First Monday, Volume 24, Number 7 - 1 July 2019

PEER-REVIEWED JOURNAL ON THE INTERNET

Improving privacy choice through design: How designing for reflection could support privacy self-management

by Arnout Terpstra, Alexander P. Schouten, Alwin de Rooij, and Ronald E. Leenes

Abstract

In today's society online privacy is primarily regulated by two main regulatory systems: (command-and-control) law and notice and consent (*i.e.*, agreeing to terms of agreement and privacy policies). Both systems prohibit reflection on privacy issues from the public at large and restrict the privacy debate to the legal and regulatory domains. However, from a socio-ethical standpoint, the general public needs to be included in the privacy debate in order to make well-informed decisions and contribute to the law-making process. Therefore, we argue that privacy regulation must shift from a purely legal debate and simple one-time yes/no decisions by 'data subjects' to public (debate and) awareness and continuous reflection on privacy and privacy decisions by users of IT systems and services. In order to allow for this reflective thinking, individuals need to (1) understand what is at stake when interacting with digital technology; (2) have the ability to reflect on the consequences of their privacy decisions; and (3) have meaningful controls to express their privacy preferences. Together, these three factors could provide for knowledge, evaluation and choice within the context of online privacy. In this paper, we elaborate on these factors and provide a design-for-privacy model that introduces friction as a central design concept that stimulates reflective thinking and thus restores the privacy debate within the public arena.

Contents

I. Introduction

In July 2018, the Dutch news platform *De Correspondent* revealed how military and intelligence personnel could easily be identified through the use of a fitness tracker, by observing (mostly publicly available) running activity near known military bases [1]. Even though the identities of military and intelligence personnel are considered highly confidential, 90 percent of individuals who tracked their runs around sensitive targets listed their name and home city publicly on their profile page, despite the option within the app of keeping such information private [2]. Moreover, by subsequently analysing the individuals' additional running activities, it was trivial to infer their home addresses: simply observe where most running activity begins and ends.

In addition, over the course of 2018 it became known that a company called Cambridge Analytica harvested the profiles of tens of millions of Facebook users without their knowledge [3]. Shortly thereafter, this did not appear to be a single instance as other companies used similar tactics to harvest personal data through Facebook [4]. The same year, the Norwegian Consumer Council published a report on how three big tech companies deceive individuals into sharing more personal data by deliberately applying cunning design patterns and hiding away privacy-friendly choices [5]. Many organisations adopt such deceptive designs because it supports them by monetising personal data [6].

That individuals are not aware of the consequences of their privacy choices or have little choice in the first place was one of the main incentives for the General Data Protection Regulation (GDPR) [7] which came into effect in 2018 within the European Union (EU), unifying the regulation of processing personal data across the EU and the European Economic Area (EEA). Key principles in the GDPR regarding the

processing of personal data relate to transparency to those whose data are being processed (data subjects) [8], as well as furthering their control over the processing of data. These principles force organizations to be more transparent about what data they collect and for what purposes and to offer more control to individual data subjects regarding the use of data and their privacy.

The United States (US) lack such omnibus regulation, but scandals like those repeatedly involving Facebook, increasingly lead to calls for developing data protection regulation in the US as well [9]. Moreover, companies themselves become increasingly aware that transparency and control over data use are paramount in order to uphold their reputation, retain their user base, and remain competitive. For example, last year's Cambridge Analytica controversy saw Facebook temporarily losing US$119 billion of their market value [10]. In response, Facebook initially denied there was a problem as all users gave their consent over sharing personal data. At the same time, however, Facebook promised to investigate current data access policies by third party apps and take further measures to limit those policies [11] as well as implement and promote new transparency and control features [12]. However, properly managing one's own privacy preferences is rather difficult for individuals (Solove, 2013; Cranor, *et al.*, 2006; Trepte, *et al.*, 2015).

It is still unclear how to properly provide individuals with information about their privacy choices (Fischer-Hübner, *et al.*, 2016). *Notice* (or transparency; informing the individual) and *consent* (or the ability to choose whether or not to use a product or service) is currently the main regulatory mechanism through which individuals legally retain responsibility for making their own privacy choices (Calo, 2014; Ben-Shahar and Schneider, 2011). It assumes a knowledge gap between an institution offering a service and an individual consuming that service (Calo, 2014; Hoofnagle and Urban, 2014). By mandating the disclosure of facts about institutional uses of personal data through a privacy policy prior to first use, this knowledge gap can be reduced. By reading privacy policies, future consumers are expected to understand in what ways their privacy might be affected, which in turn allows them to make well-informed, rational decisions. However, three problems have been identified with notice and consent.

First, privacy policies do not truly inform and thus help the individual to make better decisions. They are too lengthy and too difficult to understand for the average reader (Jensen and Potts, 2004; McDonald and Cranor, 2008; Cate, 2006; Milne, *et al.*, 2006; Grossklags and Good, 2008). Simplifying the content of privacy policies does not consistently influence disclosure behaviour and may even be used to seduce individuals to disclose even more personal information (Adjerid, *et al.*, 2013). Moreover, individuals become suspicious and instinctively share less personal information because of the mere presence of a privacy policy, even when the actual content is beneficial for the individual. Thus, the actual content of a privacy policy does not matter (Marreiros, *et al.*, 2017; John, *et al.*, 2011).

Second, human decision-making is often irrational and biased (Facione, 2015; Kahneman, 2011; Thaler and Sunstein, 2009; Acquisti and Grossklags, 2005; Acquisti, 2004; Strandburg, 2004; Kokolakis, 2017). Notice and consent assumes that more information leads to better decisions (Calo, 2014; Ben-Shahar and Schneider, 2011). However, in the context of privacy self-management, many decisions are taken rapidly and intuitively, with relatively low cognitive effort, based on cognitive strategies such as heuristics (Thaler and Sunstein, 2009; Acquisti and Grossklags, 2005; Acquisti, 2004; Simon, 1957). This indicates that the knowledge gap of notice and consent is not actually reduced. Rather, to reduce this gap, an individual is required to learn something and therefore, think critically and reflectively (Facione, 2015; Mezirow, 2003, 1997).

Third, there is no meaningful choice (Cate, 2006; Koops and Leenes, 2006). First, because meaningful choice entails understanding what the choice is about, which requires a certain degree of generic privacy literacy (Park, 2013; Trepte, *et al.*, 2015; Langenderfer and Miyazaki, 2009), as well as contextual knowledge about how specific products and services might affect an individual's privacy. Second, because there is no granularity in the choice itself. It is a take-it-or-leave-it dichotomy. When an individual disagrees with (some of) the terms, there is no room for negotiation. Third, monopolies in the information industry are common due to network effects, low marginal costs, and technical lock-in (Anderson, 2014), which leaves little room for alternatives and thus for choice. For example, if an individual's friends and relatives decided to use a certain social networking site (SNS), one has little choice but to follow their decisions, since SNSs are not interoperable (Au Yeung, *et al.*, 2009).

Two alternative regulatory mechanisms can be considered to counteract these issues: (1) more (detailed) regulation through (command-and-control) law; and, (2) steer or enforce an individual's behaviour through nudges or architecture (code) (Lessig, 2006; Murray and Scott, 2002; Calo, 2014, 2012; Brownsword, 2005) [13]. Law, when properly enforced, provides regulators with the means to dictate what is lawful and what is not. Many digital technologies are already regulated through law, *e.g.*, through copyright, defamation, and obscenity laws (Lessig, 2006). Specific regulation could be enacted to ban certain practices, such as deceptive interfaces. However, too much regulation through command-and-control law might have negative effects on innovation and competition (Calo, 2014, 2012; Posner, 1981). Furthermore, law is expensive, difficult to enforce, and often politically unattractive (Calo, 2012).

More fundamentally, both mechanisms confine the debate on privacy and how to regulate it exclusively to the domain of regulators (such as governments, public/private institutions, and policy-makers). In democratic societies, individuals also have "a say as to what the rules are to be" [14], which calls for the possibility to intentionally break a rule as a way of challenging the rules potentially leading to changes in the law (Lessig, 2006; Brownsword, 2006; Koops and Leenes, 2005). This in turn requires active citizens with critical and reflective thinking capabilities (ten Dam and Volman, 2004; Mezirow, 1997). However, both nudges and code fail to engage with the regulatee (the individual) on a moral level because they reduce individual choice to one of compliancy, or by even completely omitting the ability to choose at all (Brownsword, 2005). This affects how individuals deal with and learn about privacy and privacy issues: by depreciating the moral value of choice, individuals feel resigned (Turow, *et al.*, 2015; Hargittai and Marwick, 2016) and cannot become morally responsible agents (Brownsword, 2005; Mezirow, 2003, 1997).

Thus, both for individual privacy self-management as well as a larger societal discussion on privacy and privacy regulation, it is imperative that individuals become active citizens who regularly and deliberately think about and reflect on privacy issues and privacy choices. This entails that actual meaningful choices can be made. However, as argued, both nudges and code depreciate the moral value of choice by changing situations, not people (Brownsword, 2005). Thus, notice and consent should not be abandoned within the context of digital technology and privacy. However, the question then becomes: how can the issues identified above with notice and consent be mitigated in order to improve privacy self-management?

In this article, we argue that individuals should be encouraged through the design of the products and services they use to use their reflective thinking capabilities about privacy issues before, during, and after interacting with digital technology to make individual choices and regain a moral position. This requires at least three components: (1) a way to provoke individuals to escape their habitual behaviour and thoughts; (2) a phase of reflective thinking during which individuals actively reasons about their assumptions and beliefs and is supported by the product or service to learn about privacy (privacy literacy) and the potential consequences of privacy choices; and, (3) meaningful controls, or the ability to put newly learned thoughts and ideas into action. Together, these three elements will increase knowledge, evaluation, and choice within the context of digital technology and privacy.

Reflective thinking can be triggered through design, *i.e.*, reflective design (Sengers, *et al.*, 2005) or adversarial design (DiSalvo, 2012). Specifically, we argue that by applying friction as a disorienting dilemma, the reflective thinking process is triggered (Mezirow, 2006, 2000). Moreover, friction can guide further reflection and understanding as individuals are deliberately presented with ambiguous content and alternative viewpoints (Vasalou, *et al.*, 2015). Friction can also foster (critical) discourse which leads to communicative learning (Mezirow, 2000, 1990), a learning dimension highly that is undervalued within the context of privacy and digital technology.

In this paper, we provide the theoretical ground for how designing for reflection could improve notice and consent as a regulatory mechanism within the context of privacy and digital technology. We propose a model with high-level design guidelines which designers could use when designing digital products or services which affect an individual's privacy. When applying these guidelines, individuals are triggered to think consciously and reflectively, which increases privacy literacy and enables more deliberate decision-making. Moreover, it fosters (critical) discourse and restores the privacy debate to the public arena.

II. The complexity of privacy and individual choice

Privacy is a complex concept. Many attempts to conceptualise the term have been undertaken, but there is no single agreed upon definition (Whitman, 2004; Allen, 2000). Privacy differs amongst cultures (Moore, 2008; Altman, 1977), is "a plurality of different things" [15] and is "fundamentally dynamic" [16]. Moreover, the meaning of privacy evolves over time through personal experiences (Goldfarb and Tucker, 2012; Kezer, *et al.*, 2016) and changing norms in society (Westin, 2004). In sum, "privacy is a living, continually changing thing, a fluid concept, dependent on socio-cultural factors" (Koops and Leenes, 2006).

Adding to this complexity is that there are many types of privacy: bodily, spatial, communicational, proprietary, intellectual, decisional, associational, behavioural, and informational (Koops, *et al.*, 2016). Informational privacy refers to any piece of information about an individual, including its body, location, communication, property, thoughts, decisions, associations, and behaviour. Informational privacy can therefore be regarded as an overarching type over the other privacy dimensions. Within the context of digital technology, informational privacy is most relevant since technology typically enables the generation, storage, and distribution of personal data at a large scale.

Furthermore, there are different types of (personal) data. In a report by the World Economic Forum [17] a distinction is made between volunteered data — data created and explicitly shared by individuals, such as providing the name of one's home town to a SNS, even though this piece of data might not be required for completing the registration; observed data — data captured by recording the actions of individuals, such as locational data often embedded in pictures made with devices also equipped with a GPS sensor; and, inferred data — data about individuals based on the analysis of volunteered or observed data, such as deriving that someone is healthy based on the distance ran in the previous year, or deriving an individual's home address based on the location where running exercises frequently begin and end.

Within the context of digital technology, privacy is often viewed as the individual's ability to control the use of one's personal data (Westin, 1967; Allen, 2000; Schwartz, 1999; Koops, *et al.*, 2016). However, there are conceptual, practical and moral limitations to this view (Allen, 2000). Instead, privacy can be best viewed as contextual integrity (Nissenbaum, 2011, 2004), meaning norms of appropriateness and norms of flow or distribution prescribe what is or is not a privacy violation in a particular context. These norms originate for example socially, culturally, and politically, and may be explicit or implicit, specific, or variable and incomplete.

Norms of *appropriateness* dictate within a given context what information is "allowable, expected, or even demanded to be revealed" [18]. For instance, certain fitness trackers allow individuals to personally keep track of their progress towards becoming more fit by analysing and comparing their distinct runs. For this to work, it is appropriate for the app to collect locational data, *e.g.*, to display running routes and times within an app. Furthermore, norms of flow or *distribution* dictate how the information is (further) distributed. These norms indicate to what extent information can be shared by the recipient with others. For instance, the institution behind the fitness tracker needs to store (personal) information on their

servers (provided the app contains cloud-syncing functionality). However, when this information is, unbeknownst to the individual, shared with third parties *e.g.*, to generate additional revenue, this norm is breached. Satisfying both these norms constitutes maintaining contextual integrity. Violating either (or both) of these norms constitutes a privacy violation [19].

In addition to the above-mentioned theoretical complexity of privacy, managing one's privacy preferences in practice is difficult as well (Solove, 2013; Cranor, *et al.*, 2006; Trepte, *et al.*, 2015). Privacy self-management suffers from two types of problems (Solove, 2013): (1) structural problems, such as, there simply are too many entities involved in collecting and using personal data. It is impossible to oversee all relations and data flows between these entities. Moreover, pieces of personal data are being aggregated over time and across separate databases, which makes it very hard, if not impossible, for individuals to properly assess potential privacy harms at a fixed moment in time. Lastly, consenting to the disclosure of personal data is often treated as an individual transaction, completely disregarding the larger social dimensions of privacy. (2) Cognitive problems, which impair an individual's ability to make properly informed, rational choices as was referred to above already. Many privacy decisions are taken rapidly and intuitively, with relatively low cognitive effort, based on cognitive strategies such as heuristics (Thaler and Sunstein, 2009; Acquisti and Grossklags, 2005; Acquisti, 2004).

In order to manage one's privacy and make good privacy decisions, two dimensions of knowledge about privacy are required: (1) generic knowledge, also referred to as privacy literacy, and (2) contextual knowledge, *i.e.*, the potential consequences of disclosing personal data to a specific product or service. Privacy literacy is a combination of factual or declarative (*knowing that*) and procedural (*knowing how*) knowledge about privacy and data protection (Park, 2013; Trepte, *et al.*, 2015; Langenderfer and Miyazaki, 2009). For example, the Online Privacy Literacy Scale (OPLIS) is an instrument that measures privacy literacy according to four different factors: (1) knowledge about institutional practices; (2) knowledge about technical aspects of data protection; (3) knowledge about data protection law; and, (4) knowledge about data protection strategies (Masur, *et al.*, 2017). Privacy literacy is necessary to reason about privacy within a specific context. For example, generic knowledge about the fact that personal information is often aggregated from different sources should be used to reason about the potential consequences of a privacy decision within a specific context (*e.g.*, will the personal information given to this product or service combined with others I already use?).

Thus far we can conclude that the required amount and nature of privacy knowledge is not trivial. Moreover, it takes considerable effort to apply such knowledge in specific online contexts in order to make good privacy decisions. In fact, this complexity is one of the major factors accounting for the existence of the privacy paradox, which refers to the fact that although many individuals value their privacy, most individuals disclose significantly more personal information online than their stated intentions would predict (Norberg, *et al.*, 2007; Barnes, 2006; Acquisti and Gross, 2006; Jensen, *et al.*, 2005). Thus, in order to be able to perform meaningful privacy self-management, individuals need a proper understanding of privacy (privacy literacy) and the potential consequences of their privacy choices; and critically reflect on these.

III. Improving privacy self-management with reflective thinking

Reflective thinking provides a possible way to cope with the complexity of privacy and privacy choices and hence could be encouraged to mitigate privacy loss by bad or wrong choices. Reflective thinking, or (critical) reflection as it is often called, is the examination of previous experiences and assumptions as input for future action, assumptions and decisions (White, *et al.*, 2006; ten Dam and Volman, 2004; Ennis, 1991). It starts with an awareness that existing assumptions need to be (re-)examined, initiated by a *disorienting dilemma* (Mezirow, 2006, 2000): an "[a]nomal[y] [...] of which old ways of knowing cannot make sense" [20]. A disorienting dilemma, or breakdown (Baumer, 2015), refers to experiences, beliefs, feelings that are incompatible with an individual's existing frames of reference. It can be triggered from a sudden major event in life, *e.g.*, a crisis, or an accumulation of smaller changes over time within one's frames of reference (Mezirow, 2000) [21].

After this initial step, the reflective thinking process continues with what can be summarised as inquiry (Baumer, 2015); an examination into what caused the disorienting dilemma, *e.g.*, by critically considering one's existing assumptions or by exploring of possible solutions (Mezirow, 2006, 2000). Prior knowledge and prior experiences defined as frames of reference are used by individuals to continuously make sense of the world (Kitchenham, 2008; Mezirow, 2006; Cranton and King, 2003). Frames of reference comprises habits of mind and subsequent points of view (Kitchenham, 2008; Mezirow, 2006). Habits of mind are profound and "broad, abstract, orienting, habitual ways of thinking, feeling and acting, influenced by assumptions that constitute a set of codes" [22] and include, amongst others, sociolinguistic, moral-ethical, epistemic, philosophical, psychological, and aesthetic dimensions (Mezirow, 2006) of one's identity (Illeris, 2014). Habits of mind are in turn expressed as points of view (Kitchenham, 2008; Mezirow, 2006) which refers to "the constellation of belief, memory, value judgement, attitude and feeling that shapes a particular interpretation" [23].

An example of a habit of mind within the context of privacy and digital technology is the conviction that privacy is indeed valuable and important to protect. However, a resulting point of view based on prior experiences can be apathy and powerlessness, due to the feeling individuals have "that once information is shared, it is ultimately out of their control" [24]. A positive experience with one situation, for example a personal photograph accidentally shared with the wrong person who then does not abuse this situation and immediately deletes the picture, might change one's point of view towards that specific situation/person, but not immediately affect one's deeper habit of mind (because ultimately, the use of the photograph once received by someone else is indeed out of control for the individual). However,

when such situations occur more frequently, the individual's habit of mind might eventually change incrementally.

Lastly, the reflective thinking process closes with a review and re-evaluation of one's assumptions, leading to changes in beliefs, attitudes, and behaviour. During these phases, also referred to as transformation (Baumer, 2015), experiences are transformed into learning, *e.g.*, by which new assumptions and beliefs are incorporated into an individual's frames of reference (Mezirow, 2000).

When critical reflection is used to guide decision-making or action, it becomes (transformative) learning (Mezirow, 2000, 1990). Transformative learning refers to two types of learning: (1) instrumental learning, which is task-oriented and aims at specific steps/skills to control and manipulate the environment; and, (2) communicative which is about the meaning behind words and actions (Mezirow, 2006, 2003, 2000, 1990; Taylor, 2007). In different terms, through instrumental learning one learns *what* to do or *how* to act; through communicative learning, one learns about the reasons for *why* to act in certain ways. Within the context of privacy self-management, instrumental learning refers to privacy literacy; the factual and procedural knowledge related to privacy and privacy choices. Communicative learning on the other hand concerns critically reflecting on assumptions, beliefs, values, feelings, and meanings with regards to privacy and privacy choices.

Reflection applies to both instrumental and communicative learning, but these domains differ in how meaning is validated. Within instrumental learning, hypotheses are formed and empirically validated (Mezirow, 2000, 1990). For example, the question whether an SNS app can still be used without sharing locational data can be empirically tested by deciding not to share this data and assess whether the app still works. In communicative learning this approach cannot be used. Instead, here "meaning is validated through critical discourse" [25] which "always reflects wider patterns of relationship and power" [26]. Within communicative learning, for example, one would reflect on what it really means to share location data with an SNS: what if the SNS aggregates locational data of all one's pictures and combines it with other types of data; will the SNS then be able to deduce all kinds of extra information, *e.g.*, where one's friends live or how many times a year one goes on a holiday? Is the (free) service one gets in return for this still worth the potential privacy risks that follow? These questions really concern an individual's frames of reference and require considering a more global view (of one's assumptions, beliefs, values, feelings, and meanings), which leads to deeper, more complex reflection and to a more profound transformation of values and beliefs (Kitchenham, 2008).

Reflective thinking is usually applied within an educational context (Taylor, 2007; White, *et al.*, 2006). There, the reflective thinking process is generally triggered and guided by a present teacher who assists the learner in acquiring and enhancing skills, insights, and dispositions to become critically reflective (Mezirow, 2003, 2000). In order to do this, it is the responsibility of the teacher to create the right environment for reflective discourse to happen, by providing tools/experiences (*e.g.*, by using metaphors, questioning students' assumptions or providing feedback; Roberts, 2006) and by setting the right conditions (*e.g.*, equality between participants, a safe and open environment) (Fook, 2015; Taylor, 2007; Mezirow, 2006, 2000).

However, within other contexts there is no present teacher to trigger and guide reflection. Within the context of digital technology and privacy, the product or service is all there is; people don't read manuals or take courses. Hence, they should be designed to trigger and guide reflection. The designer thus becomes the *ex-ante* teacher by creating the right (digital) environment for reflection to occur even while the individual is not participating in an explicit learning activity. Such instructive designs, we hope, could then improve an individual's ability to make deliberate, well-informed privacy decisions and encourage participation in the public debate concerning privacy.

IV. Better privacy decisions through designing for reflection

The importance and potential of reflection by design is acknowledged in design theories, especially in the 'reflective design' (Sengers, *et al.*, 2005) and 'adverserial design' (DiSalvo, 2012) theories. Moreover, while interacting with artefacts, three levels of processing in the brain are potentially active: (1) the visceral level; (2) the behavioural level; and, (3) the reflective level (Norman, 2004).

The *visceral* level concerns itself with appearances; look and feel. On this level, an artefact really elicits an automatic, subconscious response when an individual observes or handles it. Some artefacts are beautifully designed and make an individual want to own it even though they might not be usable in practice, *e.g.*, an aluminium citrus juicer that looks great but is actually unusable because the acidic citrus fluids corrode the juicer's surface (Norman, 2004).

The *behavioural* level refers to the subconscious part of the brain and concerns itself with processes which control everyday behaviour. To appeal to this level, function, understandability, and usability come into play. On this level, the interaction between the user and the artefact elicits emotions connected with accomplishing tasks and goals, *e.g.*, whether the product actually does what the user wants and whether it does so in an efficient, understandable, and usable fashion.

The *reflective* level is what separates human beings from other organisms. Through reflection, subconscious thoughts and actions are lifted towards the conscious level, enabling individuals to become aware of visceral and behavioural responses and reason about them. For example, an individual might prefer a less attractive and less usable product or service over others, because the company's values of openness and transparency about their use of the individual's personal data prevails over appearance and usability.

Traditionally, however, designers have focused too narrowly on the visceral level (appearance) and the behavioural level (usability) (Norman, 2004; Baumer, *et al.*, 2014). There are, however, at least four reasons why designers should incorporate appealing to the reflective cognitive processes into their products and services. (1) Fair regulation: the regulatory mechanism notice and consent allows for certain freedom in offering products or services, so long as individuals are able to understand what they are deciding about. The latter is the responsibility of the institutions offering the product or service. Furthermore, a decision is only truly meaningful when made deliberately: designers can design their products and services in such a way to assist individuals in making those decisions. (2) Active citizenship: participating in democratic societies requires active citizens with critical thinking capabilities (ten Dam and Volman, 2004). Organisations can (indirectly) contribute to this by treating their users as stakeholders instead of passive consumers. (3) Values in technology: the influence technology has on society demands continuous reflection. Technology is neither good, nor bad, nor neutral (Kranzberg, 1986); it is not inherently values-blind (Verbeek, 2015, 2008; Sengers, *et al.*, 2005). Both *designers* as well as *users* should continuously reflect on technology (Sengers, *et al.*, 2005) because users and artefacts co-create the technology and its effects. (4) Long-term relationships: appealing to the reflective level allows organisations to build long-term relationships with the users of their products (Norman, 2004).

Incorporating reflection for both designers as well as users into the design of products and services served as the foundation for reflective design (Sengers, *et al.*, 2005), in which the artefact assumes the role of the teacher to trigger and guide reflection. Reflective design draws upon "several other critically-informed design practices" [27] and provides several principles and strategies for designers as guidelines on integrating reflection into their practices and designs. Apart from the first three principles, which are more generic claims that designers should apply reflection themselves and support users in doing so [28], the second three are more specific and provide useful guidance on how to support reflection [29]:

> 4. "Technology should support skepticism about and reinterpretation of its own working", which concerns implicit and explicit values inherent to the design of artefacts.
>
> 5. "Reflection is not a separate activity from action but is folded into it as an integral part of experience", which states that reflection should not be purely intellectual but also integrated into action.
>
> 6. "Dialogic engagement between designers and users through technology can enhance reflection", which is about the importance of (critical) discourse between designer and user.

Reflective thinking is also a key element for the adversarial design theory, a design theory focusing on evoking critical discourse on political topics (DiSalvo, 2012). It builds upon agonistic pluralism, which recognises that not all disagreements between participants in democratic societies can be solved by deliberation and rational discussion (hence the agonistic dimension) (Mouffe, 1999). Adversarial design aims, by means of design, to reveal contestational relationships and experiences, to evoke ongoing questioning and challenging of dominant perspectives and practices, and present alternatives by reconfiguring existing components into atypical results (DiSalvo, 2012). However, adversarial design strictly focuses on evoking debate and does not aim to provide ready-made solutions to existing problems, which limits the applicability in everyday practice [30].

Both design theories share their foundations in the realisation that products and services always contain designed-in values and that human beings (either as producer/designer or as user of the product or service) should continuously reflect on those values embedded within the product or service. They also propose to achieve reflection by applying friction, both as a trigger for reflection as well as for presenting alternative viewpoints during reflection to guide further understanding. Finally, reflection is not separated, but integrated into action: by designing-in controls that individuals are able to manipulate, the reflective thinking process is further supported.

In order to improve privacy choice by designing for reflection, we can therefore formulate three high-level design guidelines. These guidelines are developed by a synthesis of the research discussed above and should therefore be taken as a starting point for further development, extension, and empirical verification.

(1) Deliberately design-in friction to introduce disorienting dilemmas and escape habits

The first guideline is to introduce *friction* into the design of products and services containing possibilities for privacy self-management to provoke a disorienting dilemma within the individual (user) which leads to reflective thinking and thus an escape of habits of mind and behaviour.

Within user experience design, friction is commonly understood as anything that prevents a user from accomplishing their goals or completing their tasks. Hence, it often has a negative connotation because interrupting the user flow might lead to loss of customers or users (Shen and Sundaresan, 2010) and less trust (Flavián, *et al.*, 2006). When applied incorrectly, friction can indeed lead to frustration or simply the formation of new habits. For example, consider agreeing to the terms and conditions when installing new software on a personal computer. Application developers are aware that nobody actually reads those terms but simply clicks 'I Agree' to continue with the installation process. Some application developers have attempted to use friction to prevent this, by only allowing the user to click 'I Agree' after scrolling all the way down to the bottom of the (lengthy) terms, assuming the terms will be read in the meantime. However, this does not lead to better (privacy) decisions. Instead, two alternative scenarios are likely: (1) the individual is frustrated since in this case, friction did lead to (a brief period of)

reflection but also the quick realisation that demanding the terms to be read is unfair due to its length; and, ultimately, the user has no real control (it remains a take-it-or-leave-it decision); or (2) the individual quickly finds the solution to the 'problem' of not being able to continue: just scroll all the way down without actually reading the terms and proceed with the installation. The next time the user installs software with such friction again, this behaviour is repeated; new habits are thus formed.

However, friction can also improve interfaces and thus help users in achieving what they want. For instance, the 'are you sure you wish to empty the trash?' dialogue asking for confirmation before permanently deleting files causes friction, yet has saved many files from accidental deletion. Friction in this sense is thus better seen as a trigger to draw explicit user attention used at fixed moments in the individual's performance of a task. The friction(s) can be embedded in the design by the designer because they can anticipate user behaviour (to some extent).

In addition to using friction to draw user attention towards behaviour, friction can also be used to draw attention towards the individual's underlying assumptions, beliefs, values, and feelings, thus encouraging reflective thinking. For example, by deliberately designing-in ambiguous content, different and contrasting opinions or perspectives (Vasalou, *et al.*, 2015) or by asking specific questions which lead individuals to consider other perspectives (Broockman and Kalla, 2016), individuals are triggered to reflect on alternative (than one's own) habits of mind and points of view. Friction in this sense is best understood as deliberately interfering with the content of what is presented to the user.

Thus, despite the negative connotation friction generally has, we believe frictions are valuable means to trigger reflection. By applying friction within the design of products and services, emphasis can be placed on communicative learning by encouraging the individual to reflect on why behaving in certain ways is important. In addition, designers should simultaneously stimulate reflection, to ensure friction becomes more than something annoying, and provide meaningful controls, to ensure the individual can take action during and after reflection (see the following guidelines below).

(2) Foster and guide reflection for communicative and instrumental learning

The second guideline is to *foster and guide reflection* and support communicative and instrumental learning. Introducing friction is not enough if an individual is unable to explore why that friction has been introduced. Thus, apart from applying friction to *trigger* reflective thinking, further reflective thinking should also be promoted by the product or service to induce both instrumental (privacy literacy: knowing that and knowing how) and communicative learning (reflecting on users' and others' underlying assumptions, beliefs, values, feelings, and meanings: knowing why).

Within the domain of instrumental learning, meaning is validated empirically; designers should thus support the individual in forming hypotheses (*e.g.*, through friction) and validating those through controls and explanation (for example, after several uses of a fitness tracker, inferring one's home address becomes possible; once this occurs, it might be the right time to point the individual to the app's privacy settings and allow them to make changes, *e.g.*, delete all previous runs or switch from a public to a private profile). Within communicative learning, validating meaning occurs through critical discourse; designers could for example make use of openness, which means to introduce alternative opinions/viewpoints and scale privacy from a personal issue to societal issue. This can be achieved by deliberately designing-in ambiguous content and/or different and contrasting opinions (Vasalou, *et al.*, 2015). By doing so, individuals are motivated to consider an alternative worldview and reflect on their own experiences and assumptions, which in turn can lead to changed behaviour.

As an example that uses friction to support instrumental learning, consider counterfactual explanations (Wachter, *et al.*, 2018). Counterfactuals are about explaining the consequences of external facts which led complex algorithms to a certain decision. By doing so, individuals are able to learn instrumentally without having to understand the internal state or logic of a (complex) system, which can potentially consist of millions of variables. Instead, counterfactuals take the form of "[y]ou were denied a loan because your annual income was £30,000. If your income had been £45,000, you would have been offered a loan" [31].

As an example that demonstrates communicative learning, consider a smartphone game that uses personal data as revenue so that it can remain free to use. Assume this game requests permission to an individual's contact list, but that those data are not required for the game to function. Instead of only asking the individual for permission to share their contact list, designers could implement the following alternative: an extra dialogue after giving permission to share the contact list which states that in addition to asking the individual for permission, all contacts will be asked for permission as well (*e.g.*, through SMS). Even though individuals might understand the business models of free applications, they will presumably dislike it when the institution behind the application (secretly) sends messages to the individual's contacts. This may lead individuals to temporarily consider theirs and others' assumptions and values, by for instance considering what others feel when they unexpectedly receive a text message from an unknown app asking for permission on behalf of someone else. Likely, this causes the individual to think twice before continuing. Thus, after reflection, communicative learning occurred which also lead to a change in behaviour.

Thus, during this phase, friction not only triggers reflection, but also further guides reflection by allowing the individual to consider alternative views and interpretations. However, without any meaningful choice, friction and reflection only lead to frustration. For example, if individuals during installation of the game from the above-mentioned example that is about to send an SMS to all their contacts have no (granular) controls to deal with this situation, they will very likely be frustrated. Therefore, the final guideline concerns agency, or allowing individuals to make meaningful decisions.

(3) Enable agency by introducing meaningful controls

Learning is encouraged if individuals can find their own personally relevant narrative within all the information presented to them (Vasalou, *et al.*, 2015). Two elements are core to this guideline: *openness* (showing multiple perspectives; discussed above) and *agency* (allowing individuals to make their own decisions). To do so, designers should introduce controls through which individuals can make meaningful privacy decisions, during and after the reflective thinking process.

Controls are crucial for the reflective process (Miettinen, 2013; Sengers, *et al.*, 2005); not having the ability to act upon newly learned beliefs, attitudes, or behaviour depreciates the moral value of choice. Through controls and proper feedback mechanisms, meaning is validated empirically; for example, an interface that allows individuals to view their profile through the lens of other users enables them to validate whether their settings on with whom to share certain information are correct. This means that controls should go beyond just notice and consent or a simple yes/no decision and instead allow for more granular mechanisms of privacy self-management.

Moreover, providing meaningful controls allows individuals to gain the ability to actually negotiate their privacy-preferences with institutions, leading to more competition and diversity amongst digital products and services. This in turn leads to more market regulation and a fairer notice and consent regulatory mechanism. Additionally, individuals are engaged with privacy as they express their preferences and opinions through the settings they choose and the products and services they use.

What can be considered meaningful controls remains to be further researched, but to give an example, consider the previously given example of a smartphone game. The designer could for instance design-in extra controls which allow individuals to select to whom the request for permission is actually sent. This could enable negotiation between the individual and the institution behind the application; sharing too few contacts might then result in the app not being free anymore. As an example of what does *not* constitute of meaningful controls, recall the earlier example of forcing users to scroll all the way to the bottom of the terms and conditions before being able to continue. Even though this is a form of friction which potentially initiates reflection, the choice still remains a take-it-or-leave-it decision of either accepting all the terms or not be able to use the application at all.

Towards a model for designing for reflection and meaningful privacy decisions

Putting all three abovementioned guidelines together results in the model presented in Figure 1. In order to make meaningful privacy decisions, all three guidelines must be combined; otherwise they will have adverse consequences. Friction with reflection without controls leads to frustration, as reflection remains purely intellectual since the individual might want to change things but has no means to do so. Friction and controls allow for behaviour change, but without reflection will only lead to the formation of new habits and no change in underlying assumptions, beliefs, values, feelings, and meanings which guide behaviour (*e.g.*, scrolling to get to the 'I agree' button; the decision did not become more meaningful after the change in behaviour). Moreover, this does not lead to increased knowledge and/or participation in the privacy debate. Finally, when only applying controls and reflection but no friction, there is no need for the individual to start the reflective thinking process and to consider alternative views or behaviour.

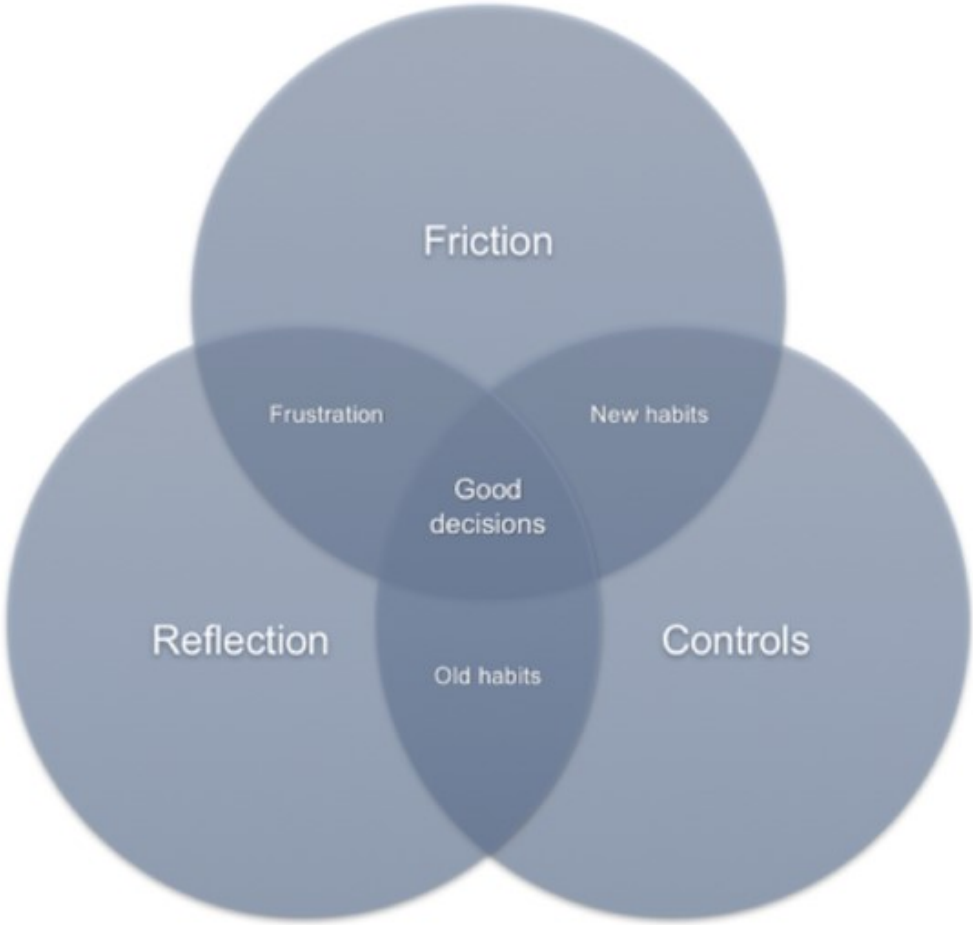

Figure 1: Proposed guidelines on designing for reflective thinking to improve privacy self-management.

V. Conclusion

In this paper we argued that through notice and consent, individuals are required to manage their own privacy preferences, despite its complexity. Privacy self-management suffers from structural (*i.e.*, conceptual and practical) and cognitive (*i.e.*, the tendency for human brains to prefer quick, intuitive decisions over more rational, deliberate decisions) limitations. While some would therefore argue to abandon notice and consent in favour of more enforcing regulation (*e.g.*, law, nudges, and/or code), others, including the authors of the present article, prefer preserving individual choice and focus on improving the known issues with privacy decision-making.

To take decisions in a world that continuously evolves (*i.e.*, through personal, societal, and technological changes), individuals use reflective thinking which leads to instrumental and communicative learning. Through instrumental learning, individuals learn how to manipulate the world (knowing that and knowing how); through communicative learning, individuals learn about theirs and others' underlying values and assumptions which guides their decisions (knowing why).

We have argued that designers of technological artefacts are responsible for triggering and guiding reflection amongst individuals interacting with their products and services. To accomplish this, we have proposed a model containing three design guidelines for the designer to incorporate into their designs: (1) friction, which serves as a trigger for further reflective thinking as well as an invitation for individuals to consider alternative values, beliefs, and assumptions; (2) reflection, which allows individuals to better understand how artefacts influence the values, beliefs, and assumptions of themselves and others; and, (3) controls, which is not only required by reflection to have an effect, but also increases the fairness of notice and consent. Further research is required to develop our proposed model into more concrete guidelines and empirically verify what works and what does not.

About the authors

Arnout Terpstra is an (external) Ph.D. student at Tilburg Institute of Law, Technology & Society (TILT), at Tilburg University, and works for SURFnet, the Dutch National Research and Education Network. As a product manager at SURFnet, he works within the field of trust & identity and is responsible for both daily operations and new innovations surrounding the National Identity Federation, SURFconext. Topics Arnout is working on include privacy and identity, group management and international collaboration. Having a specific interest in privacy and the impact of technology on humans and society, he started a Ph.D. project at TILT in 2017 to do research on how technology can be designed more responsibly. Direct comments to: a [dot] c [dot] terpstra [at] uvt [dot] nl

Dr. **Alexander P. Schouten** is assistant professor at the Department of Communication and Cognition (DCC) at Tilburg University.
E-mail: a [dot] p [dot] schouten [at] uvt [dot] nl

Dr. **Alwin de Rooij** is assistant professor at the Department of Communication and Cognition (DCC) at Tilburg University.
E-mail: alwinderooi [at] uvt [dot] nl

Prof. Dr. **Ronald E. Leenes** is professor at and director of the Tilburg Institute of Law, Technology and Society (TILT) at Tilburg University.
E-mail: r [dot] e [dot] leenes [at] uvt [dot] nl

Notes

1. M. Martijn, D. Tokmetzis, R. Bol, and F. Postma, "This fitness app lets anyone find names and addresses for thousands of soldiers and secret agents," *De Correspondent* (8 July 2018), at https://decorrespondent.nl/8480/this-fitness-app-lets-anyone-find-names-and-addresses-for-thousands-of-soldiers-and-secret-agents/1807810614720-f342d6aa, accessed 1 August 2018.

2. However, due to a bug in the software it was still possible to access private information through APIs that were not well-protected.

3. G.J.X. Dance, M. LaForgia, and N. Confessore, "As Facebook raised a privacy wall, it carved an opening for tech giants," *New York Times* (18 December 2018), at https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html, accessed 22 May 2019.

4. J. Sanders and D. Patterson, "Facebook data privacy scandal: A cheat sheet," *TechRepublic* (14 May 2019), at https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/, accessed 22 May 2019.

5. Forbrukerradet, "New analysis shows how Facebook and Google push users into sharing personal data" (27 June 2018), at https://www.forbrukerradet.no/side/facebook-and-google-manipulate-users-into-sharing-personal-data/, accessed 1 August 2018.

6. M. Eddy, "How companies turn your data into money," *PCMag.com* (10 October 2018), at https://www.pcmag.com/article/364152/how-companies-turn-your-data-into-money, accessed 22 May 2019.

7. Gdpr-info.eu, "General Data Protection Regulation (GDPR)," at https://gdpr-info.eu/, accessed 22 May 2019.

8. Article 12 of the General Data Protection Regulation (GDPR) requires data controllers at all times to be transparent about the processing of personal data, even when 'consent' is not the legal ground for the processing. "The controller shall take appropriate measures to provide any information [...] any communication [...] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means." — Article 12, GDPR, at https://gdpr-info.eu/art-12-gdpr/, accessed 1 August 2018.

9. D. Meyer, "In the wake of GDPR, will the U.S. embrace data privacy?" *Fortune* (29 November 2018), at http://fortune.com/2018/11/29/federal-data-privacy-law/, accessed 22 May 2019.

10. R. Neate, "Over $119bn wiped off Facebook's market cap after growth shock," *Guardian* (26 July 2018), at https://www.theguardian.com/technology/2018/jul/26/facebook-market-cap-falls-109bn-dollars-after-growth-shock, accessed 22 May 2019.

11. J. Carrie Wong, "Mark Zuckerberg apologises for Facebook's 'mistakes' over Cambridge Analytica," *Guardian* (22 March 2018), at https://www.theguardian.com/technology/2018/mar/21/mark-zuckerberg-response-facebook-cambridge-analytica, accessed 22 May 2019.

12. E. Egan, "Marking Data Privacy Day 2019," *Facebook Newsroom* (27 January 2019), at https://newsroom.fb.com/news/2019/01/data-privacy-day/, accessed 22 May 201.

13. A third regulatory mechanism, 'social norms', is intentionally left out of the equation, following Ryan Calo (2014).

14. Brownsword, 2006, p. 20.

15. Solove, 2007, p. 756.

16. Cohen, 2013, p. 1,906.

17. World Economic Forum, "Personal data: The emergence of a new asset class," at http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf, accessed 1 August 2018.

18. Nissenbaum, 2004, p. 120.

19. Two key elements are contained within contextual integrity: (1) the responsibility of the participants to be aware of/knowledgeable about the norms; and, (2) the responsibility of the participants (sender, receiver) to adhere to those norms. Much emphasis is placed on individual autonomy and dignity: norms are not forced onto participants in the sense that they have no choice but to comply. This also means that violations will occur.

20. Mezirow, 1990, p. 9.

21. A disorienting dilemma is often explained as a *disruption* of an individual's existing frames of reference. However, alternatively a *restoration* of one's foundational ethics can yields the same result (Lange, 2004).

22. Mezirow, 2006, p. 92.

23. *Ibid.*

24. Hargittai and Marwick, 2016, p. 3,737.

25. Mezirow, 1990, p. 11.

26. Mezirow, 2000, p. 11.

27. Sengers, *et al.*, 2005, p. 51; Participatory Design, Value Sensitive Design, Critical Design, Ludic Design, Critical Technical Practice, Reflection-in-action (Sengers, *et al.*, 2005).

28. The first three principles are "1. Designers should use reflection to uncover and alter the limitations of design practice"; "2. Designers should use reflection to re-understand their own role in the technology design process"; and, "3. Designers should support users in reflecting on their lives" (Sengers, *et al.*, 2005, p. 55).

29. Sengers, *et al.*, 2005, pp. 55–56.

30. For example, consider the Million Dollar Blocks project. Instead of visualising on a map where crime occurs, this project maps where the prison population comes from and what the associated yearly costs of imprisoning them are. As it turns out, incarcerating residents from several single housing blocks alone already exceeds one million dollars annually. By doing so, designers have reframed the (political) discussion around crime and society without providing ready-made solutions for the problem at hand; Columbia Center for Spatial Research, "Million Dollar Blocks," at http://c4sr.columbia.edu/projects/million-dollar-blocks, accessed 1 August 2018.

31. Wachter, *et al.*, 2018, p. 846.

References

A. Acquisti, 2004. "Privacy in electronic commerce and the economics of immediate gratification," *EC '04: Proceedings of the Fifth ACM Conference on Electronic Commerce*, pp. 21–29.
doi: https://doi.org/10.1145/988772.988777, accessed 22 June 2019.

A. Acquisti and R. Gross, 2006. "Imagined communities: Awareness, information sharing, and privacy on the Facebook," In: G. Danezis and P. Golle (editors). *Privacy enhancing technologies*. *Lecture Notes in Computer Science*, volume 4258. Springer, Berlin, HeidelbergLecture Notes in Computer Science, volume 4258. Berlin: Springer, pp. 36–58.
doi: https://doi.org/10.1007/11957454_3, accessed 22 June 2019.

A. Acquisti and J. Grossklags, 2005. "Privacy and rationality in individual decision making," *IEEE Security and Privacy*, volume 3, number 1, pp. 26–33.
doi: https://doi.org/10.1109/MSP.2005.22, accessed 22 June 2019.

I. Adjerid, A. Acquisti, L. Brandimarte, and G. Loewenstein, 2013. "Sleights of privacy: Framing, disclosures, and the limits of transparency," *SOUPS '13: Proceedings of the Ninth Symposium on Usable Privacy and Security*, article number 9.
doi: https://doi.org/10.1145/2501604.2501613, accessed 22 June 2019.

A.L. Allen, 2000. "Privacy-as-data control: Conceptual, practical, and moral limits of the paradigm," *Connecticut Law Review*, volume 32, number 3, pp. 861–876, and at https://scholarship.law.upenn.edu/faculty_scholarship/790/, accessed 22 June 2019.

I. Altman, 1977. "Privacy regulation: Culturally universal or culturally specific?" *Journal of Social Issues*, volume 33, number 3, pp. 66–84.
doi: https://doi.org/10.1111/j.1540-4560.1977.tb01883.x, accessed 22 June 2019.

R. Anderson, 2014. "Privacy versus government surveillance: Where network effects meet public choice," *Proceedings of 13th Annual Workshop on the Economics of Information Security*, at

https://www.econinfosec.org/archive/weis2014/papers/Anderson-WEIS2014.pdf, accessed 22 June 2019.

C.-M. Au Yeung, I. Liccardi, K. Lu, O. Seneviratne, and T. Berners-Lee, 2009, "Decentralization: The future of online social networking," *W3C Workshop on the Future of Social Networking Position Papers*, at https://www.w3.org/2008/09/msnws/papers/decentralization.pdf, accessed 22 June 2019.

S.B. Barnes, 2006. "A privacy paradox: Social networking in the United States," *First Monday*, volume 11, number 9, at https://firstmonday.org/article/view/1394/1312, accessed 1 August 2018.
doi: https://doi.org/10.5210/fm.v11i9.1394, accessed 22 June 2019.

E.P.S. Baumer, 2015. "Reflective informatics: Conceptualdimensions for designing technologies ofreflection," *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, pp. 585–594.
doi: https://doi.org/10.1145/2702123.2702234, accessed 22 June 2019.

E.P.S. Baumer, V. Khovanskaya, M. Matthews, L. Reynolds, V. Schwanda Sosik, and G. Gay, 2014. "Reviewing reflection: On the use of reflection in interactive system design," *DIS '14: Proceedings of the 2014 Conference on Designing Interactive Systems*, pp. 9–102.
doi: https://doi.org/10.1145/2598510.2598598, accessed 22 June 2019.

O. Ben-Shahar and C. E. Schneider, 2011. "The failure of mandated disclosure," *University of Pennsylvania Law Review*, volume 159, number 3, pp. 647–749, and at https://www.law.upenn.edu/journals/lawreview/articles/volume159/issue3/BenShaharSchneider159U.Pa.L.Rev.647(2011).pdf, accessed 22 June 2019.

D. Broockman and J. Kalla, 2016. "Durably reducing transphobia: A field experiment on door-to-door canvassing," *Science*, volume 352, number 6282 (8 April), pp. 220–224.
doi: https://doi.org/10.1126/science.aad9713, accessed 22 June 2019.

R. Brownsword, 2006. "Neither east nor west, is mid-west best?" *SCRIPT-ed*, volume 3, number 1, pp. 15–33, and at https://script-ed.org/wp-content/uploads/2016/07/3-1-Brownsword.pdf, accessed 22 June 2019.

R. Brownsword, 2005. "Code, control, and choice: Why east is east and west is west," *Legal Studies*, volume 25, number 1, pp. 1–21.
doi: https://doi.org/10.1111/j.1748-121X.2005.tb00268.x, accessed 22 June 2019.

R. Calo, 2014. "Code, nudge, or notice?" *Iowa Law Review*, volume 99, number 2, pp. 773–802, and at https://ilr.law.uiowa.edu/assets/Uploads/ILR-99-2-Calo.pdf, accessed 22 June 2019.

M.R. Calo, 2012. "Against notice skepticism in privacy (and elsewhere)," *Notre Dame Law Review*, volume 87, number 3, pp. 1,027–1,072, and at https://scholarship.law.nd.edu/ndlr/vol87/iss3/3/, accessed 22 June 2019.

F.H. Cate, 2006. "The failure of fair information practice principles," In: Jane K. Winn (editor). *Consumer protection in the age of the "information economy"*. Aldershot, Hamsphire: Ashgate, pp. 341–377.

J.E. Cohen, 2013. "What privacy is for," *Harvard Law Review*, volume 126, number 7, pp. 1,904–1,933, and at https://harvardlawreview.org/2013/05/what-privacy-is-for/, accessed 22 June 2019.

L.F. Cranor, P. Guduru, and M. Arjula, 2006. "User interfaces for privacy agents," *ACM Transactions on Computer-Human Interaction*, volume 13, number 3, pp. 135–178.
doi: https://doi.org/10.1145/1165734.1165735, accessed 22 June 2019.

P. Cranton and K.P. King, 2003. "Transformative learning as a professional development goal," *New Directions for Adult & Continuing Education*, volume 2003, number 98, pp. 31–38.
doi: https://doi.org/10.1002/ace.97, accessed 22 June 2019.

C. DiSalvo, 2012. *Adversarial design*. Cambridge, Mass.: MIT Press.

C.D. Ennis, 1991. "Discrete thinking skills in two teachers' physical education classes," *Elementary School Journal*, volume 91, number 5, pp. 473–487.
doi: https://doi.org/10.1086/461670, accessed 22 June 2019.

P.A. Facione, 2015. "Critical thinking: What it is and why it counts," at https://www.insightassessment.com/Resources/Importance-of-Critical-Thinking/Critical-Thinking-What-It-Is-and-Why-It-Counts, accessed 22 June 2019.

S. Fischer-Hübner, J. Angulo, F. Karegar, and T. Pulls, 2016. "Transparency, privacy and trust — Technology for tracking and controlling my data disclosures: Does this work?" In: S. Habib, J. Vassileva, S. Mauw, and M. Mühlhäuser (editors). *Trust management X. IFIPTM 2016. IFIP Advances in Information and Communication Technology*, volume 473. Cham, Switzerland: Springer, pp. 3–14.
doi: https://doi.org/10.1007/978-3-319-41354-9_1, accessed 22 June 2019.

C. Flavián, M. Guinalíu, and R. Gurrea, 2006. "The role played by perceived usability, satisfaction and consumer trust on website loyalty," *Information & Management*, volume 43, number 1, pp. 1–14.
doi: https://doi.org/10.1016/j.im.2005.01.002, accessed 22 June 2019.

J. Fook, 2015. "Reflective practice and critical reflection," In: J. Lishman (editor). *Handbook for practice learning in social work and social care: Knowledge and theory*. Third edition. London: Jessica Kingsley Publishers, pp. 363–375.

A. Goldfarb and C. Tucker. 2012. "Shifts in privacy concerns," *American Economic Review*, volume 102, number 3, pp. 349–353.
doi: https://doi.org/10.1257/aer.102.3.349, accessed 22 June 2019.

J. Grossklags and N. Good, 2008. "Empirical studies on software notices to inform policy makers and usability designers," In: S. Dietrich and R. Dhamija (editors). *Financial cryptography and data security*. *Lecture Notes in Computer Science*, volume 4886. Berlin: Springer, pp. 341–355.
doi: https://doi.org/10.1007/978-3-540-77366-5_31, accessed 22 June 2019.

E. Hargittai and A. Marwick, 2016. "'What can I really do?' Explaining the privacy paradox with online apathy," *International Journal of Communication*, volume 10, at https://ijoc.org/index.php/ijoc/article/view/4655, accessed 22 June 2019.

C.J. Hoofnagle and J.M. Urban, 2014. "Alan Westin's privacy *Homo Economicus*," *Wake Forest Law Review*, volume 49, number 2, pp. 261–317, and at https://scholarship.law.berkeley.edu/facpubs/2395/, accessed 22 June 2019.

K. Illeris, 2014. "Transformative learning and identity," *Journal of Transformative Education*, volume 12, number 2, pp. 148–163.
doi: https://doi.org/10.1177/1541344614548423, accessed 22 June 2019.

C. Jensen and C. Potts, 2004. "Privacy policies as decision-making tools: An evaluation of online privacy notices," *CHI '04: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 471–478.
doi: https://doi.org/10.1145/985692.985752, accessed 22 June 2019.

C. Jensen, C. Potts, and C. Jensen, 2005. "Privacy practices of Internet users: Self-reports versus observed behavior," *International Journal of Human-Computer Studies*, volume 63, numbers 1–2, pp. 203–227.
doi: https://doi.org/10.1016/j.ijhcs.2005.04.019, accessed 22 June 2019.

L.K. John, A. Acquisti, and G. Loewenstein, 2011. "Strangers on a plane: Context-dependent willingness todivulge sensitive information," *Journal of Consumer Research*, volume 37, number 5, pp. 858–873.
doi: https://doi.org/10.1086/656423, accessed 22 June 2019.

D. Kahneman, 2011. *Thinking, fast and slow*. New York: Farrar, Straus and Giroux.

M. Kezer, B. Sevi, Z. Cemalcilar, and L. Baruh, 2016. "Age differences in privacy attitudes, literacy and privacy management on Facebook," *Cyberpsychology>*, volume 10, number 1, article number 2.
doi: http://dx.doi.org/10.5817/CP2016-1-2, accessed 22 June 2019.

A. Kitchenham, 2008. "The evolution of John Mezirow's transformative learning theory," *Journal of Transformative Education*, volume 6, number 2, pp. 104–123.
doi: https://doi.org/10.1177/1541344608322678, accessed 22 June 2019.

S. Kokolakis, 2017. "Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon," *Computers & Security*, volume 64, pp. 122–134.
doi: https://doi.org/10.1016/j.cose.2015.07.002, accessed 22 June 2019.

B.-J. Koops and R. Leenes, 2006. "'Code' and the slow erosion of privacy," *Michigan Telecommunications and Technology Law Review*, volume 12, number 1, pp. 115–188, and at http://repository.law.umich.edu/mttlr/vol12/iss1/3, accessed 22 June 2019.

B.-J. Koops, B.C. Newell, T. Timan, I. Škorvánek, T. Chokrevski, and M. Galič, 2016. "A typology of privacy," University of Pennsylvania Journal of International Law, volume 38, number 2, pp. 483–575, and at https://scholarship.law.upenn.edu/jil/vol38/iss2/4, accessed 22 June 2019.

M. Kranzberg, 1986. "Technology and history: 'Kranzberg's laws'," *Technology and Culture*, volume 27, number 3, pp. 544–560.
doi: https://doi.org/10.2307/3105385, accessed 22 June 2019.

E.A. Lange, 2004. "Transformative and restorative learning: A vital dialectic for sustainable societies," *Adult Education Quarterly*, volume 54, number 2, pp. 121–139.
doi: https://doi.org/10.1177/0741713603260276, accessed 22 June 2019.

J. Langenderfer and A.D. Miyazaki, 2009. "Privacy in the information economy," *Journal of Consumer Affairs*, volume 43, number 3, pp. 380–388.
doi: https://doi.org/10.1111/j.1745-6606.2009.01152.x, accessed 22 June 2019.

L. Lessig, 2006. "Code, version 2.0," at http://codev2.cc/download+remix/, accessed 1 August 2018.

H. Marreiros, M. Tonin, M. Vlassopoulos, and M.C. Schraefel, 2017. "'Now that you mention it': A survey experiment on information, inattention and online privacy," *Journal of Economic Behavior & Organization*, volume 140, pp. 1–17.
doi: https://doi.org/10.1016/j.jebo.2017.03.024, accessed 22 June 2019.

P.K. Masur, D. Teutsch, and S. Trepte, 2017. "Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS)," *Diagnostica*, volume 63, number 4, pp. 256–268.
doi: https://doi.org/10.1026/0012-1924/a000179, accessed 22 June 2019.

A.M. McDonald and L.F. Cranor, 2008. "The cost of reading privacy policies," *I/S: A Journal of Law and Policy for the Information Society*, volume 4, number 3, pp. 543–568.and at http://hdl.handle.net/1811/72839, accessed 22 June 2019.

J. Mezirow, 2006. "An overview on transformative learning," In: P. Sutherland and J. Crowther (editors). *Lifelong learning: Concepts and contexts*. London: Routledge, pp. 90–105.

J. Mezirow, 2003. "Transformative learning as discourse," *Journal of Transformative Education*, volume 1, number 1, pp. 58–63.
doi: https://doi.org/10.1177/1541344603252172, accessed 22 June 2019.

J. Mezirow, 2000. "Learning to think like an adult: Core concepts of transformation theory," In: J. Mezirow and Associates (editors). *Learning as transformation: Critical perspectives on a theory in progress*. San Francisco: Jossey-Bass, pp. 3–33.

J. Mezirow, 1997. "Transformative learning: Theory to practice," *New Directions for Adult & Continuing Education*, volume 1997, number 74, pp. 5–12.
doi: https://doi.org/10.1002/ace.7401, accessed 22 June 2019.

J. Mezirow, 1990. "How critical reflection triggers transformative learning," In: J. Mezirow (editor). *Fostering critical reflection in adulthood: A guide to transformative and emancipatory learning*. San Francisco: Jossey-Bass, pp. 1–18.

R. Miettinen, 2013. "The concept of experiential learning and John Dewey's theory of reflective thought and action," *International Journal of Lifelong Education*, volume 19, number 1, pp. 54–72.
doi: https://doi.org/10.1080/026013700293458, accessed 22 June 2019.

G.R. Milne, M.J. Culnan, and H. Greene, 2006. "A longitudinal assessment of online privacy notice readability," *Journal of Public Policy & Marketing*, volume 25, number 2, pp. 238–249.
doi: https://doi.org/10.1509/jppm.25.2.238, accessed 22 June 2019.

A. Moore, 2008. "Defining privacy," *Journal of Social Philosophy*, volume 39, number 3, pp. 411–428.
doi: https://doi.org/10.1111/j.1467-9833.2008.00433.x, accessed 22 June 2019.

C. Mouffe, 1999. "Deliberative democracy or agonistic pluralism?" *Social Research*, volume 66, number 3. pp. 745–758.

A. Murray and C. Scott, 2002. "Controlling the new media: Hybrid responses to new forms of power," *Modern Law Review*, volume 65, number 4, pp. 491–516.
doi: https://doi.org/10.1111/1468-2230.00392, accessed 22 June 2019.

H. Nissenbaum, 2011. "A contextual approach to privacy online," *Daedalus*, volume 140, number 4, pp. 32–48, and at https://www.amacad.org/publication/contextual-approach-privacy-online, accessed 22 June 2019.

H. Nissenbaum, 2004. "Privacy as contextual integrity" *Washington Law Review*, volume 79, number 1, pp. 119–158.

P.A. Norberg, D.R. Horne, and D.A. Horne, 2007. "The privacy paradox: Personal information disclosure intentions versus behaviors," *Journal of Consumer Affairs*, volume 41, number 1, pp. 100–126.
doi: https://doi.org/10.1111/j.1745-6606.2006.00070.x, accessed 22 June 2019.

D.A. Norman, 2004. *Emotional design: Why we love (or hate) everyday things*. New York: Basic Books.

Y.J. Park, 2013. "Digital literacy and privacy behavior online," *Communication Research*, volume 40, number 2, pp. 215–236.
doi: https://doi.org/10.1177/0093650211418338, accessed 22 June 2019.

R.A. Posner, 1981. "The economics of privacy," *American Economic Review*, volume 71, number 2, pp. 405–409.

N. Roberts, 2006. "Disorienting dilemmas: Their effects on learners, impact on performance, and implications for adult educators," In: M.S. Plakhotnik and S.M. Nielsen (editors). *Proceedings of the Fifth Annual College of Education Research Conference: Urban and International Education Section*, pp. 100–105; version at http://digitalcommons.fiu.edu/sferc/2006/2006_suie/4/, accessed 22 June 2019.

P.M. Schwartz, 1999. "Internet privacy and the state," *Connecticut Law Review*, volume 32, number 3, pp. 815–860.

P. Sengers, K. Boehner, S. David, and J. Kaye, 2005. "Reflective design," *CC '05: Proceedings of the Fourth Decennial Conference on Critical Computing: Between Sense and Sensibility*, pp. 49–58.
doi: https://doi.org/10.1145/1094562.1094569, accessed 22 June 2019.

Z. Shen and N. Sundaresan, 2010. "Trail explorer: Understanding user experience in webpage flows," *IEEE VisWeek Discovery Exhibition*, pp. 7–8.

H.A. Simon, 1957. *Models of man: social and rational; Mathematical essays on rational human behavior in a social setting*. New York: Wiley.

D.J. Solove, 2013. "Introduction: Privacy self-management and the consent dilemma," *Harvard Law Review*, volume 126, number 7, pp. 1,880–1,903, and at

https://harvardlawreview.org/2013/05/introduction-privacy-self-management-and-the-consent-dilemma/, accessed 22 June 2019.

D.J. Solove, 2007. "'I've got nothing to hide' and other misunderstandings of privacy," *San Diego Law Review*, volume 44, number 4, pp. 745–772.

K.J. Strandburg, 2004. "Privacy, rationality, and temptation: A theory of willpower norms," *Rutgers Law Review*, volume 57, number 4, pp. 1,235–1,306.

E.W. Taylor, 2007. "An update of transformative learning theory: A critical review of the empirical research (1999–2005)," *International Journal of Lifelong Education*, volume 26, number 2, pp. 173–191. doi: https://doi.org/10.1080/02601370701219475, accessed 22 June 2019.

G. ten Dam and M. Volman, 2004. "Critical thinking as a citizenship competence: Teaching strategies," *Learning and Instruction*, volume 14, number 4, pp. 359–379.
doi: https://doi.org/10.1016/j.learninstruc.2004.01.005, accessed 22 June 2019.

R.H. Thaler and C.R. Sunstein, 2009. *Nudge: Improving decisions about health, wealth, and happiness*. New York: Penguin Books.

S. Trepte, D. Teutsch, P.K. Masur, C. Eicher, M. Fischer, A. Hennhöfer, and F. Lind, 2015. "Do people know about privacy and data protection strategies? Towards the 'Online Privacy Literacy Scale' (OPLIS)," In: S. Gutwirth, R. Leenes, and P. de Hert (editors). *Reforming European data protection law*. Dordrecht: Springer, pp. 333–365.
doi: https://doi.org/10.1007/978-94-017-9385-8_14, accessed 22 June 2019.

J. Turow, M. Hennessy, and N. Draper, 2015. "The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation," *Annenberg School of Communication, University of Pennsylvania*, at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf, accessed 22 June 2019.

A. Vasalou, A.-M. Oostveen, C. Bowers, and R. Beale, 2015. "Understanding engagement with the privacy domain through design research," *Journal of the Association for Information Science and Technology*, volume 66, number 6, pp. 1,263–1,273.
doi: https://doi.org/10.1002/asi.23260, accessed 22 June 2019.

P.-P. Verbeek, 2015. "Beyond interaction: A short introduction to mediation theory," *Interactions*, volume 22, number 3, pp. 26–31.
doi: https://doi.org/10.1145/2751314, accessed 22 June 2019.

P.-P. Verbeek, 2008. "Morality in design: Design ethics and the morality of technological artifacts," In: P. Kroes, P.E. Vermaas, A. Light, and S.A. Moore (editors). *Philosophy and design: From engineering to architecture*. Dordrecht: Springer, pp. 91–103.
doi: https://doi.org/10.1007/978-1-4020-6591-0_7, accessed 22 June 2019.

S. Wachter, B. Mittelstadt, and C. Russell, 2018. "Counterfactual explanations without opening the black box: Automated decisions and the GDPR," *Harvard Journal of Law & Technology*, volume 31, number 2, pp. 841–887, and at https://jolt.law.harvard.edu/assets/articlePDFs/v31/Counterfactual-Explanations-without-Opening-the-Black-Box-Sandra-Wachter-et-al.pdf, accessed 22 June 2019.

A.F. Westin, 2004. "A guide to understanding privacy," *Japan Privacy Resource* http://www.privacyexchange.org/japan/japanindex.html, (no longer accessible).

A.F. Westin. 1967. *Privacy and freedom*. New York: Atheneum.

S. White, J. Fook, and F. Gardner, 2006. "Critical reflection: A review of contemporary literature and understandings," In: S. White, J. Fook, and F. Gardner (editors). *Critical reflection in health and social care*. Maidenhead: Open University Press, pp. 3–20.

J.Q. Whitman, 2004. "The two Western cultures of privacy: Dignity versus liberty," *Yale Law Journal*, volume 113, number 6. pp. 1,151–1,221, and at https://digitalcommons.law.yale.edu/fss_papers/649, accessed 22 June 2019.

Editorial history

Received 2 August 2018; revised 5 June 2019; accepted 6 June 2019.

Improving privacy choice through design: How designing for reflection could support privacy self-management
by Arnout Terpstra, Alexander P. Schouten, Alwin de Rooij, and Ronald E. Leenes.
First Monday, Volume 24, Number 7 - 1 July 2019
https://firstmonday.org/ojs/index.php/fm/rt/printerFriendly/9358/8051
doi: http://dx.doi.org/10.5210/fm.v24i7.9358