial websites, Wakefield (2013) finds that trust perception, how trustworthy a website is perceived to be, is a determinant of consumer privacy behavior, i.e. disclosing personal information on the website. In a two-phased study, Tsai, et al. (2011) found that when websites make their privacy and security policy visible and easily accessible for consumers, consumers tend to prefer websites that have more robust protection. First, participants were surveyed to obtain their privacy concern while shopping online. In the second phase, the authors ran an experiment using a shopping search engine that clearly displayed privacy policy information. The authors find that individuals are willing to pay a premium for privacy when privacy information is made prominent and intuitive. Whereas many suggest that even privacy conscious consumers are unlikely to pay for online privacy (Shostack 2003) or give up rewards to protect their data (Spiekermann et al. 2001).

Similarly, counterevidence to the existence of a privacy paradox is found in the context of social networking sites (SNSs) and among younger participants. A number of studies find that SNSs users, especially young people, use a number of privacy protection strategies. Examples include providing false information (Miltgen & Peyrat-Guillard, 2014), adjusting privacy settings to restrict access to their profiles (Hargittai, 2010) and removing unwanted tags (Young & Quan-Haase, 2010). Son and Kim (2008) provide a taxonomy of Information Privacy-Protective Responses (IPPRs): (1) *refusal,* (2) *misrepresentation,* (3) *removal of information from database,* (4) *negative word of mouth,* (5) *complaints directed at online company,* and (6) *complaints directed at third-party organizations.* In a survey, they find a strong correlation between participants' privacy concerns and behaviors, as measured by use of IPPRs. Debatin, et al. (2009) survey 119 undergraduate students and find that participants' self-reported estimation of the benefits of using Facebook were higher than estimated cost that they associated with potential privacy violations. That is, the students acted in line with their concerns. Blank, et al. (2014) find that younger people are more likely to take privacy-protective measures online and especially on SNSs. They argue that the current view of a privacy paradox is no longer applicable to young people, as their privacy behavior tends to match their concerns.

3.2.1 Summary and Evaluation of Empirical Literature

In summary, there is no consensus in the literature as to the existence or non-existence of a privacy paradox. In trying to reconcile the diverging evidence, Kokolakis (2017) finds that potential causes can be grouped into one of two categories: the context-dependence of privacy

and methodological issues. The first category of issues is related to the context-dependence of privacy. There will be differences between privacy attitudes and behaviors in the context of e-commerce sites and SNSs. Similarly, whether a study is conducted in a place that a participant is previously familiar and feels safe in or not might influence results. Comparing for example the diverging results of Norberg, et al. (2007) and Tsai, et al. (2011) where the former was conducted in a classroom setting, where one might have been perceived by participants as being safer than the other. Furthermore, personal information is not one universal, uniform object, people will have different attitudes and behave differently based on the sensitivity of the information. In some contexts, age or weight might be more sensitive than height and vice versa (Huberman, et al., 2005).

In the second category, relating to methodological causes, we find a smilar litany of causes. Firstly, a large number of the studies in this field have been surveys, not optimal in order to measure actual behavior, as participants might misremember or even provide false information. Staddon, et al. (2013) compares survey responses of Google+ users with their actual behavior and finds that the accuracy of the surveys are quite low. Irregular or infrequent behaviors, e.g. changing privacy settings which would be of interest to privacy researchers, are especially difficult to estimate accurately (Staddon, et al., 2013). Thus, an experimental design would appear to be more appropriate. However, this still suffers from low external validity, due to the contextual nature of privacy discussed above (Morando, et al., 2014). Furthermore, there is no consistency in the literature as to whether privacy attitudes, concerns or intentions should be compared against privacy behavior in evaluating the privacy paradox. This makes comparison difficult, and a standardization on this end would make comparisons on the results end much easier.

A final significant methodological relates to the estimation and theoretical models that underpin the empirical analysis structure. Denlin and Trepte (2015) apply two different estimation models based on two different theoretical models in testing for the existence of the privacy paradox on the same sample and survey instrument. The application of the first method, a relatively straightforward regression analysis, supported the existence of a privacy paradox. Applying an alternative method, using structural equation modelling (SEM) analysis indicated that privacy concerns affected privacy behavior indirectly. This followed from a change in theoretical models, where the first approach was agnostic the second applied a theoretical model that differentiated between *informational*, *social* and *psychological* privacy. Thus, along with other

aspects of the methodology, Denlin and Trepte (2015) show how subtle differences in methodology, that are ostensibly minor and justifiable, can lead to researchers arriving at diametrically opposed conclusions.

3.2.2 Behavioral Economic Explanations: Hyperbolic Discounting

The privacy paradox has received much greater interest within the behavioral economic literature than other economic sub-disciplines. Consequently, a great deal of explanations for the privacy paradox are within the bounded rationality framework (Kokolakis, 2017). In their literature survey, Acquisti and Grossklags (2007) argue that in privacy decision-making situations, people are prone to cognitive biases and to the use of heuristics of which they identify six that are especially relevant: *optimism bias*, *overconfidence*, *affect bias, fuzzy-boundary benefit heuristics,* and *hyperbolic discounting.* While all these biases could be at play in explaining the privacy paradox, the most complete explanation and theoretical model for explaining the privacy paradox is based on hyperbolic discounting.

Hyperbolic discounting emerged as an explanation to another paradox, dynamic inconsistency in preference for monetary payoffs. An illustrative example is that when people were asked to state their preferences for two payoffs, e.g. $100 now or $110 four days from now, they preferred the former but, when those same payoffs were both moved forward a year, i.e. $100 a year from now or $110 a year and four days from now, the preferences were reversed (Thaler, 1981). The contemporary neo-classical model, exponential discounting, could not be used to explain the time inconsistent preferences. Laibson (1997) presented a discounting mechanism that could called hyperbolic discounting. Acquisti (2004) argues that this is the most salient explanation for the privacy paradox, what he calls the *immediate gratification bias.* He uses the following example to illustrate the point:

Consider the following individual utility function where $\delta \in [0,1]$ is the discounting factor and $\beta \in [0,1]$ is a parameter that captures time inconsistent preferences:

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

When $\beta = 1$, the agent has time consistent preferences, this is equivalent to the standard individual utility function with exponential discounting. Any value $\beta < 1$ indicates the agent has present or immediate gratification bias. With the extreme case being $\beta = 0$ where the individual cares only for her payoff today.

Acquisti (2004) argues that when participants complete a survey at time $t = 0$ about their privacy attitudes or concerns, they may consider the cost of protecting themselves at a later time, $t = s$, which they compare to the avoided cost of privacy intrusions in a more distant future, $t = s + n$. At time $t = 0$, the problem they face is given by:

$$\min_{wrt\ x} DU_0 = \beta\left[\left(E\left(c_{s,p}\right)\delta^s x\right) + \left(E\left(c_{s+n,i}\right)\delta^{s+n}(1-x)\right)\right] \tag{2}$$

The agent considers the expected cost of the privacy protection $E\left(c_{s,p}\right)$ and the expected cost of the privacy intrusion $E\left(c_{s+n,i}\right)$ and chooses a value of x, a dummy variable equal to 1 if the agent opts for the privacy protection and 0 otherwise, so that the expression in (2) is minimized. The individual will find it worthwhile to incur the cost $E\left(c_{s,p}\right)$ to protect themselves, if the following condition is met:

$$E\left(c_{s,p}\right)\delta^s < E\left(c_{s+n,i}\right)\delta^{s+n} \tag{3}$$

Now, consider the situation at time $t = s$ when the participant must obtain the protection and incur a cost in order to purchase it:

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

Comparing equation (4) and (2), the only thing that has changed is the passage of time. But at time $t = s$, the individual might choose to reverse from her optimal choice at time $t = 0$ and not incur the cost for privacy protection if the following condition is met:

$$\delta E\left(c_{s,p}\right) > \beta E\left(c_{n,i}\right)\delta^n \tag{5}$$

The inequalities in (5) and (3) can hold simultaneously for certain values of $\beta < 1$. Thus, if the agent exhibits immediate gratification bias, i.e. for certain betas smaller than one, they will reverse their choice and act in a way inconsistent with their previous choice. That is, they will no opt against obtaining the privacy protection. This can be extended through similar mathematical arguments in other privacy situations (see Acqusiti (2004) for more examples).

3.2.3 Neo-classical Economic Explanation: Exponential Discounting with Uncertainty

Little has been written in the non-behavioral economic literature on the privacy paradox. The neo-classical model assumes rational agents that maximize their utility by only disclosing information where the short term benefit is larger than the long term cost; in essence, dismissing the existence of a privacy paradox (Acquisti, 2004; Kokolakis, 2017). In a recent paper, Cofone (2015) claims that the privacy paradox is not necessarily at odds with the assumption of rationality. He bases his argument on Sozou (1998) and Azfar's (1999) refutation of Laibson's (1997) hyperbolic discounting model. Sozou (1998) and Azfar's (1999) both independently develop a mechanism that amends the (rational) exponential discounting model, augmenting the discount rate with hazard rate, that captures the risk fluctuations associated with the payment. The hazard rate is, in other words, a measure of the risk or uncertainty related to the payoff materializing at the appointed time, i.e. the payer defaulting. Uncertainty is defined as ambiguous or unquantifiable risk (Knight, 1921). They then show that when to the risk varies of the time period or there is uncertainty, exponential discounting with the inclusion of hazard rates predicts the same behavior and is all but indistinguishable from hyperbolic discounting. See Appendix I for a detailed derivation based on Sozou (1998).

An often cited example in the literature, is when the promise to pay is made by a newly started firm, i.e. a startup. The bankruptcy rate for newly started firms is very high in the first year; thus, payments promised during the first year are inherently riskier and it would be rational to have a preference for a smaller sooner payoff. After the first year, the risk of bankruptcy drops significantly to levels not significantly dissimilar from more mature firms. Hence, it would be rational to reverse preference from a smaller sooner payoff to a larger later one. In other words, it is rational to be dynamically inconsistent in this case, as the riskiness of the payment is declining. Similar arguments can be made for risk that increases over the period and for uncertainty (see Azfar, 1999; Casari, 2009).

As both hyperbolic discounting and the augmented exponential discounting model predict the same behavior, it is not easy to determine which is a better explanation for dynamic inconsistency. Casari (2009) uses an ingenious experimental design that tests the strengths of the competing explanations by testing their implications. He applies the design on dynamic inconsistency in monetary payoffs. That is, why individuals reverse their preference for a smaller now payoff ($100 now instead of $110 four days from now) to a larger later payoff ($110 in 1 year and four days instead of $100 days in 1 years' time). The first explanation is that the individual reverses her decision because she has immediate gratification bias, or present-biased preferences, he calls this a *preference-based* explanation. The competing explanation is an *uncertainty-based* one. This proposes that the reversal would be because of the implicit risk of default in future payoffs – this could be characterized by a declining hazard rate or other types of risk or uncertainty surrounding the situation in which the decision is made. As the observed behavior of the individual, choice reversal, is the same in both cases, the experiment is designed to test the implication of the two hypotheses instead. Casari argues that if *preference-based* explanation holds, assuming a sophisticated portion of the population that is aware of their immediate gratification bias, there will be demand for technology that would allow them to restrict their future choice set now. That is, to pre-commit to the decision that maximizes their long term utility, i.e. *pre-commitment technology*. Conversely, if an *uncertainty-based* explanation holds agents would not demand pre-commitment technology at all. Rather, they maximize their utility by having as broad a choice set as possible at all times in the future, as the main problem they face is the uncertainty of outcomes and not self-control. Thus, they should be willing to pay for *flexibility*.

In a multi-stage experiment, Casari first elicits the "impatience horizon", the time when participants' preferences reverse from smaller-now reward to the larger-later payoff to eliminate the effect of impatience from behavior. The impatience horizon was at most 15 days for the participants who initially preferred the smaller sooner reward. He then fixes the time to payoff, i.e. the time that would elapse between making a decision and receiving a payoff, at beyond the impatience horizon. Thereby, eliminating the effect of present bias. Participants were then placed in treatments variously making pre-commitment and flexibility costly to estimate the existence and strength of demand for either. The results of the experiment support the preference-based explanation, as there was strong demand for pre-commitment technology with little to no demand for flexibility.

3.3 Intended Contribution and Implications

This thesis adapts the research design above to the question of privacy. Cofone (2015) argues that this method would be well adapted to test the competing explanations of the privacy paradox (the uncertainty-based one, that he proposes, and, the consensus view, preference-based one). He does not conduct the experiment for privacy himself but rather leaves it as suggestion for future research, that this study will now follow through on.

The intended contribution of this thesis is threefold. Firstly, to provide further evidence for or against the existence of a privacy paradox. Secondly, this thesis presents, for the first time, an empirical test of two competing explanations for the paradox. Finally, this thesis intends to contribute to privacy policy by providing an economic foundation for understanding data subjects' privacy decisionmaking. Depending on whether datasubjects are behaving dynamically inconsistently or not, whether they are behaving rationally or not, the appropiate approach to policymaking varies significantly.

4. Method

This section outlines the research method. The first subsection provides the intuition behind the research design, building on the exposition in the section above. The second details the experimental setup. The third, and final, subsection sets out the experimental hypotheses and expected outcomes.

4.1 Briefly on the Intuition: Preference versus Uncertainty

This section builds on the mathematical example in section 3.2.1, which is not repeated here for the sake of brevity. Consider first if the privacy paradox is best explained by a preference-based explanation. Then, we would expect the individual, assuming she is aware of her immediate gratification bias, would seeks to address it. Then at time $t = 0$ she would be willing to incur some cost to restrict her choice set and pre-commit to obtaining the privacy protection at a later time $t = s$, when she knows her immediate gratification bias will lead her to making a suboptimal decision. The ability to pre-order the privacy protection is a pre-commitment technology, and a demand for such technology indicates the validity of a preference based explanation.

Conversely, let us consider the case if an uncertainty based explanation is the better fit. Let us simplify and specify that in the model above, we would have an agent without biased preferences, i.e. $\beta = 1$. A similar argument can be made for $\beta < 1$, but this simplification allows us to focus only on the effect of uncertainty. Acquisti (2010) uses the metaphor of a "blank check" to explain the uncertainty associated with disclosing personal information. Divulging personal information is like an individual writing a blank check, that might, or might not, come back with a certain price on it. Acquisti (2010, p. 15) argues that the price "could be a mild embarrassment… or a devastating case of identity theft". In short, the probability of a privacy violation is in Knight's (1921) terms, ambiguous and, up to a point, unknown, i.e. there is uncertainty. This would lead to the agent being unable to estimate the expected value of the disutility from future invasions of privacy with any degree of accuracy. If this is the case, we would expect the agent to disfavor any form of pre-commitment technology, but show a demand for technology that would minimize the cost of having the broadest possible choice set at every moment in the future. In this way, the agent maximizes her utility by being able to update her utility calculations with new information at every given moment in the time. An example from the real word of such a technology is the so called "right to be forgotten". In a landmark ruling, the European Court of Justice (2014) established the right for individuals to request data processors, in the case in question Google, to remove information about them from their databases. The Court ruled that "even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where … the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed" (European Court of Justice, 2014, p. 3). That is, a data subject has the ability to undo the unintended consequences of disclosing their personal information.

In the experiment, the behavior of participants is compared as alternatively pre-commitment and flexibility technology are costly. A control group where both are costless constitutes the baseline. In this way, we can test which has the stronger demand among participants. We also survey participants' privacy concerns and compare them to their privacy behavior in order to test for the existence of a privacy paradox. A pre-condition for being able to test the competing explanations.

	Demand for pre-commitment technology	Demand for flexibility technology
Preference-based explanation	Yes (some demand) (demand from sophisticated agents aware of present bias)	No
Uncertainty-based explanation	No	Yes (strong demand)

Figure 1 Demand for Technologies Predicted by the Competing Explanations of the Privacy Paradox

The figure above summarizes the intuition from this section, and the predictions of each explanation on the left hand side panel) for the demand for pre-commitment technology and flexibility

4.2 Research Design

The experiment was conducted on a sample of students from one high school in central Stockholm. The experiment was conducted in a classroom setting, and students were randomly assigned to one of three groups, the two treatment groups and the one control group. The first session of the experiment, in which all participants participated, took place in the classroom. Depending on the choice they made in the first session, some participants participated in a second session via email. The second session was 14 days after the first, or roughly the length of the maximum impatience horizon that Casari (2009) found for monetary payoffs.[2] In this way, we avoid the effect of immediate gratification bias in the first session. To comply with relevant regulations, participants were 15 years or older.

[2] Ideally, the second session would have been later to completely eliminate the effects of present bias. However, this was not practical for two reasons. The experiment was conducted towards the end of the school year, when more and more students left school or were more likely to be absent. Secondly, it was initially planned that the second session would be in the class room setting as well. Therefore, it made sense to have it fall exactly two or three weeks after the first, and since three weeks was too long, 2 weeks was chosen.

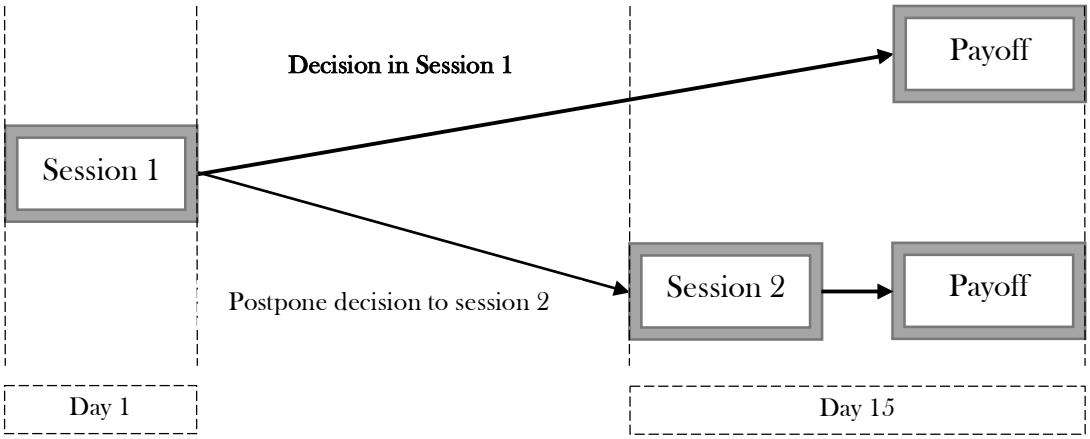

Figure 2 Experiment Design: Sequence and Timing of Sessions

In the first session, the experimenter administered a survey that consisted of three blocks: two components that were mutual to all treatment groups and one that varied across treatment groups. The first block of the survey asked for demographical information: age, gender, name and e-mail address. Name and e-mail were requested for the purpose of reaching out to those students who would choose to participate in the second phase, and the winners of the gift cards. Participants were informed that participation is voluntary and anonymous.

The second block of the survey elicited participants' privacy concerns by using the *concern for information privacy* instrument developed by Smith, et al. (1996). Originally 15 statements in 4 subscales: *collection, errors, unauthorized secondary use* and *improper access*. Participants state their agreement with the statements on a 7-point Likert scale; all statements are worded positively. It is considered one of the best and most influential instruments in measuring privacy concern, and is widely used in privacy research in general (Preibusch, 2013). To aid comparability, and in line with best-practice in the literature, the questions were unaltered from the original. However, one subscale, namely *errors*, was omitted for two reasons. First, to maintain the survey short, thereby increasing participation in the survey, avoiding fatigue and minimizing straight-lining. Straight-lining is especially a risk in this case as the instrument does not have any reverse-coded questions. Second, it was strictly recommended not to reduce the number of statements per subscale, but rather eliminate a subscale (at most) if necessary, as the *errors* subscale was the least relevant for the purposes of this study it was chosen to be eliminated.

The final block was the experimental component. The participants were placed into one of three groups: control, treatment one (pre-commitment) and treatment two (flexibility). The

details of the treatment groups are given below. Note that the order of privacy concern blocks and this last block was randomized, so that half of the participants answered the experiment-relevant questions first and vice versa. See Appendix II for the details of the administered survey.

Control: Participants were asked to choose between two gift cards[3] of two different values, 100SEK and 115SEK. To receive the latter gift card (115SEK), the participant would have to disclose some personal information (current home address) while the former requires no similar concession of personal information (name of your favorite city). Across treatments the higher value gift card required the participant to disclose their current home address (henceforth "no privacy gift card") while the other only required the participants to state their favorite city (henceforth "privacy gift card"). Participants were asked to choose between the two gift cards or postpone the decision fourteen days, i.e. the same day the gift card would be delivered. The decision to postpone is costless in the control group. That is, if a participant chose to postpone the decision they would have the same choice fourteen days from that date, i.e. 100SEK (privacy gift card) or 115SEK (no privacy gift card). This is the baseline against which the other two treatment groups are measured. Across treatments participants were reminded that the gift card is to be delivered in fourteen days' time from the first session (electronically), regardless of the choice they make regarding the type of gift card they choose and when they make the decision.

Treatment 1: In this treatment, participants got a similar choice set, but now pre-commitment was costly. In the first session, participants could choose between a gift card of value 90SEK (privacy gift card), one worth 115SEK (no privacy gift card) or postpone the decision. If they chose to postpone their choice, in fourteen days' time, they received an email asking them to choose between one of two gift cards: 100SEK (privacy) or 115SEK (no privacy). Participants were informed already in the first session that pre-commitment is costly, i.e. participants were informed that the privacy gift card would be worth 100SEK, 10SEK more, if they choose to postpone, with no change in the value of the other gift card. The difference between the proportion of participants who prefer to choose in the first session in T2 compared to the proportion who do so in the control group is a measure of the willingness to pay for pre-commitment (WTPC).

[3] Due to budgetary constraints, each participant did not receive a gift card. Rather, five participants were randomly selected to receive one. The participants were informed of this in the instructions (see Appendix II)

Treatment 2: In this treatment, participants got a similar choice set, but now flexibility was costly. In the first session, participants could choose between a gift card of value 100SEK (privacy gift card), one worth 115SEK (no privacy gift card) or postpone the decision. If they chose to postpone their choice, in fourteen days' time, they received an email asking them to choose between one of two gift cards: 90SEK (privacy) or 115SEK (no privacy). Participants were informed already in the first session that flexibility is costly, i.e. participants were informed that the privacy gift card would be worth 90SEK, 10SEK less, if they choose to postpone, with no change in the value of the other gift card. The difference between the proportion of participants who prefer to choose in the second session in T2 compared to the proportion who do so in the control group is a measure of the willingness to pay for flexibility (WTPF).

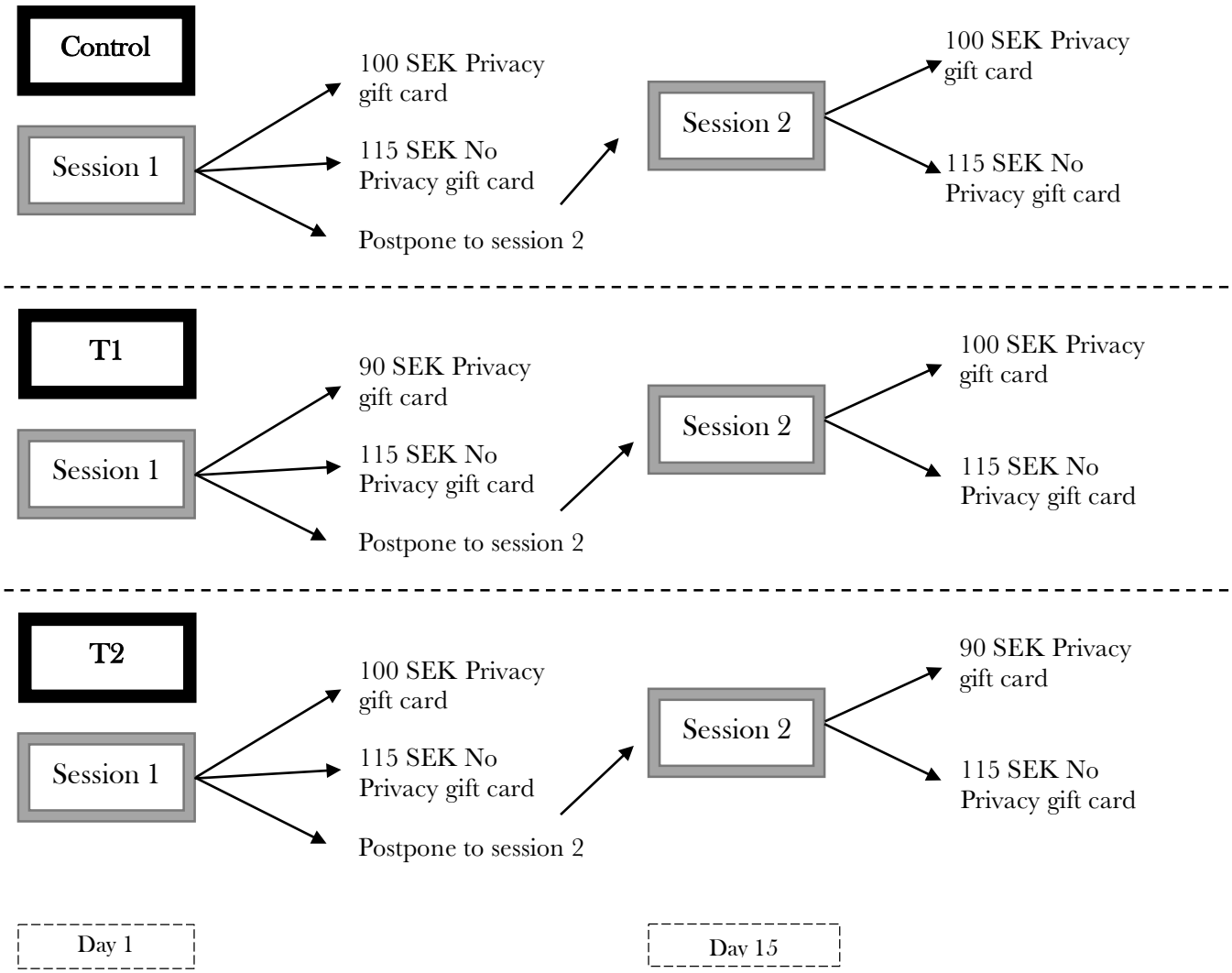

Figure 3 Experiment Design: Sequence of Decisions per Group

4.3 Hypotheses

4.3.1 Hypothesis 1: On the Existence of a Privacy Paradox

First, we are interested in establishing whether the privacy paradox exists or not. That is, whether participants' privacy concerns, as measured by Smith's instrument, are predictive of their privacy behavior, i.e. their willingness to disclose their personal information (current home address). We can estimate this using the following model:

$$Behavior_i = \beta_1 Concern_i + \beta_n Control\ variables_i + \varepsilon_i$$

Where $Behavior_i$ is a binary variable that captures whether participants' chose the no-privacy or privacy gift card and $Concern_i$ is privacy concern, the independent variable, as measured by Smith's instrument. We control for age, gender, treatment group and condition, i.e. whether participants responded to the privacy concern questions before or after the experimental questions. So the first hypothesis deals with the privacy paradox. If the privacy paradox holds we would expect there to be no or negative relation between privacy concerns and privacy behavior, a positive relation would indicate evidence to the contrary. In other words,

$$H_1: There\ is\ no\ or\ negative\ relation\ between\ privacy\ concern\ and\ behavior\colon\ \beta_1 \leq 0$$

4.3.2 Hypotheses 2-4: On the Causes of the Privacy Paradox

If that is indeed the case, and there is a privacy paradox, then we are interested in the relative preferences of the participants. Is the preference for technology that allows them to pre-commit stronger than that which gives them flexibility? We define the willingness to pay for pre-commitment (WTPC) as the difference between the share of participants who choose to decide in the first session in T2 relative the proportion of participants who do the same the control group. Furthermore, the willingness to pay for flexibility (WTPF) is defined as the share of participants who postpone their decision in T2 relative the proportion of participants who do the same in the control group. If a preference-based explanation has a stronger explanatory value, we would expect hypothesis two to be supported by the evidence. Conversely, if an uncertainty-based explanation is stronger, hypothesis three below be supported. Finally, if neither explanation is valid then we should expect evidence to support hypothesis four:

H_2: $Participants\ exhibit\ preference\ for\ pre-commitment\ over\ flexibility$: $WPTC > WPTF$

H_3: $Participants\ exhibit\ preference\ for\ flexibility\ over\ pre-commitment$: $WPTC < WPTF$

H_4: $Participants\ exhibit\ any\ strong\ relative\ preference$: $WPTC = WPTF$

To test the hypotheses, we assume that, in the baseline, the demand for either technology is roughly equal. Furthermore, in order to test the relative validity of the two explanations, we assume that participants have the same price elasticity of demand for pre-commitment and flexibility.

5. Results

There were a total of 132 high school students who participated in the experiment. 99 of the participants made their decision already in the first session, 33 chose to postpone their decision. Of these 33 participants, 23 responded to the follow up fourteen days later. That is, a bit less than 70% of those that postponed ended up making a final decision. This is a relatively high attrition rate, but only affects a small part of the sample. Nonetheless, it can be a confounding factor. See appendix III for summary statistics. In table 4 (Appendix III) we note that there is no statistically significant difference, at any of the usual levels of significance ($p>0.05$) in group means for age, gender and concern (as measured by Smith's instrument), which indicates successful random assignment into treatment groups, at least across those variables that we can, and have, measured.

5.1 The Privacy Paradox

The estimated model used to test hypothesis one, H_1, is:

$$Behavior_i = \hat{\beta}_1 Concern_i + \hat{\beta}_{2,3} Treatment\ Dummies_i + \hat{\beta}_4 Condition_i + \hat{\beta}_5 Gender_i + \hat{\beta}_6 Age_i + \hat{\beta}_0$$

The dependent variable is *Behavior*, a binary variable equal to 0 if participant chose the no privacy gift card (option B) final as final choice, and 1 if participant chose the privacy gift card (option A). We control for *Age*, *Gender*, *Condition* and the *Treatment group*. The average age of the sample is 16.8 years old. *Gender* is a dummy variable, 0 for female and 1 for male: 49.3% of the

sampled participants were female and 50.7% of the sample were male. Condition is equal to 0 for those that answered the experimental questions before the privacy survey and 1 for those who answered the privacy survey first. The independent variable of interest is *Concern*, a weighted average of the three Smith subscales. The range is 1-7, the sample mean was 5.4. The subscale means for *collection, unauthorized secondary use* and *improper access* are 3.9, 6.3, and 6.0 respectively (see Appendix III for further information). The table below presents the results of the regression estimate using a linear probability model, columns 1-4, as well as robustness checks with probit and logit models, 5 and 6. To reiterate, we are interested in the sign and significance of the coefficient on *Concern*, β_1, to test our hypothesis about the existence of the privacy paradox.

Table 1 Results of Regression: Privacy Concern on Privacy Behavior

	(1) *Behavior*	(2) *Behavior*	(3) *Behavior*	(4) *Behavior*	(5) *Behavior*	(6) *Behavior*
Age				-0.00825	-0.0297	-0.0592
				(0.0355)	(0.114)	(0.199)
Gender			0.0538	0.0524	0.166	0.300
			(0.0810)	(0.0817)	(0.257)	(0.441)
Condition		-0.0438	-0.0348	-0.0352	-0.130	-0.208
		(0.0797)	(0.0806)	(0.0810)	(0.254)	(0.431)
T1	-0.127	-0.125	-0.125	-0.125	-0.430	-0.710
	(0.0977)	(0.0982)	(0.0988)	(0.0992)	(0.311)	(0.530)
T2	-0.0337	-0.0320	-0.0340	-0.0339	-0.132	-0.201
	(0.0913)	(0.0916)	(0.0922)	(0.0927)	(0.312)	(0.537)
Concern	0.133**	0.133**	0.138**	0.138**	0.447**	0.737**
	(0.0624)	(0.0624)	(0.0618)	(0.0623)	(0.191)	(0.316)
Constant	0.0628	0.131	0.0614	0.200	-0.973	-1.469
	(0.354)	(0.385)	(0.390)	(0.700)	(2.140)	(3.593)
Observations	122	122	122	122	122	122
R-squared	0.042	0.045	0.048	0.049		

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.1

There were 122 final responses, i.e. responses from session 1 and session 2 for those who postponed the final decision in session, and an overwhelming majority 73.8% chose the privacy gift card. As can be seen from the table below, the coefficient for privacy concern β_1 is positive and statistically significant. This is evidence against hypothesis 1, against the existence of a

privacy paradox. For the purposes of interpreting the coefficients, the linear probability model has the most straightforward interpretation, a coefficient of 0.138 on Concern means that a 1-point increase in privacy concern, as measured by the Smith instrument, would lead to a participant being 13.8% more likely to choose the privacy gift card over the no privacy gift card. However, the sign of the coefficient, and not the magnitude, is what interests us. Furthermore, we can break up *Concern* into its subscale components, i.e. *Collection, Unauthorized Secondary Use* and *Improper Access.* As we can see below, only collection is statistically significant ($p < 0.001$) determinant of privacy behavior in this context. This is in line with expectations, as the behavior has to do primarily with disclosing personal information.

Table 2 Results of Regression: Privacy Concern on Privacy Behavior, by Subscale

	(1) *Behavior*	(2) *Behavior*	(3) *Behavior*	(4) *Behavior*
Age	-0.00825	-0.00132	-0.00734	-0.00728
	(0.0355)	(0.0347)	(0.0364)	(0.0368)
Gender	0.0524	0.0869	0.0310	0.0308
	(0.0817)	(0.0777)	(0.0855)	(0.0832)
Condition	-0.0352	-0.0233	-0.0411	-0.0411
	(0.0810)	(0.0772)	(0.0828)	(0.0823)
T1	-0.125	-0.152	-0.0831	-0.0930
	(0.0992)	(0.0969)	(0.101)	(0.101)
T2	-0.0339	-0.0373	-0.00574	-0.0141
	(0.0927)	(0.0898)	(0.0953)	(0.0960)
Concern	0.138**			
	(0.0623)			
Collection		0.160***		
		(0.0382)		
Unauth_sec_access			-0.00244	
			(0.0711)	
Improper acess				0.0290
				(0.0504)
Constant	0.200	0.184	0.953	0.767
	(0.700)	(0.625)	(0.832)	(0.738)
Observations	122	122	122	122
R-squared	0.049	0.122	0.012	0.016

Robust standard errors in parentheses
*** p<0.01, ** p<0.05, * p<0.001

5.2 Pre-commitment versus Flexibility

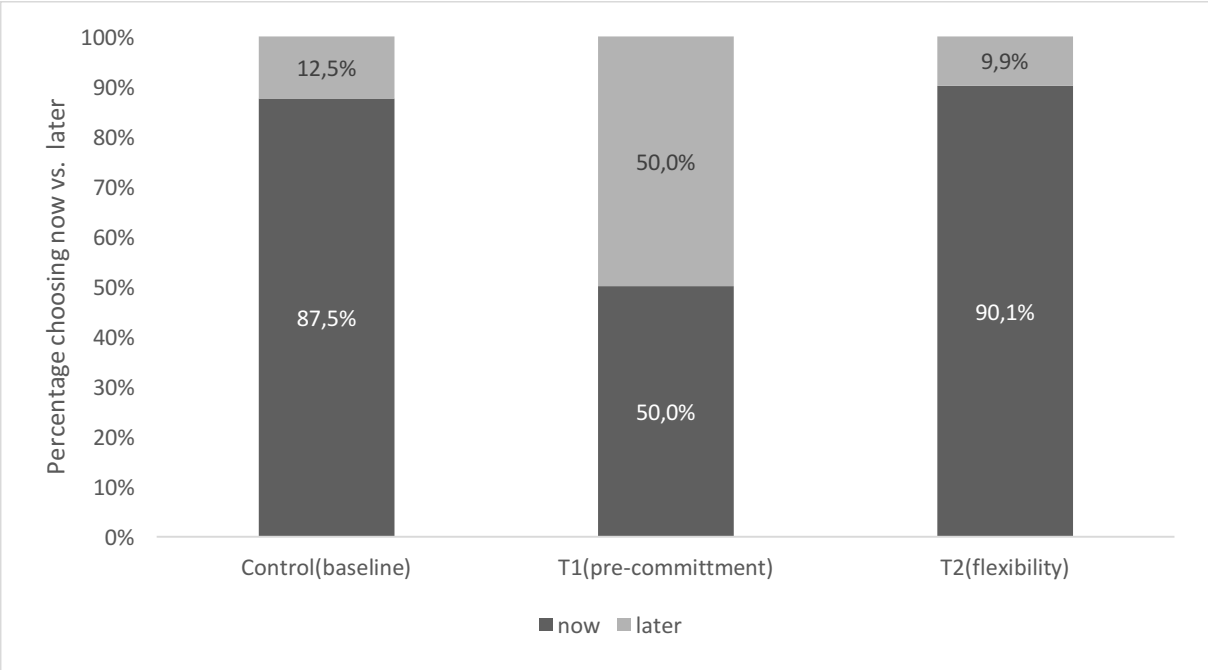

Figure 4 Results of experiment: Percentage of participants opting to decide now vs. later per group.

The figure above shows the proportion of students in each group who chose to decide during the first session (now) versus the second session (later). As a recap, in the control group or baseline, both pre-commitment and flexibility were costless. In treatment 1, pre-commitment was costly. In treatment 2, flexibility was costly. The table below shows the detailed results by treatment group.

Table 3 Detailed results of first session choices (Behavior) by treatment group .

	Behavior	***Number***	***Proportion***	***Std. error***	***95% Conf. interval***
Control	Privacy (now)	27	0.675	0.075	(0.514;0.803)
	No privacy (now)	8	0.200	0.064	(0.102;0.356)
	Postpone (later)	5	0.125	0.053	(0.052;0.271)
Total		40			
T1	Privacy (now)	11	0.229	0.061	(0.130;0.371)
	No privacy (now)	13	0.271	0.065	(0.163;0.416)
	Postpone (later)	24	0.500	0.073	(0.360;0.640)
Total		48			
T2	Privacy (now)	30	0.682	0.071	(0.529;0.804)
	No privacy (now)	10	0.227	0.064	(0.125;0.377)
	Postpone (later)	4	0.091	0.044	(0.034;0.222)
Total		44			

Returning to our hypotheses, H2-H4, we can now calculate the willingness to pay for commitment (WTPC) and the willingness to pay for flexibility (WTPF). As a recap, we define WTPC as the difference between the share of participants who choose to decide in the first session in T1 relative the proportion of participants who do the same the control group. Furthermore, WTPF is defined as the share of participants who postpone their decision in T2 relative the proportion of participants who do the same in the control group. From table 2, WTPC can be calculated by comparing the decrease in the proportion of participants make their decision in session one, i.e. 37.5%, in T1 as a share of those who do so in the control, 87.5%. That is, *the WTPC in the sample is -42.9%.* We can similarly calculate WTPF. *That is, the WTPF in the sample is -27.2%*. As WPTF>WPTC, this would indicate evidence supporting our third hypothesis: participants exhibit preference for flexibility. And evidence against hypotheses 2 and 4 respectively, i.e. that participants exhibit preference for pre-commitment over flexibility and that they do not exhibit strong relative preference for either.

However, we cannot draw any conclusions as our underlying assumptions. First, we do not find evidence for the existence of a privacy paradox, which is self-evidently necessary for any discussion of its cause. Furthermore, we assumed that in the control group when both are costless, the preference for pre-commitment or flexibility should be roughly equal. We see that this is not the case, that in the control group the preferences skew stronger to pre-commitment, with 87.5% of participants electing to choose now rather than postponing the choices. Consequently, it is also not possible to assume the same price elasticity of demand for pre-commitment and flexibility technology.

6. Discussion

6.1 On the Privacy Paradox

A high proportion of participants acted to protect their privacy. 73.8% of participants chose the lower value gift card, which required no disclosure of personal information, over the higher valued gift card that did. The results also indicate that participants' privacy concern, as measured by the Smith scale, was a statistically significant predictor of behavior. This leads us to reject our first hypothesis on the existence of a privacy paradox. This contradicts several empirical findings on the privacy paradox, e.g. Spiekermann, et al. (2001); Acquisti and Grossklags (2005); Norberg, et al. (2007) and Beresford, et al. (2012). On the other hand, the findings are line with the findings of Wakefield (2013); Tsai, et al. (2011) and Debatin, et al.

(2009). Furthermore, they support findings in the literature that younger people, in this case high school students, are more likely to be protective of their privacy (see Blank, et al. (2014)).

The implications of the result are that the privacy paradox does not seem to? exist, and that data-subjects are not prone to dynamic inconsistency. If this is the case, it would have implications for policy. First and foremost, the general policymaking approach should be to give data subjects freedom to act and tools to protect their privacy, without favoring the provision of either pre-commitment nor flexibility. This is more in line with the US than the current EU approach. While the European approach does provide more robust protection, as we have previously argued, it does sometimes unduly restrict freedom to do so. However, due to the complex nature of the issue, and contextual differences, one should be careful of drawing overly sweeping conclusions from these findings. In terms of the theoretical academic literature, our finding would lend support to the so called privacy calculus theories (Milberg, et al., 1995; Dinev & Hart, 2006) and other rational economic models of privacy that reject the existence of a privacy paradox.

It is also important to consider the internal and external validity of the study. The most significant threats to the internal validity of the study are failed randomization, measurement error and reverse causality. From table 5 (Appendix III) we can conclude that randomization was successfully achieved, at least for the variables we can and do measure. Measurement error, and reverse causality, on the other hand, are likely to be a problem, as we will discuss below. We also note that the study suffers from low external validity, due to the artificial nature of the experimental context. Furthermore, the incosistency with previous findings that support the existence of a prirvacy paradox could be due to differences in research design, measurement error or experimental context. We consider these factors below.

6.1.1 Research Design and Reverse Causality

One potential explanation for the inconsistency of this study with the many studies that find evidence of a privacy paradox, is a difference in method. One difference is the research design, a large number of studies, e.g. Acquisti and Grossklags (2005), are purely survey based. However, even comparing to studies that use an experimental design, there are still differences. Case in point, Beresford, et al. (2012) use an experimental design and find that privacy concerns did not match privacy behavior in the context of online shopping. A main methodological difference with our study is that they survey general privacy concerns, instead of specifically

regarding data collection. Their survey results show 95% of participants had a strong interest in protecting their personal information. As our results show, however, concerns about different aspects of privacy have different predictive power in determining behavior. On the subscale level, concerns over (*data) collection* seem to be the main drivers of this result, as can be seen in the results of auxiliary regressions, as shown above in the regression reported in table 2. This is exactly what we would expect if participants were acting rationally. An even more generalized measure of privacy might have led to the mistaken conclusion that privacy concern is not predictive of behavior.

Interestingly, there is quite a weak correlation in our sample between *collection* and the other two subscales *unauthorized secondary use* and *improper access.* Furthermore, as we can see in table 6 (Appendix III), *collection* has a higher standard deviation than the other two. These two observations combined could indicate that participants were more prone to straight-lining, i.e. answering the same across, on statements related to the subscales not related to data collection. Straight lining is not the only explanation. The differences in standard deviation are small. It is the mean differences that are significant, with mean for *collection* being roughly 2 points lower than the other two. This can be interpreted as participants, rationally, not being averse to data collection itself, but to the unintended harms it might lead to, further support for the finding that participants are acting rationally.

However, the greater volatility in the measure of data collection could be the result of the experiment itself making the issue of data collection more prominent in the participants' minds. This could lead them to think more carefully about those statements than others, or even match their level of concern with their behavior rather than the other way around. That is, having acted to divulge their personal information, they might answer that they are not concerned about data collection, leading to reverse causality. We attempt to capture the effect of this, by randomizing the order of the survey and the experimental question. This is captured by the control variable, *Condition,* in the regressions above. If it were a statistically significant determinant of behavior, it would be an indication of reverse causality, but, as we see from the regression tables above, it is not. Nonetheless, this might be because participants might have read in other ways than the intended order, e.g. reading everything before starting or starting in the reverse order, throwing off the usefulness of that control. Thus, we cannot eliminate the possibility of reverse causality.

6.1.2 Privacy, Context-dependence and External Validity

Differences in context are perhaps the most important cause for the divergence of empirical results on the privacy paradox, both generally and the case of this study specifically. This section outlines how the research design might have inadvertently nullified the causal mechanisms that were to be studied.

The behavioral economic, or preference-based explanation is applicable to the complex, real-world situations, where cognitive biases are more likely to manifest. When the decision making is taxing, and people's cognitive resources are diminished, they are more likely to exhibit the cognitive biases, e.g. the immediate gratification bias, that the preference-based explanation is based on (Acquisti & Grossklags, 2007). In the experiment, however, in order to ensure high participation and completion rates, the decision making situation was heavily simplified. The costs and benefits were outlined clearly and all other distractions were eliminated. This differs from other studies, for example field studies on online shopping. Here, participants had to, among other things, navigate shopping sites; evaluate their trustworthiness; weigh the benefits and costs and their willingness to pay for the goods they were purchasing, as well as the privacy policies of the websites. It is more likely that participants would exhibit cognitive biases in this situation. And indeed, some of the most convincing evidence on the privacy paradox comes from field experiments (Spiekermann, et al., 2001;Beresford, et al., 2012).

Similarly, the uncertainty-based explanation relies on complexity – a complexity that was lacking in the experiment. Participants could be relatively certain that the experimenter would not abuse their data, as the experiment was conducted in the familiar school setting. The experiment had the explicit endorsement of their teacher and the school. Furthermore, their anonymity was assured. This should have led to participants being more likely to disclose their personal information. However, our results indicate that an overwhelming majority, roughly three quarters, chose not to do so. This is because the uncertainty was low on the benefit side as well as on the demand side. The benefit was, the differential between the two gift cards, was at most 25SEK This can be juxtaposed to a more complex, real-world situation, for example choosing to join a social networking site or not. The uncertainty is not only on the cost side, i.e. on the damage that potential privacy violations might cause, but in the benefits as well. There is no clear dollar value that can be put on the benefit, unlike the neat 25SEK difference between the gift cards.

6.2 Preference-based vs. Uncertainty-based Explanation

The aim of this study, and the research question deals with empirically testing the validity of two competing hypotheses that have been used to explain the privacy paradox – a preference-based versus an uncertainty-based explanation. Unfortunately, none of the necessary prerequisites are in place in order to do so. Most importantly, we find no evidence of the prevalence of the privacy paradox in our sample. The participants acted in the same way one would expect rational agents would.

In any future adaptations of the research design applied in this study, certain aspects could be improved on. One improvement that can be made is finding a way to control or manipulate uncertainty in the experiment. This could be done both on the cost side, i.e. by influencing how participants perceive the possibility of a privacy violation, and on the benefit side, i.e. by increasing the opportunity cost of not disclosing personal information. Although not a simple task, this is the key to applying the research design to test for the privacy paradox, if it does exist. Secondary practical aspects include finding a way to avoid the imbalance in the control group regarding preferences for either pre-commitment or flexibility. In the experiment, it is possible that participants preferred pre-commitment technology due to the cost of postponing, e.g. incurring the mental effort to read through and engage in the decision making process again. At high levels of uncertainty, this effect should not matter, as the benefits of higher flexibility far outweigh the cost incurred by re-visiting the decision.

6.3 Suggestions for Future Research

The main challenge is finding a research design that can take into account the contextual nature of privacy, while allowing for the manipulation of relevant variables either directly or indirectly. As such, there are three potential avenues for future research: (i) improving the design of lab-based experiments, (ii) making greater use of field and quasi-experiments and (iii) leveraging the possibilities afforded by big data. These suggestions are mainly focused on the privacy paradox, given the scope of this study, but could be applicable to the privacy economic field in general as well.

Lab experiments, more than other types of experiments, suffer from low ecological validity. This is an especially significant weakness in the field of privacy research, which is context-sensitive Improvements should focus on increasing the ecological validity, by using real world simulations in lab experiments. That is, using an especially designed social network site or commercial

shopping website, as some researchers are already doing, e.g. Spiekermann, et al. (2001). At the same time, contexts and measures of privacy concern would benefit from being standardized, or at least harmonized, in order to aid comparability.

Field experiments are a valuable tool to confirm insights from the lab and improve the external validity of the? results. The loss in control is offset by the contextual integrity and these studies can be done at little cost, with participants' online behavior being tracked by cookies or similar trackers, as used by Beresford, et al. (2012). They also show a way to exert subtle, but effective, control even within the context of a field experiment. A limitation to this design, however, is the risk of an observer effect, leading to a change in behavior and the diminished control over the environment. Nevertheless, empirical evidence suggests that reminders of participants' privacy concerns, and of being observed, tend to wear off rather quickly (Brandimarte, et al., 2013). As such, long-term studies would minimize the consequences of the observer effect, while allowing researchers to test hypotheses with high external validity.

Finally, and somewhat ironically, one of the major threats to privacy, namely, the advent of big data, can be used to study privacy concern, attitude and behavior in a way that was previously not possible. Big data is already the case in other field of economics (Einav & Levin, 2014), even though privacy economics is even better suited than other fields of research to this type off analysis.

7. Conclusion

This thesis addressed the research question: *If the privacy paradox exists is a preference-based or an uncertainty-based explanation a better solution for it?* To do so, an experiment was conducted on a sample of 132 high school students from one school in central Stockholm. In a design adapted from Casari (2009), the predictions of the two explanations were tested by measuring the demand for pre-commitment technology versus flexibility technology. However, the results of the experiment indicate evidence against the existence of the privacy paradox, invalidating attempts to give an answer to the research question. The results contradict previous findings by, e.g. Spiekermann, et al. (2001); Acquisti and Grossklags (2005); Norberg, et al. (2007) and Beresford, et al. (2012). On the other hand, the findings are line with the findings of Wakefield (2013); Tsai, et al. (2011) and Debatin, et al. (2009). Furthermore, the results are in line with

the findings in the literature that younger people, in this case high school students, tend to be more protective of their privacy (see Blank, et al. (2014)).

Issues related to the internal and external validity of the study suggest that caution is warranted in drawing conclusions from the results. Among issues related to internal validity, there is the potential of reverse causality. Participants might have stated a level of privacy concern that matched their behavior, rather than their concern being explanatory of their behavior. Attempts were made to control for this in the design, but it is possible these were ineffective. The concerns for the external validity of the study are more serious Privacy is context-dependent. The experiment, however, simplified the decision-making process in a way that might have eliminated the very effect we seek to measure. At the center of the preference-based explanation to the paradox, is bounded rationality. This is likely to be applicable to real world situation where one has to weigh complex benefits and costs for divulging personal information, a level of complexity that was likely lacking in the experiment. Furthermore, the competing explanation relies on uncertainty. The experiment eliminates uncertainty both in the benefit and the cost, due to the concrete nature of the benefit, i.e. a monetary payoff, and the setting, which inspires trust. These weaknesses stem largely from the research design. Therefore, we recommend future research make greater use of field experiments. Moreover, researchers in privacy economics should make use of the big data tools available and are more widely used by researchers in other field of economics.

This would only be fitting, as the threats brought about by Big Data are at the center of most policy debates today. These threats have revealed the cracks in the current policy approaches in the EU and US respectively. The aim of this study was to contribute to the policy debate. Evidence against the existence of a privacy paradox has several implications for policy. If people tend to act rationally, as our results indicate, it would speak against the paternalistic approach to policy favored by the EU. Instead, the US approach would be better suited to the needs of data subjects. More research needs to be done to understand the micro-foundations of privacy behavior in order to better tailor policy to reality, to how people actually behave instead of how they are believed to do. Cooper and Wright (2017, Forthcoming), veteran policy-makers, make this point in their chapter in the upcoming book on policy making for the coming decade. As Cooper and Wright (2017, forthcoming) argue there is immense benefit to be gained from more economic research and analysis on the issue of privacy.

Bibliography

Acquisti, A., 2004. Privacy in Electronic Commerce and the Economics of Immediate Gratification. *Proceedings of the 5th ACM conference on Electronic commerce.* pp. 21-29.

Acquisti, A. & Grossklags, J., 2005. Privacy and Rationality in Individual Decision Making. *IEEE Secuirty & Privacy,* 2, pp. 24-30.

Acquisti, A. & Grossklags, J., 2007. What Can Behavioral Economics Teach us About Privacy. *Digital Privacy:Theory, Technologies and Practices,* 18, pp. 363-377.

Acquisti, A., Taylor, C. & Wagman, L., 2016. The Economics of Privacy. *Journal of Economic Literature ,* 54(2), pp. 442-492.

Acquisti, A. & Varian, H. R., 2005. Conditionining Prices on Purchase History. *Marketing Science,* 24(3), pp. 367-381.

Azfar, O., 1999. Rationalizing Hyperbolic Discounting. *Journal of Economic Behavior & Organization,* 38, pp. 245-52.

Beales, J. H. I. & Muris, T. J., 2008. Choice or Consequences: Protecting Privacy in Commercial Information. *University of Chicago Law Review,* 109, pp. 109-134.

Belleflamme, P. & Vergote, W., 2016. Monopoly Price Discrimination and Privacy: The Hidden Cost of Hiding. *Economics Letters,* 149, pp. 141-144.

Beresford, A., Kübler, D. & Preibusch, S., 2012. Unwillingness to Pay for Privacy: A Field Experiment. *Economic Letters,* 117(1), pp. 25-27.

Blank, G., Bolsover, G. & Dubois, E., 2014. *A New Privacy Paradox,* Oxford, UK: Global Cyber Security Capacity Center.

Brown, B., 2001. *Studying the Internet Experience.* [Online] Available at: http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf [Accessed 26 March 2017].

Calzolari, G. & Pavan, A., 2006. On the Optimality of Privacy in Sequential Contracting. *Journal of Economic Theory,* 130(1), pp. 168-204.

Campbell, J., Goldfarb, A. & Tucker, C., 2015. Privacy Regulation and Market Structure. *Journal of Economics & Management Strategy,* 10 February , 24(1), pp. 47-73.

Casari, M., 2009. Pre-committment and Flexibility in a Time Decision Experiment. *Journal of Risk and Uncertainty ,* 38(2), pp. 117-41.

Cofone, I., 2015. *The Value of Privacy: Keeping the Money Where the Mouth is. Working paper*

Cooper, J. C. & Wright, J. D., 2017, Forthcoming. The Missing Role of Econonmics in FTC Privacy Policy . In: J. Polonetsky, E. Selinger & O. Tene, eds. *Cambridge Handbook of Consumer Privacy* . Cambridge, UK: Cambridge University Press .

Debatin, B., Lovejoy, J., Horn, A. & Hughes, B., 2009. Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. *Journal of Computer Mediated Communication,* 15(1), pp. 83-108.

Dienlin, T. & Trepte, S., 2015. Is the Privacy Paradox a Relic of the Past? An In-depth Analysis of Privacy Attitudes and Privacy Behaviors. *European Journal of Social Psychology,* 45(3), pp. 285-297.

European Court of Justice, 2014. Press Release No 70/14. [Online] Available at: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf [Accessed 27 April 2017].

European Union , 1995. *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.* [Online] Available at: http://www.refworld.org/docid/3ddcc1c74.html [Accessed 24 March 2017].

European Union, 2012. *Charter of Fundamental Rights of the European.* [Online] Available at: http://www.refworld.org/docid/3ae6b3b70.html [Accessed 19 March 2017].

Federal Trade Comission, The, 2016. *Big Data: A Tool for Inclusion or Exclusion? Understanding the Issues.".* [Online] Available at: https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [Accessed 20 March 2017].

Gellman, R., 2016. *Fair Information Practices: A Basic History.* [Online] Available at: http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf [Accessed 19 March 2017].

Glancy, D., 1979. Invention of the Right to Privacy, The. *The Arizona Law Review ,* 21(1).

Hargittai, E., 2010. Facebook Privacy Settings: Who cares?. *First Monday,* 15(8).

Holvast, J., 1993. *Vulnerability and Privacy: Are We on the Way to a Risk-Free Society?.* Namur, Belgium, s.n.

Huberman, B., Adar, E. & Fine, L., 2005. Valuating Privacy. *IEEE Security & Privacy ,* 3(5), pp. 22-25.

Hughes-Roberts, T., 2013. *Privacy and Social Networks: Is Concern a Valid Indicator of Intention and Behavior?.* Washington,USA, SocialCom 2013.

Jentzsch, N., 2016. *State-of-the-Art of the Economics of Cyber- Security and Privacy,* Watford: IPACSO – Innovation Framework for ICT Security Deliverable, No. 4.1.

Kahn, C., McAndrews, J. & Roberds, W., 2000. *A Theory of Transaction Privacy,* Atlanta : Federal Reserve Bank of Atlanta.

Kokolakis, S., 2017. Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the privacy paradox phenomenon. *Computers & Security,* 64, pp. 122-134.

Laibson, D., 1997. Golden Eggs and Hyperbolic Discounting. *The Quarterly Journal of Economics,* 112(2), pp. 443-478.

Laudon, K., 1997. Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information. *Working paper* , January .97(4).

MacCarthy, M., 2010. *New Directions in Privacy: Disclosure,Unfairness and Externalities.* Washington,DC. *Working paper.*

Marotta-Wurgler, F., 2016. Understanding Privacy Policies: Content, Self-Regulation, and Markets. *NYU Law and Economics Research Paper, 16-18.*

McDonald, A. M. & Cranor, L. F., 2008. The Cost of Reading Privacy Policies. *ISJLP,* 4, pp. 540-565.

Miltgen, C. & Peyrat-Guillard, D., 2014. Cultural and Generational Influences on Privacy Concerns: a Qualitative Study in Seven European Countries. *European Journal of Information Systems,* 23(2), pp. 103-125.

Morando, F., Iemma, R. & Raiteri, E., 2014. Privacy Evaluation:What Empirical Research on Users' Valuation of Personal Data Tells us. *Internet Policy Review,* 3(2), pp. 1-11.

National Science Foundation, 2012. *Core Techniques and Technologies for Advancing Big Data Science & Engineering (BIGDATA).* [Online] Available at: https://www.nsf.gov/pubs/2012/nsf12499/nsf12499.htm [Accessed 20 March 2017].

Nissenbaum, H., 2010. *Privacy in Context.* Stanford, CA: Stanford University Press.

Noam, E. M., 1997. *Privacy and Self-regulation: Market for Electronic Privacy,* Washington, DC: US Department of Commerce.

Norberg, P. A. & Horne, D. R., 2007. The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors. *Journal of Consumer Affairs,* 41(1), pp. 100-126.

OECD, 2011. *The OECD Privacy Guidelines.* [Online] Available at: http://www.oecd.org/sti/ieconomy/49710223.pdf [Accessed 19 March 2017].

OECD, 2013. Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value. *OECD Digital Economy Papers,* 220.

Oomen, I. & Leenes, R., 2008. Privacy Risk Perceptions and Privacy Protection Strategies. In: F. de Leeuw, S. Fischer-Hübner, J. Tseng & J. Borking, eds. *Policies and Research in Identity Management.* London:Springer US, pp. 121-138.

Posner, R., 1977. The Right of Privacy. *George Law Review* , 12(3), pp. 393-421.

Posner, R. A., 1981. The Economics of Privacy. *The American Economic Review* , 71(2), pp. 405-409.

Preibusch, S., 2013. Guide to Measuring Privacy Concern: Review of Survey and Observational Instruments. *International Journal of Human-Computer Studies ,* 71(12), pp. 1133-1143.

Prosser, W. L., 1960. Privacy. *California Law Review,* 48(3), pp. 383-423.

Reynolds, B., Venkatanathan, J., Gonçalves, J. & Kostaos, V., 2011. *Sharing Ephemeral Information in Online Social Networks: Privacy Perceptions and Behaviours.* Lisbon, Portugal, INTERACT 2011.

Rosenberg, R., 1992. *The Social Impact of Computers.* London:Academic Press Inc.

Smith, H., Milberg, S. & Burke, S., 1996. Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Qyarterly ,* 20(2), pp. 167-196.

Solove, D., 2002. Conceptualizing Privacy. *California Law Review,* 90(4), pp. 1087-1156.

Solove, D., 2004. *The Digital Person.* 1st Edition ed. New York : New York University Press.

Son, J. & Kim, S., 2008. Internet Users' Information Privacy-Protective Responses: a Taxanomy and a Nonmological Model. *MIS Quarterly ,* 32(3), pp. 503-529.

Sozou, Peter D., 1998. On Hyperbolic Discounting and Uncertain Hazard Rates. *Royal Society of London B: Biological Sciences*, pp. 2015-2020.

Spiekermann, S., Grossklags, J. & Berendt, B., 2001. *E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior.* Florida, USA, s.n.

Staddon, J., Acquisit, A. & LeFevre, K., 2013. *Self-reported Social Network Behavior:Accuracy Predictors and Implications for the Privacy Paradox.* Washington,DC , s.n.

Stigler, G., 1980. An Introduction to Privacy in Economics and Politics. *The Journal of Legal Studies ,* 9(4), pp. 623-644.

Taylor, C. R., 2004. Consumer Privacy and the Market for Customer Information. *RAND Journal of Economics ,* 35(4), pp. 631-650.

Thaler, R., 1981. Some Empirical Evidence on Dynamic Inconsistency. *Economic Letters ,* 8(3), pp. 201-207.

Tsai, J., Egelman, S., Cranor, L. & Acquisti, A., 2011. The Effect of Online Privacy Information on Purchasing Behavior. *Information Systems Research ,* 22(2), pp. 254-268.

Tufekci, Z., 2008. Can You See me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulleting of Science, Technology & Society,* 28(1), pp. 20-36.

Wakefield, R., 2013. The Influence of User Affect in Online Information Disclosure. *The Journal of Strategic Information Systems ,* 22(2), pp. 157-174.

Varian, H., 1997. *Economic Aspects of Personal Privacy,*Washington, DC: Department of Commerce.

Varian, H., 2010. Computer Mediated Transactions. *American Economic Review,* 100(2), pp. 1-10.

Warren, S. D. & Brandeis, L., 1890. The Right to Privacy. *Harvard Law Review* , pp. 193-220.

Westin, A. F., 1967. *Privacy and Freedom.* 1st Edition ed. New York : Atheneum.

Whitman, J. Q., 2004. The Two Wester Cultures of Privacy: Dignity versus Liberty. *Yale Law Review,* 113.

Wittes, B., 2011. *Databuse: Digital Privacy and the Mosaic.* [Online] Available at: https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2011/05/GRE-Blog-May-17-2011-3.pdf [Accessed 18 March 2017].

Young, A. & Quan-Haase, A., 2010. Privacy Protection Strategies on Facebook: the Internet Privacy Paradox Revisited. *Information, Communication & Society,* 16(4), pp. 479-500.

Zafeiropoulou, A. M., Millard, D. E., Webber, C. & O'Hara, K., 2013. *Unpicking the Privacy Paradox: can Structuration Theory Help Explain Location-based Privacy Decisions?.* Paris, France, WebSci '13, p. 10.

Appendix I: Exponential Discounting with Uncertainty

Sozou's (1998) seminal model can be used to formally show (rational) exponential discounting under uncertainty. The following exposition, based on the adaptation to privacy by Cofone(2015) shows the derivation of the model and its similarities with hyperbolic discounting.

Consider an expected utility model where the agent discounts based on the risk associated with the payoff, namely the risk of the payoff not materializing:

$$u(\tau) = u_0 s(\tau) \tag{1}$$

where $u(\tau)$ is the utility an agent derives from waiting time τ. At time *t=0*, utility is equal to u_0. Finally, $s(\tau)$ is the survival function that captures the probability that the payoff will still be there after a delay of τ. The discounting mechanism is then given by

$$u(\tau) = \frac{u_o}{1 + k\tau} \tag{2}$$

Where $k > 0$ is a discount factor. Where the survival function that leads to hyperbolic time preference is given by

$$s(\tau) = \frac{1}{1 + k\tau} \tag{3}$$

Now let the hazard rate (λ), the function that captures the risk of default, be an unknown constant drawn from a known distribution $f(\lambda)$. The hazard fluctuates throughout the period, and can thus be a different value at each time. The survival function will be the aggregation of all the hazard rates over time. If λ can take any value of a finite set N, and the probability of λ_1 is p_1 , that of λ_2 is p_2 and so on until λ_N is p_N. Then the probability that the payoff will still be there until time τ is

$$s(\tau) = p_1 e^{-\tau\lambda} + p_2 e^{-\tau\lambda} + \cdots + p_N e^{-\tau\lambda} \tag{4}$$

Taking the Laplace transform of $f(\lambda)$, we get

$$s(\tau) = \int_0^\infty e^{-\tau\lambda} f(\lambda)\, d\lambda \tag{5}$$

This defines the time preference function precisely in the same way as hyperbolic discounting (Cofone, 2015). Let $f(\lambda) = a$, and $a > 0$; assuming f is continuous at 0, then the value of th integral declines hyperbolically as τ increases (Azfar, 1999).

Substituting (3) into (5), we now have that $f(\lambda)$ has to satisfy

$$\int_0^\infty e^{-\tau\lambda} f(\lambda)\, d\lambda = \frac{1}{1 + k\tau} \tag{6}$$

That gives us

$$f(\lambda) = \frac{1}{k} e^{-\frac{\lambda}{k}} \tag{7}$$

Appendix II: Questionnaire

Name:

E-mail:

_ _

Instructions: Please answer all questions to the best of your abilities. If anything is unclear, ask the experimenter for clarification.

All your answers and your participation in this study is anonymous and voluntary. If you at any time wish to withdraw you are free to do so.

What is your age?

_____

What is your gender?

Male [ ] Female [ ] Other [ ]

Below you will find a list of eleven statements. Please read them carefully, and mark the appropriate box that matches your level of agreement with each statement.

A. It usually bothers me when companies ask me for personal information.

Don't Agree						**Agree Strongly**
1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

B. Companies should not use personal information for any purpose unless it has been authorized by the individuals who provided the information.

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

C. Companies should devote more time and effort to preventing unauthorized access to personal information.

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

D. When companies ask me for personal information, I sometimes think twice before providing it.

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

E. When people give personal information to a company for a given reason, the company should never use the information for any other reason.

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

F. Computer databases that contain personal information should be protected from unauthorized access no matter how much it costs.

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

G. It bothers me to give personal information to so many companies.

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

H. Companies should never sell the personal information in their computer databases to other companies.

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

I. Companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information.

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

J. Companies should take more steps to make sure that unauthorized people cannot access personal information in their computers.

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

K. I'm concerned that companies are collecting too much personal information about me

1	2	3	4	5	6	7
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

You will now be presented with a choice between a number of alternatives. Choose only **ONE** of the alternatives. Five participants will be randomly selected to receive a gift card. The value of the gift card is determined by the choice you make below.

NOTE: Regardless of your choice of gift card and the timing of the decision below, all gift cards will be delivered in 14 days' time.

1. Control:

Consider the following options. Please take time to read them carefully, afterwards you will be asked to state your preference by choosing ONE of the options:

a) Receiving a 100SEK gift card 14 days from today. If you choose this gift card, you will be asked to write the name of your favorite city below.

b) Receiving a 110SEK gift card 14 days from today. If you choose this gift card, you will be asked to write your current home address in full below.

c) Postponing the choice to 14 days from today. You will receive an email in 14 days' time where you have to state your preference by choosing ONE of the following two options:

   a. Receiving a 100SEK gift card on the same day that you decide (14 days from today). You will be asked to write the name of your favorite city in the online form.

   b. Receiving a 110SEK gift card on the same day that you decide (14 days from today). You will be asked to write your current home address in the online form.

Mark your choice below by circling your preference and providing the relevant information.

a) Favorite city: _____

b) Address: _____

_____

c) No further information required at this time

2. Pre-commitment

Consider the following options. Please take time to read them carefully, afterwards you will be asked to state your preference by choosing ONE of the options:

a) Receiving a 90SEK gift card 14 days from today. If you choose this gift card, you will be asked to write the name of your favorite city below.

b) Receiving a 110SEK gift card 14 days from today. If you choose this gift card, you will be asked to write your current home address in full below.

c) Postponing the choice to 14 days from today. You will receive an email in 14 days' time where you have to state your preference by choosing ONE of the following two options:

   a. Receiving a 100SEK gift card on the same day that you decide (14 days from today). You will be asked to write the name of your favorite city in the online form.

   b. Receiving a 110SEK gift card on the same day that you decide (14 days from today). You will be asked to write your current home address in the online form.

Mark your choice below by circling your preference and providing the relevant information.

a) Favorite city: _____

b) Address: _____

_____

c) No further information required at this time

3. **Flexibility**

Consider the following options. Please take time to read them carefully, afterwards you will be asked to state your preference by choosing ONE of the options:

a) Receiving a 100SEK gift card 14 days from today. If you choose this gift card, you will be asked to write the name of your favorite city below.

b) Receiving a 110SEK gift card 14 days from today. If you choose this gift card, you will be asked to write your current home address in full below.

c) Postponing the choice to 14 days from today. You will receive an email in 14 days' time where you have to state your preference by choosing ONE of the following two options:

   a. Receiving a 90SEK gift card on the same day that you decide (14 days from today). You will be asked to write the name of your favorite city in the online form.

   b. Receiving a 110SEK gift card on the same day that you decide (14 days from today). You will be asked to write your current home address in the online form.

Mark your choice below by circling your preference and providing the relevant information.

a) Favorite city: _____

b) Home address: _____

_____

c) No further information required at this time

Appendix III: Summary Statistics

Table 4 Summary Statistics by Group

Group	Statistic	Age	Gender	Concern
Control	*N*	40	40	40
	Mean	16.85	.5	5.3077778
	Std. dev.	1.2919871	.50636968	.73151895
1	*N*	48	48	48
	Mean	16.854167	.47916667	5.6113426
	Std. dev.	1.0516367	.50485234	.49730949
2	*N*	44	44	44
	Mean	16.840909	.54545455	5.5061869
	Std. dev.	1.1194513	.5036862	.60210323
Total	*N*	132	132	132
	Mean	16.848485	.50757576	5.4843013
	Std. dev.	1.1424151	.50184715	.61857059
Kruskal-Wallis p-value		0.9577	0.8132	0.1453

*** p<0.01, ** p<0.05, * p<0.001

Table 5 Correlation between Subscales

	Concern	*Collection*	*Anauth. Sec. access*	*Improper access*
Concern	1.0000			
Collection	0.7327	1.0000		
Unauthorized secondary access	0.7295	0.2543	1.0000	
Improper access	0.8134	0.3158	0.5387	1.0000

Table 6 Subscale Means and Standard Deviation

Stats	***Concern***	***Collection***	***Unauth. Sec. access***	***Improper access***
N	132	132	132	132
Mean	5.4843	3.9580	6.4091	6.0859
Std. dev	0.6185	0.9199	0.6526	0.8675

Table 7 Summary Statistics of Variables Used in the Main Regressions

Variables	***Observations***	***Mean***	***Std. Dev***	***Min.***	***Max***
Behavior	122	0.738	0.441	0	1
Age	132	16.8	1.142	15	20
Gender	132	0.506	0.502	0	1
Concern	132	5.484	0.619	3.288	6.466
Collection	132	3.958	0.920	1.2	5.4
Unauthorized sec. access	132	6.401	0.653	3	7
Improper access	132	6.086	0.867	2	7