COMPUTERS & SECURITY 64 (2017) 122–134

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon

*Spyros Kokolakis* *

*Department of Information & Communication Systems Engineering, University of the Aegean, Samos 83200, Greece*

ARTICLE INFO

*Article history:*
Received 10 February 2015
Received in revised form 10 June 2015
Accepted 6 July 2015
Available online 10 July 2015

*Keywords:*
Privacy
Personal information
Information privacy
Privacy behaviour
Privacy paradox

ABSTRACT

Do people really care about their privacy? Surveys show that privacy is a primary concern for citizens in the digital age. On the other hand, individuals reveal personal information for relatively small rewards, often just for drawing the attention of peers in an online social network. This inconsistency of privacy attitudes and privacy behaviour is often referred to as the "privacy paradox". In this paper, we present the results of a review of research literature on the privacy paradox. We analyse studies that provide evidence of a paradoxical dichotomy between attitudes and behaviour and studies that challenge the existence of such a phenomenon. The diverse research results are explained by the diversity in research methods, the different contexts and the different conceptualisations of the privacy paradox. We also present several interpretations of the privacy paradox, stemming from social theory, psychology, behavioural economics and, in one case, from quantum theory. We conclude that current research has improved our understanding of the privacy paradox phenomenon. It is, however, a complex phenomenon that requires extensive further research. Thus, we call for synthetic studies to be based on comprehensive theoretical models that take into account the diversity of personal information and the diversity of privacy concerns. We suggest that future studies should use evidence of actual behaviour rather than self-reported behaviour.



## 1. Introduction

Anecdotal and empirical evidence indicate that individuals are willing to trade their personal information for relatively small rewards. For example, Carrascal et al. (2013) have found that internet users value their online browsing history for about 7 Euros, which is the equivalent a Big Mac meal.[1] On the other hand, surveys of internet users' attitudes show that users are highly concerned about their privacy and the collection and use of their personal information (e.g., TRUSTe, 2014, Pew Research Center, 2014). This dichotomy of information privacy attitude and actual behaviour has been coined the term "privacy paradox" (Brown, 2001; Norberg et al., 2007) or, to be more accurate, "information privacy paradox".

The privacy paradox has significant implications for e-commerce, e-government, online social networking, as well as for government privacy regulation. E-commerce and online social networking sites are collectors of vast amounts of personal information. A proof of the privacy paradox would encourage them to increase the collection and use of personal information. Government policy makers, on the other

* Tel.: +302273082233.
*E-mail address:* sak@aegean.gr
http://dx.doi.org/10.1016/j.cose.2015.07.002
0167-4048/

[1] It refers to the cost of a Big Mac meal in Spain, circa 2011 (Carrascal et al., 2013).

hand, justify privacy regulation on people's raised privacy concerns. The inconsistency between privacy attitude and actual behaviour weakens this justification.

Several researchers have attempted to test the privacy paradox hypothesis and to find an explanation for this "paradoxical" phenomenon. Unfortunately, relevant research provides contradicting results and incomplete explanations. In this paper, we survey current literature with an aim to investigate the following research questions:

- Does the information privacy paradox exist?
- What explains the dichotomy between privacy attitude and privacy behaviour?

After the introduction, the paper continues with presenting the scope and method of the literature review. In Section 3, we analyse studies that provide evidence for and against the privacy paradox hypothesis and provide explanations for this controversy. In Section 4, we present studies that suggest and explore different interpretations of the privacy paradox phenomenon. Finally, in Section 5 we discuss our results and provide recommendations for future research.

## 2. Literature review: scope and methodology

We may distinguish three aspects of privacy (Holvast, 1993; Rosenberg, 1992): (a) territorial privacy, which is concerned with the physical area surrounding a person, (b) privacy of a person, which refers to the protection of a person against undue interference, such as physical search, and (c) informational privacy, which is concerned with controlling whether and how personal data can be gathered, stored, processed, and disseminated. The scope of this literature review is restricted to the third aspect of privacy, informational privacy. *Privacy paradox* is used in this paper as a shortcut for the more accurate term *informational privacy paradox*.

In most relevant studies privacy paradox refers to the dichotomy between privacy attitude and privacy behaviour. Some researchers, however, compare privacy concerns with privacy behaviour. The two constructs, *privacy concerns* and *privacy attitudes*, though closely related, are fundamentally different. Privacy concerns could be quite generic and, in most cases, are not bound to any specific context, whilst privacy attitudes refer to the appraisal of specific privacy behaviours. In this literature review we have included research papers that follow both approaches.

Another distinction to be made is between *privacy behaviour* and *privacy intention*. Several studies measure privacy intention instead of privacy behaviour. These studies overlook an essential aspect of the paradox, the fact that often privacy intentions do not lead to protective behaviour. Despite that, they were also included in this literature review.

Current literature includes a few studies that attribute a completely different meaning to the term privacy paradox as referring to the tension between personalisation and privacy, especially in e-commerce. It is also often named the *personalisation-privacy* paradox. For example, Sutanto et al. (2013) examined the impact of IT-enabled personalisation and personalised marketing on smartphone users' privacy concerns and proposed a personalised, privacy-safe application that retains users' information locally on their smartphones while still providing them with personalised product messages. In addition, there is a body of literature that is concerned with the legal and ethical aspects of the privacy paradox. All these studies were excluded.

The first stage in our search for the literature involved identifying papers on *privacy paradox* in the Scopus database. Using these keywords, 53 articles were listed as relating to the privacy paradox. In the preliminary screening, we removed articles that were anonymous, erratum notifications and editorials. We also removed articles on legal and ethical aspects of the privacy paradox. Finally, we excluded articles concerned with the personalisation-privacy paradox. The remaining list included 22 articles. Scopus is a comprehensive database that covers more than 21,000 peer-reviewed journals, as well as several thousands of scientific conferences proceedings and scientific books. A similar search in Thomson's Web of Science database did not contribute any additional relevant articles.

In the second stage, we further investigated the references list of the papers identified in the first stage. Papers selected from those references lists were also screened following the same criteria as in the first stage and their references lists were investigated to identify additional relevant papers. Through this process we collected 29 articles. Most of them do not use the term privacy paradox and for this reason they were not identified in the first stage. Our final list of articles for this literature review comprised 51 articles. We believe that our review covers most of the literature pertaining to the privacy paradox and includes all significant research articles on the topic.

## 3. The debate about the privacy paradox

### 3.1. *Early studies*

In 2001, a study of internet use explored online shopping popularity and the concerns of users with regard to privacy and security, among other issues (Brown, 2001). Through a series of in-depth interviews with online shoppers, Brown uncovered "something of a 'privacy paradox'". While individuals expressed their concerns about their privacy being infringed, they were still willing to give their personal details to online retailers as long as they had something to gain in return. Interviewees said they were afraid that too much information about them was collected, but this would not stop them from buying online. They also reported that they were using loyalty cards lured by the discounts and gifts offered by several stores. These findings were consistent with previous research on loyalty cards that showed that shoppers were willing to trade information about their grocery purchases for cost savings at the cash register (Sayre and Horne, 2000).

In the same year, Spiekermann et al. (2001) presented the results of a study aiming to reveal the relation between privacy preferences and actual behaviour in the context of e-commerce. They conducted an experiment to compare self-reported privacy preferences with actual disclosing behaviour during online shopping. Participants were first asked to complete a

questionnaire on privacy attitudes and preferences and, then, to visit an online store. During their shopping in the store they were engaged in a sales dialogue with an anthropomorphic 3-D shopping bot. Participants answered a majority of questions, even if these were highly personal. This indicates that even though internet users claim that privacy is a high priority, they do not behave accordingly.

More evidence of an attitude vs. behaviour dichotomy and some preliminary interpretations of the phenomenon were provided by researchers following the *behaviour economics* approach. Acquisti (2004) claims that "[p]eople may not be able to act as economically rational agents when it comes to personal privacy." He argues that privacy-related decisions are affected by *incomplete information*, *bounded rationality* and psychological biases, such as *confirmation bias*, *hyperbolic discounting* and others. These decision-making biases have been well documented in the behavioural economics literature (e.g., Gilovich et al., 2002). Acquisti built an economic model that partly explains privacy attitude – behaviour inconsistencies. This model incorporates the *immediate gratification* bias. Immediate gratification refers to the tendency to value present benefits more than future risks. Thus, in individuals' heuristic assessment, the present benefits of information disclosure outweigh the future privacy risks. Furthermore, he argued that sophisticated privacy advocates might realise that protecting themselves from any possible privacy intrusion is unrealistic. Thus, they might not be willing to adopt a strict privacy protection strategy, since they doubt it will eventually pay-off (Acquisti, 2004).

Stepping from economic theory into empirical research, Acquisti and Grossklags (2005) collected survey data that support the hypothesis that privacy decision-making is affected by incomplete information, bounded rationality and psychological biases. They also found evidence of a privacy attitude vs. behaviour dichotomy. Whilst most of the subjects (approx. 89%) reported to be either moderately or very concerned about privacy, more than 21% of the sample admitted to having revealed their social security number for discounts or better services or recommendations, and more than 28% had given their phone numbers to merchants, raffle organisers and so forth.

Another stream of research aimed to understand the self-disclosing behaviour in online social networks, especially among young people. Barnes (2006) uses the term privacy paradox in reference to the privacy behaviour of young people in Social Networking Sites (SNSs). Young people tend not to realise that SNSs provide a public space and disclose personal information that could possibly be misused.

The term *privacy paradox* was mainly established by Norberg et al. (2007). They conducted two studies, each comprising two phases. In the first phase they asked a sample of students about their willingness to disclose specific pieces of information. Phase two took place several weeks later, when subjects were asked to provide the same kind of information to a market researcher. This study confirmed the hypothesis that individuals would actually disclose a significantly greater amount of personal information than their stated intentions indicate. In a second study that followed the same methodology they tested the effect of *risk perceptions* on stated *intentions to disclose* personal information and the effect of *trust perceptions* on actual *privacy behaviour*. They found evidence that support the risk–intention relation, but they did not find support for the trust–behaviour relation hypothesis.

### 3.2. *Evidence supporting vs. evidence challenging the existence of the privacy paradox*

Preliminary evidence by Spiekermann et al. (2001), Acquisti and Grossklags (2005) and Norberg et al. (2007) were further supported by research in both transactional situations, such as e-commerce, and social situations, as in the case of online social networks.

Studies that aimed to determine a value for personal information have indicated very low valuations that do not justify the high privacy concerns expressed by people in polls and surveys. Huberman et al. (2005) conducted a series of experimental auctions to elicit the value people place on their private data. In these auctions participants named a price for their data and the person that demanded the least was paid the second-lowest demanded price (i.e., a reverse second-price auction). The information that was put on auction was weight and age. The average demand price for age was $57.56 vs. $74.06 for weight. The experiment also revealed a tendency for a higher valuation of weight information when it is perceived as embarrassing. Also, as expected, very young people were more willing to reveal their age than older ones.

In another experiment subjects faced trade-off situations, where they were asked to choose between incomplete privacy protection and benefits such as convenience or promotions (Hann et al., 2007). It was estimated that protection against errors in personal records, improper access of personal information and secondary use of personal information is worth between $30.49 and $44.62.

Beresford et al. (2012) conducted a field experiment, in which subjects were asked to buy a DVD from one of two competing stores. The two stores were almost identical. The first store asked for income and date of birth, whilst the second store asked for favourite colour and year of birth. Obviously, the information requested by the first store is significantly more sensitive. Nevertheless, when the price was the same subjects bought from both stores equally often. When the price was set to be 1 Euro less in the first store, almost all participants chose the cheaper store, although it was asking more sensitive information. A post-experimental questionnaire tested if subjects were unconcerned about privacy issues. 75% of participants indicated that they had a strong interest in data protection and 95% said that they were interested in the protection of their personal information.

Carrascal et al. (2013) conducted an experiment aiming to determine the monetary value of several types of personal information. Using a web browser plugin they prompted users to value their personal data at the time and place they were generated. In the first phase of the experiment, the browser plugin collected data about the browsing behaviour of each subject. These data were used to calibrate the behaviour of the plugin in the second phase. In the second phase the plugin displayed popups as the participants were browsing the internet. Popups contained two kinds of questions: questions about valuating personal information and questions on participants' privacy perceptions and knowledge. Information valuation questions were framed as auctions. For example, one question was "What is the

minimum amount of money you would accept for selling 10 of the photos you have uploaded to this website to a private company?" The experiment was concluded with a post-study questionnaire. The results of this study show significantly low evaluations of personal information. Users value their browsing history at 7 Euros on average. With regard to offline personal information, such as age, address, and economic status, average valuation is approximately 25 Euros. Users gave higher valuations to data relating to interactions in social networks (12 Euros) and finance websites (15.5 Euros), when compared with activities such as search (2 Euros) and shopping (5 Euros).

On the other hand, it appears that consumers are willing to pay a premium for privacy, albeit a small one. Egelman et al. (2012) performed two experiments with smartphone users and found that when choosing among applications with similar functionality, privacy-conscious participants were willing to pay a premium of $1.50 over an initial price of $0.49. However, this occurred only when users were presented the requested permissions of each application side-by-side.

Another stream of research has focused on online social networks and the relationship between privacy concerns and information disclosure in SNSs. Tufekci (2008) reports the results of a questionnaire survey aiming to study students' self-disclosure behaviour in SNSs. The study found little to no relationship between online privacy concerns and information disclosure. Another interesting result is that students manage their concerns about unwanted audience by adjusting the visibility of information, but not by regulating the levels of disclosure. Reynolds et al. (2011) in their study also found that there was little correlation between participants' broader concern about privacy on Facebook and their posting behaviour. Contrary to Tufekci (2008) they found that the portion of posts that were visible to a large audience appeared to be independent of general privacy attitude. Hughes-Roberts (2013), based on a questionnaire survey and an examination of participants' Facebook profiles, concluded that a general statement of user concern is not a valid indicator of privacy behaviour within the network. However, he questioned the appropriateness of surveys as instruments for studying the privacy paradox.

A web survey by Taddicken (2014) also showed that privacy concerns hardly impact self-disclosure. The relation between privacy concerns and self-disclosure is moderated by various variables. In particular, *perceived social relevance* and the *number of other social web applications used* have a strong moderating effect. In this study social relevance mainly refers to the disclosing behaviour of communication partners indicating that disclosure proceeds in a quid pro quo basis, i.e. "you tell me and I tell you".

Lee et al. (2013) also confirmed the existence of an attitude vs. behaviour dichotomy. They conducted a series of semi-structured in-depth interviews and an experiment to assess the influence of expected benefit and expected risk on users' intention to share personal information. They concluded that users actively share personal information despite their concerns, because they do not only consider risk but also the expected benefit of sharing.

A study by Zafeiropoulou et al. (2013) specifically examined location data, which is a form of personal information increasingly used by mobile applications. Their survey also found evidence that supports the existence of privacy paradox for location data. Finally, Oomen and Leenes (2008) studied privacy risk perception in relation to the use of privacy enhancing technologies. Their survey data indicate that a high perception of privacy risk is an insufficient motivator for people to adopt privacy protecting strategies, while knowing these exist.

All the aforementioned studies provide evidence that support the hypothesis of a paradoxical dichotomy between privacy attitudes and privacy behaviour. Nevertheless, several researchers have provided evidence that raise doubts about the existence of a privacy paradox. Individuals disclose personal information when they see some benefit to it, but, at the same time, they are significantly affected by the way this information is handled. They are significantly concerned about secondary use of personal data and these concerns do lead to a cautious behaviour.

The absence of secondary disclosure has a stronger influence than a 10% price cut, and is just 8% lower than a 25% price cut, according to a study by D'Souza and Phelps (2009). They conducted two online surveys to study the influence of price and secondary use on purchase likelihood and concluded that privacy concerns do matter and there is a measurable relationship with purchase behaviour. This study uses online questionnaires, rather than factual purchase data, which limits the validity of results.

A survey of visitors in two commercial websites (Wakefield, 2013) also provided evidence that supports the hypothesis that perceived website trust is an important determinant of consumers' intention to disclose personal information.

Also, when privacy policies are displayed prominently, consumers tend to purchase from online retailers that better protect their privacy. Tsai et al. (2011) conducted a two-phase study that involved an online concerns survey and an online shopping experiment. In the experiment they used a shopping search engine that compactly displays privacy policy information. They found that consumers provided with salient privacy information take that information into account and make purchases from online shops that offer medium or high levels of privacy protection. They conclude that "…contrary to the common view that consumers are unlikely to pay for privacy, consumers may be willing to pay a premium for privacy."

In the realm of online social networks several studies challenge the common assumption that young people do not protect their private information. Young people use a variety of protection strategies, such as using pseudonyms and giving false information (Miltgen and Peyrat-Guillard, 2014), restricting access to their profiles and adjusting their privacy settings (boyd and Hargittai, 2010), limiting friendship requests, and deleting tags and photos (Young and Quan-Haase, 2013).

Information disclosure and information control in online social networks are not closely related. Disclosure is driven by the need for popularity, which explains why young people tend to disclose personal information. On the other hand, low levels of trust lead to control strategies, such as denying friend requests in order to control who has access to personal profiles (Christofides et al., 2009).

Privacy-concerned users may employ various privacy-protection responses. Son and Kim (2008) provide a taxonomy of Information Privacy-Protective Responses (IPPRs) that includes the following six types of IPPRs: refusal (i.e. users refuse to provide information), misrepresentation (i.e. users provide false information), removal of information from online companies databases, negative word-of-mouth, complaining directly to online companies, and complaining indirectly to third-party

**Table 1 – Studies that provide evidence that support the privacy paradox hypothesis.**

| Study | Context | Methodology | Participants |
|---|---|---|---|
| Acquisti (2004) | e-Commerce | Conceptual/analytic | Not applicable (not an empirical research) |
| Acquisti and Grossklags (2005) | e-Commerce | Survey | Students and graduates (mean age 24) |
| Barnes (2006) | SNSs | Students survey/ literature review | Students |
| Beresford et al. (2012) | Online shopping | Experiment | Mainly students |
| Brown (2001) | Online shopping | In-depth interviews | Internet users (mean age 28) |
| Carrascal et al. (2013) | Email/entertainment/finance/ news/search/e-shopping/SNSs | Survey | Web users (mean age 32) |
| Egelman et al. (2012) | Smartphone applications | Experiment | Smartphone users, over 18 years old |
| Hann et al. (2007) | e-Business/e-services | Experiment | Students |
| Huberman et al. (2005) | Personal information trade | Experiment | Internet users (mean age 40) |
| Hughes-Roberts (2013) | SNSs | Survey | Students |
| Lee et al. (2013) | SNSs/location data | Focus groups/experiment | Experiment: users of SNSs (mean age 25)/ focus group: users of Location-Based Social Network Services (mean age 29) |
| Norberg et al. (2007) | Finance services | Experiment | Students |
| Oomen and Leenes (2008) | Internet use | Survey | Students |
| Reynolds et al. (2011) | SNSs | Survey | Facebook users |
| Spiekermann et al. (2001) | Online shopping | Experiment | Mainly students |
| Taddicken (2014) | SNSs | Survey | Users of SNSs (average age in the range of 30–39 years) |
| Tufekci (2008) | SNSs | Survey | Students |
| Zafeiropoulou et al. (2013) | Location data | Survey | Internet users (average age in the range of 26–34 years) |

organisations. They also conducted a survey that revealed a strong correlation between information privacy concern and all types of responses, except for misrepresentation.

Moreover, contrary to previous research, Blank et al. (2014) found that younger people are more likely to take action to protect their privacy than older ones. In addition, studies show a positive correlation between privacy concerns and protection behaviour. Lutz and Strathoff (2014) conducted a telephone survey in Switzerland employing a questionnaire that covered several privacy-related constructs. This survey confirmed a weak but statistically significant influence of privacy concerns on protection behaviour.

Recent surveys show that privacy concerns trigger protective responses, such as uninstalling mobile applications. A survey of smartphone users by the Pew Internet Project (Boyles et al., 2012) revealed that 54% of mobile application users have decided to not install a cell phone application when they discovered how much personal information they would need to share in order to use it and 30% of cell phone application users have uninstalled an application that was already on their cell phone because they learned it was collecting personal information that they did not wish to share. On the other hand, only 19% of cell phone owners have turned off the location tracking feature on their cell phone.

Table 1 provides a list of the studies that provide evidence that support the privacy paradox hypothesis and Table 2 lists the studies that provide evidence that challenge it.

**Table 2 – Studies that provide evidence that challenge the privacy paradox hypothesis.**

| Study | Context | Methodology | Participants |
|---|---|---|---|
| Blank et al. (2014) | SNSs | Survey | Users of SNSs (random sample) |
| boyd and Hargittai (2010) | SNSs | Survey | Students |
| Christofides et al. (2009) | SNSs | Survey | Students |
| D'Souza and Phelps (2009) | e-Commerce | Survey | Students (mean age 21)/alumni (mean age 47) |
| Egelman et al. (2012)[a] | Smartphone applications | Experiment | Smartphone users, over 18 years old |
| Lutz and Strathoff (2014) | Internet use/SNSs | Survey | Sample of the general population (average age in the range of 30–49 years) |
| Miltgen and Peyrat-Guillard (2014) | Internet use | Focus groups | Internet users (average age in the range of 25–44 years) |
| Son and Kim (2008) | e-Commerce | Survey | Internet users (median age of 41) |
| Tsai et al. (2011) | Online shopping | Survey/experiment | Survey: Internet users (mean age 30)/experiment: Internet users |
| Wakefield (2013) | e-Commerce | Survey | Random sample (average age above 35 years) |
| Young and Quan-Haase (2013) | SNSs | Survey | Students |

[a] The results of this research can be interpreted in two ways, thus it appears in both the list of studies that support the privacy paradox hypothesis and those that challenge it.

### 3.3. *Understanding the controversy*

Research on the privacy paradox phenomenon has produced contradictory results. Several studies have shown a dichotomy between privacy concerns and attitudes and actual privacy behaviour, whilst other studies indicate that individuals' privacy behaviour is in line with their concerns and attitudes. In this section we investigate the causes of this contradiction and make recommendations for research to overcome the controversy.

First, there is an issue of *interpretation*. Studies of individuals' valuation of privacy have provided price estimations that can be interpreted in, at least, two ways. A value of 7 Euros that users price their browsing history (Carrascal et al., 2013) can be consider too low to match the privacy concerns people express, but it also shows that people do value their privacy. We should consider, as well, that users are aware that these data are practically unprotected. We should also consider the ethical parameter. Individuals may be willing to sell, or even to give away, some personal information to a specific recipient, but they still strongly object to the uncontrolled exploitation of the same data without their consent. Similarly, a premium of $1.50 for a privacy-preserving mobile application (Egelman et al., 2012) is low as an absolute value, but it can also be interpreted as a high valuation if we consider that it is three times the initial price of $0.49.

The studies presented in Sections 3.1 and 3.2 have investigated the privacy paradox in several different contexts. Most of them are concerned either with e-Commerce or SNSs. Smartphone applications have been considered in only one study (Egelman et al., 2012) and other important online services, such as Internet telephony, remain unexplored.

Privacy behaviour is a highly *contextual phenomenon* (Morando et al., 2014). We should not expect individuals to demonstrate the same behaviour in different contexts. Consider, for example, the studies by Norberg et al. (2007) and Tsai et al. (2011). In the first study a sample of students were first asked about their willingness to disclose specific pieces of information. Twelve weeks later a confederate visited campus under the guise of carrying out research for a pilot program for a bank. The confederate distributed data collection booklets that the students were asked to complete. Students provided significantly more information about themselves in comparison with what they stated they were willing to disclose a few weeks earlier. This study took place in the familiar environment of their classroom where students feel "protected". Even though students were told that the market researcher was not associated with faculty, yet the influence of the environment was obviously strong. This may not diminish the validity of this research; nevertheless it is perilous to compare the results of this study with the results of a study of the kind Tsai et al. (2011) have conducted. The latter study involved an online shopping experiment where a shopping search engine displayed privacy policy information about online shops. In this very different context, individuals were found willing to pay a premium for privacy. Thus, we may conclude that generalisation of results is unsafe and contradicting results should be expected when studies are conducted in different contexts.

Personal information is not a coherent object. There are several types of personal information and people attribute different valuations to them. Data such as location, health status, browsing history, age and weight are treated differently by individuals. Thus, it is not appropriate to compare studies that refer to different types of personal information. Sensitivity of information is an important moderator that is often neglected and, as Mothersbaugh et al. (2012) suggest, the privacy paradox may result from a failure to account for information sensitivity. Similarly, there are several types of privacy concerns, such as concerns about social threats (including bullying and stalking), organisational threats (including secondary use by the data collector, secondary use by a third party, and marketing), and improper access by employers or the public (Krasnova et al., 2009).

Most importantly, a variety of research methodologies can be found in privacy research. Most studies are surveys, many of them online. Surveys might be appropriate for exploring beliefs and attitudes, but they are not appropriate for studies of actual behaviour. Also, surveys are not reliable when examining irregular or infrequent behaviour. Staddon et al. (2013) examined the accuracy of self-reported behaviour by comparing survey responses of Google+ users with their actual behaviour. They found that irregular or infrequent behaviours (e.g. changing privacy settings) are particularly difficult to report accurately.

Experiments appear to be more appropriate, but again the experiment setting affects the generalisability of results (Morando et al., 2014). For example, two studies that are based on experimental auctions have produced very different results for the same type of personal information. Huberman et al. (2005) estimated that the average demand price for age was $57.56, whilst Carrascal et al. (2013) estimated the average valuation for age, gender, address, and salary to be 25 Euros (approx. $30).[2] Both studies used the same type of auction (reverse second price auction), but the experiment setting and sample were different.

In experiments it is also important to have a realistic environment. Moreover, we should not expect individuals that know they are participating in an experiment to behave the same way as they would normally do. Even if they are given false information about the experiment, so as not to suspect that it is about privacy, they would not behave the same way in a laboratory or a classroom as they would at home or at work.

Model structure and method of analysis are also important. Dienlin and Trepte (2015) used two different methodological approaches to test the privacy paradox, based on the same sample and survey instrument. Initially, they applied regression analysis to test if privacy concerns were related to specific privacy behaviours, such as the indication of (a) authentic first name, (b) authentic last name, (c) personal address, (d) mobile phone number, (e) political or religious views, and (f) frequency of posts on SNSs. Regression analysis showed privacy concerns to be unrelated to the online disclosure of first and last name, the online disclosure of mobile phone number, postings of political or religious views, and the frequency of posts on SNSs. Only the disclosure of personal address was found to be related to privacy concerns. Thus, the existence privacy paradox was adequately supported.

[2] Calculated according to the exchange rate at the time the study was conducted.

Following an alternative methodological approach, they differentiated between *informational*, *social*, and *psychological* privacy and constructed a model that introduced *privacy attitude* and *privacy intention* as moderators. A Structural Equation Modeling (SEM) analysis revealed that privacy concerns affected privacy behaviour indirectly. Specifically, they found that privacy concerns positively influence privacy attitudes, which in turn positively influence privacy intentions, which positively influence privacy behaviours. Thus, when a new methodological approach was followed the privacy paradox was dissolved (Dienlin and Trepte, 2015). Thus, this research demonstrated that the use of different research models and methods of analysis can lead to contradictory results.

## 4. Interpretations of the privacy paradox and new insights

Current research is focusing on interpreting the gap between privacy attitude and privacy behaviour. Interpretations of the privacy paradox are derived from five research areas: (a) privacy calculus theory, (b) social theory, (c) cognitive biases and heuristics in decision-making, (d) decision-making under bounded rationality and information asymmetry conditions, and (e) quantum theory homomorphism.

### 4.1. *Privacy calculus and the benefits of self-disclosure*

Privacy calculus theory postulates that individuals perform a calculus between the *expected loss of privacy* and the *potential gain of disclosure*. Their final behaviour is determined by the outcome of the privacy trade-off (Dinev and Hart, 2006; Jiang et al., 2013; Xu et al., 2011). Thus, it is assumed that individuals decide to disclose personal information when potential gains surpass expected losses. In social interactions rewards are mostly intangible and thus difficult to observe. As a result the disclosing behaviour of users often seems unreasonable and inconsistent with their privacy concerns. However, if we consider the intangible rewards involved, then the disclosing behaviour of users becomes more understandable. In fact, several studies have confirmed that users of SNSs weigh risks and benefits of sharing private information and disclose personal information when perceived benefits outweigh observed risks (Debatin et al., 2009; Lee et al., 2013).

Active participation in online social networks, which involves self-disclosure, is associated with three fundamental needs: (a) the need for diversion and entertainment, (b) the need for social relationships, and (c) the need for identity construction (Debatin et al., 2009). Thus, for most users, satisfying the above needs overweighs the observed risks of disclosing personal data. This holds even for users that have experienced privacy invasion, although these users are more likely to change their privacy settings. In addition, the use of online social networking has been ritualised and built into users' daily life (Debatin et al., 2009), thus, for them, it is difficult to deviate from the routine of self-disclosure.

Benefits of information sharing that users value the most include *self-clarification*, *social validation*, *relationship development*, *social control*, and *self-representation* (Lee et al., 2013). Self-clarification refers to understanding oneself and clarifying one's views and feelings about issues of interest. Social validation is the validation of one's views or values by other people. Relationship development is realised by enhancing the nature of significant relationships. Social control is achieved by influencing others and changing their attitude or behaviour and self-representation refers to establishing an image of oneself.

Social networking is a way of gaining *social capital*. Social capital refers to the accumulated resources derived from the relationships among people within a specific social context or network (Ellison et al., 2011). Individuals disclose personal information in order to earn social capital. For example, an individual that discloses a medical diagnosis will be more likely to receive supporting messages from network members (Stutzman et al., 2012).

### 4.2. *Social theory–based interpretations*

There are also strong motivations for self-disclosure stemming from the way online social networks have been embedded into the social lives of users, who in order to maintain their social lives, must disclose information on them despite their privacy concerns (Blank et al., 2014). Social theory may enhance our understanding of this phenomenon. Lutz and Strathoff (2014) adopt a perspective of online social networks as *social collectives* and make a distinction between social collectives that are held together by its members' *internalised emotional ties* and *implicit rules* and social collectives that are held together by more *rational calculations* and the corresponding mechanisms, such as contracts and legal rules. The former are known in the relevant literature as *Gemeinschaften* (communities), whilst the latter are known as *Gesellschaften* (societies) (Tönnies, 2003). Online social networks have several characteristics that would justify their characterisation as *Gemeinschaften*, rules of behaviour in online social networks are mostly implicit and individuals foster their relationships and search for a feeling of belonging. In such *Gemeinschaft*-like forms of social collectives individuals are willing to provide information and data about themselves as this is an implicit part of being a member of the community (Lutz and Strathoff, 2014).

On the other hand, SNSs are formal institutions, mostly private companies such as Facebook Inc., with formal rules and policies. Thus, there is both a *Gemeinschaft* and *Gesellschaft* side in SNSs. When considering privacy hazards, users may adopt the *Gesellschaft* perspective and make rational calculations of privacy risks, whilst when acting as part of the online community they may adopt the *Gemeinschaft* perspective. Thus, the emotional attraction of being part of a community collides with the calculated hazards of data misuse. This collision is often resolved in favour of the *Gemeinschaft* perspective as the emotional rewards of belonging to a community, being concrete and immediate, override the abstract, calculated risks of data misuse (Lutz and Strathoff, 2014).

An alternative social theory that can be used to explain the privacy paradox is *structuration theory* (Giddens, 1984). Structuration theory is a sociological model that has emerged in an attempt to resolve the debate between social theories that emphasise the role of human *agency* (i.e., individuals' ability to act based on their free choices) and those that underline the role of the social *structure*. Structuration theory discards

the discretion between agency and structure and claims that these do not exist independently from one another, but they rather form two sides of the same phenomenon. According to Giddens (1984, 377) structure exists only as "memory traces" and is instantiated in action. In other words, people's actions produce, reproduce, or alter social structure, which at the same time constraints people's actions; this process is referred to as *structuration*.

Zafeiropoulou et al. (2013) draw upon structuration theory to provide an explanation of the privacy paradox in the context of location data, which are produced by mobile devices and used by numerous mobile applications and SNSs. They posit that privacy decisions can be seen as part of a process of structuration, where individuals do not make information-sharing decisions as entirely free agents and are instead heavily influenced by contextual factors (e.g., social norms, trust in the mobile application) during trade-off decisions (Zafeiropoulou et al., 2013).

Online privacy is a new social phenomenon that people are still struggling to understand. The *social representations* that would allow people to understand privacy as a concept have not emerged yet, as an empirical study by Oetzel and Gonja (2011) has shown. A social representation is a conceptual scheme that comprises values, ideas, metaphors, beliefs, and practices that are shared among the members of a community. The *theory of social representation* suggests that individuals understand new concepts based on established schemes, through the processes of *objectification* and *anchoring* (Oetzel and Gonja, 2011). Anchoring involves the ascribing of meaning to new phenomena by means of integrating them into existing conceptual schemes, so that they can be interpreted and compared to available knowledge (i.e. things already known). In the process of objectification abstract concepts become concrete through the emergence of new social representations. Since a social representation of online privacy has not been established yet, often individuals do not succeed to develop a reliable perspective on online privacy.

### 4.3. *Cognitive biases and heuristics in privacy decision-making*

The privacy calculus theory is based on the assumption that individuals make privacy decisions as rational agents, in the economic sense, by means of calculating risks and benefits. However, research in behavioural economics has shown that human decision-making is affected by cognitive biases and heuristics (Acquisti and Grossklags, 2007). It is unlikely that privacy decisions are not affected by the same biases and heuristics. The latter include *optimism bias*, *overconfidence*, *affect bias*, *fuzzy-boundary and benefit heuristics*, and *hyperbolic discounting*.

Optimism bias refers to the consistent tendency of individuals to believe that they are less at risk of experiencing a negative event compared to others. Optimism bias has a neurological basis (Sharot et al., 2007), which explains why it is so pervasive. Cho et al. (2010) have tested empirically the effect of optimism bias on privacy behaviour. Relying on data from a telephone survey they found that individuals display a strong optimism bias about online privacy risks, judging themselves to be significantly less vulnerable than others to these risks. Baek et al. (2014) confirmed that individuals perceive the likelihood of personal online privacy infringement to be lower than that of other individuals (comparison targets) in a study that was based on large-scale online survey data. Comparative optimism (i.e., the perceived difference between personal and target risk) is more pronounced when the comparison target is younger, as people tend to believe that young people are significantly more susceptible to privacy infringements. In addition, they found that optimism regarding online privacy breach is negatively related to the adoption of privacy protective behaviours. In other words, optimism bias hinders people from protecting themselves.

Moreover, individuals tend to exhibit overconfidence in their skills and knowledge. In a relevant study (Jensen et al., 2005) participants were asked if they knew about certain privacy enhancing technologies and, then, were asked a follow-up question to probe their knowledge. Less than 25% of participants who claimed to know a technology were able to answer simple questions about it. In addition, when individuals are given more control over the release and accessibility of their information (i.e., they are able to control which information will be published), they tend to reveal more personal information, exposing themselves to higher privacy risks (Brandimarte et al., 2013).

*Affect heuristic* is one of the most established human decision-making and behaviour biases (Slovic et al., 2002). It refers to a mental shortcut that allows people to make judgments and decisions quickly based on their affective impressions. A consequence of the affect heuristic is that individuals tend to underestimate risks associated with things they like and overestimate them when associated with things they dislike. Positive affect (e.g. enjoyment) is positively related to an individual's intention to disclose personal information (Wakefield, 2013). Affect is expected to influence the assessment of risks of self-disclosure, as well as the assessment of the benefits of self-disclosure (Kehr et al., 2013, 2014). Users tend to underestimate the risks of information discloser when confronted with a user interface that elicits positive affect (Kehr et al., 2015).

Sundar et al. (2013) conducted an experiment, in which they tested the effect of two heuristics, the fuzzy-boundary and the benefit heuristics, on disclosure of personal information. A group of participants were shown a video that illustrated how personal information could be misused by third parties (i.e. fuzzy-boundary condition) and another group was shown a video that presented the benefits of personalisation (i.e. benefit condition). Later, participants in both groups were given a questionnaire to fulfill, which included several personal questions. Individuals who were primed with the fuzzy boundary heuristic were less likely to disclose personal information, whilst those who were primed with the benefit heuristic tended to disclose more information about them. Based on these results the authors suggest an explanation of the privacy paradox arguing that the self-reports of increased privacy concerns noted in surveys could be a product of systematic processing, whilst actual privacy behaviours are probably determined by heuristic processing.

The tendency to discount future benefits, i.e. to value future benefits less than present ones, has been extensively studied by economics research. One of the most prominent models of discounting is *hyperbolic discounting* (Acquisti and Grossklags,

2003). Hyperbolic discounting theory claims that humans discount the future in a time-inconsistent manner; their preferences change as they approach the time to choose among options. Hyperbolic discounting has a direct effect on privacy-related decisions. When individuals are asked about their intention to adopt a privacy-protection strategy, they calculate the benefits of privacy protection against the benefits of information disclosure and they may find the former to be more significant. However, when they make these calculations and express their intention to adopt a privacy-protection strategy, they are thinking about a decision to be taken in the future. When future comes and they have to actually make that decision, their preferences change, as they now discount the future benefits of privacy protection by a higher factor than they did earlier. Thus, the dichotomy between intentions and behaviour can be interpreted as an inability of individuals to predict their future decisions, as their preferences on which they base their decisions are time-inconsistent.

Wilson and Valacich (2012) identified two more factors that contribute to "irrational behaviour", *benefit immediacy* and *risk diffusion*. According to their model, when individuals perceive the benefits of disclosure to be immediate rather than delayed, they tend to perceive risks to be lower and benefits to be higher. Analogously, when risk is diffused, e.g. if personal information is expected to be collected in 1–2 years from the time consent when was given, individuals tend to perceive risks to be lower and benefits to be higher. However, the above model has not been empirically tested.

### 4.4. *Bounded rationality, incomplete information, and information asymmetries*

Most people are lacking the cognitive ability to calculate privacy risks and disclosure benefits and do not have access to all necessary information in order to make informed judgments about the trade-offs that are involved in privacy decisions. Individuals make privacy decision in limited time having incomplete information about risks and benefits. Moreover, as cognitive psychology has shown, they are not able to calculate all the relevant parameters (Camerer, 1998). Thus, their privacy decisions are constrained by *incomplete information* and *bounded rationality* (Acquisti and Grossklags, 2005), two conditions that affect decision-making in several contexts (e.g. economics, business administration, etc.). Bounded rationality refers to the cognitive limitations facing a human decision maker – limitations of both knowledge and computational capacity.

*Information asymmetries* prevail in the relationship between consumers and providers in the Internet and mobile market. For example, mobile application consumers have very little knowledge of how their personal data are used. Mobile application consumers do not rely on the information provided by application vendors on the collection and use of personal data, when they decide which application to download. They consider information from their social group and the app store to be more important and trustworthy (Buck et al., 2014).

Baek (2014) showed that the dichotomy between privacy concerns and behavioural intention disappears when individuals are presented with arguments either for or against the use of personal information by online businesses. Participants in Baek's study were divided in three groups. The first group was presented with a short message promoting regulation on the collection and use of personal data, the second group was presented with a message with arguments supporting the collection and use of personal data, and the third group was given no message at all. Then, all participants were asked to complete a survey questionnaire that measured privacy concerns and intention to disclose personal information. Concerns and intentions were positively related in the first two groups, whilst concerns and intentions were unrelated in the third group.

### 4.5. *Quantum theory homomorphism*

Expanding the variety of disciplines that provide a basis for explaining the privacy paradox, Flender and Müller (2012) engage concepts from quantum theory to provide an understanding for the privacy paradox. They consider human decision-making to be analogous to the measurement process in quantum experiments. This new perspective allows incorporating effects like *indeterminacy*, i.e. the outcome of a decision making process is determined at the time the decision is made but not prior to it, in descriptions of privacy decision making. Privacy decisions are affected by the indeterminacy effect as individuals may alter their preferences indeterminately, i.e. at the time an actual decision is made.

## 5. Discussion and recommendations

Research on the privacy paradox has followed a dialectic course. Initial studies that revealed a dichotomy between privacy attitude and actual privacy behaviour were followed by others that showed a significant influence of privacy attitude on privacy behaviour. This debate triggered significant research that has aimed to resolve the paradox either by interpreting the phenomenon or by building comprehensive models that unveiled the complex nature of the phenomenon. Thus, the dichotomy between privacy attitude and behaviour should not be considered a paradox anymore, since recent literature provides several logical explanations. It is, however, a complex phenomenon that has not been fully explained yet. Current research has shed light to various aspects of the paradox, but it is still infeasible to put the pieces of the puzzle together so as to form the "whole picture". Table 3 summarises the various explanations presented at the end of Section 3 and in Section 4.

Research on the privacy paradox can be categorised in terms of the *theoretical background*, the *methodological approach*, and the *context* in which it is examined. Researchers have turned to various disciplines in search for theories that can contribute to the conceptualisation of the phenomenon and the investigation of probable explanations. These include social theory, behavioural economics, psychology, and quantum theory. Several researchers have studied privacy paradox from a social theory perspective, using theories such as structuration theory (Zafeiropoulou et al., 2013), media theories (Debatin et al., 2009), communicative privacy management theory (Lee et al., 2013), gemeinschaft/gesellschaft theory (Stutzman et al., 2012), and the theory of social representation (Oetzel and Gonja, 2011).

Behavioural economics have contributed the concepts of *bounded rationality* and *incomplete information* that have been used

**Table 3 – Explanations of the privacy paradox.**

| Explanations | Studies |
|---|---|
| Individuals perform a *privacy calculus* | Dinev and Hart (2006); Jiang et al. (2013); Xu et al. (2011) |
| Perceived benefits of SNS participation (e.g. satisfying fundamental needs) outweigh observed risks | Debatin et al. (2009); Lee et al. (2013) |
| Habitual use of SNSs and integration into daily life | Blank et al. (2014); Debatin et al. (2009) |
| Individuals disclose information so as to gain *social capital* | Ellison et al. (2011); Stutzman et al. (2012) |
| Participating in a community (Gemeinschaften) vs. participating in a society (Gesellschaften) | Lutz and Strathoff (2014) |
| Individuals do not make information-sharing decisions as entirely free agents (Structuration Theory perspective) | Zafeiropoulou et al. (2013) |
| Privacy decisions are affected by cognitive biases and heuristics (e.g. optimism bias, overconfidence, affect bias, fuzzy-boundary and benefit heuristics, hyperbolic discounting) | Acquisti and Grossklags (2003; 2007); Baek et al. (2014); Brandimarte et al. (2013); Cho et al. (2010); Jensen et al. (2005); Kehr et al. (2013; 2014); Kehr et al. (2015); Sundar et al. (2013); Wakefield (2013); Wilson and Valacich (2012) |
| Privacy decisions are affected by bounded rationality, incomplete information and information asymmetries | Acquisti and Grossklags (2005); Baek (2014); Buck et al. (2014) |
| Individuals have not developed a reliable perspective on online privacy, since a *social representation* of online privacy has not been established yet | Oetzel and Gonja (2011) |
| Privacy decisions are affected by the *indeterminacy effect* (quantum theory perspective) | Flender and Müller (2012) |
| Methodological explanations: Inappropriate/incomplete models, missing factors, inappropriate research methods, etc. | Dienlin and Trepte (2015); Morando et al. (2014); Mothersbaugh et al. (2012); Staddon et al. (2013) |

to explain privacy decisions (Acquisti and Grossklags, 2005). Also, behavioural economics have unveiled the role of cognitive biases and heuristics in decision making. Several researchers have studied the privacy paradox under the perspective of psychological/cognitive biases and heuristics (Acquisti, 2004; Acquisti and Grossklags, 2003, 2005, 2007; Baek, 2014; Baek et al., 2014; Brandimarte et al., 2013; Buck et al., 2014; Cho et al., 2010; Jensen et al., 2005; Kehr et al., 2013, 2014, 2015; Sundar et al., 2013; Wakefield, 2013; Wilson and Valacich, 2012).

Finally, there is one attempt to explain the privacy paradox in terms of quantum theory concepts (Flender and Müller, 2012). Although quantum theory is obviously not a neighbouring discipline, quantum theory concepts, such as *indeterminacy*, applied isomorphically provide an interesting conceptualisation of the phenomenon.

With regard to methodology, there are mainly two approaches: surveys and experiments (see Table 4). Most surveys are based on convenience samples (e.g. students), which raises an issue of validity. Surveys rely on self-reported behaviour, which often differs from actual behaviour. This issue is addressed by the experimental approach. Nevertheless, most experiments in the relevant literature fail to recreate a realistic context.

The privacy paradox has been studied in various contexts. Mainly, two types of context have been studied: social situations and transactional situations. Studies of privacy in social situations are primarily concerned with SNSs, such as Facebook and Google+ , and online chatting. Transactional situations include a variety of cases, including DVD stores, mobile applications, e-shops, and finance web-sites.

**Table 4 – Methodological approaches.**[a]

| Methodological approach | Studies |
|---|---|
| Survey | Acquisti and Grossklags (2005); Baek et al. (2014); Barnes (2006); Blank et al. (2014); boyd and Hargittai (2010); Buck et al. (2014); Carrascal et al. (2013); Cho et al. (2010); Christofides et al. (2009); D'Souza and Phelps (2009); Debatin et al. (2009); Dienlin and Trepte 2015); Ellison et al. (2011); Hughes-Roberts (2013); Jiang et al. (2013); Krasnova et al. (2009); Lutz and Strathoff (2014); Son and Kim (2008); Oomen and Leenes (2008); Reynolds et al. (2011); Stutzman et al. (2012); Taddicken (2014); Tufekci (2008); Wakefield (2013); Young and Quan-Haase (2013); Zafeiropoulou et al. (2013) |
| In-depth interviews/focus groups | Brown (2001); Debatin et al. (2009); Ellison et al. (2011); Lee et al. (2013); Miltgen and Peyrat-Guillard (2014); Young and Quan-Haase (2013) |
| Analysis of (actual) data | Hughes-Roberts (2013); Reynolds et al. (2011); Staddon et al. (2013) |
| Experiment | Baek (2014); Beresford et al. (2012); Brandimarte et al. (2013); Egelman et al. (2012); Hann et al. (2007); Huberman et al. (2005); Jensen et al. (2005); Kehr et al. (2014; 2015); Lee et al. (2013); Mothersbaugh et al. (2012); Norberg et al. (2007); Spiekermann et al. (2001); Sundar et al. (2013); Tsai et al. (2011); Xu et al. (2011) |
| Conceptual/analytic | Acquisti (2004); Acquisti and Grossklags (2003; 2007); Barnes (2006); Flender and Müller (2012); Kehr et al. (2013); Oetzel and Gonja (2011); Son and Kim (2008); Wilson and Valacich (2012) |

[a]Studies that appear in more than one category use a combination of methods.

### 5.1. *Recommendations*

The studies presented in this paper refer to several different types of personal information. The latter include age, weight, phone number, address, date of birth, income, photos, browsing history, location data, SNS posts, religious and political beliefs, etc. Personal information is not homogeneous and individuals' attitudes vary depending on the type of personal information concerned. Moreover, different types of privacy concerns are considered, such as social threats (e.g., bullying and stalking), organisational threats (e.g. secondary use), and improper access by employers or the public. It should be expected that some types of privacy concerns have a stronger influence on attitudes and behaviour than others.

Since most of the above studies focus on individual aspects of the privacy paradox phenomenon, there is a need for synthetic studies that would be based on comprehensive theoretical models that take into account the diversity of personal information, as well as the diversity of privacy concerns. Studies of this kind would allow us to build a clearer picture of the relation between privacy attitudes and behaviour. Also, current research has not considered the diversity of privacy harms (Solove, 2006). This is an important variable that should be further investigated.

Regarding the research methodology, both surveys and experiments are useful research instruments. Nevertheless, future research should address the shortcomings of these methods that we have witnessed in previous research. Survey research should take into account the fact that self-reports on privacy behaviour are unreliable, especially when they refer to infrequent events (e.g. adjusting privacy settings in SNSs). Therefore, future research should make more use of "hard data", i.e. evidence of actual behaviour, rather than self-reports.

Surveys should also consider that the privacy paradox is not a symptom of young people, but it concerns users of all ages. Therefore, samples should be as representative as possible. Future research could also focus on specific age and cultural groups, such as elderly individuals, rural cultural groups, etc.

Both survey and experimental research should take into account the fact that privacy is a highly contextual phenomenon. Particularly experiments should be conducted in realistic settings that provide a rich and relevant context. Comparative studies could also examine privacy attitudes and behaviour in different contexts, such as online shopping, SNSs and e-government services.

With regard to background theories although the privacy paradox has been studied through a variety of theoretical lenses, no theoretical model has prevailed, thus there is still room for new theoretical perspectives. In particular, there are several behavioural science theories that could be considered, such as *social cognitive theory* and its derivatives (Bandura, 2001).

Finally, we may notice that the privacy paradox has been studied in isolation. The relation of privacy behaviour with privacy awareness campaigns, with the technological environment and the availability of privacy enhancing technologies, has been under-researched. Moreover, a better understanding of the privacy paradox may enable a new perspective on the legal and ethical framework of information privacy. Concluding, we may argue that although there has been a large volume of research on the privacy paradox, it remains a wide open issue.

## REFERENCES


Acquisti A. Privacy in electronic commerce and the economics of immediate gratification. In: Proceedings of the 5th ACM conference on electronic commerce, May 17–20, 2004, New York, USA; 2004.

Acquisti A, Grossklags J. Losses, gains, and hyperbolic discounting: an experimental approach to information security attitudes and behavior. In: Proceedings of the 2nd annual workshop on economics and information security (WEIS 2003), May 29–30, 2003, Maryland, USA; 2003.

Acquisti A, Grossklags J. Privacy and rationality in individual decision making. IEEE Secur Priv 2005;2:24–30.

Acquisti A, Grossklags J. What can behavioral economics teach us about privacy. In: Acquisti A, Gritzalis S, Lambrinoudakis C, di Vimercati S, editors. Digital privacy: theory, technology, and practices. Auerbach Publications; 2007. p. 363–77.

boyd D, Hargittai E. Facebook privacy settings: who cares? First Monday 2010;15(8).

Baek YM. Solving the privacy paradox: a counter-argument experimental approach. Comput Human Behav 2014;38:33–42.

Baek YM, Kim EM, Bae Y. My privacy is okay, but theirs is endangered: why comparative optimism matters in online privacy concerns. Comput Human Behav 2014;31:48–56.

Bandura A. Social cognitive theory: an agentic perspective. Annu Rev Psychol 2001;52(1):1–26.

Barnes SB. A privacy paradox: social networking in the United States. First Monday 2006;11(9).

Beresford AR, Kübler D, Preibusch S. Unwillingness to pay for privacy: a field experiment. Econ Lett 2012;117(1):25–7.

Blank G, Bolsover G, Dubois E. A new privacy paradox. 2014. Working Paper, University of Oxford, Global Cyber Security Capacity Centre.

Boyles JL, Smith A, Madden M. Privacy and data management on mobile devices. Pew Research Center. <http://pewinternet.org/Reports/2012/Mobile-Privacy.aspx>; 2012 [accessed 10.02.15].

Brandimarte L, Acquisti A, Loewenstein G. Misplaced confidences privacy and the control paradox. Soc Psychol Pers Sci 2013;4(3):340–7.

Brown B. Studying the internet experience. HP Laboratories Technical Report (HPL-2001-49). <http://www.hpl.hp.com/techreports/2001/HPL-2001-49.pdf>; 2001 [accessed 10.02.15].

Buck C, Horbel C, Germelmann CC, Eymann T. The unconscious app consumer: discovering and comparing the information-seeking patterns among mobile application consumers. In: Proceedings of the 2014 European conference on information systems (ECIS2014), June 9–11, 2014. Tel Aviv, Israel; 2014.

Camerer C. Bounded rationality in individual decision making. Exp Econ 1998;1(2):163–83.

Carrascal JP, Riederer C, Erramilli V, Cherubini M, de Oliveira R. Your browsing behavior for a Big Mac: economics of personal information online. In: Proceedings of the 22nd international conference on World Wide Web (pp. 189–200), May 13–17, 2013, Rio de Janeiro, Brazil; 2013.

Cho H, Lee JS, Chung S. Optimistic bias about online privacy risks: testing the moderating effects of perceived controllability and prior experience. Comput Human Behav 2010;26(5):987–95.

Christofides E, Muise A, Desmarais S. Information disclosure and control on Facebook: are they two sides of the same coin or two different processes? Cyber Psychol Behav 2009;12(3):341–5.

Debatin B, Lovejoy JP, Horn AK, Hughes BN. Facebook and online privacy: attitudes, behaviors, and unintended consequences. J Comput-Med Commun 2009;15(1):83–108.
Dienlin T, Trepte S. Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. Eur J Soc Psychol 2015;45(3):285–97.
Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions. Inform Syst Res 2006;17(1):61–80.
D'Souza G, Phelps JE. The privacy paradox: the case of secondary disclosure. Rev Market Sci 2009;7(1).
Egelman S, Felt AP, Wagner D. Choice architecture and smartphone privacy: there's a price for that. In: Proceedings of the 11th annual workshop on the economics of information security (WEIS2012), June 25–26, Berlin, Germany; 2012.
Ellison NB, Vitak J, Steinfield C, Gray R, Lampe C. Negotiating privacy concerns and social capital needs in a social media environment. In: Privacy online. Berlin Heidelberg: Springer; 2011. p. 19–32.
Flender C, Müller G. Type indeterminacy in privacy decisions: the privacy paradox revisited. In: Quantum interaction. Berlin Heidelberg: Springer; 2012. p. 148–59.
Giddens A. The constitution of society: outline of the theory of structuration. University of California Press; 1984.
Gilovich T, Griffin D, Kahneman D, editors. Heuristics and biases: the psychology of intuitive judgment. Cambridge University Press; 2002.
Hann IH, Hui KL, Lee SYT, Png IP. Overcoming online information privacy concerns: an information-processing theory approach. J Manage Inform Syst 2007;24(2):13–42.
Holvast J. Vulnerability and privacy: are we on the way to a risk-free society? In: Proceedings of the IFIP-WG9.2 conference, May 20–22, 1993, Namur, Belgium; 1993.
Huberman BA, Adar E, Fine LR. Valuating privacy. IEEE Secur Priv 2005;3(5):22–5.
Hughes-Roberts T. Privacy and social networks: is concern a valid indicator of intention and behaviour? In: Proceeding of the international conference on social computing (SocialCom 2013), September 8–14, 2013, Washington, USA. 2013.
Jensen C, Potts C, Jensen C. Privacy practices of Internet users: self-reports versus observed behavior. Int J Hum Comput Stud 2005;63(1):203–27.
Jiang Z, Heng CS, Choi BC. Research note: privacy concerns and privacy-protective behavior in synchronous online social interactions. Inform Syst Res 2013;24(3):579–95.
Kehr F, Wentzel D, Mayer P. Rethinking the privacy calculus: on the role of dispositional factors and affect. In: Proceedings of the thirty fourth international conference on information systems, December 15–18, 2013, Milan, Italy; 2013.
Kehr F, Wentzel D, Kowatsch T. Privacy paradox revised: pre-existing attitudes, psychological ownership, and actual disclosure. In: Proceedings of the thirty fifth international conference on information systems, December 14–17, 2014, Auckland, New Zealand; 2014.
Kehr F, Kowatsch T, Wentzel D, Fleisch E. Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. Inform Syst J 2015;doi:10.1111/isj.12062. [Last Access 27.04.15]. Published online.
Krasnova H, Günther O, Spiekermann S, Koroleva K. Privacy concerns and identity in online social networks. Ident Inform Soc 2009;2(1):39–63.
Lee H, Park H, Kim J. Why do people share their context information on Social Network Services? A qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk. Int J Hum Comput Stud 2013;71(9):862–77.
Lutz C, Strathoff P. Privacy concerns and online behavior – not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. Working paper, April 15, 2014. <http://dx.doi.org/10.2139/ssrn.2425132>; 2014 [access 10.02.15].
Miltgen CL, Peyrat-Guillard D. Cultural and generational influences on privacy concerns: a qualitative study in seven European countries. Eur J Inform Syst 2014;23(2):103–25.
Morando F, Iemma R, Raiteri E. Privacy evaluation: what empirical research on users' valuation of personal data tells us. Internet Policy Rev 2014;3(2):1–11.
Mothersbaugh DL, Foxx WK, Beatty SE, Wang S. Disclosure antecedents in an online service context: the role of sensitivity of information. J Serv Res 2012;15(1):76–98.
Norberg PA, Horne DR, Horne DA. The privacy paradox: personal information disclosure intentions versus behaviors. J Consum Aff 2007;41(1):100–26.
Oetzel MC, Gonja T. The online privacy paradox: a social representations perspective. In: Proceedings of CHI'11 extended abstracts on human factors in computing systems, May 7–12, Vancouver, Canada; 2011.
Oomen I, Leenes R. Privacy risk perceptions and privacy protection strategies. In: de Leeuw E, Fischer-Hübner S, Tseng J, Borking J, editors. Policies and research in identity management. USA: Springer; 2008. p. 121–38.
Pew Research Center. Public perceptions of privacy and security in the post-snowden era. Pew Research Center. <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>; 2014 [accessed 10.02.15].
Reynolds B, Venkatanathan J, Gonçalves J, Kostakos V. Sharing ephemeral information in online social networks: privacy perceptions and behaviours. In: Proceedings of the 13th IFIP TC13 conference on human-computer interaction (INTERACT 2011), September 5–9, Lisbon, Portugal; 2011.
Rosenberg R. The social impact of computers. Academic Press Inc; 1992.
Sayre S, Horne D. Trading secrets for savings: how concerned are consumers about club cards as a privacy threat? Adv Consum Res 2000;27(1):151–5.
Sharot T, Riccardi AM, Raio CM, Phelps EA. Neural mechanisms mediating optimism bias. Nature 2007;450:102–5.
Slovic P, Finucane M, Peters E, MacGregor DG. The affect heuristic. In: Gilovich T, Griffin DW, Kahneman D, editors. Heuristics and biases. Cambridge University Press; 2002. p. 397–420.
Solove DJ. A taxonomy of privacy. Univ PA Law Rev 2006;154(3):477–560.
Son JY, Kim SS. Internet users' information privacy-protective responses: a taxonomy and a nomological model. MIS Quart 2008;32(3):503–29.
Spiekermann S, Grossklags J, Berendt B. E-privacy in 2nd generation e-commerce: privacy preferences versus actual behavior. In: Proceedings of the 3rd ACM conference on electronic commerce. October 14–17 Florida, USA; 2001.
Staddon J, Acquisti A, LeFevre K. Self-reported social network behavior: accuracy predictors and implications for the privacy paradox. In: Proceedings of the 2013 international conference on social computing (SocialCom 2013), September 8–14, Washington, USA; 2013.
Stutzman F, Vitak J, Ellison NB, Gray R, Lampe C. Privacy in Interaction: exploring disclosure and social capital in Facebook. In: Proceedings of the 6th international conference on weblogs and social media (ICWSM 2012), June 4, Dublin, Ireland; 2012.
Sundar SS, Kang H, Wu M, Go E, Zhang B. Unlocking the privacy paradox: do cognitive heuristics hold the key? In: Proceedings of CHI'13 extended abstracts on human factors in computing systems, April 27–May 2, Paris, France; 2013.

Sutanto J, Palme E, Tan C-H, Phang CW. Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on smartphone users. MIS Quart 2013;37(4):1141–64.
Taddicken M. The 'privacy paradox' in the social web: the impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure. J Comput-Med Commun 2014;19(2):248–73.
Tönnies F. Community and society. New York: Dover Publications Inc; 2003.
TRUSTe. Consumer opinion and business impact. TRUSTe Research Report. <http://info.truste.com/lp/truste/Web-Resource-HarrisConsumerResearchUS-ReportQ12014_LP.html>; 2014 [accessed 10.02.15].
Tsai JY, Egelman S, Cranor L, Acquisti A. The effect of online privacy information on purchasing behavior: an experimental study. Inform Syst Res 2011;22(2):254–68.
Tufekci Z. Can you see me now? Audience and disclosure regulation in online social network sites. Bull Sci Technol Soc 2008;28(1):20–36.
Wakefield R. The influence of user affect in online information disclosure. J Strat Inform Syst 2013;22(2):157–74.
Wilson D, Valacich JS. Unpacking the privacy paradox: irrational decision-making within the privacy calculus. In: Proceedings of the 33rd international conference on information systems (ICIS2012), December 16–19, Florida, USA; 2012.
Xu H, Luo XR, Carroll JM, Rosson MB. The personalization privacy paradox: an exploratory study of decision making process for location-aware marketing. Dec Support Syst 2011;51(1):42–52.
Young AL, Quan-Haase A. Privacy protection strategies on Facebook: the Internet privacy paradox revisited. Inform Commun Soc 2013;16(4):479–500.
Zafeiropoulou AM, Millard DE, Webber C, O'Hara K. Unpicking the privacy paradox: can structuration theory help to explain location-based privacy decisions? In: Proceedings of the 5th annual ACM Web science conference, May 2–4, Paris, France; 2013.

Spyros Kokolakis is an Assistant Professor at the Department of Information and Communication Systems Engineering at the University of the Aegean, Greece. He received a B.Sc. in Informatics from the Athens University of Economics and Business in 1991 and a Ph.D. in Information Systems from the same university in 2000. His current research interests include information systems security management, risk analysis, and security policies design and implementation. He is a member of AIS.