The Illusion of Control in Privacy Trade-Offs: Does Familiarity Play a Role?

Ivana de Boer
Radboud University
Nijmegen, The Netherlands

Eelco Herder*
eelcoherder@acm.org
Radboud University
Institute for Computing and Information Sciences
Nijmegen, The Netherlands

Marc van Lieshout
marc.vanlieshout@ru.nl
Radboud University
iHub - Interdisciplinary Hub for Security, Privacy and Data Governance
Nijmegen, The Netherlands

ABSTRACT

Contemporary legislative and scientific trends stress the importance of control as an instrument to manage informational privacy. Still, privacy decision-making remains far from optimal as there is a discrepancy between privacy attitudes and privacy behaviours. To interpret this gap, this study builds upon the systematic biases found in behavioural economics theory, more specifically the illusion of control. This study examines the effects of the illusion of control through stimulus familiarity on privacy behaviour. More specifically, we compared the participants' willingness to provide personal data between a very familiar web store and a web store unknown to them. The results from a sample of 171 students in the Netherlands indicate that, even though the level of perceived control and the amount of data disclosure are higher in the familiar condition, stimulus familiarity does not induce an illusion of control in privacy trade-offs. Moreover, this relationship is slightly weaker for sensitive disclosure. However, this study did find evidence of gender differences in sensitive disclosure: in this sample, women disclosed significantly less sensitive information than men, possibly due to risk-aversion.

CCS CONCEPTS

• **Security and privacy → Economics of security and privacy**; **Social aspects of security and privacy**.

KEYWORDS

Privacy, personal data, illusion of control, behavioural economics

ACM Reference Format:
Ivana de Boer, Eelco Herder, and Marc van Lieshout. 2021. The Illusion of Control in Privacy Trade-Offs: Does Familiarity Play a Role?. In *Adjunct Proceedings of the 29th ACM Conference on User Modeling, Adaptation and Personalization (UMAP '21 Adjunct), June 21–25, 2021, Utrecht, Netherlands.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3450614.3464471

*Contact author

UMAP '21 Adjunct, June 21–25, 2021, Utrecht, Netherlands

ACM ISBN 978-1-4503-8367-7/21/06…$15.00
https://doi.org/10.1145/3450614.3464471

1 INTRODUCTION

Privacy is one of the most pressing issues in the digital age, as control over personal data is limited. Decades ago, influential legal scholars already recognized control as an important instrument to manage privacy, including informational privacy [6, 25]. Since then, the control perspective on privacy has become even more relevant. This is not only reflected by the development of new data protection laws, such as the GDPR[1], that specifically adopt a control approach, but also by the connectivity of the data economy through which individuals lose control over their personal data. Empirical evidence suggests that a higher level of perceived control leads to a more positive privacy attitude and alleviates privacy concerns [16, 17, 26]. Yet, individuals do not always act in accordance with their privacy attitudes. Even though we feel entitled to the protection of our privacy, we end up exchanging the same information for relatively small rewards or out of convenience.

The discrepancy between privacy attitudes and privacy behaviours has been coined 'the information privacy paradox'. There is a large volume of research about the privacy paradox debate (e.g. [12, 18, 23]), however, the question why privacy behaviours are not in line with privacy attitudes remains largely unanswered. This study builds upon the psychological and behavioural economics literature to bridge this gap. Behavioural economics theory advocates that deviations from rationality in decision-making are caused by behavioural biases [5]. Likewise, due to emotional and cognitive inconsistencies, individuals can engage in irrational privacy behaviour. Several systematic biases have already been identified in the privacy domain.

To extend the framework of behavioural biases, this study will focus on the *illusion of control*. Based on Langer's theory about illusory control [20], *stimulus familiarity* is used to induce an illusion of control. Langer found that individuals are likely to experience little control in situations if the object is unfamiliar because it is difficult to foresee which actions bring about the desired results. Moreover, preliminary evidence about the control paradox indicates that a higher level of perceived control over the publication of personal data can paradoxically lead to *more* data disclosure [9]. Therefore, the research question addressed in this paper is: "What are the effects of the illusion of control on privacy behaviour?".

Understanding how individuals are affected by the illusion of control is of significant importance to legislators and policy makers,

[1] https://gdpr-info.eu/

as more insights into the role of perceived control in privacy trade-offs can contribute to more effective policies. Currently, control fulfils a pronounced role in data protection laws. Yet, as *control can paradoxically lead to more data disclosure*, some researchers suggest that control is a necessary but not sufficient means to protect our privacy [3, 9] In addition, knowledge about the illusion of control can be of great importance to actors involved with the development of e-commerce as they could use this knowledge to alleviate privacy concerns of their customers or exploit it to elicit more data disclosure. This is especially relevant now that the retail industry is undergoing a discontinuous shift from offline to online.

This study adopts an exploratory research approach and uses an online survey-based experiment to examine the effects of the illusion of control on privacy behaviour in the context of e-commerce. In the experiment, participants were asked to create a personal account for a web store, that was either very familiar or unfamiliar to the subject, in exchange for a virtual credit. It was predicted that higher familiarity with a web store leads to more data disclosure due to the overestimation of control. Also, this relationship was expected to be stronger for sensitive personal information.

The results from a sample of 171 students in The Netherlands indicate that, even though perceived control and (sensitive) data disclosure is higher in the familiar condition, stimulus familiarity does not induce an illusion of control in privacy trade-offs. Since website familiarity reduces complexity and uncertainty in privacy decisions, it is likely that individuals find it more difficult to manage their privacy in the unfamiliar condition [14]. An unexpected finding in this study are the gender differences in the amount of sensitive disclosure. In this sample, women disclose significantly less sensitive information than men.

2 LITERATURE REVIEW

This section explores the body of literature relevant for this study. Control has multiple implications for privacy, both legally and empirically. Therefore, this section builds upon the knowledge from various academic fields such as legal scholarship, privacy research, psychology and behavioural economics theory.

2.1 Privacy as control

Even though privacy theory found its origin decades ago, the conceptualization of privacy is still ongoing. The umbrella term 'privacy' covers, among others, what privacy is, what privacy should protect and what comprises a privacy violation [19]. The aspects are widely disputed, as there is no universally accepted definition of privacy. Nevertheless, several approaches to privacy can be identified and distinguished from each other. There are three main approaches to privacy in legal scholarship, i.e. i) privacy as confidentiality, ii) privacy as identity construction or as practice and iii) privacy as control [11].

To start, the privacy as confidentiality perspective was formalized by Warren & Brandeis (1890) in their 'right to be let alone' [8]. The rise of innovations at the time allowed journalists, newspapers and gossip press to disclose unauthorized information about individuals, which was previously considered as private. In their seminal article, the authors consider whether the law could afford a principle to counter these privacy violations. In this view, privacy is seen as the protection from intrusion to one's personal life.

The second perspective, privacy as identity construction or as practice, considers privacy as the freedom from unreasonable constraints on the construction of one's own identity through social relationships [4]. An important determinant for privacy in this perspective is context [21]. Privacy violations often involve (mis)using personal data from one context in another context. For instance, individuals might disclose specific medical data to doctors but not to their colleagues. The rise of new technologies often breaks down existing contexts. This perspective of privacy is particularly relevant for activities such as profiling and micro-targeting.

Even though the perspectives of privacy as confidentiality and identity construction provide relevant insights for the concept of privacy, this study will focus on the *privacy as control paradigm*, given its importance in today's informational society. This is not only reflected by the fundamental role of control in current data protection laws such as the EU General Data Protection Regulation (GDPR), but also by the rise of the data economy. The data economy brings potential benefits for both businesses and individuals through competitive advantage, innovations and social relationships [15]. However, it has consequences for our informational privacy. Data brokers monetize personal data by collecting personal data from various sources, including social networking sites (SNSs), the Internet of Things (IoT) and e-commerce businesses, and distributing it among unaffiliated parties.

2.2 Privacy attitudes

People have different stances about informational privacy, some feel more positively or negatively inclined about it than others. This has been researched extensively in the literature, often conceptualized by either privacy concerns (e.g. [10, 26]) or privacy attitudes (e.g. [10, 16, 22]).

Only a handful of studies examine the relationship between perceived control and privacy attitudes or concerns. To start, [16] examine the effect of perceived control of information on privacy attitudes, the intention to disclose information and actual disclosing behaviour. Second, a study by [17] study the behavioural reasons behind privacy concerns among users after the implementation of a new feature of Facebook: Facebook News Feed. When Facebook introduced this new feature, there was a privacy outcry among its users in the U.S. To investigate the reasons behind these concerns, the authors carried out a survey among Facebook users from a large U.S. university. Third, in the context of location-based services (LBS), [26] studies the effect of perceived control on privacy concerns. In an online experiment, the author examined the level of perceived control and privacy concerns of mobile phone users in Singapore. The results show that there are multiple mechanisms to increase perceived control in the LBS context.

2.3 The privacy paradox debate

Since the level of perceived control influences privacy attitudes, control could provide guidance for privacy decisions. However, privacy decision-making remains far from optimal, as individuals find it difficult to act in accordance with their privacy preferences. Empirical evidence suggests that even though we feel entitled to the

protection of our informational privacy, we end up exchanging the same information for relatively small rewards or out of convenience.

Various researchers studied the privacy paradox and found inconsistent results (e.g. [1, 12, 18]. The findings are twofold: some researchers find that privacy attitudes are not correlated with privacy behaviour, implying that individuals engage in paradoxical behaviour with regard to privacy decisions, while another stream of research suggests that the privacy paradox can be understood as privacy behaviour that can be partially explained by individual attitudes.

2.4 The illusion of control

The illusion of control is a psychological tendency that has significant influence on decision-making, also in the privacy domain. A clear distinction needs to be made between control and illusory control. Simply put, control is associated with an outcome that can actually be determined by the actor, whereas the illusion of control relates to the mere feeling of being in control, when in fact the outcome cannot be controlled. Experimental evidence of the illusion of control was first found in chance games by psychologist Langer [20].

In privacy decisions, control is more nuanced, as some parts can actually be controlled and other parts can only be partly controlled. [9] conducted three survey-based experiments in the context of SNSs among a group of U.S. students to examine the effects of perceived control on data disclosure. They found that individuals tend to focus on parts that can be controlled (i.e. publication) and neglect other significant parts that are less controllable (i.e. access and use), which gives them an illusory sense of control when making privacy decisions.

2.5 The behavioural economics of privacy

This study builds upon the psychological and behavioural economics literature to explain the discrepancy between privacy attitudes and behaviours. Behavioural economics theory advocates that some phenomena can be better understood by models in which agents do not act fully rational [7]. This deviation from rationality is borrowed from the psychological literature that recognizes a dual system of human thinking. The terms 'System 1 and System 2 thinking' were later introduced by [24]. System 1 operates automatically and unconscious, whereas system 2 requires more effort and deliberate mental processing. Both systems are used interchangeably to limit cognitive effort and to optimize performance.

3 METHODOLOGY

This study builds upon the psychological and behavioural economics literature on the illusion of control and privacy research on the control paradox. In the privacy literature, there seems to be no evidence for a direct relationship between familiarity and perceived control. In fact, little is known about the role of familiarity in general. Only a handful of studies address website familiarity. For instance, [13] found that familiarity of e-commerce websites contributes to website trust.

In line with these studies, we hypothesize that 1) higher familiarity with a web store leads to more data disclosure. Further, we expect that 2) the positive relationship between website familiarity and data disclosure is stronger for privacy sensitive data.

3.1 Procedure

Prior to the actual experiment, a prestudy was conducted. The goal of the prestudy was twofold. First, to examine the level of familiarity with two selected web stores, and second, to test and verify the level of privacy sensitiveness of the survey questions used in the actual experiment. Afterwards, similar to [9], participants were presented a list of disclosure items and asked to rate them for their level of privacy sensitiveness. In total, 41 participants participated in the prestudy. The results of the prestudy are reported in the result section.

The study itself was carried out as a survey-based online experiment. The target group for the experiment are mainly students in the Netherlands. In total, 216 participants were recruited for the experiment via social media.

In the experiment, participants were placed in a fictive scenario and asked to create a personal account for a web store in the online shopping industry. In exchange for creating the account, participants receive a virtual credit, dependent on the level of data disclosure. Apart from two mandatory questions, data disclosure was completely voluntary. A Fashioncheque[2] is chosen as a reward, because it can be used for a wide variety of web stores, in order to eliminate web store specific effects other than familiarity.

The setup was identical for both groups, except that website familiarity is manipulated: participants in Condition 1 receive a privacy trade-off from a (local) web store with low familiarity (Den Haan) and participants in Condition 2 receive a privacy trade-off from a web store with high familiarity (Zalando[3]) – the choices for these stores were verified by our prestudy. Participants are randomly redirected to one of the conditions, resulting in a between-subjects design.

The experiment starts with a screenshot of the starting page of the web store with a 'create an account' pop-up message. Participants are informed that, apart from two mandatory questions that are necessary for the creation of the account, data disclosure is completely voluntary and that their personal data will be used to provide targeted discounts and suggestions. The questions are mostly demographics that can be linked to online shopping behaviour. Only a few of the disclosure items were purposely inappropriate, such as relationship status (e.g. "Are you monogamous"), to examine whether participants would also provide sensitive data that are not connected to the activities of the web store. For every answered question, subjects receive € 1.00 on the Fashioncheque – see Figure 1. Finally, participants are asked to provide some additional information, which is used for the control variables in the analysis. The survey questions were identical for both groups and consisted of 20 questions in total.

3.2 Data analysis

The outcome variable in the analysis in H1, data disclosure, is measured by the number of disclosure items participants are willing to provide. Likewise, the outcome variable in H2, privacy sensitive

[2]https://www.fashioncheque.com/
[3]https://zalando.com/

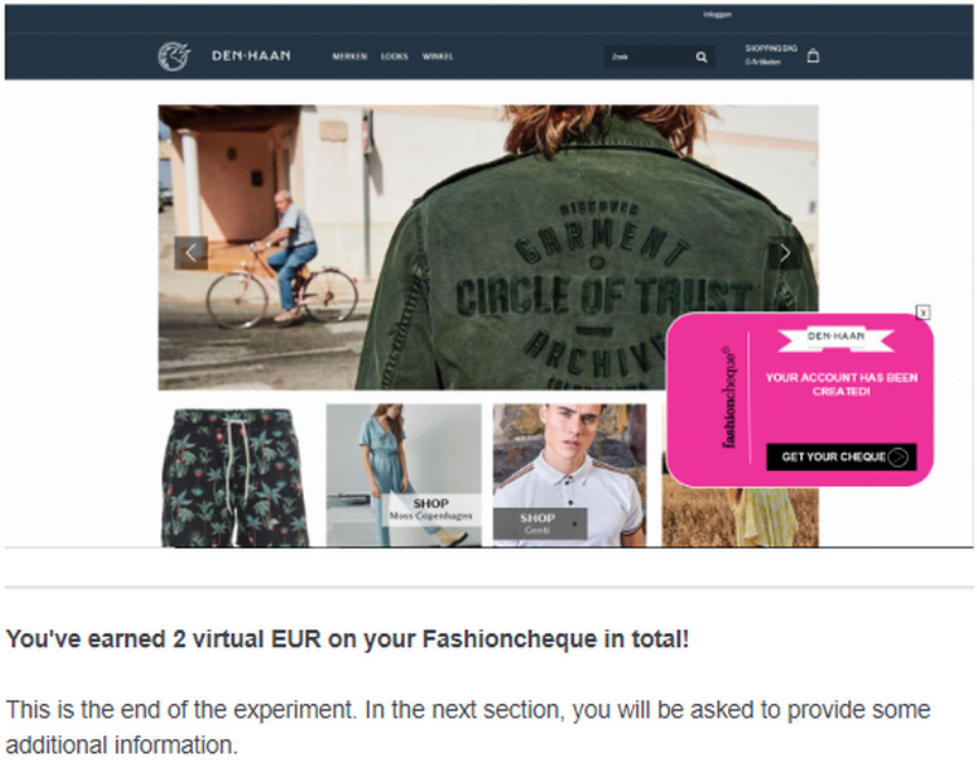

Figure 1: Screenshot of the total reward given at the end of the study.

data disclosure, is measured by the number of sensitive questions participants are willing to answer. Sensitive disclosure is measured by two proxies, i) the total amount of disclosure items labelled as very intrusive and ii) by the total amount of disclosure items labelled as very intrusive or moderately intrusive

Several control variables are included in the analysis. The control variables are exploratory, as there is no prior literature indicating an existing relationship between any variable and the effect of website familiarity and perceived control on (sensitive) data disclosure. To start, *gender* is incorporated in the analysis to account for possible differences. [16] found that females assign more weight to perceived control when disclosing information on SNSs. This finding indicates that women might be more affected by the illusion of control than men. To date, there is too little evidence in the privacy literature to draw such a conclusion. Second, *age* is included to check whether this affects the amount of personal data that subjects disclose. Third, *field of education or profession* is included to test whether participants with an education or profession in the field of privacy or computing science produce different results. Lastly, *privacy literacy* is included to see whether there are any differences between less and more privacy literate subjects.

4 RESULTS

This section describes the empirical results of the prestudy and the actual experiment. The participants from the prestudy did not take part in the actual experiment.

4.1 Results of the prestudy

Before testing the level of familiarity between the web stores, descriptive statistics were used to remove obvious outliers. Two outliers were removed after data visualization through a histogram and a box plot, reducing the sample from 41 to 39 subjects. The results of the Wilcoxon signed-rank test confirm that the level of familiarity of Zalando (Mdn = 4.50) is significantly higher than the level of familiarity of Den Haan (Mdn = 1.03), $T = 780$, $p = .000$, $R = 0.90$.

Frequency tables were used to determine the category of privacy intrusiveness of the disclosure items. The disclosure items could be categorized by the subjects as i) not at all intrusive, ii) moderately intrusive or iii) very intrusive. For each disclosure item, the category with the highest frequency was assigned. Overall, only five questions were considered not at all intrusive, seven questions as moderately intrusive and eight as very intrusive.

4.2 Results of the experiment

In total, 216 people participated in the study. From this sample, 12 participants were removed as they already participated in the prestudy. Further, 33 outliers were removed after data visualization through histograms and boxplots, reducing the sample to 171 subjects. Out of the total sample, 72 participants were male and 99 were female. Most of the participants, notably 140, fell in the age group of 19-25, which is a representative age groups for students.

When looking at the overall sample, data disclosure (Mean = 12.56), including sensitive disclosure (Mean = 4.80 for proxy 1 and

Variable	Den Haan (N = 86)	Zalando (N = 85)
Disclosure	12.30	12.81
Sensdisclosure1	4.16	4.76
Sensdisclosure2	8.92	9.39
Percontrol	5.63	5.73
Privacyliteracy	2.65	1.55

Table 1: Compared means (N=199)

9.15 for proxy 2), is relatively high. Also, participants experience a relatively high amount of control when disclosing their information (Mean = 5.68). Finally, participants demonstrate a good understanding of privacy regulations (Mean = 2.82).

The mean values for the variables are compared in Table 1, based on the grouping variable *treatment*. For participants in the familiar condition (Zalando), perceived control is higher (5.73 vs. 5.63) and data disclosure is higher (12.81 vs. 12.30) than in the unfamiliar tradition (Den Haan), including sensitive data disclosure (4.76 vs. 4.16 for proxy 1 and 9.39 vs. 8.92 for proxy 2). The mean values of Den Haan and Zalando are in line with the hypotheses and indicate that higher familiarity with a web store leads to a higher level of perceived control and more (sensitive) data disclosure. The score for privacy literacy is lower for Zalando than for Den Haan (1.55 vs. 2.65).

Figure 2 represents for each disclosure item per condition the percentage of participants that were willing to disclose this item. The response rates of the disclosure items are all relatively high. However, there is a clear difference in response rates between general demographics, such as gender, and more sensitive information, such as phone number. The low response rate for phone number compared to other very intrusive disclosure items can be explained by the fact that the future consequences of disclosing a phone number, i.e. receiving marketing calls, are more clear.

To test whether the mean differences between Condition 1 and Condition 2 significantly differ, two separate two-way independent ANOVA's are performed instead of one MANOVA, because the outcome variables demonstrate high multicollinearity ($P > .9$). A two-way independent ANOVA for each outcome variable indicates a positive relationship, meaning that higher familiarity results in more (sensitive) data disclosure. However, as the coefficients are not significant and relatively small, it does not support the proposed model.

In contrast, there is a significant effect between perceived control and personal data disclosure ($P = .188$) as well as between perceived control and sensitive data disclosure ($P = .185$) for a 90% confidence interval.

For the control variables, only gender has a significant effect on data disclosure ($P = -.172$) and sensitive data disclosure ($P = -.188$) for a 95% confidence interval. The other control variables (age, field of education or profession, privacy literacy) are non-significant for data disclosure.

5 DISCUSSION

Even though there was no significant effect, the results for H1 are partially in line with the theoretical model, as higher familiarity leads to a higher level of perceived control and overall to more data disclosure. In addition, the results for the familiar condition are consistent with the control paradox [9]. However, in the unfamiliar condition, individuals seem to manage their privacy differently. There is no clear relationship between the level of perceived control and the amount of data disclosure. This suggests that the control paradox has limitations for unfamiliar websites.

Empirical evidence suggests that individuals find it more difficult to manage their privacy at an unfamiliar web store, because website familiarity reduces complexity and uncertainty [13]. In addition, website familiarity helps in understanding the context because individuals can rely on prior experiences [14].

For H2, the results are not in line with the proposed model, as the relationship described in H1 is not stronger for sensitive data disclosure, but slightly weaker. This is in contrast with prior literature, that indicates a stronger relationship for the control paradox in the case of sensitive disclosure [9].

An unexpected finding in the amount of sensitive disclosure are the gender differences. Gender differences in disclosing behaviour were not the primary focus of this study, but only an exploratory control variable for the analysis. The results show that females disclose significantly less sensitive information than men. The privacy literature about the effect of gender on disclosing behaviour specifically is very limited and inconclusive.

5.1 Implications

The results of this study have implications for legislators and policy makers and actors involved with e-commerce businesses. To start, data protection laws, such as the GDPR, adopt an explicit control approach, by granting data subjects several control rights to manage their privacy. However, this study shows that a higher level of perceived control over the publication of personal data leads to more (sensitive) data disclosure on familiar websites. This suggests that *control is not a sufficient means to protect informational privacy on larger web stores*. More knowledge about the control paradox on unfamiliar web stores could possibly lead to distinct GDPR requirements for larger and smaller web stores.

Furthermore, the results are relevant for actors involved with e-commerce businesses, as this study suggests that individuals find it difficult to manage their privacy on unfamiliar websites. Designers could address this issue by providing additional social cues to reduce complexity and uncertainty in the privacy decision-making process.

Conversely, however, larger e-commerce businesses could use the same mechanisms to increase individual control over the publication of personal data to elicit *more* data disclosure, as it is likely that users are not aware that they disclose more personal data when they feel in control. Therefore, it is necessary to educate users about the presence of the control paradox and the potential future damages of data disclosure.

5.2 Limitations

There are several limitations to this study worth to be mentioned. To start, a significant proportion of the total sample experienced limited control over the publication of personal data when in fact disclosure was almost completely voluntary. This indicates that these subjects did not carefully read the instructions of the experiment and assumed that all the disclosure items were mandatory. It

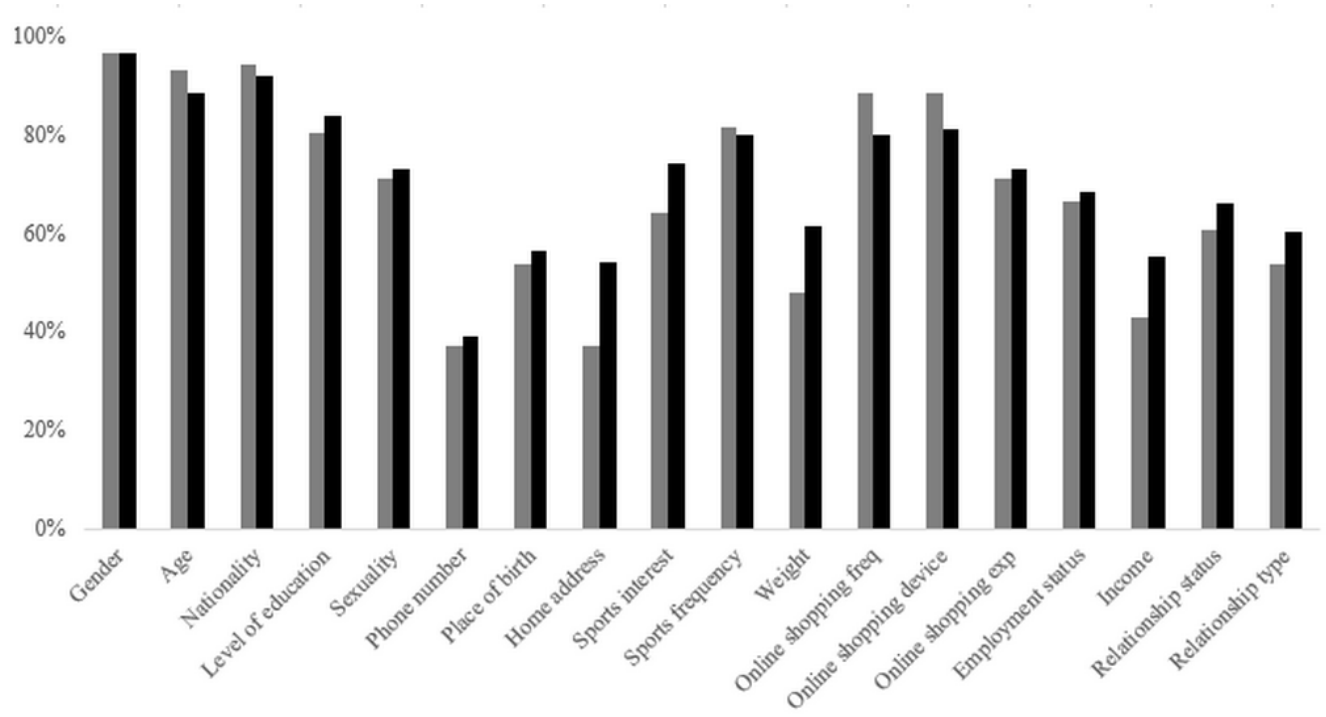

Figure 2: Percentage of participants answering the disclosure items in the unfamiliar condition 1 (grey, N = 86) and in the familiar condition 2 (black, N = 85).

is not unlikely, though, that individuals make a similar 'mistake' when they create personal accounts on actual e-commerce websites.

Second, the survey-based design of the account creation page is different from an actual environment in which the creation of an account usually takes place. Even though participants were actively reminded through text and graphics at which web store they were creating an account, the difference in environment could have influenced the results.

So far, the illusion of control has not been researched extensively in the privacy domain. Hence, there are no common control variables to include in the analysis. This study proposed several control variables, but only gender was significantly correlated with the outcome variables. Including more covariates in the analysis would increase the overall rate of variance explained.

6 CONCLUSIONS

To increase the understanding of the dichotomy between privacy attitudes and behaviour, this study extended the research on behavioural biases in privacy trade-offs. This study analysed whether website familiarity leads to more (sensitive) data disclosure through the overestimation of perceived control.

The research question can be answered by two sub questions. First, does website familiarity induce an illusion of context of regular disclosure (H1)? Second, is this relationship stronger for sensitive disclosure (H2)? The results report that there was no evidence for the illusion of control through stimulus familiarity. Hence, participants in the familiar condition did not significantly disclose more (sensitive) personal data than in the unfamiliar condition. Also, the relationship in H1 was not stronger but slightly weaker for sensitive disclosure. In conclusion, this study found no evidence for the illusion of control in privacy trade-offs. This study did find preliminary evidence of gender differences in sensitive disclosure. In this sample, females disclose significantly less sensitive information than men.

Future research could focus on other characteristics from that facilitate an illusion of control such as i) choice, ii) involvement and iii) competition [20]. It would be interesting to translate Langer's theory to the privacy domain and combine it with existing privacy research. A greater understanding of the illusion of control provides more insight in how individuals deal with perceived control and contributes to the framework of behavioural biases that are present in privacy trade-offs. Notably, [1–3, 9] already found evidence of various behavioural biases that influence privacy trade-offs. Still, a large part of the theory is still unexplored. New studies could identify other systematic biases that are present in the privacy domain.

Moreover, this study shows that our current understanding of the control paradox and website familiarity in privacy trade-offs is limited. Especially the limited knowledge of perceived control in privacy trade-offs is surprising, considering that current privacy laws are based on the control paradigm.

REFERENCES

[1] Alessandro Acquisti. 2004. Privacy in electronic commerce and the economics of immediate gratification. In *Proceedings of the 5th ACM conference on Electronic commerce*. 21–29.

[2] Alessandro Acquisti and Jens Grossklags. 2005. Uncertainty, Ambiguity and Privacy.. In *WEIS*.

[3] Idris Adjerid, Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2013. Sleights of privacy: Framing, disclosures, and the limits of transparency. In *Proceedings of the ninth symposium on usable privacy and security*. 1–11.

[4] Philip E Agre and Marc Rotenberg. 1998. *Technology and privacy: The new landscape*. Mit Press.

[5] Esma Aïmeur, Nicolás Díaz Ferreyra, and Hicham Hage. 2019. Manipulation and malicious personalization: exploring the self-disclosure biases exploited by deceptive attackers on social media. *Frontiers in Artificial Intelligence* 2 (2019), 26.

[6] Irwin Altman. 1975. The environment and social behavior: privacy, personal space, territory, and crowding. (1975).

[7] Nicholas Barberis and Richard Thaler. 2003. A survey of behavioral finance. *Handbook of the Economics of Finance* 1 (2003), 1053–1128.

[8] Louis Brandeis and Samuel Warren. 1890. The right to privacy. *Harvard law review* 4, 5 (1890), 193–220.

[9] Laura Brandimarte, Alessandro Acquisti, and George Loewenstein. 2013. Misplaced confidences: Privacy and the control paradox. *Social psychological and personality science* 4, 3 (2013), 340–347.

[10] Barry Brown. 2001. Studying the Internet experience. *HP laboratories technical report HPL* 49 (2001).

[11] Claudia Diaz and Seda Gürses. 2012. Understanding the landscape of privacy technologies. *Proceedings of the information security summit* 12 (2012), 58–63.

[12] Giles D'Souza and Joseph E Phelps. 2009. The privacy paradox: The case of secondary disclosure. *Review of Marketing Science* 7, 1 (2009).

[13] David Gefen. 2000. E-commerce: the role of familiarity and trust. *Omega* 28, 6 (2000), 725–737.

[14] David Gefen and Detmar W Straub. 2004. Consumer trust in B2C e-Commerce and the importance of social presence: experiments in e-Products and e-Services. *Omega* 32, 6 (2004), 407–424.

[15] Makrufa Sh Hajirahimova and Aybeniz S Aliyeva. 2017. About big data measurement methodologies and indicators. *International Journal of Modern Education and Computer Science* 9, 10 (2017), 1.

[16] Nick Hajli and Xiaolin Lin. 2016. Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics* 133, 1 (2016), 111–123.

[17] Christopher M Hoadley, Heng Xu, Joey J Lee, and Mary Beth Rosson. 2010. Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry. *Electronic commerce research and applications* 9, 1 (2010), 50–60.

[18] Spyros Kokolakis. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & security* 64 (2017), 122–134.

[19] Bert-Jaap Koops, Bryce Clayton Newell, Tjerk Timan, Ivan Skorvanek, Tomislav Chokrevski, and Masa Galic. 2016. A typology of privacy. *U. Pa. J. Int'l L.* 38 (2016), 483.

[20] Ellen J Langer. 1975. The illusion of control. *Journal of personality and social psychology* 32, 2 (1975), 311.

[21] Helen Nissenbaum. 2004. Privacy as contextual integrity. *Wash. L. Rev.* 79 (2004), 119.

[22] Bernardo Reynolds, Jayant Venkatanathan, Jorge Gonçalves, and Vassilis Kostakos. 2011. Sharing ephemeral information in online social networks: privacy perceptions and behaviours. In *IFIP Conference on Human-Computer Interaction*. Springer, 204–215.

[23] Sarah Spiekermann, Jens Grossklags, and Bettina Berendt. 2001. E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior. In *Proceedings of the 3rd ACM conference on Electronic Commerce*. 38–47.

[24] Keith E Stanovich and Richard F West. 2000. Individual differences in reasoning: Implications for the rationality debate? *Behavioral and brain sciences* 23, 5 (2000), 645–665.

[25] Alan F Westin. 1968. Privacy and freedom. *Washington and Lee Law Review* 25, 1 (1968), 166.

[26] Heng Xu. 2007. The effects of self-construal and perceived control on privacy concerns. *ICIS 2007 proceedings* (2007), 125.