Behaviour & Information Technology

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tbit20

Conceal or reveal: (non)disclosure choices in online information sharing

Yefim Shulman, Agnieszka Kitkowska, Mark Warner & Joachim Meyer

To cite this article: Yefim Shulman, Agnieszka Kitkowska, Mark Warner & Joachim Meyer (29 Jan 2024): Conceal or reveal: (non)disclosure choices in online information sharing, Behaviour & Information Technology, DOI: 10.1080/0144929X.2024.2304613

To link to this article: https://doi.org/10.1080/0144929X.2024.2304613

Published online: 29 Jan 2024.

BEHAVIOUR & INFORMATION TECHNOLOGY
https://doi.org/10.1080/0144929X.2024.2304613

Conceal or reveal: (non)disclosure choices in online information sharing

Yefim Shulman [a]*, Agnieszka Kitkowska [b]*, Mark Warner [c]* and Joachim Meyer [a]

[a]Department of Industrial Engineering, Tel Aviv University, Tel Aviv, Israel; [b]Service Research Center (CTF) and Department of Mathematics and Computer Science, Karlstad University, Karlstad, Sweden; [c]Department of Computer Science, University College London, London, UK

ABSTRACT

People typically enhance their online personas by sharing favourable personal information. Nevertheless, sharing of unfavourable information about oneself still occurs and is essential in some online contexts (e.g. allowing negative reviews). It remains unclear why people reveal potentially damaging information. We conducted an online experiment ($N = 462$) to explore the effects of feedback properties and individual characteristics on online information sharing in two contexts (social and socioeconomic) where personal ratings are essential. We allowed users to conceal their personal rating if it dropped below a threshold. The context was the primary determinant of the threshold users chose. Control availability and feedback content triggered additional considerations and caused some users to change their (non)disclosure choices. However, many users relied on their priors (experience, assumptions) rather than on new information. Our findings show how people may fail to identify the impact of nondisclosure, which may signal undesirable information to others. These findings challenge the reliance on holding users solely accountable for their 'informedness' vis-à-vis disclosure of their personal information.

ARTICLE HISTORY
Received 13 June 2022
Accepted 5 January 2024

KEYWORDS
(Non)disclosure; feedback; self-presentation; decision-making; controls; sharing economy

1. Introduction

Individuals manage their public image online and in interpersonal interactions by deciding which personal information to reveal and which to conceal. The decisions regarding the disclosure or nondisclosure of information often depend on the individual's experiences, traits, and perceptions (Gerber, Gerber, and Volkamer 2018; Y. Li 2012; Paine et al. 2006). People form impressions of a person using the information the person chooses to reveal, as well as drawing on assumptions around information the person chooses to conceal. A person's choice not to disclose information may be interpreted as an attempt to hide information, with negative inferences made around the undisclosed information (Warner et al. 2020). People may not necessarily consider the self-presentation implications of not revealing certain information.

In online interactions, user decisions to conceal or reveal information can be informed by feedback from systems (e.g. indications and alerts, privacy notices) and from other people (e.g. friends' opinions, news media messages). We define *feedback* as 'the transmission of evaluative or corrective information about an action, event, or process to the original or controlling source' (Merriam-Webster, "feedback", n 2021) to improve knowledge, performance, outcomes, etc. For instance, an online social platform may provide its users with feedback (via notifications) regarding who may view each item of personal information they share or inform its users about sharing delay to give time for additional considerations, in line with Wang et al. (2014). In addition to providing social cues on direct actions (sharing of particular information), feedback may also inform users regarding collective behaviour – i.e. social norms – what common, expected or acceptable sharing looks like based on other users' behaviour (e.g. dating platforms informing their users that reacting to a potential partner's profile prompt, as a first step, increases the chances for setting a date by a certain amount). Even though there has been steadily increasing interest in factors affecting decision-making regarding disclosure (Dinev, McConnell, and Smith 2015; Hoyle et al. 2017; Joinson et al. 2010; Paine et al.

CONTACT Yefim Shulman efimshulman@mail.tau.ac.il, ye.m.shulman@gmail.com Department of Industrial Engineering, Tel Aviv University, Tel Aviv, Israel

*During the peer–review process, Yefim Shulman changed affiliation to Erasmus School of Social and Behavioural Sciences, Erasmus University Rotterdam. While working on the paper, Agnieszka Kitkowska changed affiliation to the Department of Computer Science and Informatics, Jönköping University. Part of work on the paper was carried out while Mark Warner was affiliated with the Department of Computing and Information Sciences, Northumbria University.

2006; Shulman and Meyer 2019; Tsai et al. 2009), little is known about the ability of feedback to inform (non)disclosure and aid decision-making regarding the sharing of potentially unfavourable information that may influence users' self-presentation and social and economic opportunities.

In this paper, we examine people's decisions to conceal or reveal reputational information. Such decisions are part of the impression management process (i.e. the decisions people make to control information flows in social interactions to be perceived in a desired way by others – Section 2.1), and they affect users' online image. We concentrate on the effects of technological rather than social feedback, delivered via on-screen indications (i.e. system notifications), as it is a common means to inform users. We focus on specific properties of feedback, such as the feedback timing relative to decision-making (before vs. after) combined with the availability of control actions, and the feedback content. We consider concrete choices around concealing or revealing reputational information (i.e. a rating score) and compare two different online sharing economy contexts, defining sharing economy as an 'economic activity that involves individuals buying or selling usually temporary access to goods or services especially as arranged through an online company or organisation' (Merriam-Webster, "Sharing Economy", n 2021). People in such environments often rate each other and rely on such ratings when making decisions. The first context is a social meet-up platform connecting travelling companions (a horizontal matching between peers). The second is a short-term employment platform as a hierarchical interaction between potential employers and employees. We also consider intrinsic factors that may affect nondisclosure decisions, such as participants' intention to give personal information, privacy risk beliefs, perceived information control, and privacy concerns.

Overall, we aim to better understand people's decisions to conceal or reveal potentially unfavourable personal information as a part of the impression management process in online social platforms and how privacy-related feedback may affect this behaviour. To do so, we combine feedback-related, contextual, and individual factors in our research approach.

Our results contribute to the understanding of how people decide about their self-presentation and online privacy – whether to conceal or to reveal externally assigned reputational information (e.g. ratings, scores, reviews) as part of impression management on platforms facilitating the online sharing economy:

- We empirically show with experiment-based evidence how the context of a given interaction may be among the strongest predictors of decisions to conceal or reveal personal reputational information.
- We empirically demonstrate that both the availability of control actions and feedback content may influence user preference for a status quo – i.e. prior user set choices.
- The availability of control actions (ease of use) at different times during the interaction can be a recognisable and helpful feature.
- The results show the reciprocity between the self-presentation considerations and preferences for the counterpart's image. The results also uncover positive relations between online (non)disclosure of reputational information and the intention to give personal information and the attitude regarding impression formation based on average rating scores.
- Our findings open a discussion on how many people may think of their personal information as simple and complete facts, not realising that the choice not to reveal information may be informative and signal undesirable information. This also challenges the existing legalistic reliance on the user 'informedness'.
- Finally, our analyses highlight that the strength of, and the role that users' priors (e.g. knowledge, experience) play in online behaviour should not be overlooked in research and practice.

2. Background

In this paper, we address the online disclosure and nondisclosure of personal information in social and socioeconomic contexts as an instrument for online impression management. We use the term '(non)disclosure' for brevity when discussing decisions to conceal or reveal personal information. As privacy-related decisions may be affected by an interplay of factors and processes (Dinev, McConnell, and Smith 2015; Gerber, Gerber, and Volkamer 2018), we combine several factors and user characteristics in our study of (non)disclosure. We study how such (non)disclosure decisions may be informed by feedback delivered before or after the decisions were made (*feedback timing*) and affected by the ease of adjusting decisions (*availability of control actions*, i.e. intervenability, as per Hansen, Jensen, and Rost 2015). We focus on people's (non)disclosure motivations, modulated by social norms and the framing of feedback, because these factors may often influence people's disclosure motivations (Acquisti et al. 2017; Mirsch, Lehrer, and Jung 2017), and we aim to determine how such informative cues may affect people's decisions regarding online privacy and self-presentation. Additionally,

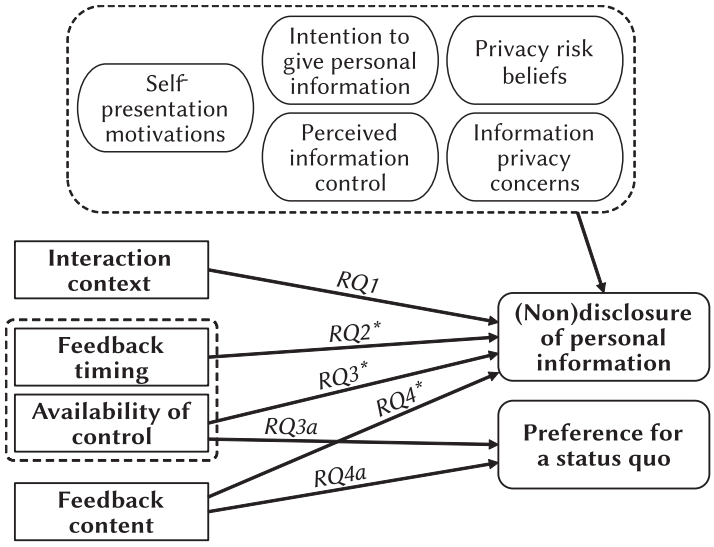

Figure 1. The research model representing the relations between the factors and outcome variables. *Factors predicted to have an interaction effect; RQ2 and RQ3 represent a compound factor for the purposes of the empirical study (Section 3): Timing-Control.

to address the complexity of factors potentially affecting (non)disclosure behaviour (Dinev, McConnell, and Smith 2015), we account for select individual characteristics, such as privacy-related attitudes and ad hoc impression management motivations. Figure 1 depicts the overall research model, comprised of the aforementioned factors and measures.

2.1. (Non)disclosure of personal information: concealing or revealing

Disclosure of personal information normally allows others to learn the content of said information, while nondisclosure is meant to allow people to keep the information to themselves. However, under certain conditions, nondisclosure can signal information to others, letting them learn or assume facts about those who do not disclose. Whenever others perceive disclosure of an attribute as low-cost and desirable, those who do not disclose may endure negative consequences to their image and reputation. This may cause (non)disclosure of personal information not to be of voluntary character anymore. Such a process, termed 'privacy unravelling' (Peppet 2011), echoes the effect of the unravelling of information disclosure in economics and decision-making research (for prototypical markets, e.g. Roth and Xing 1994, H. Li and Rosen 1998 and Ostrovsky and Schwarz 2010; and for empirical studies of institutional (non)disclosure, e.g. Bederson et al. 2018, Sah and Read 2020 and Butler and Read 2021). Benndorf, Kübler, and Normann (2015) studied the disclosure of personal information in a prototypical labour market, indicating that the least productive workers' decisions to disclose information may strongly depend on the most productive workers' productivity disclosure decisions. Warner et al. (2020) and Warner et al. (2018) studied the disclosure of human immunodeficiency virus (HIV) status by the users of an online dating platform. The authors revealed differences in ratings between the HIV statuses, suggesting that negative inferences develop around users who choose not to disclose their HIV status. Yet, it remains unclear whether this affects people's disclosure behaviours and whether people consider the potential negative consequences of (non)disclosure. In our study, personal information is a user's rating – the average of the scores obtained from multiple people on a website (sharing economy platform). Unlike HIV status or the productivity measure (a result of personal effort), the average score is assigned externally. Moreover, we ask people to indicate a threshold value rather than a binary fact (e.g. the HIV status).

(Non)disclosure motivations resonate with the signalling theory in economics (Connelly et al. 2011), originating in studies of decision-making under information asymmetry (Spence 1973). Signaling information about oneself to others serves to distinguish oneself and meet the expectations of a potential observer, thus affecting one's image and reputation – impressions others have about oneself. Accordingly, the impression management theory is concerned with how people control information flows in social interactions to create and maintain the desired impression of themselves as perceived by others (Goffman 1959). Self-disclosure is one of the methods of impression management and self-presentation. With the development of mediated communications, it is receiving attention alongside the problematic aspects of privacy

(Joinson 2001; Kobsa, Patil, and Meyer 2012). Empirical research addressed the behaviour of users of online social networks, showing that attention allocation, information control, self-efficacy, and certain personality traits may predict self-disclosure choices (Feaster 2010; Krämer and Winter 2008). Additionally, past research suggests that privacy expectations and self-presentation may be contextual (Emanuel et al. 2014; Martin and Nissenbaum 2016; Nissenbaum 2004; van Dijck 2013), which may lead to differences in self-disclosure across contexts, even when the disclosed information remains the same. Although literature looked at some of the effects of contextual factors on (non)disclosure, to the best of our knowledge, there is a lack of empirical research into the influence of the interaction context and self-presentation motivations for non-disclosure of reputational information on sharing economy platforms, specifically.

In this paper, we rely on the premises of impression management and signalling theories and assume that developing and maintaining a positive image of oneself can be context-dependent and can motivate and drive personal information (non)disclosure. We test the same feedback design in two different contexts, in which (non)disclosure may define people's reputation: one assuming peer-to-peer interaction (a social context, motivated by self-presentation) and another one assuming hierarchical employer-employee interaction (a socioeconomic context, motivated by self-presentation and financial considerations). We aim to obtain empirical evidence for context-dependency of privacy behaviour regarding (non)disclosure (Figure 1):

RQ1: How does the (non)disclosure of personal information vary between interaction contexts?

We hypothesise that the (non)disclosure of personal reputational information will systematically differ between the interaction contexts.

As (non)disclosure occurs in the presence of feedback, we further focus on how the properties of feedback – feedback timing, availability of control actions in response to feedback, and feedback content – may affect (non)disclosure behaviour.

2.2. Informing personal information (non)disclosure

2.2.1. Feedback enabling control

In this paper, we rely on one of the most prominent approaches to privacy as a form of control over the personal domain (Altman 1977; Culnan and Bies 2003; Warren and Brandeis 1890; Westin 1970). Such control should be dynamically adjustable and context-dependent (Acquisti, Brandimarte, and Loewenstein 2015; Altman 1977; Palen and Dourish 2003; Toch, Wang, and Cranor 2012). One way to execute control is to decide what information can be revealed and what information should be concealed from others. Control decisions can be informed by visual cues (indications) such as notices, permission requests, or warnings. Past research has demonstrated that the same visual cues may lead to different privacy attitudes and disclosure behaviours in different contexts, enhancing or diminishing users' privacy (Kitkowska et al. 2020). These indications can provide informative and relevant feedback to the users (Bellotti and Sellen 1993; Shulman and Meyer 2019), enabling personal control, aiding impression management, and accommodating the privacy as practice paradigm (Berendt 2012). Feedback on the privacy implications of actions may alleviate privacy concerns (Tsai et al. 2009). It can also be used to balance personal information disclosure against the potential benefits of using technology (Hoyle et al. 2017). The usability of a privacy-enhancing technology aiming to increase the transparency of data processing, i.e. a transparency-enhancing tool (for a review of systems considering usable transparency, see, for instance, Murmann and Fischer-Hübner 2017), relies on timely, yet not cumbersome feedback. Transparency and feedback mechanisms are related concepts crucial for engineering both 'privacy by policy' and 'privacy by interaction' (Gürses 2016). Timing is an indispensable element for the implementation of feedback mechanisms. It has already been in the scope of privacy-related empirical research. For instance, the timing was studied, confounded with the placement of 'privacy indicators' during cost-benefit analyses, prior to making a decision regarding a purchase (Egelman et al. 2009). The timing affected comprehension of privacy notices in a mobile app store (Balebako et al. 2015). Timing was also operationalised as an interruption of an activity (Patil et al. 2015). However, the challenge of appropriate and relevant ad hoc feedback (from a systems engineering standpoint, Spiekermann and Cranor 2009) remains far from resolved.

We extend past research on feedback timing effects to the study of the timing of feedback before or after a user commits to a decision, as shown in Figure 2. We assume that feedback arrives as indications and may be actionable (as discussed in detail below). This timing configuration may be a crucial parameter for feedback relevance and helpfulness in user privacy management (and, therefore, impression formation). Thus, we aim to investigate (Figure 1):

RQ2: How does the timing of informative feedback (i.e. indications) – before vs. after making a decision – affect (non)disclosure of personal information?

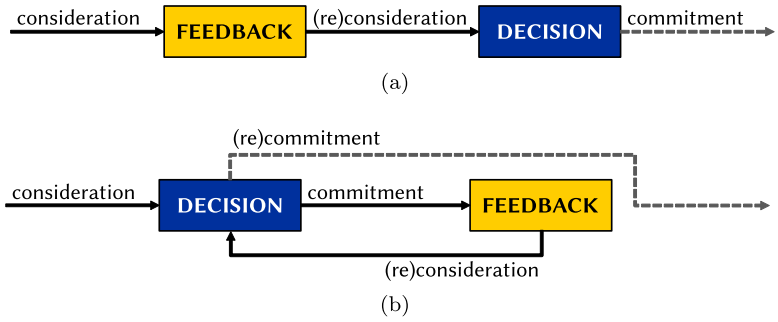

Figure 2. Timing of feedback in relation to decision-making. (a) Before a decision and (b) After a decision.

We hypothesise that people receiving feedback before committing to a (non)disclosure decision will be more restrictive regarding revealing or concealing their reputational information compared with people receiving feedback after the decision is executed.

The decisions to conceal or reveal information online are usually effected through some form of action. Feedback actionability has been shown to play a role in how people respond to feedback (Patil et al. 2014). Actionability may be related to the degree of available control rather than to the effort needed to exercise control (Krol and Preibusch 2016).

The usability, understood here as ease of use of control actions, may affect the actual use of a system (Adams, Nelson, and Todd 1992; Karahanna and Straub 1999). It is the primary focus of usability testing (Nielsen 1994). Perceived control is among the determinants of how people perceive ease of use (Venkatesh 2000). Thus, control affordance to the users is one of the key problems in usability engineering, as reflected in the usability heuristics methodologies (Nielsen 1994; Tan, Liu, and Bishu 2009). Empirical privacy research asserts that slight design changes to user controls may affect how usable and useful people find the control actions (Habib et al. 2020, 2019).

To further corroborate this argument and empirically test how the actionability of feedback may be affecting (non)disclosure behaviour, we inquire (Figure 1):

RQ3: How does the availability of control at different interaction times affect the (non)disclosure of personal information?

We hypothesise that the (non)disclosure of personal reputational information will systematically differ, depending on how actionable the feedback is – whether the control is afforded within the interaction frame (indication) or requires additional actions.

The problem of usable and useful control mechanisms is exacerbated when these mechanisms are intended to enable adjustment of already made disclosure (i.e. to another level of disclosure or nondisclosure), especially when disclosure actions are ongoing and occur after the initial configuration of privacy settings (Adjerid, Acquisti, and Loewenstein 2019). Adjustment requires additional effort, depleting people's cognitive resources.

Among the most relevant cognitive effects that discourage people from reconsidering the previously made choices are the default effect (Dinner et al. 2011), and the status quo bias (Kahneman, Knetsch, and Thaler 1991; Samuelson and Zeckhauser 1988). The former often appears with the concept of 'nudging' (Sunstein 2014; Thaler and Benartzi 2004). It manifests itself in that out of a given set of options, people tend to choose the pre-selected one. The status quo bias – usually associated with behavioural decision-making research – manifests itself in people's preference to maintain any current state of affairs, perceiving any change to it as a loss, regardless of the direction of such a change. The implications of the status quo bias in human-computer interaction and privacy research have been widely discussed (Mirsch, Lehrer, and Jung 2017; Steinfeld 2016), together with the default effect (Acquisti, Brandimarte, and Loewenstein 2015; Johnson, Bellman, and Lohse 2002). Both the default effect and the status quo bias were found to affect privacy attitudes and behaviours, enhancing or deteriorating user privacy, with the default effect directly affecting information disclosure, while the status quo affecting the choice of privacy settings and willingness to disclose information (Kitkowska et al. 2020).

The default effect involves the default options set by an external agent (e.g. a service provider) rather than by the users themselves, so the users choose whether to adhere to the default options. The status quo bias involves user choices, regardless of whether the 'status quo' was created by default options or by previous user choices. In this paper, we consider the status quo bias as we study how people make decisions – active

choices – regarding concealing or revealing reputational information at their own, individually 'comfortable', levels of disclosure without having a specific default option to bias their choices.

Psychological effects can limit people's responses regarding the adjustment of disclosure, which may be detrimental to their online image and privacy when the disclosure settings are far from some optimal level. Therefore, we add to RQ3 (Figure 1):

RQ3a: Does the availability of control affect the preference for a status quo?

We hypothesise that when control is afforded within the interaction frame, people are more likely to reconsider and adjust their prior (non)disclosure choices compared with people in the situation when control requires additional actions.

Feedback conveys information, and the nature of such information should play a role in how people decide to conceal or reveal information. To complete our model and make it more holistic, we include select parameters of feedback content, which may modulate (non)disclosure, namely information framing and social norms.

2.2.2. Feedback content: framing and social norms

Feedback appealing to self-presentation can affect disclosure choices, depending on how the corresponding feedback message is framed. The framing effect is a cognitive bias usually manifested as a change in a risk-taking tendency regarding choice options, depending on the connotations used to describe those choice options (Kühberger 1998; Tversky and Kahneman 1981). Privacy research has extensively used the notion of framing in the visual design of privacy-related communication (Kitkowska et al. 2020; Mirsch, Lehrer, and Jung 2017). The effect of framing has been shown for privacy policy interactions (Johnson, Bellman, and Lohse 2002) and disclosure (e.g. Adjerid, Acquisti, and Loewenstein 2019; Choe et al. 2013; Habib et al. 2020). [1] The framing effect may influence users' disclosure decisions in response to indications, either informing about outcomes (affecting judgment) or communicating some reference point (affecting choices) – Kühberger (1998).

Another way to enrich the feedback content is to communicate the social norms, facilitating the spread of information regarding commonly acceptable practices and aiding the integration of new users into an online environment. Much research in the social sciences, including communication studies (Lapinski and Rimal 2006), focuses on the social norms closely related to disclosure behaviours (Lapinski et al. 2013). When a user receives explicit feedback regarding social norms, it may affect the configuration of that user's privacy settings, which influences self-disclosure (Spottswood and Hancock 2017). Extensive empirical findings suggest that social norms may align both privacy attitudes and behaviours of people to those asserted by the norms, strongly driving information disclosure (Kitkowska et al. 2020; Mirsch, Lehrer, and Jung 2017).

Both framing and social norm communication may be considered closely related to the concept of 'nudging' (Thaler and Benartzi 2004), i.e. altering decisions in a predictable way without forbidding any options, using a choice architecture. Past research on personal information disclosure referred to some behavioural interventions as 'nudging' and highlighted both the advantages of nudging privacy decisions (e.g. achieving some individually 'comfortable' level of disclosure) and its detriments (e.g. manipulating users into over-disclosure) – Mirsch, Lehrer, and Jung (2017), Acquisti et al. (2017) and Nouwens et al. (2020). However, not every behavioural intervention should fall within the definition of a 'nudge', as, in empirical studies, 'nudging' interventions may be loosely defined and have varying effectiveness across contexts (Hummel and Maedche 2019). Both the utility and applicability of nudging are debated topics, especially for governance and policy-making (Kosters and der Heijden 2015; Willis 2013).

In this paper, we extend the existing empirical privacy literature on informing users' decisions entailing consequences for their online image and privacy and investigate whether and how privacy-related feedback may affect user decisions to conceal or reveal information as a part of the impression management process (and whether such an intervention may be helpful to the users). We assume that personal information (non)disclosure is motivated by the need for self-presentation and maintaining a positive image of oneself, constrained by social norms and framed feedback (Figure 1):

RQ4: How does the feedback message content influence (non)disclosure of personal information?

We hypothesise that the (non)disclosure of personal reputational information will systematically differ across the message content conditions: (a) neutral content; (b) neutral content with framed information, inducing self-presentation considerations; (c) neutral content with framed information, inducing self-presentation consideration, and communicating a social norm.

When people receiving feedback can rely on the choices of others and can change their prior decisions, they may prefer to use the opportunity and adjust

Table 1. Independent variables.

Variable	Levels	Research Questions
V1 – *Context* (Context of interaction, i.e. situation context)	1 – *Traveling* (Platform *TravelFriend* for travelling together – peer-to-peer relationships)	RQ1
	2 – *Employment* (Platform *EmployOnline* for short-term employment – hierarchical relationships)	RQ1
V2 – *Timing-Control* (Feedback actionability, dependent on timing and control action)	1 – *Before* (Feedback before choosing a minimal score to share)	RQ2
	2 – *After* (After choosing a minimal score to share with a button allowing to go back and adjust the chosen threshold)	RQ2, RQ3, RQ3a
	3 – *After+Slider* (After choosing a minimal score to share with an embedded option to adjust the chosen threshold)	RQ3, RQ3a
V3 – *Content* (Feedback content)	1 – *Neutral* (Neutral message, i.e. control group)	RQ4, RQ4a
	2 – *Self-presentation* (Message inducing self-presentation considerations)	RQ4, RQ4a
	3 – *Social norm* (Message inducing self-presentation considerations and communicating a social norm)	RQ4, RQ4a

such prior decisions to conform with the social norms or to reflect their self-presentation considerations better. Hence, we add to the RQ4 (Figure 1):

RQ4a: Does the feedback message content affect the preference for a status quo?

We hypothesise that when the message induces self-presentation considerations with or without a social norm, people are more likely to reconsider and adjust their prior (non)disclosure choices, compared with people who see a neutral message.

Additionally, we predict an interaction between the feedback timing and the availability of control (a compound of RQ2 and RQ3) and feedback content (RQ4) in their effect on (non)disclosure of personal reputational information (Figure 1. The two interacting variables contain three levels each (Section 3.1 and Table 1). We expect no differences in the neutral content condition, moderated by the timing and control conditions. We also expect no differences in the after condition, moderated by the message content conditions. We expect significant differences both in the before and after+slider condition: a social norm communicating message will lead to less restrictive (non)disclosure choices, compared with a neutral message, whereas a message inducing self-presentation considerations will result in more restrictive (non)disclosure choices, compared with a neutral message. Should this interaction occur, it might negate the main effects of feedback timing-control and content, hypothesised in RQ2, RQ3, and RQ4, if the differences are similar in magnitude (and expected to be opposite in direction).

2.3. Privacy attitudes and perceptions as individual characteristics

According to the prevalent findings in the empirical privacy literature (Gerber, Gerber, and Volkamer 2018) and the APCO (Antecedents → Privacy Concerns → Outcomes) model (Dinev, McConnell, and Smith 2015), disclosures result from a complex model of decision-making, involving, among other things, privacy-related attitudes and perceptions, as well as the behavioural intention to disclose. Note that the behavioural intention does not necessarily result in actual behaviour (Ajzen and Fishbein 1977; Dienlin and Trepte 2015; Fazio and Roskos-Ewoldsen 2005; LaPiere 1934; Sheeran and Webb 2016). We argue that it is not unreasonable to assume that some of these factors may play a role in decisions regarding nondisclosure. To complete our research approach in this paper, we include the individual's privacy concerns, privacy risk beliefs, perceived information control, and intention to give personal information as stable factors, potentially affecting decisions to conceal or reveal information (Figure 1) in the two contexts of interest.

3. Method

We conducted an online experiment to investigate the effects that feedback delivered through indications may have on user decisions regarding the (non)disclosure of potentially unfavourable personal information. The study was conducted as an online experiment, as we did not focus on a specific and difficult-to-reach population. Online experiments enable access to a large number of participants with timely data collection and allow participants to complete the experimental task in a way convenient to them. We chose an experimental design to manipulate and measure multiple variables and enable data analyses using general linear models and non-parametric tests. We considered individual characteristics to account for their potential influence on user (non)disclosure decisions. We hypothesised that the timing of the indications with the availability of control actions, the type of information in the indication, and the context of the interaction (Table 1) could affect the (non)disclosure of personal information.

Table 2. Indication setups across experiment conditions.

Timing-Control (V2)	*Content* (V3)			Interactive buttons
	Neutral (V3-1)	*Self-presentation* (V3-2)	*Social norm* (V3-3)	
Before (V2-1)	'Would you like to:'	'{*Sharing your average score*} may impact how other people perceive you, and decide whether they would like to travel with you (hire you).'	'{*When you don't share your average score, it*} may impact how other people perceive you, and decide whether they want to travel with you (hire you). {*People may assume your score is low.*}'	Left: [Go back to read the instructions] Right: [Continue]
After (V2-2)	Same as *Before*	Same as *Before*	Same as *Before*	Left: [Adjust your sharing score] Right: [Continue]
After+Slider (V2-3)	'Would you like to adjust your sharing score?'	Same as *Before*, appended: 'Would you like to adjust your sharing score?'	Same as *Before*, appended: 'Would you like to adjust your sharing score?'	Left: None Right: [I'm satisfied with my choice, proceed]

3.1. Design

We designed the experiment as two fictitious sharing-economy-related services, differing in the context of interaction (i.e. *Context* manipulation, Table 1): a travel partner search application and a short-term online employment platform. The fictitious applications would allow users to collect scores from their reviewers (either as a travel companion or an employee). After accumulating some scores, users would be able to publicly share their average ratings, and decide at which point the score should be disclosed to other users (decide when to conceal and when to reveal). In both contexts of our study, the participant's task was to set their preferred score disclosure threshold. Feedback regarding their threshold choice was delivered via on-screen indications either before or after participants committed to their (non)-disclosure decision. The participants who received feedback after committing to the decision were able to adjust their prior choice either by going back to settings or immediately within the indication (i.e. *Timing-Control* manipulation, Tables 1 and 2). The indications communicated either (1) the available actions, (2) the available actions and self-presentation implications, or (3) the available actions with self-presentation implications and a social norm (i.e. *Content* manipulation, Tables 1 and 2).

We used a full factorial experimental design to study the RQs in combination and explore potential interactions between the variables. The full factorial $2 \times 3 \times 3$ experiment design resulted in 18 between-subject groups. The participants were randomly assigned to each group.

Independent variables. Table 1 contains the description of the levels of the independent variables in the experiment. The conditions were designed to accommodate the research questions (Section 2) in the way shown in Table 1. The examples of the indication designs resulting from the factorial combination of the independent variables are shown in Figure 3. The messages communicated via the indications are shown in Table 2. All designs were responsive.

Dependent variables. The dependent variables in the experiments included:

(1) *Final score threshold* (FST) measured numerically from 0 to 10 (11 points) – a score above which the participants would prefer to share (made public) their average ratings. Selecting a 0 would result in revealing the average score, unless it is exactly at 0, whereas selecting a 10 would lead to effectively concealing the score (as the average should not normally climb above 10). The FST is the measure of (non)disclosure of personal information for RQ1, RQ2, RQ3, and RQ4:

(a) In the *Before* condition, the FST is the score threshold the participants chose, having encountered the indications. In this condition, the participants could not change their initial choice of score threshold.

(b) In the *After* and *After+Slider* conditions, participants could change their initial choice of the score threshold. Therefore, here the FST is either the initial score threshold the participants chose before encountering the indications or, if a participant used the opportunity to adjust the initial score threshold, that adjusted score threshold.

(2) *Score threshold adjustment behaviour* (for *After* and *After+Slider* conditions) measured categorically (3 categories) to address RQ3a and RQ4a. We measured the score thresholds the participants chose and the adjustments they made (if any), and recorded which buttons in the indications they clicked and how much time they spent on each of these screens, thus registering three typical behaviours:

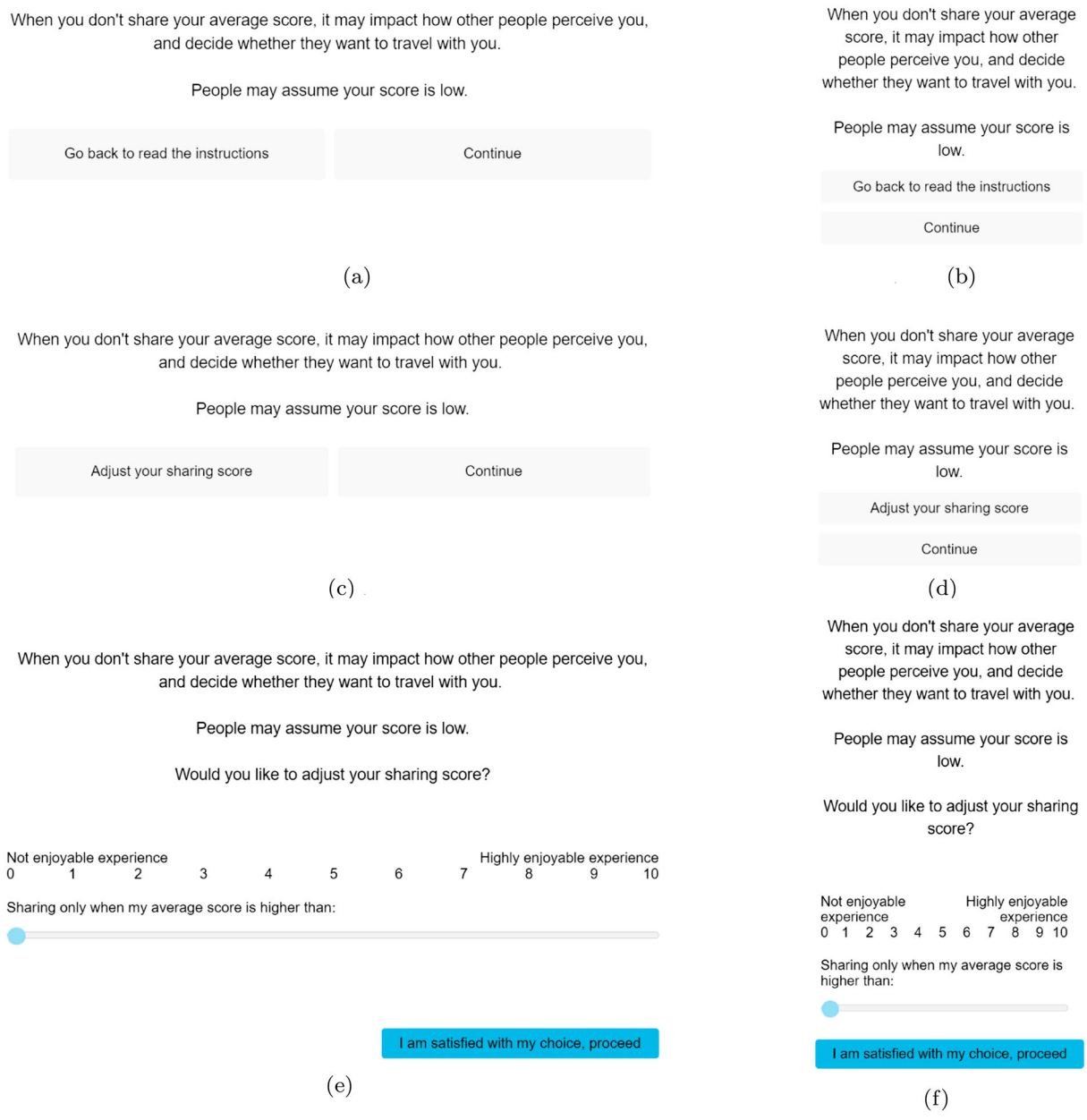

Figure 3. Samples of the indications used in the experiment (*TravelFriend+Social norm* conditions only). Other conditions differed only in texts (Table 2). (a) *Before*, web. (b) *Before*, mobile. (c) *After*, web. (d) *After*, mobile. (e) *After+Slider*, web. and (f) *After+Slider*, mobile.

(1) reconsidering and changing the initial score threshold, making the adjusted score threshold the FST;
(2) showing interest in changing the initial score threshold by interacting with the adjustment option but submitting the same initial score threshold value in the end, which would make that value the FST;
(3) showing no interest in changing the initial score threshold by ignoring the adjustment option. The initial score threshold would be recorded as the FST.

Covariates. We controlled for several individual characteristics to address our research questions more comprehensively. Using validated and (or) frequently used multi-item scales adapted from literature (Section 3.3), we measured four psychological constructs: Intention to give personal information (IGPI), Privacy risk beliefs (PRB), Perceived information control (PIC), and Individual's privacy concerns (IPC). We also measured two attitudes that are relevant to self-presentation motivations (impression management): *Preferred score for a counterpart* and *Attitude to impression formation* (Section 3.3).

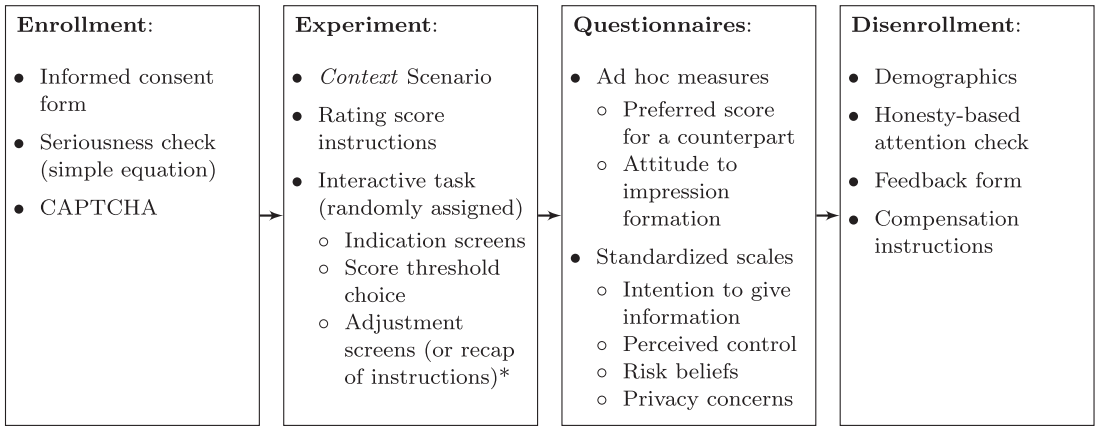

Figure 4. Description of the experimental flow (*Depending on the randomly assigned condition and the participant's choice.)

3.2. Procedure

The experiment flow contains four main stages (Figure 4):

Enrollment. We asked participants to acknowledge the information provided in the informed consent form, to solve a simple mathematical equation, and to interact with a reCAPTCHA [2] as a precaution against automated responses.

Experiment. In this stage, we introduced manipulations and measured the dependent variables. In each condition, participants saw a relevant scenario (Appendix 2), followed by the experimental screens (Figure 3 and Section 3.3). The scenarios informed participants that they had been using their respective platforms for about a year, during which they had accumulated several reviews (i.e. scores). We recorded participants' button clicks in all the conditions (Table 2). The 'Go back to read the instructions' button (added to keep the conditions in the experiment equivalent in terms of time and flexibility) sent the participants to the screen repeating the instructions, after which the participants inevitably proceeded to choose their sharing score threshold, and then to the questionnaires stage. The 'Adjust your sharing score' button led the participants to the screen, where they could change their previous sharing score threshold choice and then to the questionnaire stage. The 'Continue' and 'I'm satisfied with my choice, proceed' buttons sent the participants directly to the questionnaire stage.

Questionnaires. The participants across all conditions proceeded to answer questionnaires, where we collected responses that provided measurements for the covariates (Section 3.3).

Disenrollment. Finally, the participants answered demographics questions, reported how much attention they gave to the experiment (honesty-based), and provided free-form feedback if they so desired.

3.3. Materials

The experiment was implemented using the Qualtrics platform. It contained different indication messages (Table 2), as well as scales measuring various psychological constructs.

Indications. The onscreen indications differed in message texts and available buttons across conditions. Table 2 presents the detailed content of all indications, while Figure 3 shows their visual design.

Measurements of individual characteristics (psychological constructs and attitudes). To measure psychological constructs, we adapted four instruments from the literature to use in our experiment:

(1) The intention to give personal information (IGPI) measurement was adapted from Malhotra, Kim, and Agarwal (2004), being adjusted to fit our scenarios. The IGPI was measured on a 7-point semantic differential scale with four items.
(2) The privacy risk beliefs (PRB) measurement was also adapted from Malhotra, Kim, and Agarwal (2004) and measured on a 7-point Likert scale with five items. Both IGPI and PRB are validated instruments.
(3) The perceived information control (PIC) measurement was adapted from Dinev et al. (2013) [3]. The measure employed a 7-point Likert scale with four items.
(4) We measured the individual's privacy concerns (IPC) with a validated instrument adapted from Smith, Milberg, and Burke (1996). The measurement was taken on a 7-point Likert scale with the

15 original unmodified items, encompassing four subscales: *Collection*, *Errors*, *Unauthorized Secondary Use*, and *Improper Access*.

The details of the scales used in our study are provided in Appendix 1.

We also measured two attitudes related to impression management (self-presentation) motivations:

(1) *Preferred score for a counterpart* (PSC). We asked the participants to indicate the minimal preferred score for their potential travel partner or employee, were they to switch roles in the experimental scenario: thinking either from the standpoint of a user searching for a travel partner or from the standpoint of an employer looking for an employee. The PSC was measured identically to the FST on a scale from 0 to 10 (11 points).
(2) *Attitude to impression formation* (AIF). We asked the participants to evaluate the way they would feel when people formed an impression about them based on the score they published online. That single-item question was measured on a 7-point Likert-type scale anchored 'Very negative' through 'Very positive'.

3.4. Participants

We recruited participants through the CloudResearch panels. The users of CloudResearch are U.S. residents. Overall, having estimated the minimal required sample size using G*Power 3 (Faul et al. 2007) and having considered potential errors (e.g. due to attention check failure), we collected $N = 616$ complete responses. Table 3 contains both full and modified (Section 4.1) sample demographics.

The initial distribution of participants across the groups was balanced ($M = 34.22$, $SD = 1.70$, range: 32−38). The majority (45.2%, $n = 345$) had some experience with platforms similar to the ones we presented. Most participants (59.6%, $n = 367$) completed the experiment on mobile platforms, and the rest $n = 249$ – on desktop or laptop computers.

Participation in the experiment was voluntary, and the participants were remunerated upon completion of the tasks in accordance with CloudResearch panels' rates [4]. We did not provide an additional incentive (e.g. performance-based or context-related). The participants could terminate their involvement in our research at any point, with no negative consequences for themselves. They were instructed accordingly and had to acknowledge the consent form before participating in the experiment. The experiment and the informed consent form underwent the university's ethical committee approval process.

4. Results

4.1. Preparatory analyses

Before the main analyses, we examined the time the participants spent on the screen describing the experiment scenario (i.e. *Context* scenario, Appendix 2 and Figure 4). Insofar as paying attention to the scenarios was necessary to understand the task and the scenario descriptions contained 198 and 212 words for *TravelFriend* and *EmployOnline*, respectively, we excluded the participants who fell in the first quartile of the distribution on that timing variable [5]. From the initial sample of $N = 616$ we reached a modified sample of $N = 462$ (Table 3 contains the modified sample demographics). The resulting distribution of participants across the groups in the modified sample remained comparable, $M = 25.67$, $SD = 3.25$, range: 20−30 (above the threshold recommended by an a priori power analysis to account for potential interaction effects). Scale evaluation and descriptive statistical analyses were performed on both samples – initial and reduced – to ensure consistency. We report the results of further analyses using the $N = 462$ sample unless stated otherwise.

4.1.1. Measurement scales used in the experiment

We evaluated the validity and reliability of the scales used to measure the latent variables needed for the main analyses: the IGPI, PRB, PIC, and IPC.

We used an exploratory factor analysis (EFA) with oblique rotation to evaluate the convergent and divergent validity of the four scales. The EFA resulted in six factors: three factors corresponded correctly to the single-construct IGPI, PRB, and PIC, and three factors were extracted from the IPC scale. The IPC *Collection* (IPCC) and *Errors* (IPCE) subscales loaded separate factors, while the other two IPC subscales (about *Unauthorized Secondary Use* and *Improper Access*) loaded a single factor (IPCU). The split of the IPC scale was not unexpected, as the scale was designed to include four subscales. One PRB item was removed from the analysis (Appendix A.2) as it had a low loading and low correlations with all factors. The average loadings for the IGPI, PRB, PIC, IPCC, and IPCU factors were higher than $\lambda = .74$, indicating high within-factor correlations and providing strong support for the convergent validity of the scales (Carlson and Herdman 2012). The average loading for the IPCE factor was at $\lambda = .68$, indicating acceptable convergent validity for this subscale (Carlson and Herdman 2012). The

Table 3. Participants' demographics: initial full sample and modified sample used in the analysis.

		Full		Modified	
Demographic	Level	*n*	%	*n*	%
Gender	Female	369	60.0	285	61.7
	Male	242	39.4	173	37.4
	Other	4	0.6	3	0.7
	Preferred not to say	1	0.1	1	0.2
Age cohort	18–24	67	10.9	38	8.2
	25–34	145	23.6	86	18.6
	35–44	157	25.5	121	26.2
	45–54	90	14.6	75	16.2
	55–64	76	12.3	67	14.5
	65 or older	79	12.8	74	16.0
	Preferred not to say	2	0.3	1	0.2
Highest completed level of education	No formal schooling / education	2	0.3	1	0.2
	Some high school, no diploma	17	2.8	14	3.0
	High school diploma or an equivalent	126	20.4	91	19.7
	Some college credit, no degree	133	21.6	94	20.4
	Trade, technical, vocational training	71	11.5	55	11.9
	Associate's degree or an equivalent	6	1.0	6	1.3
	Bachelor's degree or an equivalent	149	24.2	107	23.2
	Master's degree or an equivalent	86	14.0	72	15.6
	Doctorate degree or an equivalent	24	3.9	21	4.5
	Other	0	0.0	0	0.0
	Preferred not to say	2	0.3	1	0.2
Total		616		462	

variance extracted (AVE) between the pairs of the factors was higher than the squared correlations between the pairs of the factors (shared variance), providing support for the divergent validity of the scales (Franke and Sarstedt 2019; Voorhees et al. 2016). We controlled method variance by ensuring that all possible procedural remedies were implemented in the study design (separation of measurement: temporal, psychological, and methodological; emphasised participants' anonymity and reduced evaluation apprehension; used validated psychometric scales (Podsakoff et al. 2003) and found no evidence of bias due to the common method variance in the measures (all the items accounted for 21.81% of explained variance in the Harman's single factor test (Kock, Berbekova, and Assaf 2021).

Intention to Give Personal Information (IGPI). A principal component analysis (PCA) for the IGPI resulted in one factor, as expected, accounting for 72.26% of explained variance with the Kaiser-Meyer-Olkin measure (KMO) at .75 and the Bartlett's Test of Sphericity significant at $p<.001$. The measurement reliability was good, based on the McDonald's[6] $\omega = .87$.

Privacy Risk Beliefs (PRB). All five PRB items loaded into a single factor, explaining 66.01% of the variance, based on PCA ($KMO = .86$, Bartlett's test at $p<.001$). Despite the good reliability (McDonald's $\omega = .88$), we removed one item from the final score calculation (Appendix A.2), as its deletion increased the reliability to the McDonald's $\omega = .90$, and it was previously excluded from the validity evaluation.

Perceived Information Control (PIC). PIC loaded into one factor based on PCA, as anticipated, accounting for 79.84% variance explained with $KMO = .85$ and Bartlett's Test of Sphericity at $p<.001$. Reliability of the measurements deemed excellent – McDonald's $\omega = .92$, and deletion of any item would result in a reduction of the ω level.

Individual's Privacy Concerns (IPC). The IPC scale loaded three factors instead of the four suggested in the original instrument. The three factors accounted for 66.37% of variance explained with $KMO = .91$ and Bartlett's Test of Sphericity at $p<.001$. Our analysis identified two original privacy concerns subscales: about *collection* (IPCC) and *errors* (IPCE). Another two original subscales (about *unauthorized secondary use* and *improper access*) loaded into a single factor (IPCU). IPCC and IPCE reliabilities were at McDonald's $\omega = .83$ and $\omega = .80$, respectively. The IPCU boasted excellent reliability at McDonald's $\omega = .91$. Hence, we retain the three subscales (IPCC, IPCE, and IPCU) for further analyses.

4.1.2. Descriptive analysis

Inspection of the Pearson correlations between the different variables (Table 4) revealed medium to strong associations between the final score threshold (FST) and the preferred score for a counterpart (PSC), indicating that the impression communicated to others and the impression desired from others are correlated. The small to medium positive correlation between the FST and the attitude to impression formation (AIF) based

on scores is not unreasonable either. Interestingly, the FST was only weakly positively correlated with the IGPI and was not related to the PRB. The PIC appeared to be weakly increasing with the increase in the FST, and moderately increasing with the increase in the AIF.

4.2. Conceal or reveal: choices of the final score threshold

In the online experiment, we manipulated three variables with discrete levels and measured several individual characteristics. To investigate their joint effects on the choice of the FST and address RQ1, RQ2, RQ3, and RQ4 in combination, we performed a factorial analysis of covariance (ANCOVA). The univariate factorial 3-way ANCOVA was built, testing the effects of *Context* (RQ1), *Timing-Control* (RQ2 and RQ3), and *Content* (RQ4) on the FST the participant chose to share [7]. The analysis of the FST included the score threshold chosen by the subjects in the *Before* condition, as well as the score threshold after possible adjustment in the *After* and *After+Slider* conditions of the *Timing-Control* variable. The model also included the PSC, AIF, IGPI, PIC, and IPCE as covariates. As the PRB, IPCC, and IPCU did not correlate with the FST, we excluded these variables from the final model[8]. We inspected the data for the ANCOVA-relevant assumptions. Linearity, homogeneity of variances (Levene's test, $F(14, 444) = .61$, $p < .89$), homoscedasticity, normality, and multicollinearity were all met. Table A1 in Appendix 3 presents the overall results of the ANCOVA model.

4.2.1. Context and (non)disclosure

Overall, we found a small-to-medium main effect of the *Context* of the interaction (RQ1), $F(1, 439) = 6.85$, $p<.01$, $\eta_p^2 = .02$ on the FST. The analysis also revealed significant adjustors of the FST: the PSC, $F(1, 439) = 162.61$, $p < 0.001$, $\eta_p^2 = .27$; IGPI, $F(1, 439) = 5.33$, $p<.05$, $\eta_p^2 = .01$; and AIF, $F(1, 439) = 25.94$, $p<.001$, $\eta_p^2 = .06$. Examination of the means showed that the participants in the more egalitarian peer-to-peer context of *Traveling* were comfortable revealing their average review score starting at a lower FST level, $M = 6.77$, 95% CI[6.54, 6.99], than the participants in the more hierarchical context of *Employment*, $M = 7.21$, 95% CI[6.97, 7.45].

4.2.2. Timing-Control, content, and (non)disclosure

There were no significant effects of *Timing-Control* (RQ2, RQ3) and *Content* (RQ4) on the users' choice of FST, indicating that these two factors did not independently affect the decisions to reveal or conceal personal information. However, an interaction between *Timing-Control* and *Content*, $F(4, 439) = 2.09$, $p = .08$, $\eta_p^2 = .02$, may be noteworthy for future research, as we anticipated detecting such an interaction (Section 2), yet it did not meet the statistical requirements to be confirmed (as per the a priori power analysis).

4.2.3. Influence of covariates on the final score threshold

Three out of five covariates were significantly related to the FST in the main ANCOVA model. To investigate the effects of these factors (reflecting some of the user attitudes) in combination, we performed a simultaneous multiple regression analysis on all five covariates. The data were checked for regression assumptions. The resulting model (Table 5) was significant, $F(5, 456) = 55.00$, $p < .001$, adjusted $R^2 = .37$. The PSC was the strongest predictor of the FST choice, which means that when the minimum acceptable score for a travel partner or an employee (PSC) increased, the participants' own minimal threshold for their score disclosure (FST) also increased. The more positive the participants felt about being judged, based on some average rating they publish online (AIF), the higher their chosen FST, as well. Additionally, an increase in the behavioural intention to disclose information (IGPI) led to a small increase in the minimal acceptable FST. Corroborating the main ANCOVA model, PIC and IPCE had no significant effect on the FST choice.

4.3. Score threshold adjustment behaviour

To investigate RQ3a and RQ4a, we examined how people behaved regarding the adjustment of the score threshold. We excluded participants in the *Before* condition because they could not change their choice of the score threshold during the experiment, unlike the participants in the *After* and *After+Slider* conditions. Therefore, here we analyse the sample of $N = 302$ participants. In the sample, not enough participants adjusted the initial score threshold they chose; hence we did not have a sufficient sample size for a general linear model analysis. Thus, we proceed with a non-parametric analysis, using χ^2 test of independence, which allows testing the relation between pairs of categorical variables, such as our manipulated (*Timing-Control* and *Content*) and dependent (*Score threshold adjustment behaviour*) variables.

4.3.1. Timing-Control

Overall, in the reduced sample, 32 and 35 participants used the opportunity to adjust the FST in the *After*

Table 4. Pearson correlations: Final score threshold (FST), Preferred score for a counterpart (PSC), Attitude to impression formation (AIF), experience with similar services (ESS, calculated as a count of familiarity with similar applications), and the constructs measured with existing scales: Intention to give personal information (IGPI), Privacy risk beliefs (PRB), Perceived information control (PIC), and Individual's privacy concerns for Collection (IPCC), Errors (IPCE), and Unauthorized Secondary Use & Improper Access (IPCU).

	PSC	AIF	ESS	IGPI	PRB	PIC	IPCC	IPCE	IPCU
FST	.56***	.37***	.23***	.21***	.05	.20***	−.04	.17***	.08
PSC	1	.27***	.15***	.10*	.11*	.21***	.06	.23***	.09
AIF		1	.28***	.35***	−.05	.45***	−.16***	.18***	.00
ESS			1	.11*	−.04	.23***	−.12**	.13**	.04
IGPI				1	−.28***	.36***	−.15**	.21***	.20***
PRB					1	−.13***	.54***	.07	−.01
PIC						1	−.16***	.29***	.10*
IPCC							1	.22***	.30***
IPCE								1	.69***
IPCU									1

***$p < .001$, **$p < .01$ and *$p < .05$. $N = 462$.

and *After+Slider* conditions, respectively. Six participants in the *After* condition returned to adjust the initial score threshold but decided to submit the FST without change. In comparison, 30 participants in the *After+Slider* condition interacted with the slider window but did not change the initial score threshold in the end. The rest (i.e. 113 and 86, respectively) showed no intention to reconsider their initial choice of threshold.

We used a χ^2 test of independence to analyse whether the participants' choice was represented across the two *Timing-Control* conditions proportionally to their number in the sample (RQ3a). The results showed that there was a significant difference, $\chi^2 = 19.80$, $df = 2$, $p < .001$, $\phi_c = .26$, in the way people behaved across the two *Timing-Control* conditions. The tendency to reconsider prior choices was somewhat higher in the *After+Slider* condition, where the participants were able to take control actions directly in the indication, compared with the *After* condition, which required one additional button click.

4.3.2. Content

The distribution of participants in the three *Content* conditions across the *Score threshold adjustment behaviour* categories is shown in Table 6. A χ^2 test looking for the differences in the participants' behaviour (RQ4a) was significant, $\chi^2 = 54.58$, $df = 4$, $p < .001$, $\phi_c = .30$, indicating that the intention to reconsider prior choices was the highest in the *Social norm* condition and lowest in the *Neutral* condition. Moreover, we repeated the analysis, only looking at two behaviours: whether the participants changed (behaviour category (1), Section 3.1) or did not change the score thresholds (behaviour categories (2) and (3) together, Section 3.1) across the *Content* conditions. The χ^2 test showed a significant difference, $\chi^2 = 30.10$, $df = 2$, $p<.001$, $\phi_c = .32$, in how the participants' actions were represented across the three conditions. Crucially, these results confirmed that the choices to adjust prior settings were most frequent among the subjects exposed to the *Social norm* message, compared to the subjects exposed to the *Self-presentation* (more than twice as frequent) and *Neutral* messages (more than four times as frequent).

Table 5. Joint influence of the Preferred scored for a counterpart (PSC), Attitude to impression formation (AIF), Intention to give personal information (IGPI), Perceived information control (PIC), and Individual's privacy concerns about errors (IPCE) on the choice of the Final score threshold.

Predictor	β	$t(456)$	p	r_p
PSC	.50	12.81	<.001	.51
AIF	.22	5.10	<.001	.23
IGPI	.10	2.48	<.05	.12
PIC	−.05	−1.14	.25	-.05
IPCE	.00	0.11	.91	.01

5. Discussion

In this paper, we aimed to advance our understanding of people's decisions to conceal or reveal potentially unfavourable personal information as a part of the impression management process and how privacy-related feedback may affect this behaviour. The experiment results indicated the importance of contextual cues and prior experiences and beliefs for user decision-making regarding the disclosure or nondisclosure of reputational information on online sharing economy platforms. Our analysis revealed that the *Context* did indeed affect the *Final score threshold* (FST, RQ1): users preferred to share their average rating score with the potential employer from a significantly higher cutoff point, compared with potential peers in the *Traveling* scenario. Even though we observed a null effect of feedback timing and availability of controls on (non)disclosure of personal information (RQ2 and RQ3), the results showed that the *Timing-Control* factor effectively altered participants' score threshold adjustment behaviour (i.e. affected the preference for a status

Table 6. The distribution of participants across the Content variable conditions and the Score threshold adjustment behaviour categories.

	Score threshold adjustment behaviour			
	Did not change the score			
Content condition	No interest to change	Showed interest to change	Changed the score	Total
Neutral message	86	5	9	100
Self-presentation message	77	10	19	106
Social norm message	36	21	39	96
Total	199	36	67	302

quo, RQ3a). Specifically, the mere exposure to available controls (*After+Slider* condition) caused significantly more people to either change their initial threshold choice or to at least consider altering their initial threshold choice, compared with the condition requiring additional effort to reach the point where the score threshold could be adjusted (*After* condition).

Moreover, despite a null effect of message content on (non)disclosure of personal information (RQ4), *Feedback content* significantly affected the preference for a status quo (RQ4a), as well: the propensity to reconsider the status quo – i.e. prior choices – was strongest when the feedback communicated the *Social norm*, compared with feedback that contained the *Self-presentation* and *Neutral* messages. Finally, the correlations between the FST and stable privacy attitudes (PRB, IGPI, and PIC) hinted that online nondisclosure might be connected to risk compensation behaviour, similar to the observations regarding disclosure in prior literature (Aïmeur, Lawani, and Dalkir 2016; Brandimarte, Acquisti, and Loewenstein 2013; Krol and Preibusch 2016). We discuss the implications, considering the results of our experiment.

5.1. Context and priors are major cues for (non)disclosure decisions

The context of the interaction affected user considerations and resulted in different choices as to concealing and revealing reputational information, depending on people's familiarity with, and understanding of the context (RQ1). This finding provides experiment-based empirical evidence to the otherwise theoretically and qualitatively postulated argument that users' privacy-related decision-making may rely on norms inferred from contextual information (in line with Nissenbaum 2004). It extends and substantiates that the effect of context on 'privacy expectations' (Martin and Nissenbaum 2016) can translate into choices to conceal or reveal information. This finding also extends the significance of context for self-presentation through (non)disclosure (Emanuel et al. 2014) to externally assigned personal information (ratings), to online contexts facilitating the sharing economy, and across broader demographics. Finally, this finding empirically supports the argument that users may need (and should be able to) use multiple different 'personas' to fulfill their self-presentation intentions, despite some service providers' interest to 'push for users' 'uniform' online identity' (van Dijck 2013).

Our results suggest that the *Employment* scenario prompted people to adopt a more economically motivated, benefit-seeking behaviour, resulting in a preference for higher minimal average scores to be displayed to potential employers as benefactors. This indicates that the 'external evaluation' concerns regarding self-presentation and (non)disclosure might be more pressing in the socioeconomic (*Employment*) context, compared with the purely social context (*Traveling*). Such a finding may be attributed to routinised decision-making (Betsch, Haberstroh, and Hohle 2002), or unconscious influences and primes-to-behaviour (Newell and Shanks 2014). In a new decision scenario, users may be, consciously or not, matching the contextual cues with their most relevant experiences.

The minimal average score participants required for their counterparts to be considered acceptable (PSC) was most strongly correlated with the FST, followed by their attitude to impression formation, based on average rating scores published online (AIF). The results indicate that the more users expect from others, the higher their own minimum score must be, while the more positively they feel about being judged based on some score, the higher their minimum score must be. Overall, the correlations between the IGPI and FST on the one hand, and the PRB, PIC, and individual's privacy concerns on the other hand, appeared to be in line with the APCO model (Dinev, McConnell, and Smith 2015), which considers these perceptions and attitudes as possible predictors of the 'behavioural reactions', such as personal information disclosure (APCO does not always differentiate between intention and behaviour). Further, the correlations between IGPI, PRB, and PIC (Table 4) are also in line with a view on online personal information disclosure, connecting it to risk compensation behaviour (Aïmeur, Lawani, and Dalkir 2016; Brandimarte, Acquisti, and Loewenstein 2013; Krol and Preibusch

2016). Thus, when engaging in a new online interaction, users seem to rely on a somewhat predefined idea of how to present themselves to peers and 'superiors', based on the context and priors rather than proactively considering how to manage the impression others have of them, which may be potential evidence for thinking with heuristics. In other words, people may be entering online interactions (a) with preferences already set prior to joining and (b) being influenced by their perceptions of the *Context*. These preferences may have been defined by the expectations about the potential audience, dynamics, and outcomes of the interaction, preexisting mental models, and experiences, or may be based on the apparent similarities of this new interaction with previously experienced ones.

5.2. Nondisclosure outcomes may be misleading

We offered users control over their personal image in the eyes of their counterparts in two distinct scenarios. There appears to be reciprocity between self-presentation and preferences for the counterpart's image (Section 4.1.2 and Table 5). However, users may fail to realise that by not revealing certain information (setting the minimal sharing score threshold too high) they may allow others to presumptively derive this information ('if the average score is not shown, it must be low'). By providing feedback in different configurations (RQ2, RQ3, RQ4), we intended to raise participants' awareness of how nondisclosure might influence their online impression by being suggestive of some other information through concealing (withholding) the 'actual' information. However, this feedback seemed not to systematically affect people's disclosure preferences regarding reputational information. In other words, the cases when not sharing may signal wrong and self-defeating messages may be overlooked.

Motivated by our findings, human-computer interaction (HCI) and social computing researchers could further investigate ways to raise user awareness and comprehension of various online social scenarios in which people can commit to non-optimal self-presentation choices. More research is needed to understand the limiting factors leading people to such behaviours. Meanwhile, system designers should be careful in how they present their apps and platforms and describe their functionality to users.

5.3. Indications facilitating control help users fulfill their preferences

In our study, we used onscreen indications to inform users, aiming to assist their decision-making, while the indications themselves offered different availability of control. The main findings regarding whether the feedback content and availability of control affect the preference for a status quo (Section 4.3, RQ3a, RQ4a) suggest that onscreen indications (notices, notifications) can serve people's considerations and inform privacy-related decisions, influencing user preference for a status quo (i.e. prior user set choices, in our study). The availability of controls (*Timing-Control*, RQ3a), supplementing the self-presentation and social norm cues (RQ4a), allowed some to adjust their initial (non)disclosure choices. Giving participants feedback and control enabled them to reflect on the decision: even when they did not change the score, they noticed the indication and the controllability option and interacted with the latter. This indicates that the useably positioned controls, message framing, and communication of the social norms may help users meet their preferences regarding (non)disclosure of reputational information, supporting and informing user decision-making. This finding extends the existing literature on the role of heuristics and biases in privacy decision-making, adding further experimental evidence to research on usable privacy communications (Acquisti et al. 2017; Kitkowska et al. 2020; Schaub et al. 2015). Actionability (and relevance) of information within notices are crucial in influencing user preference for a status quo. This may raise or lower users' control of their image and privacy, enhancing or deteriorating them, depending on how the indications are designed.

System designers should seek to provide indications that are context-specific and actionable. Actionability implies affording users with the easiest and most effortless way to productively respond to indications 'at the moment'. That 'moment' translates to relevance and characterises context specificity, as well.

Researchers from multiple fields should be interested in studying the interplay between user experiences, beliefs, and other priors on the one hand, and new information acquisition on the other. Additionally, investigating the relative impact of different cognitive biases and effects may shed light on how to design online systems to ensure that user actions best match the user's actual interests and preferences.

5.4. Self-Presentation and (non)disclosure need to be informed

In the experiment, we informed users about the potential outcomes of their choices (implications for their online impressions) and expected behaviour (social norms) (RQ4), both relevant in the social and socioeconomic sharing economy contexts (RQ1).

(Non)disclosure was central: users were deciding upon revealing or concealing the information generated outside of their control (an average score, based on a collection of reviews). Having seen external information, most participants followed through with their interpretation of the potential implications of their actions vis-á-vis sharing their scores in both contexts. Overall, our findings substantiate the notion that people disclosing personal information (such as scores) in the online sharing economy may indeed not be fully attentive to the implications of their disclosures or may overlook advice, resulting in disclosures based on prior beliefs (RQ2, RQ3, RQ4). Alternatively, the seeming inattentiveness exhibited by many participants (given the potential influence of priors) may be evidence for the relative strength of people's psychological biases. Specifically, in online interactions, the status quo bias may be affecting user decision-making and behaviour more profoundly than the availability of control and the effects of framing and social norms.

However, information and controls provided to the users helped some adjust their (non)disclosure choices (RQ3a, RQ4a). Thus, user attentiveness can be improved by communicating social norms in conjunction with an appropriate message framing. Users' personal choices and preferences can be facilitated by readily available 'in-context' controls. Social norms appeared to be most prominent to users (compared with the neutral and framed messages), extending the findings by Spottswood and Hancock (2017) regarding the effects of explicit social norms to contexts where disclosure of potentially unfavourable information is motivated by self-presentation.

These implications are important not only for system designers but for regulators, policymakers, and legal practitioners, indicating a way to support and enhance privacy behaviour while highlighting a major malicious potential regarding the effects of framed and socially persuading communications. For instance, inconsiderate or callous online service providers might be able to abuse such communications by convincing the users to commit to potentially unintended or detrimental choices. The outcomes of such choices would be desirable for the service providers' stakeholders rather than the users (i.e. dark patterns in user interface design – Mathur et al. 2019). This is especially relevant for the online sharing economy where a shifted balance of power between users and the platform may cause regulatory challenges, while reliance on reputation systems (e.g. ratings) may amplify biases based on social, racial, or personal prejudice, leaving users vulnerable to discrimination (Cheng and Foley 2018; Katz 2015; Rahman 2021). System designers and privacy practitioners should be aware that providing information to users should be part of a solution. The legalistic reliance on the idea that 'informedness' is obtained sufficiently from privacy notices and consent should be revisited in theoretical and practical endeavours to aid user privacy management.

5.5. Limitations and future work

We note several limitations of the study. First, the online experiment's ecological validity (i.e. mundane realism) may be limited because of the use of vignettes. However, we argue that the simplicity of the design and the low effort and short time required to complete the task correspond to how similar online interactions occur in reality. Additionally, non-strict attention checks and feedback received from the participants provided a degree of confidence in the reliability of the results. Second, the sampling procedures might have limited the experiment's external validity. We were unable to extend our investigation to non-English speakers and nonresidents of the USA. Additionally, we studied particular instances of score sharing, which might not generalise to dissimilar instances of online information sharing. However, the obtained sample structure, the observed reliability of the measurements, and the critical test values may have value for understanding the processes underlying privacy-related behaviours at large and warrant future research.

Future research may focus on developing theoretical models of nondisclosure, partially based on the empirical findings reported in this paper. Future research may also deal with broadening the scope to new contexts and additional properties of notices and indications. The absence of the pure timing effect (*Before* vs. *After*) on (non)disclosure decisions contrasts with prior literature, where other timing-related factors affected purchasing preferences (Egelman et al. 2009), comprehension of privacy notices (Balebako et al. 2015), or mismatch between stated and revealed location-sharing preference (Patil et al. 2015). Thus, other types of timing or timing-related factors, as well as visual design, interactivity, and actionability of information delivery (indications, alerts, etc.) can be studied further in different settings both in relation to (non)disclosure or previously studied privacy attitudes and behaviours. Moreover, the interaction of factors, such as timing and content of indications, could be further studied (e.g. longitudinally). Our conjecture that priors (such as past experiences) may be a paramount factor in decision-making regarding (non)-disclosure of reputational information will need to be tested in future research, as well, alongside other unobserved factors. How and whether the different elements constituting context may drive the (non)disclosure decisions is another avenue for future research.

All participants received a financial incentive for the completion of the study, rather than different incentives for the employment- and recreation-related contexts. Such a design allowed us to compare the contexts without confounding factors. This helps us to better understand the generalizability of the results but limits us in drawing context-specific conclusions. Therefore, to learn more about particular contextual effects, future research may need to include context-related incentives or some form of a performance-based incentive (especially in a longitudinal design). Considering extended methodologies, future studies can utilise additional dependent variables: for instance, quantitative measures can be made more context-specific and performance-related (e.g. real accumulation of scores over time), whereas behavioural measures can track changes with more precision or sensitivity (e.g. recording time spent on decisions, threshold dynamics over time, eye-tracking in the lab for specific user interface design factors).

Additionally, future research may investigate the relative strength of psychological biases underlying decision-making. Finally, another research direction may study the extent to which the self-presentation and online (non)disclosure decisions are based on the information learned within the interaction, compared with reliance on the information learned from experiences.

6. Conclusion

This paper presents an online experiment aimed to improve our understanding of (non)disclosure – concealing or revealing potentially unfavourable information – as a part of users' impression management processes in online platforms facilitating social and socioeconomic interactions. The results extend the knowledge on aiding user decision-making with information regarding the potential outcomes of their actions. We found that context can be one of the most dominant sources of information for people engaging in new interactions. Simultaneously, the information presented in the form of indications (i.e. pop-up notices) can trigger considerations regarding already made choices yet may not necessarily lead to modifications of these choices in a predictable way. Overall, our findings challenge the ubiquitous reliance on the notion of the user 'informedness' obtained solely from privacy notices or consent forms. The results have important implications, highlighting that, for some, it might be imperceptible that concealing certain information may reveal or signal unwanted information to an observer (information receiver). For others, affording controls and providing information can indeed help them adjust their (non)disclosure choices.

Notes

1. In privacy research, the framing effect studies contain colour- and content-rich visual cues, which could prime the participants' risk perception outside of the semantic frame (Gerend and Sias 2009), and obscure the effect of framing itself.
2. A CAPTCHA ('completely automated public Turing test to tell computers and humans apart') version by Google LLC.
3. The PIC scale was originally derived from Xu (2007) without validation.
4. CloudResearch policy states, 'Upon completion of the study, you will receive compensation in the amount that you have agreed to with the platform through which you entered this survey.'
5. The strict criterion was applied due to the time the participants spent on scenario familiarisation not being normally distributed.
6. Dunn, Baguley, and Brunsden (2014)
7. As we used a balanced full factorial design, the order of factors entered into the model would not affect the overall results, unlike with unbalanced factorial analyses, (e.g. Landsheer 2015).
8. The inclusion of the participants' experience with similar services (ESS) did not have a significant effect in the ANCOVA model for the final score threshold (FST). Therefore, it was excluded from the final model, as well.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This research was supported by the EU Horizon 2020 research and innovation programme under the H2020 Marie Skłodowska-Curie Actions grant agreement No 675730 'Privacy and Us'.

ORCID

Yefim Shulman http://orcid.org/0000-0002-3163-9726
Agnieszka Kitkowska http://orcid.org/0000-0001-7384-4552
Mark Warner http://orcid.org/0000-0002-7494-6275
Joachim Meyer http://orcid.org/0000-0002-1801-9987

References

Acquisti, A., I. Adjerid, R. Balebako, L. Brandimarte, L. F. Cranor, S. Komanduri, and S. Wilson. August, 2017. "Nudges for Privacy and Security: Understanding and Assisting Users' Choices Online." *ACM Computing Surveys* 50 (3). https://doi.org/10.1145/3054926.

Acquisti, A., L. Brandimarte, and G. Loewenstein. 2015. "Privacy and Human Behavior in the Age of Information." *Science* 347 (6221): 509–514. https://doi.org/10.1126/science.aaa1465.

Adams, D. A., R. R. Nelson, and P. A. Todd. 1992. "Perceived Usefulness, Ease of Use, and Usage of Information Technology: A Replication." *MIS Quarterly* 16 (2): 227–247. https://doi.org/10.2307/249577.

Adjerid, I., A. Acquisti, and G. Loewenstein. 2019. "Choice Architecture, Framing, and Cascaded Privacy Choices." *Management Science* 65 (5): 2267–2290. https://doi.org/10.1287/mnsc.2018.3028.

Aïmeur, E., O. Lawani, and K. Dalkir. 2016. "When Changing the Look of Privacy Policies Affects User Trust: An Experimental Study." *Computers in Human Behavior* 58:368–379. https://doi.org/10.1016/j.chb.2015.11.014.

Ajzen, I., and M. Fishbein. 1977. Attitude-behavior Relations: A Theoretical Analysis and Review of Empirical Research (Vol. 84) (No. 5). *Psychological Bulletin* 84:888–918. https://doi.org/10.1037/0033-2909.84.5.888.

Altman, I. 1977. "Privacy Regulation: Culturally Universal Or Culturally Specific?." *Journal of Social Issues* 33 (3): 66–84. https://doi.org/10.1111/j.1540-4560.1977.tb01883.x.

Balebako, R., F. Schaub, I. Adjerid, A. Acquisti, and L. Cranor. 2015. "The Impact of Timing on the Salience of Smartphone App Privacy Notices." In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, 63–74. New York, NY, USA: Association for Computing Machinery.https://doi.org/10.1145/2808117.2808119.

Bederson, B. B., G. Z. Jin, P. Leslie, A. J. Quinn, and B. Zou. February, 2018. "Incomplete Disclosure: Evidence of Signaling and Countersignaling." *American Economic Journal: Microeconomics* 10 (1): 41–66. https://doi.org/10.1257/mic.20150178.

Bellotti, V., and A. Sellen. 1993. "Design for Privacy in Ubiquitous Computing Environments." In *Proceedings of the Third European Conference on Computer-Supported Cooperative Work 13–17 September 1993, Milan, Italy ECSCW '93*, edited by G. de Michelis, C. Simone, and K. Schmidt. Dordrecht: Springer. https://doi.org/10.1007/978-94-011-2094-4_6.

Benndorf, V., D. Kübler, and H. T. Normann. 2015. "Privacy Concerns, Voluntary Disclosure of Information, and Unraveling: An Experiment." *European Economic Review* 75:43–59. https://doi.org/10.1016/j.euroecorev.2015.01.005.

Berendt, B. 2012. "More Than Modelling and Hiding: Towards a Comprehensive View of Web Mining and Privacy." *Data Mining and Knowledge Discovery* 24 (3): 697–737. https://doi.org/10.1007/s10618-012-0254-1.

Betsch, T., S. Haberstroh, and C. Hohle. 2002. "Explaining Routinized Decision Making: A Review of Theories and Models." *Theory & Psychology* 12 (4): 453–488. https://doi.org/10.1177/0959354302012004294.

Brandimarte, L., A. Acquisti, and G. Loewenstein. 2013. "Misplaced Confidences: Privacy and the Control Paradox." *Social Psychological and Personality Science* 4 (3): 340–347. https://doi.org/10.1177/1948550612455931.

Butler, D., and D. Read. 2021. "Unravelling Theory: Strategic (Non-) Disclosure of Online Ratings." *Games* 12 (4): 73. https://doi.org/10.3390/g12040073.

Carlson, K. D., and A. O. Herdman. 2012. "Understanding the Impact of Convergent Validity on Research Results." *Organizational Research Methods* 15 (1): 17–32. https://doi.org/10.1177/1094428110392383.

Cheng, M., and C. Foley. 2018. "The Sharing Economy and Digital Discrimination: The Case of Airbnb." *International Journal of Hospitality Management* 70:95–98. https://doi.org/10.1016/j.ijhm.2017.11.002.

Choe, E. K., J. Jung, B. Lee, and K. Fisher. 2013. "Nudging People Away from Privacy-Invasive Mobile Apps through Visual Framing." In *Human-Computer Interaction – Interact 2013*, edited by P. Kotzé, G. Marsden, G. Lindgaard, J. Wesson and M. Winckler, 74–91. Berlin. Heidelberg: Springer Berlin Heidelberg.

Connelly, B. L., S. T. Certo, R. D. Ireland, and C. R. Reutzel. 2011. "Signaling Theory: A Review and Assessment." *Journal of Management* 37 (1): 39–67. https://doi.org/10.1177/0149206310388419.

Culnan, M. J., and R. J. Bies. 2003. "Consumer Privacy: Balancing Economic and Justice Considerations." *Journal of Social Issues* 59 (2): 323–342. https://doi.org/10.1111/1540-4560.00067.

Dienlin, T., and S. Trepte. 2015. "Is the Privacy Paradox a Relic of the Past? An in-depth Analysis of Privacy Attitudes and Privacy Behaviors." *European Journal of Social Psychology* 45 (3): 285–297. https://doi.org/10.1002/ejsp.2049.

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. https://doi.org/10.1287/isre.2015.0600.

Dinev, T., H. Xu, J. H. Smith, and P. Hart. 2013. "Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-related Concepts." *European Journal of Information Systems* 22 (3): 295–316. https://doi.org/10.1057/ejis.2012.23.

Dinner, I., E. J. Johnson, D. G. Goldstein, and K. Liu. 2011. "Partitioning Default Effects: Why People Choose Not to Choose." *Journal of Experimental Psychology: Applied* 17 (4): 332–341. https://doi.org/10.1037/a0024354.

Dunn, T. J., T. Baguley, and V. Brunsden. 2014. "From Alpha to Omega: A Practical Solution to the Pervasive Problem of Internal Consistency Estimation." *British Journal of Psychology* 105 (3): 399–412. https://doi.org/10.1111/bjop.12046.

Egelman, S., J. Tsai, L. F. Cranor, and A. Acquisti. 2009. "Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 319–328. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1518701.1518752.

Emanuel, L., G. J. Neil, C. Bevan, D. S. Fraser, S. V. Stevenage, M. T. Whitty, and S. Jamison-Powell. 2014. "Who Am I? Representing the Self Offline and in Different Online Contexts." *Computers in Human Behavior* 41:146–152. https://doi.org/10.1016/j.chb.2014.09.018.

Faul, F., E. Erdfelder, A. G. Lang, and A. Buchner. May 01, 2007. "G*Power 3: A Flexible Statistical Power Analysis Program for the Social, Behavioral, and Biomedical

Sciences G*power 3: A Flexible Statistical Power Analysis Program for the Social, Behavioral, and Biomedical Sciences." *Behavior Research Methods* 39 (2): 175–191. https://doi.org/10.3758/BF03193146.

Fazio, R. H., and D. R. Roskos-Ewoldsen. 2005. "Acting as We Feel: When and How Attitudes Guide Behavior." In *Persuasion: Psychological Insights and Perspectives*, 41–62. 2nd ed. Thousand Oaks, CA, US: Sage Publications, Inc.

Feaster, J. C. October, 2010. "Expanding the Impression Management Model of Communication Channels: An Information Control Scale." *Journal of Computer-Mediated Communication* 16 (1): 115–138. https://doi.org/10.1111/j.1083-6101.2010.01535.x.

"feedback", n. 2021. "Merriam-webster.com dictionary." Merriam-Webster. https://www.merriam-webster.com/dictionary/feedback.

Franke, G., and M. Sarstedt. January 01, 2019. "Heuristics Versus Statistics in Discriminant Validity Testing: a Comparison of Four Procedures." *Internet Research* 29 (3): 430–447. https://doi.org/10.1108/IntR-12-2017-0515.

Gerber, N., P. Gerber, and M. Volkamer. August, 2018. "Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior." *Computers & Security* 77:226–261. https://doi.org/10.1016/J.COSE.2018.04.002.

Gerend, M. A., and T. Sias. 2009. "Message Framing and Color Priming: How Subtle Threat Cues Affect Persuasion." *Journal of Experimental Social Psychology* 45 (4): 999–1002. https://doi.org/10.1016/j.jesp.2009.04.002.

Goffman, E. 1959. *The Presentation of Self in Everyday Life*. Garden City, New York: Anchor Publishing.

Gürses, S. March, 2016. "Privacy Engineering: Shaping An Emerging Field of Research and Practice." *IEEE Security Privacy* 14 (2): 40–46. https://doi.org/10.1109/MSP.2016.37.

Habib, H., S. Pearman, J. Wang, Y. Zou, A. Acquisti, L. F. Cranor, and F. Schaub. 2020. " 'It's a Scavenger Hunt': Usability of Websites' Opt-Out and Data Deletion Choices." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–12. New York, NY, USA: Association for Computing Machinery.https://doi.org/10.1145/3313831.3376511.

Habib, H., Y. Zou, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, and F. Schaub. August, 2019. "An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites." In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*. Santa Clara, CA: USENIX Association.

Hansen, M., M. Jensen, and M. Rost. 2015. "Protection Goals for Privacy Engineering." In *2015 IEEE Security and Privacy Workshops, San Jose, CA, USA*, 159–166. IEEE. https://doi.org/10.1109/SPW.2015.13.

Hoyle, R., S. Das, A. Kapadia, A. J. Lee, and K. Vaniea. 2017. "Viewing the Viewers: Publishers' Desires and Viewers' Privacy Concerns in Social Networks." In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, 555–566. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2998181.2998288.

Hummel, D., and A. Maedche. 2019. "How Effective is Nudging? A Quantitative Review on the Effect Sizes and Limits of Empirical Nudging Studies." *Journal of Behavioral and Experimental Economics*80:47–58. https://doi.org/10.1016/j.socec.2019.03.005.

Johnson, E. J., S. Bellman, and G. L. Lohse. 2002. "Defaults, Framing and Privacy: Why Opting In-Opting Out." *Marketing Letters* 13 (1): 5–15. https://doi.org/10.1023/A:1015044207315.

Joinson, A. N. 2001. "Self-disclosure in Computer-mediated Communication: The Role of Self-awareness and Visual Anonymity." *European Journal of Social Psychology* 31 (2): 177–192. https://doi.org/10.1002/ejsp.36.

Joinson, A. N., U. D. Reips, T. Buchanan, and C. B. P. Schofield. February, 2010. "Privacy, Trust, and Self-Disclosure Online." *Human–Computer Interaction* 25 (1): 1–24. https://doi.org/10.1080/07370020903586662.

Kahneman, D., J. L. Knetsch, and R. H. Thaler. March, 1991. "Anomalies: The Endowment Effect, Loss Aversion, and Status Quo Bias." *Journal of Economic Perspectives* 5 (1): 193–206. https://doi.org/10.1257/jep.5.1.193.

Karahanna, E., and D. W. Straub. 1999. "The Psychological Origins of Perceived Usefulness and Ease-of-use." *Information & Management* 35 (4): 237–250. https://doi.org/10.1016/S0378-7206(98)00096-2.

Katz, V. 2015. "Regulating the Sharing Economy." *Berkeley Technology Law Journal* 30 (4): 1067–1126. https://www.jstor.org/stable/26377749

Kitkowska, A., Y. Shulman, L. A. Martucci, and E. Wästlund. 2020. "Psychological Effects and Their Role in Online Privacy Interactions: A Review." *IEEE Access* 8:21236–21260. https://doi.org/10.1109/ACCESS.2020.2969562.

Kobsa, A., S. Patil, and B. Meyer. 2012. "Privacy in Instant Messaging: An Impression Management Model." *Behaviour & Information Technology* 31 (4): 355–370. https://doi.org/10.1080/01449291003611326.

Kock, F., A. Berbekova, and A. G. Assaf. 2021. "Understanding and Managing the Threat of Common Method Bias: Detection, Prevention and Control." *Tourism Management* 86:104330. https://doi.org/10.1016/j.tourman.2021.104330.

Kosters, M., and J. V. der Heijden. 2015. "From Mechanism to Virtue: Evaluating Nudge Theory." *Evaluation* 21 (3): 276–291. https://doi.org/10.1177/1356389015590218.

Krämer, N. C., and S. Winter. 2008. "Impression Management 2.0." *Journal of Media Psychology* 20 (3): 106–116. https://doi.org/10.1027/1864-1105.20.3.106.

Krol, K., and S. Preibusch. 2016. "Control versus Effort in Privacy Warnings for Webforms." In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*, 13–23. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2994620.2994640.

Kühberger, A. 1998. "The Influence of Framing on Risky Decisions: A Meta-analysis." *Organizational Behavior and Human Decision Processes* 75 (1): 23–55. https://doi.org/10.1006/obhd.1998.2781.

Landsheer, J. A., and G. van den Wittenboer. March 25, 2015. "Unbalanced 2 X 2 Factorial Designs and the Interaction Effect: a Troublesome Combination." *PloS One* 10 (3): e0121412–e0121412. https://doi.org/10.1371/journal.pone.0121412.

LaPiere, R. T. February, 1934. "Attitudes Vs Actions." *Social Forces* 13 (2): 230–237. https://doi.org/10.2307/2570339.

Lapinski, M. K., E. K. Maloney, M. Braz, and H. C. Shulman. January, 2013. "Testing the Effects of Social Norms and Behavioral Privacy on Hand Washing: a Field Experiment." *Human Communication Research* 39 (1): 21–46. https://doi.org/10.1111/j.1468-2958.2012.01441.x.

Lapinski, M. K., and R. N. Rimal. January, 2006. "An Explication of Social Norms." *Communication Theory* 15 (2): 127–147. https://doi.org/10.1111/j.1468-2885.2005.tb00329.x.

Li, Y. 2012. "Theories in Online Information Privacy Research: A Critical Review and An Integrated Framework." *Decision Support Systems* 54 (1): 471–481. https://doi.org/10.1016/j.dss.2012.06.010.

Li, H., and S. Rosen. 1998. "Unraveling in Matching Markets." *The American Economic Review* 88 (3): 371–387.

Malhotra, N. K., S. S. Kim, and J. Agarwal. 2004. "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model." *Information Systems Research* 15 (4): 336–355. https://doi.org/10.1287/isre.1040.0032.

Martin, K., and H. Nissenbaum. 2016. "Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables." *Columbia Science & Technology Law Review* 18:176.

Mathur, A., G. Acar, M. J. Friedman, E. Lucherini, J. Mayer, M. Chetty, and A. Narayanan. 2019. "Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites." Proceedings of the ACM on Human-Computer Interaction, Volume 3 (CSCW), Austin, Texas. https://doi.org/10.1145/3359183

Mirsch, T., C. Lehrer, and R. Jung. 2017. "Digital Nudging: Altering User Behavior in Digital Environments." In *Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI 2017)*, 634–648. St. Gallen, Switzerland: Association for Information Systems. AIS Electronic Library (AISeL).

Murmann, P., and S. Fischer-Hübner. 2017. "Tools for Achieving Usable Ex Post Transparency: A Survey." *IEEE Access* 5:22965–22991. https://doi.org/10.1109/ACCESS.2017.2765539.

Newell, B. R., and D. R. Shanks. 2014. "Unconscious Influences on Decision Making: A Critical Review." *Behavioral and Brain Sciences* 37 (1): 1–19. https://doi.org/10.1017/S0140525X12003214.

Nielsen, J. 1994. "Usability Inspection Methods." In *Conference Companion on Human Factors in Computing Systems*, 413–414. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/259963.260531.

Nissenbaum, H. 2004. "Privacy As Contextual Integrity." *Washington Law Review* 79 (1): 119–157.

Nouwens, M., I. Liccardi, M. Veale, D. Karger, and L. Kagal. 2020. "Dark Patterns After the GDPR: Scraping Consent Pop-Ups and Demonstrating Their Influence." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. New York, NY, USA: Association for Computing Machinery.https://doi.org/10.1145/3313831.3376321.

Ostrovsky, M., and M. Schwarz. May, 2010. "Information Disclosure and Unraveling in Matching Markets." *American Economic Journal: Microeconomics* 2 (2): 34–63. https://doi.org/10.1257/mic.2.2.34.

Paine, C., A. N. Joinson, T. Buchanan, and U. D. Reips. 2006. "Privacy and Self-Disclosure Online." In *CHI '06 Extended Abstracts on Human Factors in Computing Systems*, 1187–1192. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1125451.1125674.

Palen, L., and P. Dourish. 2003. "Unpacking Privacy' for a Networked World Unpacking 'Privacy' for a Networked World." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 129–136. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/642611.642635.

Patil, S., R. Hoyle, R. Schlegel, A. Kapadia, and A. J. Lee. 2015. "Interrupt Now or Inform Later? Comparing Immediate and Delayed Privacy Feedback." In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 1415–1418. New York, NY, USA: Association for Computing Machinery.https://doi.org/10.1145/2702123.2702165.

Patil, S., R. Schlegel, A. Kapadia, and A. J. Lee. 2014. "Reflection or Action? How Feedback and Control Affect Location Sharing Decisions." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 101–110. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2556288.2557121.

Peppet, S. R. 2011. "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-disclosure Future." *Northwestern University Law Review* 105:1153.

Podsakoff, P. M., S. B. MacKenzie, J. Y. Lee, and N. P. Podsakoff. 2003. "Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies." *Journal of Applied Psychology* 88 (5): 879–903. https://doi.org/10.1037/0021-9010.88.5.879.

Rahman, H. A. 2021. "The Invisible Cage: Workers' Reactivity to Opaque Algorithmic Evaluations." *Administrative Science Quarterly* 66 (4): 945–988. https://doi.org/10.1177/00018392211010118.

Roth, A. E., and X. Xing. 1994. "Jumping the Gun: Imperfections and Institutions Related to the Timing of Market Transactions." *The American Economic Review* 84 (4): 992–1044.

Sah, S., and D. Read. 2020. "Mind the (information) Gap: Strategic Nondisclosure by Marketers and Interventions to Increase Consumer Deliberation." *Journal of Experimental Psychology: Applied* 26 (3): 432–452. https://doi.org/10.1037/xap0000260.

Samuelson, W., and R. Zeckhauser. 1988. "Status Quo Bias in Decision Making." *Journal of Risk and Uncertainty* 1 (1): 7–59. https://doi.org/10.1007/BF00055564.

Schaub, F., R. Balebako, A. L. Durity, and L. F. Cranor. July, 2015. "A Design Space for Effective Privacy Notices." In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, 1–17. Ottawa: USENIX Association.

"Sharing Economy", n. 2021. "Merriam-webster.com dictionary." Merriam-Webster. https://www.merriam-webster.com/dictionary/sharing%20economy.

Sheeran, P., and T. L. Webb. 2016. "The Intention–Behavior Gap." *Social and Personality Psychology Compass* 10 (9): 503–518. https://doi.org/10.1111/spc3.12265.

Shulman, Y., and J. Meyer. 2019. "Is Privacy Controllable?." In *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data: 13th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School,*

Vienna, Austria, August 20–24, Revised Selected Papers, edited by E. Kosta, J. Pierson, D. Slamanig, S. Fischer-Hübner, and S. Krenn, 222–238. Springer International Publishing. https://doi.org/10.1007/978-3-030-16744-8_15.

Smith, H. J., S. J. Milberg, and S. J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *MIS Quarterly* 20 (2): 167–196. https://doi.org/10.2307/249477.

Spence, M. 1973. "Job Market Signaling." *The Quarterly Journal of Economics* 87 (3): 355–374. https://doi.org/10.2307/1882010.

Spiekermann, S., and L. F. Cranor. January, 2009. "Engineering Privacy." *IEEE Transactions on Software Engineering* 35 (1): 67–82. https://doi.org/10.1109/TSE.2008.88.

Spottswood, E. L., and J. T. Hancock. March, 2017. "Should I Share That? Prompting Social Norms That Influence Privacy Behaviors on a Social Networking Site." *Journal of Computer-Mediated Communication* 22 (2): 55–70. https://doi.org/10.1111/jcc4.12182.

Steinfeld, N. 2016. "'I Agree to the Terms and Conditions': (How) Do Users Read Privacy Policies Online? An Eye-tracking Experiment." *Computers in Human Behavior* 55:992–1000. https://doi.org/10.1016/j.chb.2015.09.038.

Sunstein, C. R. 2014. "Nudging: A Very Short Guide." *Journal of Consumer Policy* 37 (4): 583–588. https://doi.org/10.1007/s10603-014-9273-1.

Tan, W.-S., D. Liu, and R. Bishu. 2009. "Web Evaluation: Heuristic Evaluation Vs User Testing." *International Journal of Industrial Ergonomics* 39 (4): 621–627. Special issue: Felicitating Colin G. Drury. https://doi.org/10.1016/j.ergon.2008.02.012.

Thaler, R. H., and S. Benartzi. 2004. "Save More Tomorrow™: Using Behavioral Economics to Increase Employee Saving Save More Tomorrow™: Using Behavioral Economics to Increase Employee Saving." *Journal of Political Economy* 112 (S1): S164–S187. https://doi.org/10.1086/380085.

Toch, E., Y. Wang, and L. F. Cranor. 2012. "Personalization and Privacy: a Survey of Privacy Risks and Remedies in Personalization-based Systems." *User Modeling and User-Adapted Interaction* 22 (1): 203–220. https://doi.org/10.1007/s11257-011-9110-z.

Tsai, J. Y., P. Kelley, P. Drielsma, L. F. Cranor, J. Hong, and N. Sadeh. 2009. "Who's Viewed You? The Impact of Feedback in a Mobile Location-Sharing Application." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2003–2012. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/1518701.1519005.

Tversky, A., and D. Kahneman. 1981. "The Framing of Decisions and the Psychology of Choice." *Science*211 (4481): 453–458. https://doi.org/10.1126/science.7455683.

van Dijck, J. 2013. "'You Have One Identity': Performing the Self on Facebook and LinkedIn." *Media, Culture & Society* 35 (2): 199–215. https://doi.org/10.1177/0163443712468605.

Venkatesh, V. 2000. "Determinants of Perceived Ease of Use: Integrating Control, Intrinsic Motivation, and Emotion Into the Technology Acceptance Model." *Information Systems Research* 11 (4): 342–365. https://doi.org/10.1287/isre.11.4.342.11872.

Voorhees, C. M., M. K. Brady, R. Calantone, and E. Ramirez. January 01, 2016. "Discriminant Validity Testing in Marketing: An Analysis, Causes for Concern, and Proposed Remedies." *Journal of the Academy of Marketing Science* 44 (1): 119–134. https://doi.org/10.1007/s11747-015-0455-4.

Wang, Y., P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh. 2014. "A Field Trial of Privacy Nudges for Facebook." In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2367–2376. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/2556288.2557413.

Warner, M., A. Gutmann, M. A. Sasse, and A. Blandford. 2018. "Privacy Unraveling Around Explicit HIV Status Disclosure Fields in the Online Geosocial Hookup App Grindr." Proceedings of the ACM on Human-Computer Interaction 2 (CSCW), New York City, NY. https://doi.org/10.1145/3274450.

Warner, M., A. Kitkowska, J. Gibbs, J. F. Maestre, and A. Blandford. 2020. "Evaluating 'Prefer Not to Say' Around Sensitive Disclosures." In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–13. New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3313831.3376150.

Warren, S. D., and L. D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review* 4 (5): 193–220. https://doi.org/10.2307/1321160.

Westin, A. 1970. *Privacy and Freedom. 1967*. New York: Atheneum.

Willis, L. E. 2013. "When Nudges Fail: Slippery Defaults." *University of Chicago Law Review* 80 (3): 1155–1230. https://doi.org/10.2139/ssrn.2142989.

Xu, H.. 2007. The Effects of Self-Construal and Perceived Control on Privacy Concerns." Proceedings of the 28th International Conference on Information Systems, ICIS 2007, Montreal, Quebec, Canada, December 9–12.

Appendices

Appendix 1. Psychometric scales used in the experiment

A.1. Intention to give personal information

Four items adapted from Malhotra, Kim, and Agarwal (2004) with minor modification to anchors. The scale reliability was reported in the original paper as Composite Reliability (CR) and Average Variance Extracted (AVE) at the levels of $CR(IGPI) = .95$ and $AVE(IGPI) = .86$.

Participant instructions. Think again about using Travel-Friend to find travel companions. Given this hypothetical application, specify the extent to which you would reveal your average ratings through [*TravelFriend* / *EmployOnline*].

Rating scale and anchoring. Seven-point semantic differential rating scale anchored with paired statements:

(1) I'm unlikely to reveal – I'm likely to reveal
(2) For me, revealing is not probable – For me, revealing is probable
(3) For me, revealing is possible – For me, revealing is not possible [Anchoring reversed]
(4) I'm willing to reveal – I'm unwilling to reveal [Anchoring reversed]

A.2. Privacy risk beliefs

Five items adapted from Malhotra, Kim, and Agarwal (2004). The scale reliability was reported in the original paper as $CR(PRB) = .92$ and $AVE(PRB) = .74$.

Participant instructions. Over the next pages you will see statements concerning personal beliefs. Please, consider them carefully for yourself, and indicate to what extent you agree or disagree with these statements.

Item statements.

(1) In general, it would be risky to give my employment history to online companies.
(2) There would be high potential for loss associated with giving my employment history to online firms.
(3) There would be too much uncertainty associated with giving my employment history to online firms.
(4) Providing online firms with my employment history would involve many unexpected problems.
(5) I would feel safe giving my employment history to online companies. [Reversed item] [Item removed after analysis]

Rating scale and anchoring. Seven-point Likert-type rating scale anchored verbally: *Strongly disagree – Disagree – Slightly disagree – Neither agree nor disagree – Slightly agree – Agree – Strongly agree.*

A.3. Perceived information control

Four items adapted from Dinev et al. (2013) with minor modifications to item statements to relate to context. The scale reliability was reported in the original paper with $CR(PIC) = .92$, $AVE(PIC) = .74$, and Cronbach's $\alpha = .89$.

Participant instructions. Still thinking about using [*Travel-Friend* / *EmployOnline*] to find [travel companions / short time employment], please, consider the four following statements carefully for yourself, and indicate to what extent you agree or disagree with these statements.

Item statements.

(1) I think I have control over what personal information can be released by [*TravelFriend* / *EmployOnline*].
(2) I believe I have control over how personal information can be used by [*TravelFriend* / *EmployOnline*].
(3) I believe I have control over what personal information can be collected by [*TravelFriend* / *EmployOnline*].
(4) I believe I can control my personal information provided to [*TravelFriend* / *EmployOnline*].

Rating scale and anchoring. Seven-point Likert-type rating scale anchored verbally: *Strongly disagree – Disagree – Slightly disagree – Neither agree nor disagree – Slightly agree – Agree – Strongly agree.*

A.4. Individual's privacy concerns

Fifteen items adapted from Smith, Milberg, and Burke (1996). In the original paper, the reliabilities of all the subscales were reported with $CR > .8$ and $AVE > .5$.

Participant instructions. Over the next pages you will see statements concerning personal beliefs. Please, consider them carefully for yourself, and indicate to what extent you agree or disagree with these statements.

Item statements.

(1) It usually bothers me when companies ask me for personal information.
(2) All the personal information in computer databases should be double-checked for accuracy – no matter how much this costs.
(3) Companies should not use personal information for any purpose unless it has been authorised by the individuals who provided the information.
(4) Companies should devote more time and effort to preventing unauthorised access to personal information.
(5) When companies ask me for personal information, I sometimes think twice before providing it.
(6) Companies should take more steps to make sure that the personal information in their files is accurate.
(7) When people give personal information to a company for some reason, the company should never use the information for any other reason.
(8) Companies should have better procedures to correct errors in personal information.

(9) Computer databases that contain personal information should be protected from unauthorised access – no matter how much it costs.
(10) It bothers me to give personal information to so many companies.
(11) Companies should never sell the personal information in their computer databases to other companies.
(12) Companies should devote more time and effort to verifying the accuracy of the personal information in their databases.
(13) Companies should never share personal information with other companies unless it has been authorised by the individuals who provided the information.
(14) Companies should take more steps to make sure that unauthorised people cannot access personal information in their computers.
(15) I'm concerned that companies are collecting too much personal information about me.

Rating scale and anchoring. Seven-point Likert-type rating scale anchored verbally: *Strongly disagree – Disagree – Slightly disagree – Neither agree nor disagree – Slightly agree – Agree – Strongly agree.*

Measured constructs. The instrument measures the individual's information privacy concerns in four dimensions (as per the original paper): statements (1), (5), (10), (15) constitute the privacy concerns about 'Collection'; items (2), (6), (8), (12) constitute the privacy concerns about 'Errors'; statements (3), (7), (11), (13) constitute the privacy concerns about 'Unauthorized secondary use'; statements (4), (9), (14) constitute the privacy concerns about 'Improper access'. In our analyses, the data revealed the 'Collection' and 'Errors' dimensions, following the original paper. The 'Unauthorized secondary use' and 'Improper access' subscales from the original paper loaded single factor and were treated as a single combined dimension.

Appendix 2. Participant Instructions: Scenarios and Scores

Introducing TravelFriend	**Introducing EmployOnline**
TravelFriend is an online application, allowing you to connect with people who are about to travel to places you also want to visit. To make it easier to find new travel companions, all users collect reviews from people they have previously traveled with. The reviews indicate how pleasant, reliable, and interesting they found you when traveling with you.	*EmployOnline* is an online platform for short time employment. The platform's aim is to match an employee with an employer. After completion of each job, the employer provides each employee with a review, and an overall score. The score indicates the quality of the job performed, the reliability of the employee, effectiveness, and other such things.
The reviews are given on a scale ranging from 0 to 10, where 0 means that the experiences of traveling with a companion were really bad, and 10 means that the experiences of traveling were very good. The app will automatically compute an average score for you that is based on all reviews by people who traveled with you.	The employer's reviews are given on a scale ranging from 0 to 10, where 0 means that the experiences of working with the employee were really bad, and 10 means that the experiences of working with the employee were very good. The platform will automatically compute an average score for the employee that is based on all reviews by the employers whose jobs the employee has finished.
With *TravelFriend* you don't need to share your average score with others. You can simply select above which point you would like to share your score. For example, if you set to share at 1, then you will only share your average score if it is 1 or higher. Alternatively, if you set to share at 10, then you will only share your average score if it is 10.	Think of yourself as an employee. With *EmployOnline*, you don't need to share your average score with the potential employers. You can simply select above which point you would like to share your score. For example, if you set to share at 1, then you will only share your average score if it is 1 or higher. Alternatively, if you set to share at 10, then you will only share your average score if it is 10.
You can see the example of the *TravelFriend* interface below:	You can see the example of the *EmployOnline* interface below:
Imagine that you have been using *TravelFriend* for about a year, and you have accumulated a number of reviews.	Imagine that you have been working through *EmployOnline* for about a year, and you have accumulated a number of reviews.
Now you have to decide above which point (between 0 and 10) you want the app to show your average score to others.	Now you have to decide above which point (between 0 and 10) you want the platform to show your average score to the potential employers.
This is how the score will be displayed:	This is how the score will be displayed:

Appendix 3. Full ANCOVA Results

Table A1. The effects of the independent variables and covariates on the Final score threshold in the ANCOVA model.

Effect	F	p	η_p^2
Context	6.85*	.009	.02
Timing-Control	0.87†	.418	.00
Content	0.48†	.616	.00
Context × Timing-Control	0.01†	.989	.00
Context × Content	0.97†	.379	.00
Timing-Control × Content	2.09‡	.082	.02
Context × Timing-Control × Content	1.05‡	.378	.01
Preferred score for a counterpart	162.61*	<.001	.27
Attitude to impression formation	25.94*	<.001	.06
Intention to give personal information	5.33*	.021	.01
Perceived information control	1.27*	.260	.00
Individual's privacy concerns (errors)	0.00*	.951	.00

*$F(1, 439)$, †$F(2, 439)$, ‡$F(4, 439)$.