Digital Nudges for Privacy Awareness: *From consent to informed consent?*

Bergram, Kristoffer, University of Neuchâtel, Neuchâtel, Switzerland, kristoffer.bergram@unine.ch

Gjerlufsen, Tony, Space10, Copenhagen, Denmark, tony@space10.com

Maingot, Paul, Space10, Copenhagen, Denmark, paul@space10.com

Bezençon, Valéry, University of Neuchâtel, Neuchâtel, Switzerland, valery.bezencon@unine.ch

Holzer, Adrian, University of Neuchâtel, Neuchâtel, Switzerland, adrian.holzer@unine.ch

This is the authors' version of a work that has been published in the following outlet:

Bergram, Kristoffer; Bezençon, Valéry; Maingot, Paul; Gjerlufsen, Tony; and Holzer, Adrian, "Digital Nudges for Privacy Awareness: From consent to informed consent?" (2020). In Proceedings of the 28th European Conference on Information Systems (ECIS), An Online AIS Conference, June 15-17, 2020.

DIGITAL NUDGES FOR PRIVACY AWARENESS: FROM CONSENT TO INFORMED CONSENT?

Research paper

Bergram, Kristoffer, University of Neuchâtel, Neuchâtel, Switzerland, kristoffer.bergram@unine.ch

Gjerlufsen, Tony, Space10, Copenhagen, Denmark, tony@space10.com

Maingot, Paul, Space10, Copenhagen, Denmark, paul@space10.com

Bezençon, Valéry, University of Neuchâtel, Neuchâtel, Switzerland, valery.bezencon@unine.ch

Holzer, Adrian, University of Neuchâtel, Neuchâtel, Switzerland, adrian.holzer@unine.ch

Abstract

Maintaining a private life in our digital world is gradually becoming harder. With Internet services having ever increasing access to personal data, it is crucial to raise user awareness about what privacy guarantees they offer. Regulations have recently been enacted such as the European General Data Privacy Regulation (GDPR). Yet, online service providers still have terms and privacy policies to which users tend to agree without ever viewing or reading them. By using digital nudges, this paper explores how small changes in the choice architecture can be designed to increase the informed consent and privacy awareness of users. The results from a double-blind online experiment (n = 183) show that phrasing the agreement differently and providing a highlights alternative to the existing quick-join choice architecture can significantly increase the number of users who view and read the terms and privacy policy. However, these digital nudges seem to not increase the users' recollection of what they have agreed to. The experimental results are complemented by a field test using one of the proposed designs in the IKEA Place app (n = 81'431).

Keywords: digital nudging, persuasive technology, online privacy, choice architecture, design features, HCI, privacy policy, terms and conditions, privacy awareness, informed consent, biggest lie on the Internet

1 Introduction

I have read and agree to the terms and conditions. This is known as the biggest lie on the internet (Obar and Oeldorf-Hirsch, 2020). When browsing online, we often find ourselves in a ubiquitous choice environment right before we are about to use any kind of digital service. With current regulations, online companies are forced to require informed consent from users before they can harvest their data in exchange for their 'free' services. This informed consent usually involves some complex agreement in the terms of services (ToS) and privacy policy (PP) regarding when, how and why our personal data is being collected and shared. Internet users can view these if they desire before clicking the 'I agree' button. In reality, only a small number of people ever click the adjacent link to the ToS and PP. Most people just proceed and thereby perpetrate the biggest lie on the Internet.

1.1 Poor Ability and Motivation

While fruitful research has been conducted related to macro-level privacy concerns (Dinev, McConnell, and Smith, 2015; Smith, Dinev, and Xu, 2011), we will leave privacy calculus models on the side and focus more on the observed behavior of users. When it comes to explaining why Internet users tend to not read the ToS and PP of digital services, the scientific jury is still out. Several factors might explain our dwindling ability and motivation to read the ToS and PP. Previous research on this topic highlights information overload on the part of the user (Furnell and Phippen, 2012; Obar and Oeldorf-Hirsch, 2020), that most users have "nothing to hide" (Obar and Oeldorf-Hirsch, 2020), and the fact that these complex agreements are very hard for the average Internet user to understand (Ermakova et al., 2014; Furnell and Phippen, 2012; McDonald and Cranor, 2008; Obar and Oeldorf-Hirsch, 2020). Even while leaving out the above factors, online privacy seems to be one of the contexts where many of the dials are turned in the wrong direction for optimal human decision-making (Kokolakis, 2017). Instead of having a rational wind at our back when making decisions about our online privacy, we seem to have a torrent of biases working against our better judgement (Acquisti, 2009; Acquisti, Brandimarte, and Loewenstein, 2015; Cho, J.-S. Lee, and Chung, 2010; Kokolakis, 2017; Tsai et al., 2011; Wang, Norcie, et al., 2011).

1.2 Information and Power Asymmetry

To further compound the confusion of Internet users, there is a large information gap between the providers and the end-users of digital services (Acquisti, Brandimarte, and Loewenstein, 2015). That is, service providers know with a high degree of specificity what data they want to collect from the user, whereas the user tends to have little to no idea about what data they share with the provider or other third parties (Acquisti, Adjerid, et al., 2017). Users also tend to keep better track of the benefits of an online service rather than the privacy risks that might be associated with that service (Marreiros et al., 2017). Scholars have also suggested that Internet users have trouble distinguishing between their own publication control and control related to the access of their personal information (Acquisti, 2009). To illustrate: If one decides to publish an album of their kids' and share this with their Facebook friends – this does not necessarily mean that only their friends will have access to this data and its associated metadata. However, this distinction is hard to make for many Internet users. On top of this, earlier findings suggest rather deep misconceptions among Internet users. One survey conducted in the US suggested that 62% of the sample thought that if a website had a PP, it meant that the site could not share one's data with other companies (Hoofnagle and Urban, 2014). On a general level, Internet users also seem to have a poor understanding of how their personal data is connected to the economics of these free and data-driven online services (Carrascal et al., 2013).

1.3 Towards Better Choice Architecture

Our decisions are often influenced by the choice architecture that we happen to be presented with (Thaler and Sunstein, 2009). The insight that choice environments can affect the likelihood of certain decisions and their associated behaviors have given rise to the concept of "nudging" (Mirsch, Lehrer, and Jung, 2017). In the context of human computer interaction (HCI), digital nudging refers to the use of user-interface design features that guide people's choices or behaviors in online decision environments (Weinmann, Schneider, and Brocke, 2016). Online privacy awareness is a promising problem for software designers to tackle, especially from the standpoint of choice architecture and nudging (Acquisti, 2009). Several studies have already been conducted in the context of digital nudging and online privacy (Acquisti, Adjerid, et al., 2017; Harbach et al., 2014; Kroll and Stieglitz, 2019; Wang, Leon, et al., 2013). This paper will focus exclusively on the choice architecture that potential users encounter right before they decide to join or use an online service. This is the first chance users have to inform themselves about what privacy guarantees that are offered (or lack thereof).

Yet, research suggests that most users simply ignore this opportunity and thereby perpetrate the biggest lie on the Internet (Obar and Oeldorf-Hirsch, 2020). In this paper, we address this problem by employing design considerations related to digital nudging and persuasive technology. Specifically, we will investigate how system and software designers can improve user's privacy awareness through design modifications to the current choice architecture that is being used by companies such as Facebook, Microsoft and Twitter.

2 Methodology

To investigate this topic, this paper follows a design science research methodology in accordance with the steps outlined by Peffers et al. (2007). The rest of the paper is structured as follows: Section 3 discusses the problem statement and Section 4 defines the objectives of a solution in the context of previous literature. Section 5 presents the design of a novel choice architecture for raising privacy awareness. We then present an experimental evaluation of the previously presented designs. Section 6 shows a real demonstrator of one of the novel choice architectures with the example of the IKEA Place app and discusses the observed user behavior in the field. Finally, the last section ends with a discussion and concluding remarks for the research community.

3 Backgound

At the turn of the 21^{st} century, countries around the globe built the legal infrastructure to accommodate online privacy, electronic contracting and consumer protection (Kunkel, 2002). During the last two decades, the means of extracting, cleaning, warehousing, analyzing and monetizing consumer data have arguably evolved (Phillips-Wren et al., 2015). Yet, the choice architecture that has been provided for consumers to 'agree' or to 'not agree' to these practices seems rather fixed.

3.1 Shrinkwrap, Clickwrap, Browsewrap and Quick-join

Kunkel (2002) presented case law distinctions between *shrinkwrap*, *clickwrap* and *browsewrap* that still provide an instructive background today. These distinctions can be thought of as different historical choice architectures to what eventually became online privacy. Kunkel (2002) outlined that before the Internet matured, shrinkwrap licenses got their name from the clear plastic wrapping that enclosed software packages. The packaged software contained a notice that by tearing open the shrinkwrap, the user agreed to the software terms enclosed within. The term clickwrap agreements emerged when software vendors began distributing software by means other than CD's as when the software was downloaded over the Internet. During installation or first use of an application, the classical dialog box containing the terms of the license would open for the user to read. The user was then asked to signal their informed consent by clicking 'I agree' or 'I do not agree' (Kunkel, 2002). The last category called browsewrap agreements are not as overt as the former. They do not appear on the screen and the user is not compelled to accept or reject the terms in order to proceed with the installation, download or sign-up procedure. A browsewrap agreement only appears as a link that is accessed by clicking i.e., it is optional and not required to view the actual agreement. In the early days of the Internet, this choice architecture or form of contract was successfully challenged in US courts due to the legal reason that it lacked a reasonable notice and that consumers required a more earnest opportunity to review the terms they agreed to (Hillman and Rachlinski, 2002). Today, several of the largest online service providers (e.g. Facebook, Twitter, Microsoft) offer a fusion of the browsewrap and the clickwrap architecture. One has to indicate their agreement with the click of a button but viewing the actual contents of the ToS and PP can still be a matter of choice meaning that the agreements are at least readily available through an adjacent link. Obar and Oeldorf-Hirsch (2017) now refer to this fusion category as a 'quick-join' option while noting how services like Instagram and Twitter employ this choice architecture to ensure that prospective users can join quickly without having to be bothered by scrolling through any terms or policies before accepting them.

While the current quick-join environment speeds up the collection and sharing of personal data, it does little to facilitate the informed choices of Internet users. With this choice architecture, users are given a timely prompt in the form of a link right before they agree to any potential terms or privacy policies. However, recent research highlights that the majority of users rarely act on this signal.

3.2 The Problem & Reality of Online Privacy

A few data points from Obar and Oeldorf-Hirsch (2020) will suffice to underline the main problem that this paper is addressing. In the process of joining a fictitious social networking service, 74% of a sample of US college students joined without even looking at the privacy policy. Of those that did read it, the average reading time was 1 minute and 14 seconds. Obar and Oeldorf-Hirsch (2020) estimate that it should have taken roughly 30 minutes to read the full PP that was used in their study. An even more disturbing finding was that less than 5% of the sampled participants expressed concerns around the fact that the ToS of the social networking service outlined that their data would be shared with prospective employers, insurance companies and the National Security Agency (NSA). Additionally, according to the ToS, each participant agreed to sign over their first-born child as intellectual property to the social networking service. Fortunately, the enslavement of an unborn child would not be upheld in a modern court system. However, complex data sharing practices are a real ubiquitous concern when it comes to online privacy. As mentioned in the Introduction, there are several explanations as to why we tend not to read the ToS and PP of online service providers. Research on this topic suggests that the primary factors explaining our lacking motivation and ability to look at online ToS / PP relates to information overload (Furnell and Phippen, 2012; Obar and Oeldorf-Hirsch, 2020), that most of us have "nothing to hide" (Obar and Oeldorf-Hirsch, 2020) and the sheer difficulty of reading and understanding their contents (Ermakova et al., 2014; Furnell and Phippen, 2012; McDonald and Cranor, 2008; Obar and Oeldorf-Hirsch, 2020). The reasons why we tend to not read online terms and policies can also be illuminated through a more psychological lens. Studies in economic and behavioral science suggest that we often place less weight on the future than on the present, this systematic bias is known as hyperbolic discounting (Dasgupta and Maskin, 2005; O'Donoghue and Rabin, 2000). In short, when keeping other factors constant, our preferences related to pay-offs and hazards tend to change depending on how close these pay-offs and hazards are in terms of time. Internet users seem to stay true to this inconsistency when they make decisions related to their online privacy. Scholars have argued that people also put less weight on long-term risks and losses while acting in privacy-sensitive situations (Acquisti and Grossklags, 2003). This fact makes people likely to trade their long-term privacy for relatively modest short-term pay-offs (Acquisti and Grossklags, 2005). Another study highlighted how a nationwide sample of people from Singapore displayed a strong optimistic bias regarding their online privacy (Cho, J.-S. Lee, and Chung, 2010). The participants in the sample tended to judge themselves less vulnerable than "others" to online privacy infringement. To summarize, the current choice architecture around online privacy already offers a small prompt in the form a adjacent link that one can click to review the ToS and PP before using an online service. Previous research suggests that this privacy dialog box rarely engages Internet users to inform themselves before they consent to these terms and policies. Our contention is that by employing design considerations related to nudging and persuasive technology, this problem can hopefully be mitigated.

3.3 Digital Nudges and Persuasive Technology

There is still a lot of debate around what exactly qualifies as a nudge (Hansen, 2016; Hansen and Jespersen, 2013; Hausman and Welch, 2010). However, Thaler and Sunstein (2009, p. 9) defined a nudge as "... any aspect of the choice architecture that alters people's behavior in a predictable way without forbidding any options or significantly changing their economic incentives". If a software designer works with any aspect of HCI, they are responsible for organizing the digital context in which their users make decisions (Jameson et al., 2013). That is, they are designing choice architecture.

The concept of 'digital nudging' simply refers to when peoples' choices or behaviors are being guided by user-interface design features in digital decision environments (Weinmann, Schneider, and Brocke, 2016). The use of digital nudges has been studied in a range of online contexts such as reward-based crowdfunding (Schneider, Weinmann, and Vom Brocke, 2018), social sharing (Huang et al., 2018), privacy (Kroll and Stieglitz, 2019) and digital addiction (Purohit, Barclay, and Holzer, 2020). Digital nudging is becoming increasingly relevant because people are making more and more consequential choices in online decision environments.

The study of computers as persuasive technologies or 'captology' is an inquiry into the overlap between computer science and the psychological theories related to persuasion (Fogg, 1998). One of the outputs of that research is Fogg's Behavioral Model (FBM). As a model, it offers three wide paths to aim for when persuasively designing for a new target behavior: Motivation, ability and prompts. That is, FBM emphasizes that to perform any target behavior, a person must be sufficiently motivated, have the ability to perform the behavior and be appropriately prompted or reminded to perform the behavior (Fogg, 2009). In other words, FBM is predicated on introducing pre-designed prompts while taking the user's ability and motivation into account. These pre-designed prompts come in three different varieties: *Signals* that remind the user of the task at hand, *sparks* that aim to increase the user's motivation to perform the task and *facilitators* that simplify the task for the users (Fogg, 2009). Other scholars have already attempted to combine FBM with the notion nudges. Caraban et al. (2019) reviewed and categorized 23 distinct mechanisms of nudging and presented them in a framework for technology-mediated nudging. They also grouped these 23 nudging mechanisms into the three types of prompts proposed by FBM. Relevant to the current research, Caraban et al. (2019) categorized one nudge called *throttling mindless activity* as spark. That is, this nudge can be used to modify users' motivation in tasks were users tend to mindlessly proceed. Further, they categorized a nudge called *suggesting user alternatives* as a facilitator to increase users' ability i.e., providing an attractive alternative to users can nudge them away from making a bad choice. These two nudges will be used to facilitate online privacy awareness.

4 Designing for Informed Consent

To increase users' online privacy awareness, they need to gain some meaningful facts about how their personal data is being processed. Such facts are addressed within the ToS and PP of online services. To increase their online privacy awareness users therefore need to view, read and recall some of the facts from the ToS and PP. This is what we mean by moving users towards more informed consent. The quick-join environment offers a good benchmark and is consistent with several major online service providers like Facebook or Twitter (Obar and Oeldorf-Hirsch, 2017). Yet, only a minority of users respond to this design (by actually clicking the adjacent link to the ToS and PP). Through the lens of FBM, what seems to be lacking is a privacy dialog box that sparks the users' motivation and increases the users' ability to inform themselves about their online privacy. Our design solution aims to take these two aspects into account by introducing two nudges. First, we suggest to spark users' motivation by throttling mindless activity. The current quick-join environment offers a small signal in the form of a link right before users agree to any potential terms or privacy policies. This is a type of choice architecture that resembles an opt-in policy where ignorance is the default, see Figure 1 A) on the next page. The quick-join choice architecture asks the users for consent but does not confront users with the fact that they have actively chosen to ignore the ToS and PP by not clicking the link. They have to opt-in to inform themselves. Prior research in the context of organ donations has demonstrated that a neutral choice compared to an opt-in policy is far more effective in soliciting organ donations (Johnson and Goldstein, 2003). A problem framed as an explicit choice between two equal alternatives compared to an opt-in policy is a way to increase the salience of the signal that is associated with the target behavior (Cohen, Andrade, et al., 2018). This can be achieved by designing a privacy dialog box with two buttons instead of an adjacent link. Such a choice architecture can be represented as a fork in the road, see Figure 1 B). This leads to the following hypotheses:

H1$_a$ A privacy dialog box that prompts users to make an explicit choice will increase the proportion of users that view the ToS and PP compared to a control group with an opt-in choice architecture.

H2$_a$ A privacy dialog box that prompts users to make an explicit choice will increase reading time of ToS and PP compared to a control group with an opt-in choice architecture.

H3$_a$ A privacy dialog box that prompts users to make an explicit choice will increase privacy policy recall compared to a control group with an opt-in choice architecture.

Secondly, to facilitate the users' ability to inform themselves about their own online privacy, we can suggest more alternatives related to how they view a ToS and PP. Solutions such as making content more intelligible and reducing information overload can often be facilitated by system and software designers. The design consideration of suggesting alternatives has been successfully employed in diverse contexts such as increasing the security of user's passwords (Forget et al., 2008), facilitating college choices (Bettinger et al., 2012) and increasing healthy food choices (Forwood et al., 2015). In the context of online privacy this can be accomplished by adding a brief summary of the full terms and privacy policy. Additionally, this kind of alternative has the added benefit of being a middle-option which increases its likelihood of being chosen (Simons et al., 2017; Simonson, 1989). This choice architecture can be illustrated as a roundabout, see Figure 1 C). This leads to the following hypotheses:

H1$_b$ A privacy dialog box that prompts users to make an explicit choice and offers a summarized alternative will increase the proportion of users that view the ToS and PP compared to a control group which only prompts users to make an explicit choice.

H2$_b$ A privacy dialog box that prompts users to make an explicit choice and offers a summarized alternative will increase reading time of ToS and PP compared to a control group which only prompts users to make an explicit choice.

H3$_b$ A privacy dialog box that prompts users to make an explicit choice and offers a summarized alternative will increase privacy policy recall compared to a control group which only prompts users to make an explicit choice.

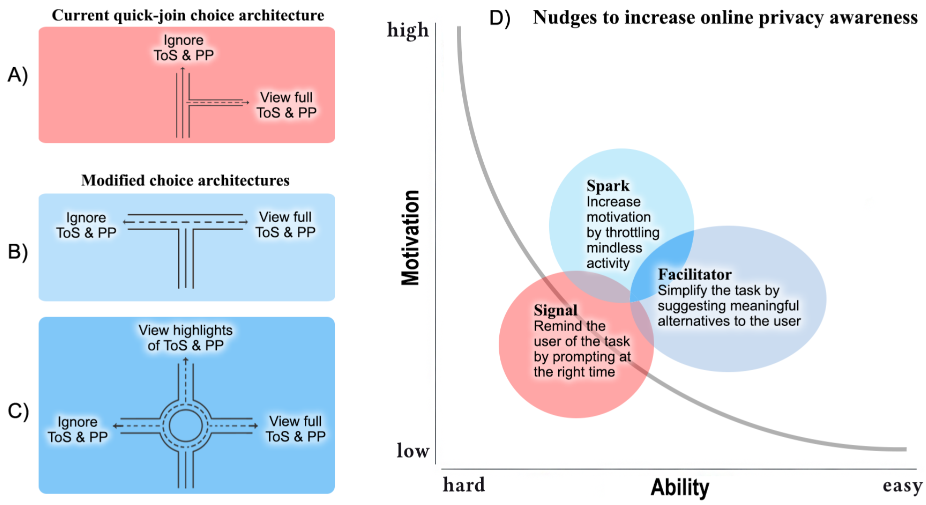

Figure 1. The choice architectures and the nudges of the proposed design solution mapped into FBM

The two proposed nudges can now be illustrated within the context FBM as in Figure 1 D). The downward slope in the model is what Fogg (2019) refers to as the action line. FBM highlights that prompts or nudges that occur on the right side of this line are more likely to achieve a specific target behavior. The standard quick-join choice architecture occurs mostly on the left side of the action line i.e., only moving a minority to the right side of the line. Our argument is that by designing nudges that also target ability and motivation, we can increase the online privacy awareness of most users. The next section outlines how these nudges were employed in the final design solution.

4.1 Proposed User Interface

Figure 2 below presents a potential privacy dialog box that implements both of the previously described nudges. The middle image shows a prompt that uses the roundabout choice architecture, i.e., providing an explicit choice while adding a summarized alternative of the ToS and PP. The 'Nothing really' button is the same choice as clicking Next. The 'Just the highlights' button leads to a summarized version of the ToS and PP. The 'Everything' button features the full content of the ToS and PP. The proposed choice architectures will be described in more detail in the following section.

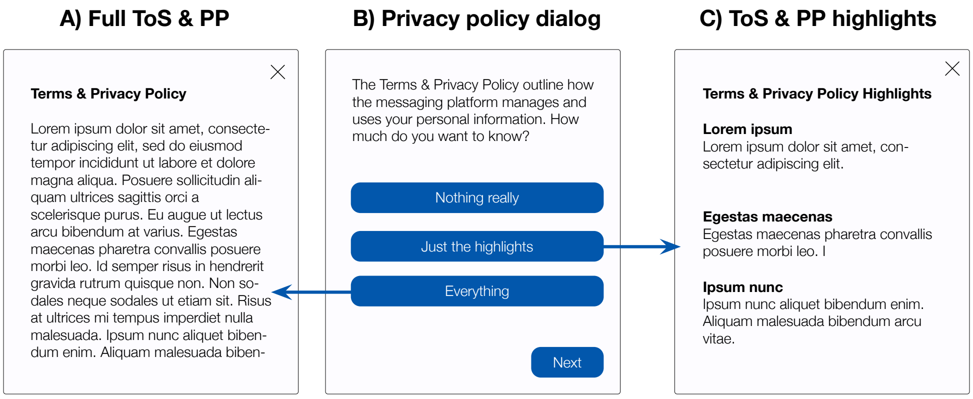

Figure 2. The user experience of the two nudges in the privacy dialog box

5 Evaluation

To investigate how software designers can improve user's privacy awareness we used the quick-join standard as a benchmark and compared it on a number of dependent measures to two modified choice architectures through an experimental design. The experimental design was cleared beforehand with the university's ethics board.

5.1 Procedure

The data collected for the experiment was drawn using Amazon's Mechanical Turk (Mturk) in accordance with Paolacci, Chandler, and Ipeirotis (2010) recommendations. Participants were filtered based on the location provided by their IP addresses, only selecting participants from the US Mturk population. From Mturk, the online participants were directed to a anonymous Qualtrics link. The participants were asked to take a survey and perform a usability evaluation of a third-party online messaging platform. The online participants were not made aware that the research concerned nudging or online privacy. During the data collection, a double-blind procedure was also used, i.e., the researchers were unaware of which group each participant ended up in and this knowledge was also hidden from each participant. The online participants were selected from the US MTurk population using the following qualifications:

(HIT Approval Rate $> 98\%$, Number of HITs Approved > 5000). A pilot experiment ($n = 56$) consisting of Swiss students suggested that the experiment took a maximum of 15 minutes to complete. Based on those results, the Mturkers were compensated \$2 US for their participation. The online participants first had to read the instructions and agree to the conditions of the study. After this, each participant was confronted with a randomly assigned choice architecture, see Figure 3. These designs will now be referred to as privacy dialog boxes (PDB). Apart from these designs, everything else in each experimental group was identical. Immediately after the participants had clicked passed these dialog boxes they received 10 questions regarding the contents of the ToS and PP. After that, they performed the usability evaluation of a messaging platform and answered some more questions related to their general online privacy concerns, the trust they felt towards the messaging service and demographical information. At the end of the online experiment all of the participants were debriefed.

5.2 Measures

To test our hypotheses the following independent measure was devised: *choice architectures*. The following dependent measures were also used: *Viewed ToS and PP, Reading Time* and *Recall*. These measures will be operationalized below. Two control measures were also used: *General concern for privacy* from (Schumann, Wangenheim, and Groene, 2014) and a question regarding the level of *trust* that users felt towards the messaging service measured on a Likert-scale from lowest (0) to highest (10).

5.2.1 Choice Architectures

Figure 3 below presents the three experimental conditions. PDB 1 (control) is an example of the current quick-join choice architecture where users have to opt-in to see the the ToS and PP like in Figure 1 A). PDB2 was nudged by an explicit choice i.e., a fork in the road as in Figure 1 B). PDB3 was also nudged with an explicit choice but with an additional suggested alternative i.e., a roundabout design.

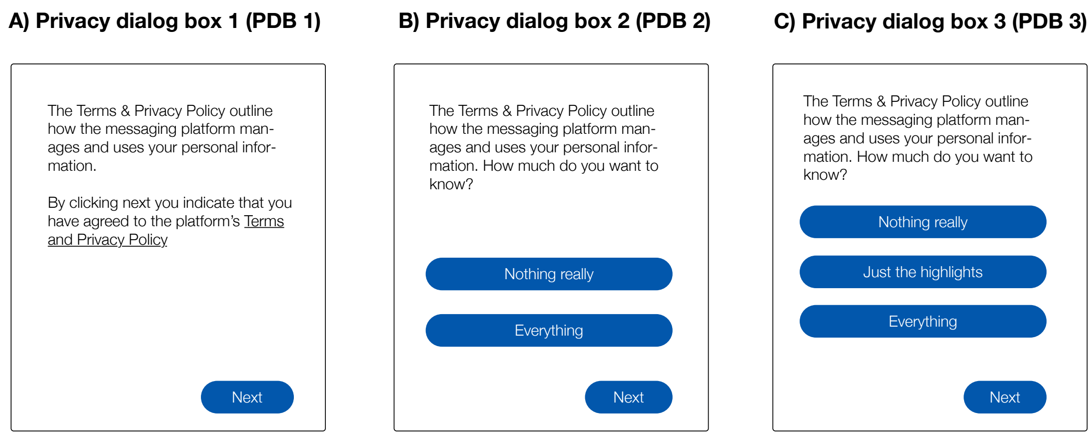

Figure 3. The choice architectures of each experimental group

5.2.2 Viewed ToS and PP

As Figure 3 illustrated, when the participants arrived on one of the randomized choice architectures, the ToS and PP were hidden. One had to click either a link or a button to view them. This dependent variable measured that click as a proxy of whether the ToS and PP was viewed. This created a binary outcome (viewed vs. did not view). As the results section will later show, this variable can be dissected further by separating the proportion of participants who clicked on the 'Highlights' button in PDB3, see Figure 3 C) above. One could also just click the 'Next' button on each dialog box to ignore the terms and policies. In other words, the choice to completely ignore the ToS and PP was not constrained by any of the designs.

5.2.3 Reading Time

This variable measured the time that each participant spent on the privacy dialog boxes. The count started when they arrived and stopped once they clicked Next. This variable was measured in seconds and was considered a proxy of reading time.

5.2.4 Recall

To measure recall of the ToS and PP contents, we devised a battery of 10 multiple choice questions with 5 alternatives each. Each question concerned a specific detail related to users' personal data and all of these facts could be found within both the full and summarized versions of the ToS and PP. The right answer gave one point and the wrong answer gave zero points creating a scale from $0-10$ that could readily be transformed to a percentage of correct answers.

5.3 Results

In total, 186 online participants were gathered for the online experiment. Three of these participants were excluded from the final analysis because they failed to submit a unique code that was generated for each run of the experiment. Out of the remaining sample ($n = 183$) there were 84 females, 98 males and one participant specified "other" as their gender. All the participants were between 19 and 68 years old ($M = 35.2$, $SD = 8.8$). The reporting of these results conform to the statistical standard of significance described by Benjamin et al. (2018). Since the dependent variables of this study did not conform to an approximate normal distribution, all inferential conclusions will stem from non-parametric tests. On the two control measures related to general privacy concerns and trust, no significant differences were found between the three choice architectures. Due to the different proportions of participants between the control group and the two experimental groups, a χ^2 test for the goodness-of-fit was conducted. The test indicated that there were no significant differences in the proportion of participants in the three randomized experimental groups $(50, 67, 66)$ as compared to the expected proportions of $(61, 61, 61)$, χ^2 $(df = 2, n = 183) = 2.98, p = .24$.

5.3.1 How choice architecture affected views (H1$_a$ & H1$_b$)

In relation to the above research hypotheses, a χ^2 test of independence highlighted a significant association between the three choice architectures and whether the participants clicked to view the terms and privacy policy, χ^2 $(df = 2, n = 183) = 27.27, p = 0.000$, Cramer's V = 0.386. Follow-up tests with a Bonferroni correction revealed a significant difference in the proportion of clicks between PDB1 and PDB2, χ^2 $(df = 1, n = 117) = 7.88, p = 0.005$ and a suggestive difference between PDB2 and PDB3, χ^2 $(df = 1, n = 133)$ = $7.47, p = 0.006$ which is in line with H1$_a$ and H1$_b$. See Figure 4 A) on the next page for a graphical illustration.

5.3.2 How choice architecture affected reading time (H2$_a$ & H2$_b$)

A Kruskal-Wallis test was used to adjudicate whether there was a statistically significant difference between the three groups in terms of the time they spent on the privacy diolog boxes. The three groups had significant differences in the time they spent on the privacy dialog boxes χ^2 $(df = 2, n = 183) = 13.02, p = 0.001$. As a follow-up, Dunn's tests were conducted between two pairs of the experimental groups using a Bonferroni correction. These tests indicated a suggestive difference between PDB1 and PDB2 ($z = -2.84, p = 0.009$). This result is in line with H2$_a$. However, in relation to H2$_b$ no differences were found between PDB2 and PDB3 ($z = -0.67, p = 1.000$), see Figure 4 B).

5.3.3 How choice architecture affected recall ($H3_a$ & $H3_b$)

Another Kruskal-Wallis test was used to gauge differences between the three groups in terms of their immediate recall scores. When all participants per group are taken together (viewers and non-viewers), the test showed no significant difference in recall scores between the three groups $\chi^2\ (df = 2, n = 183) = 0.26, p = .879$. In other words, if all the bars in Figure 4 C) are aggregated within each experimental group, no differences are detected. $H3_a$ and $H3_b$ are therefore not supported. Yet, a Mann-Whitney U-test revealed a significant difference in recall scores between those that viewed any portion of the terms and privacy policy i.e., Everything or Highlights $(Md = 7, n = 118)$ compared to those that did not $(Md = 3, n = 65)$, $U = 1746.5$, $z = 6.14$, $p = 0.000$, $r = 0.45$. Figure 3 D) demonstrates this difference.

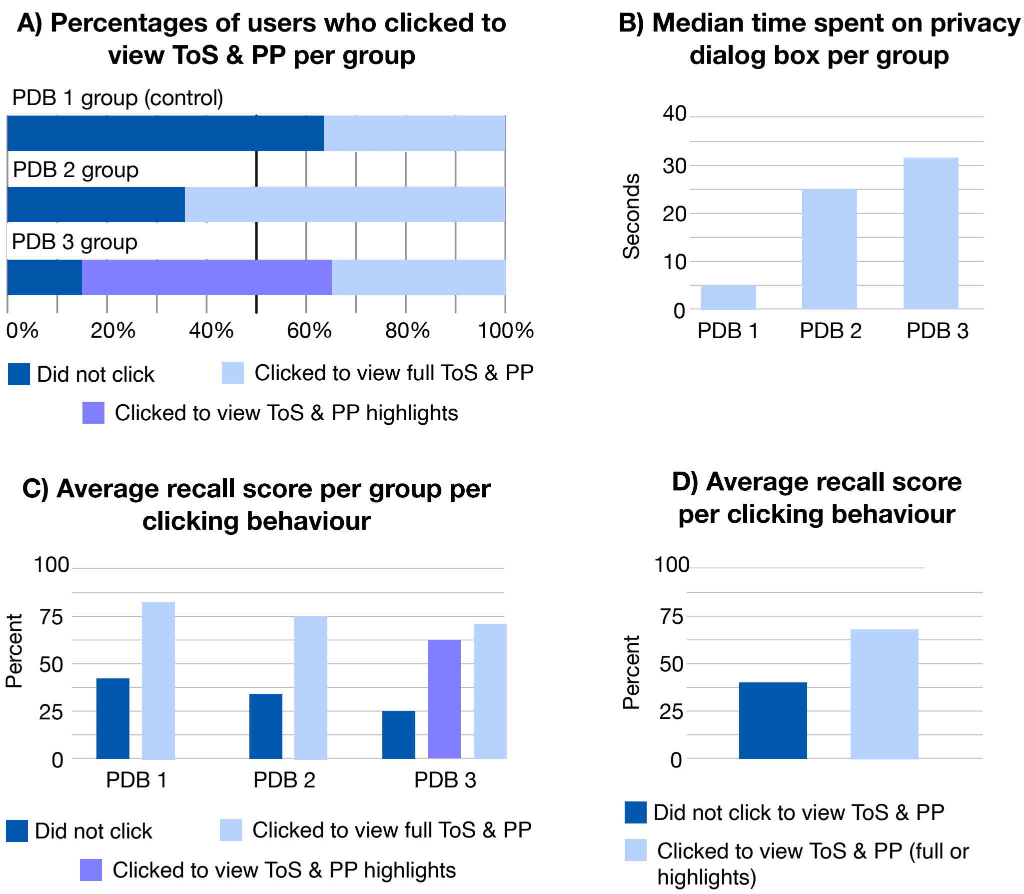

Figure 4. Visualizations of the data from the randomized online experiment (n = 183)

6 Field Study - IKEA Place App

IKEA Place is an example of a mobile application using the choice architecture featured in PDB3. Place is an augmented reality app that lets people virtually place true-to-scale 3D models of IKEA products (e.g. a chair) in their own space (e.g. their kitchen). Even though this augmented reality app does not ask for user identity, it requires access to the camera of the user's device to work properly. Furthermore, as the app is aimed to be used in the user's home, it can potentially access sensitive information. Thus, raising the user's awareness about the app's ToS and PP is important to build trust with users. Figure 5 shows the UI of the IKEA Place app. When opening the app, users can choose between 3 options just as in PDB3: 'Nothing really', 'Just the Highlights' or 'Everything'.

If they choose option 1, they are directly brought to the agreement page where they have to confirm that they have read, understood and accepted the ToS and PP. If they choose option 3 'Everything', they are shown the full ToS and PP. They can then press continue and they arrive on the agreement screen. If they choose option 2 'Just the highlights', they are presented with the summary of the Tos and PP. The summary take the form of four successive screens, with an image on each screen along with a short explanation. These screens include the camera, improving the app, keeping data safe and your rights as shown in Figure 5.

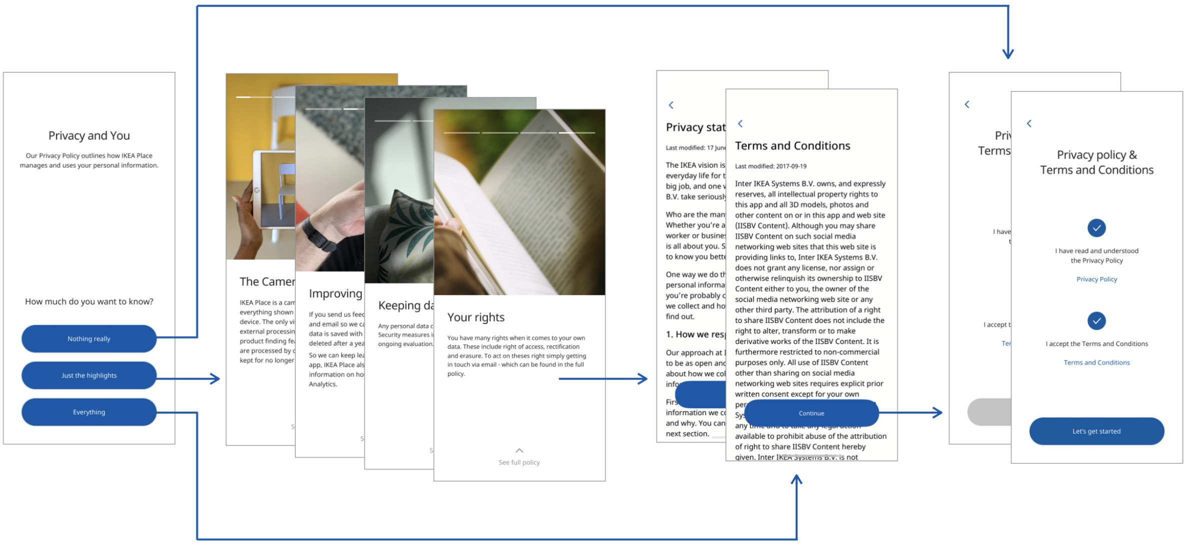

Figure 5. The user experience related to online privacy in the IKEA Place app

6.1 Evaluation in the Wild

To gain further insights into how this choice architecture affected actual user behavior, we analyzed anonymous usage data from the IKEA Place app. To do so, we deployed an analytics engine to record activity traces from November 7th 2019 to November 27th 2019. During that period, 81'431 users were active on the app. We mainly focused on the option selected by users when they opened the app for the first time. Dropout rates were also recorded during the process, as well as viewing behavior of the full ToS and PP.

6.1.1 How many users viewed the ToS and PP

The results revealed that (46%) of the users chose to read the ToS and PP. Here, Option 1 (Nothing really) is chosen 54% of the times, while Option 2 (Just the highlights) is chosen 20% of the time, and Option 3 (Everything) 26% of the time, see Figure 6.

6.1.2 How many users proceeded to accept the ToS and PP

The results showed 97.5% of users who selected Option 1 (Nothing really), proceeded to accept the ToS and PP and started using the service. This percentage was 92.2% for users who selected Option 3 (Everything) and 76.6% for users who selected Option 2 (Just the highlights). The dropout rate includes users who abandoned the app and those who went back to the privacy dialog and potentially selected another option. These descriptive results might indicate that the implementation of Option 2, which forces users to stay a fixed amount of time on each one of the highlight screens, might add too much friction to the user experience. Further analysis of the user behavior of those who selected Option 3 indicates that only 11% of users scrolled through 50% or more of the ToS and PP. These results further illustrate that bringing users to view the ToS and PP is a necessary but not sufficient action to raise privacy awareness.

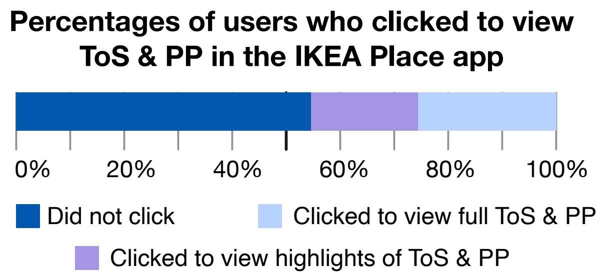

Figure 6. Data visualization related to the IKEA Place app users (n = 81'431)

7 Discussion and Conclusion

In this paper we investigated how the design of new choice architectures could mitigate what is called the biggest lie on the Internet: The fact that people confirm they have read the ToS and PP without doing so. As Walker (2016, p. 153) argued, "privacy notices are incredibly detailed legalese designed to indemnify the firm, not protect the consumer". As a result, users lack motivation and ability to read this content. The problem is aggravated by service providers using the quick-join choice architecture, which encourages users to ignore the ToS and PP by default. To tackle this problem, we used two digital nudges to design two privacy dialog boxes: One aimed at sparking users' motivation by throttling mindless activity with an explicit choice (PDB2) instead of having an opt-in default (PDB1). Similarly, the other privacy dialog box was designed as an explicit choice but also aimed at facilitating the user's ability by providing a meaningful summarized alternative (PDB3). Our experimental results show that with both these designs, the number of users who view the ToS and PP is significantly higher than with the quick-join design. Interestingly, when we compare the quick-join standard with the PDB3, adding the (highlights) option converts non-readers into highlight readers but does not lead those who read the full ToS and PP to only read the highlights when that alternative is suggested, see Figure 4 A). Our results converge with prior research showing that framing the choice as a neutral question (PDB1 vs. PDB2) rather than an opt-in policy can drastically change users' choices (Cohen, Andrade, et al., 2018; Johnson and Goldstein, 2003). Furthermore, the results show that suggesting a simpler alternative also drives viewing behavior in the context of privacy awareness. This design consideration has worked in other contexts as well (Bettinger et al., 2012; Forget et al., 2008; Forwood et al., 2015).

However, the results of this study are mixed. Although a strong case can be made that viewing and reading the ToS and PP should increase participants' recollection of that content, neither one of the two choice architectures changed the average recall score. Based on the description of the data in Figure 4 C), we observe that users who read the ToS and PP in PDB1 tended to recall it better than those who read the ToS in PDB2 and 3. The same pattern is observed for those who completely ignored the terms and privacy policy. Thus, although PDB2 / - 3 vs. the quick-join group (PDB1) increase the proportion of users who view/read the ToS (or its highlights), those who read it, recall it less accurately. The additional users who read the ToS and PP due to the new choice architectures may be users who are less interested in the actual content (compared to those who read the ToS and PP from the quick-join environment). Although they click and read because of the nudges (which entails a quite automatic processing of the information), they might only read the content superficially, using limited cognitive resources. A possible risk in using nudging techniques that tap onto the automatic mind, is their lack of any educational effects (M. K. Lee, Kiesler, and Forlizzi, 2011). This could explain the unchanged recall scores in the nudged groups. Reading is an important outcome because many users confirm they have read and agreed to ToS and PP without reading it, which engage their legal responsibilities towards online service providers. Yet, is recall an important outcome? If the aim is to move users towards more informed consent of the ToS and PP, then recall seems to be a good proxy. An alternative aim for future research could be to encourage users to act based on this knowledge. An example would be by changing the privacy settings of the actual app either via the application itself or a plugin. Another future research avenue could be to investigate whether user actions are contingent on their reading or recollection of the privacy policy (or on none of them). The implications of this research are salient at a time when technology allows for new types of data to be collected without much user awareness (Buck, 2017; Obar and Oeldorf-Hirsch, 2020). These results provide an initial step to raise users' awareness by nudging them to view and read the relevant information related to their data privacy (even if they do not necessarily recall it better). If regulation and policy does not sufficiently assist or protect consumers, will service providers have an interest to increase privacy awareness among their users? One answer could come from organizations which strive to establish trust with their customers. The IKEA Place app is one example of a company willing to raise users' privacy awareness. If users become more aware of how their data is treated by each service provider, they can demand that these services become more sensitive to online privacy. The type of data that is collected and the way it is used could become part of the value proposition together with the service itself.

7.1 Limitations

Our proposed implementation of the digital nudges represents one instance among many possible alternative designs, which implies that our solution can be further optimized by both researchers and practitioners. The following limitations should be noted. First, our data from the IKEA Place app is only used for a descriptive purpose to show that that these digital nudges can be readily implemented by large online service providers to facilitate the informed consent of their users. We cannot validate that this design is superior in the field due to the lack of comparable control groups. We only do that in the randomized online experiment. Second, the MTurk population was compensated to conduct the task we proposed. Some participants might have felt that it was part of their task to read the ToS and PP even if we did not make any such suggestions. Indeed, compared to real users of the IKEA Place app, a higher proportion of online experiment participants viewed both the highlights and the full ToS and PP. Prior scholars have suggested that the Mturk population can be more attentive than average students (Hauser and Schwarz, 2016). However, differences such as these do not change across the groups of the online experiment. Third, we cannot control for novelty effects in our findings i.e., that new choice architectures such as in PDB2 - / 3 facilitated viewing and reading behavior by the fact that the participants had not seen this particular design before. Yet, we did take steps during the analyses of the online experiment by following Benjamin et al. (2018) recommendations to reduce the rate of false positives for new findings.

7.2 Concluding Remarks

With more and more personal data being gathered and processed online, raising the bar for informed consent is an important challenge. Today, companies are legally compelled to inform their users. Yet, few users are informed when they consent to how, why and where their personal information is processed. In this paper we have shown that HCI and system designers can affect the privacy awareness of users through digital nudges that increase the likelihood that the ToS and PP is read. The proposed design that implemented two nudges (PDB3) showed around a 75% decrease in number of users who just agreed the ToS and PP without even viewing them. This significant reduction in users who committed the so-called biggest lie on the Internet is a promising start. While the results showed that clicking the ToS and PP did increase the users recall of the contents, the proposed designs did not inherently increase recall among users. The field study with over 80'000 users of the IKEA Place app demonstrates that these digital nudges can be readily implemented by large companies. Yet, there is still a lot of work and research to be conducted before we can generally claim that users have given their informed consent online.

Acknowledgements

We like to extend a special thanks to James Howard and Morten Rosendal at Barkas for their design contributions to IKEA Place's UI around privacy.

References

Acquisti, A. (2009). "Nudging privacy: The behavioral economics of personal information." *IEEE security & privacy* 7 (6), 82–85.

Acquisti, A., I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, P. G. Leon, N. Sadeh, F. Schaub, M. Sleeper, et al. (2017). "Nudges for privacy and security: Understanding and assisting users' choices online." *ACM Computing Surveys (CSUR)* 50 (3), 1–41.

Acquisti, A., L. Brandimarte, and G. Loewenstein (2015). "Privacy and human behavior in the age of information." *Science* 347 (6221), 509–514.

Acquisti, A. and J. Grossklags (2003). "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior." In: *2nd Annual Workshop on Economics and Information Security-WEIS*. Vol. 3, pp. 1–27.

— (2005). "Privacy and rationality in individual decision making." *IEEE security & privacy* 3 (1), 26–33.

Benjamin, D. J., J. O. Berger, M. Johannesson, B. A. Nosek, E.-J. Wagenmakers, R. Berk, K. A. Bollen, B. Brembs, L. Brown, C. Camerer, et al. (2018). "Redefine statistical significance." *Nature Human Behaviour* 2 (1), 6.

Bettinger, E. P., B. T. Long, P. Oreopoulos, and L. Sanbonmatsu (2012). "The role of application assistance and information in college decisions: Results from the H&R Block FAFSA experiment." *The Quarterly Journal of Economics* 127 (3), 1205–1242.

Buck, C. (2017). "Stop disclosing personal data about your future self." In: *23th Americas Conference on Information Systems (AMCIS)*, pp. 1–10.

Caraban, A., E. Karapanos, D. Gonçalves, and P. Campos (2019). "23 Ways to Nudge: A Review of Technology-Mediated Nudging in Human-Computer Interaction." In: *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, p. 503.

Carrascal, J. P., C. Riederer, V. Erramilli, M. Cherubini, and R. de Oliveira (2013). "Your browsing behavior for a big mac: Economics of personal information online." In: *Proceedings of the 22nd international conference on World Wide Web*. ACM, pp. 189–200.

Cho, H., J.-S. Lee, and S. Chung (2010). "Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience." *Computers in Human Behavior* 26 (5), 987–995.

Cohen, J. B., E. B. Andrade, et al. (2018). "The ADF Framework: A Parsimonious Model for Developing Successful Behavior Change Interventions." *Journal of Marketing Behavior* 3 (2), 81–119.

Dasgupta, P. and E. Maskin (2005). "Uncertainty and hyperbolic discounting." *American Economic Review* 95 (4), 1290–1299.

Dinev, T., A. R. McConnell, and H. J. Smith (2015). "Research commentary—informing privacy research through information systems, psychology, and behavioral economics: thinking outside the "APCO" box." *Information Systems Research* 26 (4), 639–655.

Ermakova, T., A. Baumann, B. Fabian, and H. Krasnova (2014). "Privacy Policies and Users' Trust: Does Readability Matter?" In: *Twentieth americas conference on information systems*. Savanna, pp. 1–12.

Fogg, B. J. (1998). "Persuasive computers: perspectives and research directions." In: *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM Press/Addison-Wesley Publishing Co., pp. 225–232.

— (2009). "A behavior model for persuasive design." In: *Proceedings of the 4th international Conference on Persuasive Technology*. ACM, pp. 1–7.

Fogg, B. J. (Sept. 2019). *Fogg Behavior Model*. Website. Available at: https://www.behaviormodel.org/.
Forget, A., S. Chiasson, P. C. Van Oorschot, and R. Biddle (2008). "Improving text passwords through persuasion." In: *Proceedings of the 4th symposium on Usable privacy and security*. ACM, pp. 1–12.
Forwood, S. E., A. L. Ahern, T. M. Marteau, and S. A. Jebb (2015). "Offering within-category food swaps to reduce energy density of food purchases: a study using an experimental online supermarket." *International Journal of Behavioral Nutrition and Physical Activity* 12 (1), 85.
Furnell, S. and A. Phippen (2012). "Online privacy: a matter of policy?" *Computer Fraud & Security* 2012 (8), 12–18. ISSN: 1361-3723.
Hansen, P. G. (2016). "The definition of nudge and libertarian paternalism: Does the hand fit the glove?" *European Journal of Risk Regulation* 7 (1), 155–174.
Hansen, P. G. and A. M. Jespersen (2013). "Nudge and the manipulation of choice: A framework for the responsible use of the nudge approach to behaviour change in public policy." *European Journal of Risk Regulation* 4 (1), 3–28.
Harbach, M., M. Hettig, S. Weber, and M. Smith (2014). "Using personal examples to improve risk communication for security & privacy decisions." In: *Proceedings of the SIGCHI conference on human factors in computing systems*, pp. 2647–2656.
Hauser, D. J. and N. Schwarz (2016). "Attentive Turkers: MTurk participants perform better on online attention checks than do subject pool participants." *Behavior research methods* 48 (1), 400–407.
Hausman, D. M. and B. Welch (2010). "Debate: To nudge or not to nudge." *Journal of Political Philosophy* 18 (1), 123–136.
Hillman, R. A. and J. J. Rachlinski (2002). "Standard-form contracting in the electronic age." *NYUL Rev.* 77, 429.
Hoofnagle, C. J. and J. M. Urban (2014). "Alan Westin's privacy homo economicus." *Wake Forest L. Rev.* 49, 261.
Huang, N., P. Chen, Y. Hong, and S. Wu (2018). "Digital nudging for online social sharing: Evidence from a randomized field experiment." In: *Proceedings of the 51st Hawaii International Conference on System Sciences*.
Jameson, A., B. Berendt, S. Gabrielli, F. Cena, C. Gena, F. Vernero, and K. Reinecke (2013). "Choice Architecture for Human-Computer Interaction." *Interaction* 7 (1-2), 1–235.
Johnson, E. J. and D. Goldstein (2003). "Do defaults save lives?" *Science* 302 (5649), 1338.
Kokolakis, S. (2017). "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon." *Computers & security* 64, 122–134.
Kroll, T. and S. Stieglitz (2019). "Digital nudging and privacy: improving decisions about self-disclosure in social networks." *Behaviour & Information Technology*, 1–19.
Kunkel, R. G. (2002). "Recent developments in shrinkwrap, clickwrap and browsewrap licenses in the United States." *Murdoch University Electronic Journal of Law* 9 (3).
Lee, M. K., S. Kiesler, and J. Forlizzi (2011). "Mining behavioral economics to design persuasive technology for healthy choices." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, pp. 325–334.
Marreiros, H., M. Tonin, M. Vlassopoulos, and M. Schraefel (2017). "“Now that you mention it": A survey experiment on information, inattention and online privacy." *Journal of Economic Behavior & Organization* 140, 1–17.
McDonald, A. M. and L. F. Cranor (2008). "The cost of reading privacy policies." *ISJLP* 4, 543.
Mirsch, T., C. Lehrer, and R. Jung (2017). "Digital nudging: Altering user behavior in digital environments." *Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik (WI 2017)*, 634–648.
O'Donoghue, T. and M. Rabin (2000). "The economics of immediate gratification." *Journal of Behavioral Decision Making* 13 (2), 233–250.
Obar, J. A. and A. Oeldorf-Hirsch (2017). "Clickwrap impact: Quick-join options and ignoring privacy and terms of service policies of social networking services." In: *Proceedings of the 8th International Conference on Social Media & Society*, pp. 1–5.

Obar, J. A. and A. Oeldorf-Hirsch (2020). "The biggest lie on the internet: Ignoring the privacy policies and terms of service policies of social networking services." *Information, Communication & Society* 23 (1), 128–147.

Paolacci, G., J. Chandler, and P. G. Ipeirotis (2010). "Running experiments on amazon mechanical turk." *Judgment and Decision making* 5 (5), 411–419.

Peffers, K., T. Tuunanen, M. A. Rothenberger, and S. Chatterjee (2007). "A design science research methodology for information systems research." *Journal of management information systems* 24 (3), 45–77.

Phillips-Wren, G. E., L. S. Iyer, U. R. Kulkarni, and T. Ariyachandra (2015). "Business Analytics in the Context of Big Data: A Roadmap for Research." *CAIS* 37, 23.

Purohit, A. K., L. Barclay, and A. Holzer (2020). "Designing for Digital Detox: Making Social Media Less Addictive with Digital Nudges." In: *Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems*. CHI EA '20. Honolulu, HI, USA: ACM.

Schneider, C., M. Weinmann, and J. Vom Brocke (2018). "Digital nudging: guiding online user choices through interface design." *Communications of the ACM* 61 (7), 67–73.

Schumann, J. H., F. von Wangenheim, and N. Groene (2014). "Targeted online advertising: Using reciprocity appeals to increase acceptance among users of free web services." *Journal of Marketing* 78 (1), 59–75.

Simons, A., M. Weinmann, M. Tietz, and J. vom Brocke (2017). "Which reward should I choose? Preliminary evidence for the middle-option bias in reward-based crowdfunding." In: *Proceedings of the 50th Hawaii International Conference on System Sciences*.

Simonson, I. (1989). "Choice based on reasons: The case of attraction and compromise effects." *Journal of consumer research* 16 (2), 158–174.

Smith, H. J., T. Dinev, and H. Xu (2011). "Information privacy research: an interdisciplinary review." *MIS quarterly* 35 (4), 989–1016.

Thaler, R. H. and C. R. Sunstein (2009). *Nudge: Improving decisions about health, wealth, and happiness*. Penguin.

Tsai, J. Y., S. Egelman, L. F. Cranor, and A. Acquisti (2011). "The effect of online privacy information on purchasing behavior: An experimental study." *Information Systems Research* 22 (2), 254–268. ISSN: 1047-7047.

Walker, K. L. (2016). "Surrendering information through the looking glass: Transparency, trust, and protection." *Journal of Public Policy & Marketing* 35 (1), 144–158.

Wang, Y., P. G. Leon, K. Scott, X. Chen, A. Acquisti, and L. F. Cranor (2013). "Privacy nudges for social media: an exploratory Facebook study." In: *Proceedings of the 22nd International Conference on World Wide Web*, pp. 763–770.

Wang, Y., G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor (2011). "" I regretted the minute I pressed share" a qualitative study of regrets on Facebook." In: *Proceedings of the seventh symposium on usable privacy and security*, pp. 1–16.

Weinmann, M., C. Schneider, and J. vom Brocke (2016). "Digital nudging." *Business & Information Systems Engineering* 58 (6), 433–436.