Franz, Anjuli; Benlian, Alexander

Exploring interdependent privacy – Empirical insights into users' protection of others' privacy on online platforms

Electronic Markets

Provided in Cooperation with:
Springer Nature

Suggested Citation: Franz, Anjuli; Benlian, Alexander (2022) : Exploring interdependent privacy – Empirical insights into users' protection of others' privacy on online platforms, Electronic Markets, ISSN 1422-8890, Springer, Berlin, Heidelberg, Vol. 32, Iss. 4, pp. 2293-2309, https://doi.org/10.1007/s12525-022-00566-8

Electronic Markets (2022) 32:2293–2309
https://doi.org/10.1007/s12525-022-00566-8

RESEARCH PAPER

Exploring interdependent privacy – Empirical insights into users' protection of others' privacy on online platforms

Anjuli Franz[1] · **Alexander Benlian**[1]

Received: 16 December 2021 / Accepted: 20 June 2022 / Published online: 22 July 2022

Abstract

Recent information privacy research has started to spark a debate about privacy infringements that happen not on an individual, but on a multi-party level. Here, a person's own information privacy is affected by the decisions of others – a phenomenon referred to as interdependent privacy. Building on the 3R Interdependent Privacy Protection Framework, we explore the underlying mechanisms of how and why interdependent privacy violations happen and how they can be remedied. Drawing on an online vignette experiment (N = 330), we investigate the efficacy of an interdependent privacy salience nudge and reveal that it can decrease the likelihood that users disclose others' personal information by 62%. Furthermore, we develop a novel measurement instrument and empirically validate that users' decision to disclose others' personal information to an online platform is formed via a serial mediation mechanism through users' realization of the data transfer, recognition of others' ownership, and respect for others' rights. We discuss important implications for both theory and practice.

Keywords Interdependent privacy · Peer disclosure · Online platforms · Privacy nudge · Online vignette study · Serial multiple mediation

JEL Classification O30 · D91

Introduction

Privacy issues challenge researchers and regulators because of their immense complexity, and have been discussed through various lenses. Modern perspectives have matured from viewing privacy as a transactional process of information disclosure, to viewing it as a multi-faceted, socially constructed phenomenon that is closely tied to real-world modern networked technologies, and that we should endeavor to embed in the design of the tools and services we use daily (Bélanger & James, 2020; Knijnenburg et al., 2022). Particularly in the context of online platforms, where personal data is being generated and shared at lightning speed, privacy losses and violations are far from trivial to perceive and decide upon, and often remain unconsidered (Lowry, Dinev, et al., 2017; Garcia, 2017).

When investigating privacy concerns or disclosure decisions, the preponderance of privacy literature has limited its scope to a dyadic understanding of privacy, e.g., a dyadic information transfer between a company and an individual (Kamleitner & Mitchell, 2019). In contrast, recent research has called for a more versatile multi-level understanding of privacy to be able to explore complex disclosure decisions in progressively sophisticated digital environments (Bélanger & James, 2020). One crucial factor that makes privacy a highly complex affair are the various types of inherent connections among individuals. Since human beings are socially embedded and bond with each other by exchanging personal information, their personal data is often not only owned by themselves, but also co-owned by others. For example, chances are high that there are hundreds of co-owners of your phone number and email address (e.g., friends who have stored your contact information in their address book), and that a social platform (e.g., LinkedIn) has collected various information on your interests and preferences. This makes privacy protection an interdependent phenomenon (e.g., Biczók & Chia 2013; Cao et al., 2018; Wirth et al., 2019), since the violation

Responsible Editor: Reima Suomi

✉ Anjuli Franz
franz@ise.tu-darmstadt.de
https://www.ise.tu-darmstadt.de/index.en.jsp

[1] Fachgebiet ISE, Technische Universität Darmstadt, Hochschulstrasse 1, 64289 Darmstadt, Germany

of an individual's privacy rights can happen through others, potentially without the original owner even noticing.

In recent years, several research streams have approached this phenomenon employing, for example, economic models (e.g., Cao et al., 2018; Symeonidis et al., 2018) or empirical studies on users' behavior (e.g., Olteanu et al., 2018; Pu & Grossklags, 2015, 2017), have analyzed legal aspects (e.g., Symeonidis et al., 2018) or developed conceptual frameworks (e.g., Jia & Xu 2016; Kamleitner & Mitchell, 2019). Among the latter, Kamleitner & Mitchell (2019) have proposed the "3R Interdependent Privacy Protection Framework", which postulates a sequential chain of the underlying mechanisms *realization of the data transfer (RE)*, *recognition of others' ownership (RC)*, and *respect for others' rights (RS)* forming an individual's decision to protect others' personal data. While the 3R framework advances our understanding of how interdependent privacy decision-making might unfold and can inform future research, it has not been empirically validated to date. Furthermore, while information privacy research on the individual level has investigated interventions such as transparency tools to help users make informed decisions (e.g., Almuhimedi et al., 2015; Wang et al., 2014), we have little knowledge on effective countermeasures that can help to mitigate interdependent privacy violations. This is reflected in current regulatory efforts to protect individuals' and third parties' privacy, for example, the European Union General Data Protection Regulation (GDPR, European Parliament and Council, 2016): Whereas the GDPR has achieved major improvements to protect users' own information (e.g., mandatory opt-in mechanisms when collecting users' data for marketing purposes), little has been done to protect users from interdependent privacy violations by their peers. Since others' decisions on our privacy can have significant impacts on our everyday lives, we argue that it is paramount that we (1) understand the underlying mechanisms of interdependent privacy violations, and (2) find effective remedies that can serve as design suggestions for novel regulatory strategies. In this work, we therefore raise the following research questions:

RQ1: To what extent can the 3R mechanisms underlying users' interdependent privacy decision-making be empirically validated?
RQ2: How can interdependent privacy infringements be reduced via design choices, such as an interdependent privacy salience nudge?

To answer our research questions, we draw on the theoretical lens of the "3R Interdependent Privacy Protection Framework" established by Kamleitner & Mitchell (2019). We conduct a quantitative vignette-based online experiment with N = 330 Instagram users, motivated by an actual Instagram prompt that encourages users to violate others' privacy. In our experiment, we investigate the effect of an interdependent privacy salience nudge that aims to increase the salience of the other in the data transfer. We analyze our experimental data employing a serial multiple mediation analysis, which supports our hypotheses. Our post-hoc analysis of qualitative statements gives richer insights into participants' motives, and further confirms our theoretical model.

Our study contributes to research on interdependent privacy in several important ways. First, we investigate the effect of an interdependent privacy salience nudge and show that it can significantly improve users' protection of their peers' privacy online. Second, we empirically evaluate the "3R Interdependent Privacy Protection Framework" (Kamleitner & Mitchell, 2019). Our results indicate a three-stage mediation of the effect of our interdependent privacy salience nudge on users' disclosure of others' information through *RE*, *RC*, and *RS*, which validates Kamleitner and Mitchell (2019)'s theoretical model of users' interdependent privacy decision-making. Lastly, as part of our study, we develop and validate a measurement instrument for *RE*, *RC*, and *RS*, which can be useful for future research in this field. Our work implicates valuable insights for regulators, as it can serve as a starting point for overcoming current policy inadequacies (e.g., in the GDPR) with regard to interdependent privacy infringements.

The remainder of this paper is organized as follows. In the second section, we first introduce the phenomenon of interdependent privacy in the context of social platforms by giving several real-world examples as well as a brief overview of pertinent literature. We then introduce Kamleitner & Mitchell (2019)'s "3R Interdependent Privacy Protection Framework" as a theoretical lens for our study. Lastly, we turn to the concept of digital nudging in privacy, hence laying the conceptual foundation for the interdependent privacy salience nudge employed in our experiment. In the third section, we then develop our research model and hypotheses. We proceed with describing our research methodology and introducing the concept of serial mediation in the fourth section. After presenting the quantitative and qualitative results of our empirical study in the fifth section, we discuss our findings as well as our contributions to theory and practice in the sixth section. Finally, in the seventh section, we summarize the findings of this article.

Theoretical background

Privacy interdependence

In 1970, long before mobile devices and social networking platforms have emerged as omnipresent parts of our lives, Westin (1970) has defined privacy as "the ability to control, edit, manage, and delete information" about oneself and to "decide when, how, and to what extent information

is communicated to others" (p. 7). Since then, privacy has arisen to be one of the most crucial concepts of our time: While personal information (e.g., photos, preferences or location data) is being generated and shared online at a rapid pace, recent sociopolitical movements (e.g., Harwell & Harris 2021; Isaak & Hanna, 2018) demonstrate why privacy rights are of paramount importance for individuals' freedom and sovereignty. In 2018, based on the concept of privacy as a fundamental human right, the European Union (EU) has issued the General Data Protection Regulation (GDPR) (European Parliament and Council, 2016). The GDPR regulates the processing of personal data related to citizens of the EU and has acted as a catalyst for major transformations of privacy policies worldwide (Li et al., 2019; Linden et al., 2020). In an online context, however, privacy losses or violations represent intricate problems for both users and regulators, since they are often nontrivial to perceive and decide upon (Garcia, 2017). Contrarily, privacy is a highly complex affair, with one crucial factor being the various types of inherent connections among human beings and their personal data (Biczók et al., 2021). In the following, we will illustrate this interconnectedness drawing on the example of online platforms.

Imagine a purely individualistic perspective, where a person's own privacy is affected only by their own decisions. Here, common theoretical approaches such as the privacy calculus model (e.g., Dienlin & Metzger 2016; Dinev & Hart, 2006; Kehr et al., 2015) can give insight into users' analysis of perceived costs (e.g., privacy risks) and benefits (e.g., entertainment), and hence the formation of their intention to disclose their own information. With respect to online platforms, such as Facebook or LinkedIn, this assumption would hold only if individuals used such platforms in isolation. This is, however, not the case: For many online platforms, the interconnectedness of their users' data lies at the core of their business. For example, when a user installs a third-party application on Facebook, the application might collect not only a focal user's, but also their friends' personal information (Symeonidis et al., 2018). This has laid the foundation for the Cambridge Analytica scandal, which came to light in 2018 (Isaak & Hanna, 2018): While only 270.000 users installed the company's app-based personality quiz on Facebook, Cambridge Analytica harvested the personal data of an estimated 87 million people and used it for micro-targeting during the 2016 US election campaign (Kamleitner & Sotoudeh, 2019). As a second example, LinkedIn, a professional social network, relies on users' opinions on their contacts' skills (e.g., "Help us identify Anna Smith's top skill") in order to offer and sell personalized job opportunities. These examples demonstrate that a person's own privacy is not only affected by their own decisions, but is also controlled by the actions of other individuals or organizations. We refer to this phenomenon as *interdependent privacy*, where "personal information is shared without the knowledge and/or direct consent of the data subject" (Biczók et al., 2021). The notion of privacy interdependence renders the aforementioned perspective of an individual privacy calculus obsolete.

In recent years, researchers from various fields (such as information security, information systems, economics or marketing) have started to spark a debate of the consequences, risks and potential mitigations of privacy interdependence. Reviewing recent literature, we found that one central concept is users' awareness of interdependent privacy risks (e.g., Biczók & Chia 2013; Symeonidis et al., 2018): While, in an analog world, interdependent privacy protection seems to work according to implicitly negotiated "norms about what, why, and to whom information is shared within specific relationships" (Martin, 2016, p. 551), these negotiations appear to be largely absent when we consider interdependent privacy in an online context (Kamleitner & Mitchell, 2019). Prior research has demonstrated across data types (e.g., contact information or photos) that users are less considerate towards the privacy of their peers, compared to their own (Marsch et al., 2021). At the same time, new information and communication technologies allow for a tremendously larger scope of potential interdependent privacy violations, since users are able to automatically and effortlessly collect and disclose others' information. To illustrate this, we borrow from a fictive scenario introduced by Kamleitner and Sotoudeh (2019), and imagine a person called Ada, who is on a trip to explore a foreign city. Ada is looking for a nice place to stay, and asks a woman passing by if she has any tips. The woman responds: "Well I do have some really good recommendations, but first give me the name and phone number of your father, and maybe also a picture of him." Ada is baffled, refuses, and walks away. She implicitly feels that this information is personal, and not hers to share. In an online setting, however, Ada would consult a travel booking app, with hundreds of accommodation options being just one click away. The app might ask for access to her contacts. Her contact list includes information (such as a name, phone number, picture, and birthday) on her father, as well as pretty much anyone Ada knows. Yet, she might simply click "Allow Access", hence becoming a sharer of her contacts' data to an online platform without her contacts even knowing about it.

Presently, the issue of interdependent privacy displays a regulatory loophole for the GDPR (Kamleitner & Sotoudeh, 2019). The GDPR limits its scope to a dyadic understanding of privacy (e.g., between a company and a consumer), while leaving room for gray area with regard to interdependent privacy infringements. It specifies informed consent by the original data subject as a lawful prerequisite for the processing of personal data (Art. 6, GDPR), and further specifies that the original owner needs to be notified and provided

with easy withdrawal of consent (Art. 7, GDPR). This regulation assumes that it is always clear who the original owner of personal information is. However, whereas Ada gives consent to share her contacts' data, her contacts might claim the ownership and privacy rights towards this information. While the GDPR specifically excludes the processing of personal information for household or purely personal purposes (Art. 2, GDPR), it is questionable if this exception covers the transfer of personal information of several hundred individuals to a company, such as an online platform, that processes this information as part of its business model. The negligence of interdependent privacy phenomena hence poses a major shortcoming of the GDPR in its current version.

Previous literature has approached the concept of interdependent privacy from various angles. In a recent meta-analysis, Humbert et al. (2019) have summarized and analyzed prior works across the research landscape. While "interdependent privacy" seems to be the most widely used term, a variety of different terminologies is being used, such as collective privacy (e.g., Squicciarini et al., 2009), multiparty privacy (e.g., Thomas et al., 2010), or peer disclosure (e.g., Cao et al., 2018; Chen et al., 2015). Several researchers have employed game-theoretical models to investigate the externalities of privacy interdependence (e.g., Biczók & Chia, 2013; Cao et al., 2018). For example, Symeonidis et al. (2018) have calculated the extent of collateral information collection by third-party apps on Facebook, finding that a user's chance of having their personal data shared with third-party apps through their friends is greater than 80%. This enables practices such as shadow profiling, where a company composes profiles of individuals based on data gathered from other users on a large scale (Garcia, 2017). Other works have focused on empirically exploring interdependent privacy behavior, for example, by investigating the monetary value which users of online services place on their contacts' personal information (Marsch et al., 2021; Pu & Grossklags, 2015), or by analyzing the roles of information sensitivity (Wirth et al., 2019) or sharers' anonymity (Pu & Grossklags, 2017).

Whereas previous research has yielded important insights into the topic of privacy interdependence, we have only little knowledge on the *how* and *why*, that is, on the underlying mechanisms of interdependent privacy behavior. By mechanisms, we refer to social mechanisms that act as "building blocks for the construction of causal explanations of social phenomena" (Avgerou, 2013, p. 407), which drive the process of forming an interdependent privacy decision and explain the observed behavior. One approach to tackle the *how* and *why* of interdependent privacy behavior is Kamleitner & Mitchell (2019)'s conceptual "3R Interdependent Privacy Protection Framework", which we will introduce in the following section.

The 3R interdependent privacy protection framework

In their framework, Kamleitner and Mitchell (2019) have approached the phenomenon of interdependent privacy infringements by drawing on the conceptual commonality between personal data and property. Individuals feel a sense of ownership for property, and the protection of such property necessitates the "cooperation of others and their respect of what is 'ours'" (Kamleitner & Sotoudeh, 2019, p. 2). While individuals also feel a sense of ownership for personal information, property and personal information differ with regards to their tangibility. Property refers to the right to one's possession, that is, to goods that are mostly tangible. For example, a house can be touched and seen, and can be held by only one or few individuals at a time. We are hence usually aware that someone owns it. On the contrary, personal information is mostly intangible. Imagine, for example, a phone number. Since it can be held by an unlimited amount of people at a time, it is practically impossible to oversee how often it has been shared. Moreover, while the transfer of property usually takes place via an active acquisition (for instance, buying a house), the transfer of personal information often arises as a side effect of our daily activities. For example, when using an online platform, personal information is being shared to other individuals or organizations without the transfer of data as a good being in the focus of attention. Kamleitner and Mitchell (2019) argue that these fundamental differences make it much easier to trespass on privacy, that is, the right to one's personal information, than property. While property infringements mostly arise from a failure of respect, interdependent privacy violations can be caused by failures at antecedent stages (Kamleitner & Sotoudeh, 2019; Kamleitner & Mitchell, 2019) have derived three sequential steps that users need to take in order to protect others' personal information online: *realization of the data transfer (RE)*, *recognition of others' ownership (RC)*, and lastly *respect for others' rights (RS)*. Figure 1 illustrates these steps based on the introductory example of Ada downloading an app.

According to the 3R framework, users' *realization of the data transfer* (*RE)* represents the first step toward protecting others' personal information. Imagine a sharer synchronizing their address book with the Instagram app. In order to realize that this implies transferring co-owned data, the sharer first needs to realize that they are about to transfer a good to another party at all. Users' *RE* is based on the presence of two conditions: The sharer first needs to overcome the intangible nature of information which makes it difficult to truly comprehend data as a good, and then must realize that this good is about to be transferred from one party to another. In our example, Ada might press "Allow Access" without realizing that this will transfer data from her phone to the app

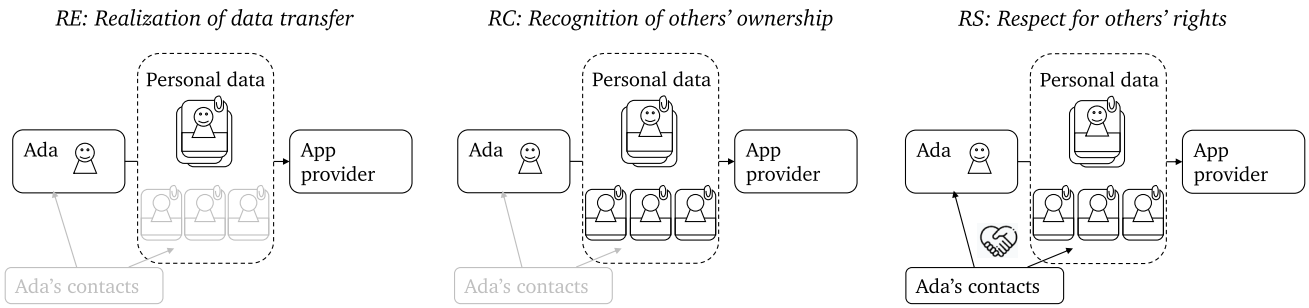

Fig. 1 The 3R interdependent privacy protection framework (Kamleitner & Mitchell, 2019), illustrated by the example of Ada (sharer) sharing her contacts' (others') personal information with an app provider (recipient)

provider, which would, in this moment, leave her unable to recognize others' being involved in the data transfer.

Provided that a sharer realizes that they are about to transfer a good, they then need to *recognize others' ownership*[1]*(RC)* of this good. When the app asks Ada for access to "her" contacts, she might not even consider the possibility of others holding a stake. Furthermore, the feeling of self-entitlement might weaken her recognition of others' ownership: Ada might recognize that others are somewhat involved in the data about to be transferred, but might feel self-entitled to this data. This feeling of entitlement might arise, for example, if the sharer has self-collected the information on a device that they own (e.g., their phone), or if they are in close relationship to the other (e.g., a partner or parent). Both the visibility of the other and the recognition of others' entitlement are hence important prerequisites for users' *RC*.

Lastly, *respect for others' rights (RS)* presents the final stage to prevent interdependent privacy violations: Once the sharer has recognized that what they are about to share belongs to another person, their respect towards others' privacy rights affects their further actions. There are several options for a sharer to respect others' privacy, for example, by refraining from the data transfer at all, or by obtaining consent from the other. According to Kamleitner and Mitchell (2019), there are two main antecedent forces that play a role in users' formation of *respect for others' rights*. First, while, in an analog world, norms of respect for what belongs to others are implicitly negotiated, society seems to trivialize disrespect towards others' privacy in digital settings. Users might thus consider it socially acceptable to infringe on others' privacy, because "everyone does it". Second, users might weigh their own benefit of the interdependent privacy violation against their own or others' costs, and hence deliberately infringe on others' privacy by knowingly putting their own interests above those of others.

The 3R Interdependent Privacy Protection Framework hence postulates three sequential steps where RE is a prerequisite for RC, and RC in turn is a prerequisite for RS. Together, the three steps act as a mechanism for users' formation of an interdependent privacy decision.

Privacy nudging

Since Thaler and Sunstein (2008) have introduced the concept of nudging in 2008, it has found widespread attention in both research and practice. Nudges describe design elements that target automatic cognitive processes, such as biases or heuristics, to gently push individuals to perform the "right" behavior without limiting their choice set. Examples from the analog world include default options in organ donation or speed signs displaying smiling or frowning emoji. In information privacy research, prior works have started to investigate the potential of digital nudges (Schneider et al., 2018) in persuading users to act in a privacy-preserving manner in individual privacy contexts (e.g., Acquisti et al., 2017; Almuhimedi et al., 2015; Wang et al., 2014). Furthermore, recent research has started to call for the design and evaluation of nudges and permission interfaces "that approach privacy not simply as an individual issue, but as an interdependent and collective concern" (Marsch et al., 2021, p. 17).

Reviewing the vast body of literature on nudging, we find that nudges can take on various designs. Popular mechanisms are, for example, default options, positioning or color coding, reminding of the consequences, or enabling social comparison (Caraban et al., 2019). In their paper on the 3R framework, Kamleitner and Mitchell (2019) have suggested several interventions to improve interdependent privacy protection across stakeholders, e.g., requiring additional steps of decision control in the transfer process, or a preview of the actual data which is about to be shared. These suggestions

[1] While Kamleitner and Mitchell (2019) refer to the second stage as "recognition of others' rights", we chose to use the term "recognition of others' ownership", since we think that it (1) better represents the underlying concept and (2) is more distinguishable from the third stage, "respect for others rights".

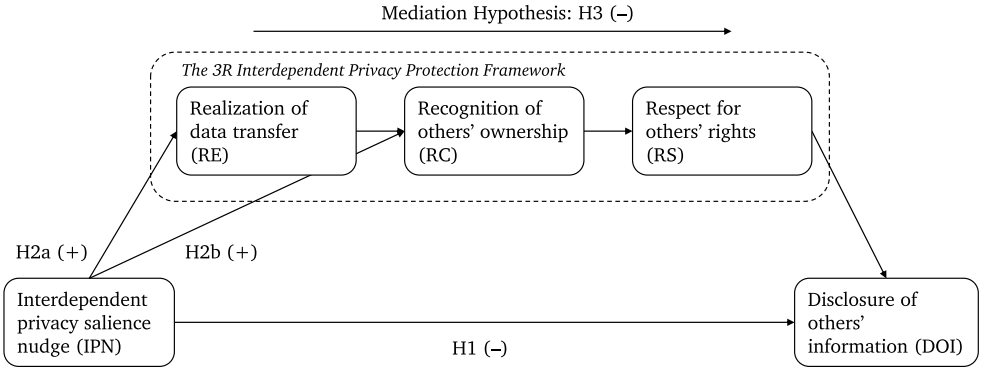

Fig. 2 Research model

provide a valuable basis for the design of nudges in an interdependent privacy context.

Research model and hypothesis development

Building upon prior works on privacy nudging (e.g., Almuhimedi et al., 2015; Wang et al., 2014; Zhang & Xu, 2016) and interdependent privacy protection (Kamleitner & Mitchell, 2019), we develop a research model which suggests that users' *RE*, *RC*, and *RS* carry over the effect of an interdependent privacy salience nudge *(IPN)* to users' decision to disclose others' information *(DOI)*. Figure 2 depicts our proposed research model.

Prior research on privacy nudging suggests that nudges that are designed to enable informed decision-making can facilitate privacy-aware behavior (Almuhimedi et al., 2015; Wang et al., 2014). For instance, confronting users with feedback on how often their location data was shared with apps has been shown to make users control their app permissions more restrictively (Almuhimedi et al., 2015). Regarding the violation of interdependent privacy, we thus hypothesize the following:

> H1: The presence (vs. absence) of an interdependent privacy salience nudge (IPN) decreases users' disclosure of others' information (DOI).

In our remaining hypotheses, we aim to dive deeper into the underlying mechanisms of this effect. We use Avgerou (2013)'s definition of social mechanisms as sequences of events unfolding in time, that generate causal processes and ultimately observed outcomes. Social mechanisms might show, for example, how individuals develop specific meanings of an information system, or why they act in a particular way when interacting with technology in a certain context. We draw on the 3R framework (Kamleitner & Mitchell, 2019), where the salience of the good (i.e., the personal data about to be transferred) and the salience of the transfer have been suggested as antecedents of users' realization of the data transfer. Prior research has demonstrated that providing users with salient and accessible privacy information guides users' attention towards the information disclosure and its potential risks (Tsai et al., 2011). Getting back to our example of Ada downloading an app, we argue that it would have been easier for her to realize the data transfer if the app would have provided her with transparent and detailed information instead of simply asking for access to her contacts. For an *IPN* that increases the salience of both the data and the transfer, we hypothesize the following:

> H2a: The presence (vs. absence) of an interdependent privacy salience nudge (IPN) increases users' realization of the data transfer (RE).

Analogously, the salience of the other has been named as the antecedent of users' recognition of others' ownership when sharing information in an interdependent privacy context (Kamleitner & Mitchell, 2019). Increasing the salience of the other will hence increase the user's attention towards the role of others' ownership during the data transfer: If the app had explicitly informed Ada that she was about to share information that does not belong to her, but to others, she would have been more likely to recognize others' ownership of the data. For an *IPN* that increases the salience of the other, we hence posit:

> H2b: The presence (vs. absence) of an interdependent privacy salience nudge (IPN) increases users' recognition of others' ownership (RC).

H2a and *H2b* reflect our expectation of how the salience and accessibility of the displayed interdependent privacy information affect users' RE and RC.

Drawing on the 3R Interdependent Privacy Protection Framework (Kamleitner & Mitchell, 2019), we predict that *RE* will feed into users' *RC*, which will in turn increase their *RS*, and ultimately decrease their *DOI*. In other words, we

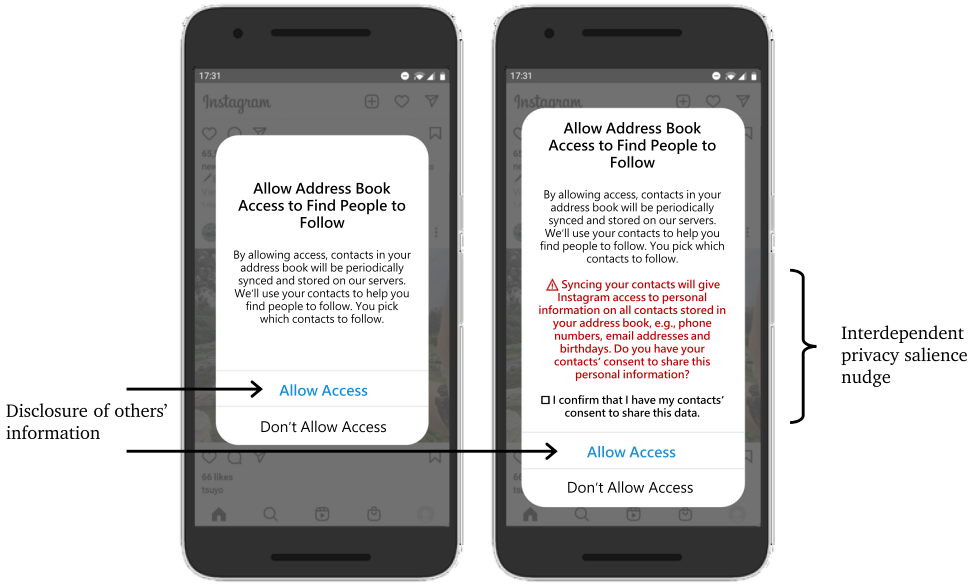

Fig. 3 Mobile screenshots of an Instagram prompt asking for permission to access the address book and synchronize contacts. Control group (left) and treatment group with interdependent privacy salience nudge (right)

posit that the effect of the *IPN* on users' *DOI* takes place via a three-stage serial mediation through *RE*, *RC*, and *RS*:

> H3: Users' realization of the data transfer (RE), recognition of others' ownership (RC), and respect for others' rights (RS) will act as a three-stage serial mediator for the effect of the interdependent privacy salience nudge (IPN) on users' disclosure of others' information (DOI).

Research methodology

Experimental design and procedure

To test our hypotheses, we conducted an online experiment and embedded our treatments based on vignettes depicted in an online survey. The vignette methodology has been validated as an effective measurement technique for assessing users' perceptions of and responses to specific information privacy-related conditions (Benlian et al., 2020; Lowry, Moody, et al., 2017; Warkentin et al., 2017). We chose the social networking platform Instagram as the context for our study for two main reasons. First, Instagram and its parent company, Meta Platforms (formerly Facebook), have been increasingly facilitating users' voluntary information disclosure about not only their own, but also others' information (Alsarkal et al., 2018; Symeonidis et al., 2018). Employing a vignette scenario on Instagram hence allowed us to use a real-world prompt which encourages interdependent privacy violations on online platforms. Second, Instagram is among the most popular social networks as of 2021 (Statista, 2021), which allowed for a large amount of potential participants in our study.

In our online vignette experiment, participants were welcomed and told that they participated in a study on Instagram use. They were asked to answer all questions honestly, and were told that there were no right or wrong answers. Furthermore, they were informed about their anonymity and the intended use of the collected data. Participants where then asked to imagine that they were logged into their personal Instagram account. They were told to imagine that, while browsing their Instagram feed, a prompt pops up, which was shown to them in the form of a screenshot. We employed a between-subject 2×1 experimental design with one control group, who saw the regular Instagram prompt asking for access to their address book (see Fig. 3, left side), and one experimental group, who saw the same prompt enriched with an interdependent privacy salience nudge (*IPN*, right side).

Drawing on prior literature on privacy nudging, we designed our interdependent privacy salience nudge (IPN) with the following ideas in mind: Building on Kamleitner and Mitchell (2019)'s suggestions for interventions to improve interdependent privacy protection, we aimed to implement additional steps of decision control into the data transfer process by including an opt-in mechanism that requires users to actively confirm that they have their contacts' consent to share their personal information. Furthermore, we provide examples of the actual data about to be transferred to Instagram by specifying that it includes the phone numbers, email addresses and birthdays of all contacts stored in one's address book, to increase both the salience of the data and the data transfer as well as the salience of the other individuals involved. We hence designed our *IPN* with the aim to increase both users' *RE* and their *RC*. Our nudge design is in alignment with prior research on users' preferences regarding the design of privacy nudges by

employing a default mechanism (i.e., allowing access is by default not possible without opting in) along with color (red font), framing (warning sign), and privacy-related information (Schöbel et al., 2020). These design choices are also in agreement with the design principles for effective privacy nudging provided by (Barev et al., 2020).

In both the treatment and the control group, participants were asked how they would like to proceed with the Instagram prompt. After having selected one of two options, they were asked to shortly state why they chose the respective option in a free-text field. They were then redirected to our post-experimental questionnaire, where we recorded our mediation constructs, control variables, and socio-demographic information. Lastly, participants had the option to give feedback on the experiment on a voluntary basis, were debriefed, and informed that they finished the study.

Measured variables

Measurement of the dependent variable In our experiment, participants chose between the following two options on how to proceed with the Instagram prompt: (1) "Press 'Allow Access' to sync my contacts" for the control group and "Check the box 'I confirm that I have my contacts' consent to share this data' and press 'Allow Access' to sync my contacts" for the treatment group, respectively; (2) "Press 'Don't Allow Access' and not sync my contacts" for both groups. We measured our dependent variable, that is, participants' *disclosure of others' information (DOI)* by capturing if they chose to "Allow Access" (which we counted as "1") or "Don't Allow Access" (which we counted as "0").

Scale development for RE, RC, and RS To measure our three mediation constructs *RE*, *RC*, and *RS*, we developed a measurement instrument based on the 3R Interdependent Privacy Protection Framework. In line with previous literature on scale development (e.g., MacKenzie et al., 2011; Moore & Benbasat, 1991), we started the process with a conceptual definition of the constructs, which was provided in detail by Kamleitner and Mitchell (2019). We then created a list of eight candidate items per construct that we thought to be suitable to represent the respective construct. Next, we asked six experienced researchers of the field of information systems to sort our items into the three constructs (*RE*, *RC*, *RS*), and to give feedback on the understandability of each item. This allowed us to assess the content validity of the items, to confirm the clustering into constructs, and to refine our wording. In a pretest experiment with 50 participants, we then evaluated the reliability of our items using Cronbach's Alpha (Cronbach, 1951). Based on the pretest results, we again refined our measurement instrument and finally chose 4 items per construct to use in our experiment (see Table 4 in the Appendix).

Control variables In addition to the constructs presented in our research model, we measured several alternative drivers of users' disclosure of others' information as controls in our experiment. Drawing on previous literature on users' information disclosure (e.g., Dinev & Hart 2006; Krasnova et al., 2012), we measured participants' general *privacy concerns* (Pavlou et al., 2007; Smith et al., 1996) towards Instagram. Furthermore, we collected information on subjects' *Instagram use*, as well as *sociodemographic information* (i.e., gender, age, education, and nationality). Lastly, we measured users' *normative beliefs* towards disclosing others' information online (Primack et al., 2008). For a full list of all items used in our questionnaire, please refer to Table 4 in the Appendix.

Data collection and sample

In line with previous research, we recruited 349 participants via Prolific, a platform for recruiting subjects for social and economic science experiments (Palan & Schitter, 2018). All participants were EU citizens and were pre-screened as Instagram users by Prolific. Subjects were payed $0.53 (USD) for their participation. We excluded 19 participants because they failed to answer our attention check correctly (11 participants) or finished the study in less than half of the average completion time (8 participants), resulting in our final sample of 330 participants. Of the subjects in our study, 174 identified as females, 154 as males, and 2 as other. Participants exhibited an average age of 29.4 years, with 57% being younger than 25 years and 4% being older than 44 years. Our sample included 20 nationalities of the EU, with 95% of participants stating that they used Instagram at least several times a week, and 82% using it every day.

Serial mediation analysis

In our data analysis, we employ a serial mediation model with our three mediators *RE*, *RC*, and *RS*. In contrast to parallel mediation, where two or more mediators are hypothesized to explain the effect of an independent variable on a dependent variable while the mediators themselves do not causally influence one another, serial mediation describes two or more mediators that are linked together in a causal chain (Hayes, 2018). In our research model, we investigate the direct and indirect effects of our *IPN* on users' *DOI* while modeling a process in which the *IPN* increases *RE* and *RC* (the latter both directly and indirectly through *RE*), *RC* in turn feeds into *RS*, concluding with *DOI* as the final consequence. We hence empirically test Kamleitner and Mitchell (2019)'s 3R framework, who have postulated that *RE* is causally prior to *RC*, which is causally prior to *RS*. The serial mediation approach is most fitting to explore research contexts

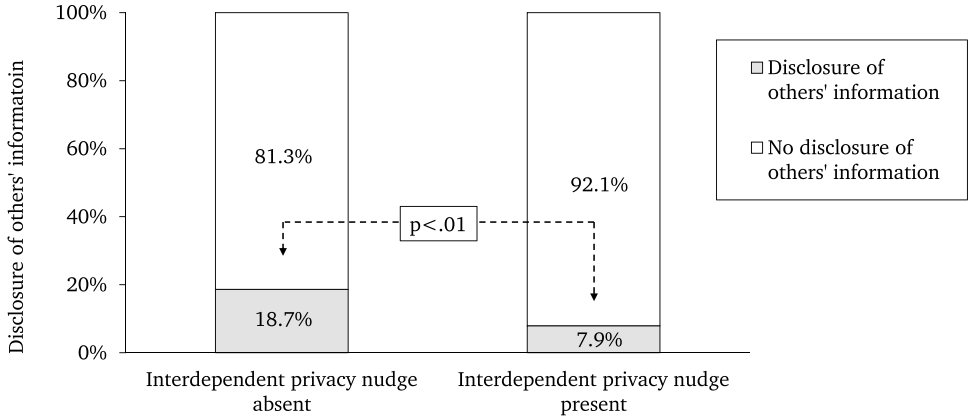

Fig. 4 Disclosure of others' information across experimental groups; N = 330

where temporally ordered stages are central to theorizing (e.g., Casciano & Massey 2012; Valentine et al., 2014).

Results

Measurement validation

To confirm the random assignment of participants across our two experimental conditions (*IPN* absent vs. present), we performed a series of one-way ANOVAs for all control variables. There were no significant differences in *gender* ($F = 0.005$; $p > .1$), *age* ($F = 1.82$; $p > .1$), *education* ($F = 1.70$; $p > .1$), *nationality* ($F = 1.59$; $p > .05$), *privacy concerns* ($F = 0.94$; $p > .1$), *normative beliefs* ($F = 1.22$; $p > .1$) or *Instagram use* ($F = 0.32$; $p > .1$) among the two experimental conditions. It is therefore reasonable to conclude that the random assignment of participants to our conditions was successful, and that the participants' demographics and relevant controls did not confound the effects of our experimental manipulations. We assessed our item scales for reliability using Cronbach's alpha (Cronbach, 1951), which yielded values greater than 0.88 for all constructs (see Table 4 in the Appendix).

Direct effect of the interdependent privacy salience nudge on users' Disclosure of others' information

Of the 330 participants, 13.3% chose to disclose others' information by synchronizing their contacts with Instagram. A significant two-proportion Z test revealed that participants' choice varied across the two experimental conditions ($\chi^2 = 8.25$; $p < .01$), see Fig. 4: In the control group (*IPN* absent), 18.7% of participants chose to disclose others' information, whereas among participants who received the treatment (*IPN* present), only 7.9% chose to do so.

In order to test our hypothesis H1, we conducted a binary logistic regression on our dependent variable *DOI* without and with control variables (see Table 1). We examined the main effects of the *IPN* and any potential effect of the controls on participants' *DOI*. The results of our regression analysis demonstrate a significant negative effect ($B = -0.98$; $p < .05$; $Exp(B) = 0.38$) of the *IPN* on participants' *DOI*. Participants that were confronted with an interdependent privacy salience nudge were hence 62% less likely to disclose others' information than when the nudge was absent, **supporting H1**.

Serial mediation analysis through the lens of the 3R framework

Our remaining hypotheses focus on the explanatory mechanism through which the formation of users' decision to *DOI* takes place. In H2a and H2b, we hypothesized that the introduction of an *IPN* will increase users' *RE* as well as *RC*. In H3, we then argued that the *IPN* influences users' *DOI* negatively through a three-stage mediation via *RE*, *RC* and subsequently *RS*. To evaluate our hypotheses, we performed a serial multiple mediaton analysis using Hayes' (2018) PROCESS macro (version 3.5). We applied model 6 and entered *RE*, *RC* and *RS* as potential mediators between the independent and dependent variable while controlling for all direct and indirect paths. Additionally, we controlled the dependent variable as well as all mediators for participants' socio-demographics. Furthermore, we controlled the dependent variable as well as *RE* and *RC* for participants' *privacy concerns*, and, drawing on Kamleitner and Mitchell (2019), *RS* for participants' *normative beliefs*. We estimated our model using a bootstrapping approach based on 10,000 samples and 95% bias-corrected confidence intervals for the indirect effects. Figure 5 illustrates all direct effects as well as the explained variance of each constructs in our model. For a detailed stepwise presentation of all mediation effects, please refer to Table 4 in the Appendix.

The model revealed a positive and statistically significant direct effect of the *IPN* on participants' *RE* ($B = 3.97$; $p < .01$). Furthermore, we found a positive and statistically significant direct effect of the *IPN* on participants' *RC* ($B = 0.400$; $p < .05$). This corroborates our **hypotheses H2a**

Table 1 Logistic regression analysis on participants' disclosure of others' information (DOI)

	Binary logistic regression without controls			Binary logistic regression with controls		
Construct	B	*SE*	Exp(B)	B	*SE*	Exp(B)
Intercept	–1.47***	0.20	0.23	–0.74	1.25	2.10
Manipulation						
Interdependent privacy salience nudge (IPN)	–0.98**	0.35	0.38	–0.98*	0.38	0.38
Controls						
Privacy concerns	-	-	-	–0.68***	0.13	0.51
Gender (male)	-	-	-	1.03**	0.37	2.80
Age	-	-	-	–0.46	0.255	0.63
Education	-	-	-	0.30	0.16	1.35
Nationality	-	-	-	–0.03	0.03	0.97
Instagram use	-	-	-	–0.32	0.38	0.73
Model fit						
Log Likelihood	–125.35	-	-	–103.48	-	-
Nagelkerke R^2	0.05	-	-	0.27	-	-
Omnibus χ^2	8.47**	-	-	52.20***	-	-

* $p < .05$; ** $p < .01$; *** $p < .001$; $N = 330$

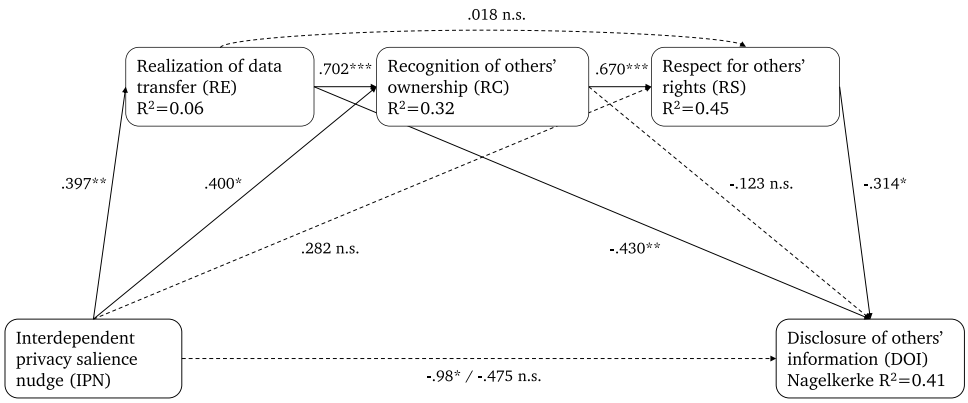

Fig. 5 Results from the serial multiple mediation analysis for the effect of an IPN on users' DOI through the 3R model. Note: The first coefficient on a given path represents the direct effect without the mediators in the model; the second represents the direct effect when the mediators are included in the model. *** $p < .001$; ** $p < .01$; * $p < .05$; n.s. not significant; $N = 330$

and H2b, and implicitly confirms that our experimental treatment worked as intended.

In addition, Table 2 sheds further light on the indirect effects of RE, RC and RS on participants' DOI. We found evidence of three significant mediation paths, indicated by estimates of effect sizes that did not include zero in the given confidence interval. Path (1) demonstrates a significant indirect effect of the IPN on DOI through RE alone (effect size = –0.170; CI = [–0.4325, –0.0119], which has not been theorized in our research model. Path (6) consists of two significant specific indirect effects, namely through RC and RS as mediators (effect size = –0.084; CI = [–0.2247, –0.0004]. Furthermore, the direct effect of RC on DOI in our model is statistically insignificant ($p > .05$), suggesting a complete mediation through RS. Lastly, path (7) reveals a significant indirect effect of all three mediators RE, RC and RS (effect size = –0.059; CI = [–0.1619, –0.0023], hence **supporting our hypothesis H3**. As the direct effect of IPN on DOI (B = –0.98; $p < .01$) became insignificant after entering RE, RC and RS as mediators (B = 0.475; $p > .1$), this represents a full mediation through the 3R mechanisms (Hayes, 2018).

Post-hoc analysis of qualitative results

After the participants of our experiment had decided how they would like to proceed with the Instagram prompt (by choosing either "Allow Access" or "Don't Allow Access"), we asked them to shortly state why they decided the way they did. This provided us with qualitative free-text answers and hence richer insights into participants' motives. Drawing on literature on the analysis of qualitative data (Mayring, 2014), we chose an inductive approach and coded all answers into categories that illustrated a reflection of the data material. Some statements were sorted into more than one category, and some statements were too imprecise and

Table 2 Results from the serial multiple mediation analysis (indirect effects of IPN on participants' DOI through RE, RC, and RS)

Indirect Effect Paths	Effect size	Boot SE	BootLLCI	BootULCI
(1) IPN → RE → DOI	**−0.170**	**0.107**	**−0.4325**	**−0.0119**
(2) IPN → RC → DOI	−0.049	0.086	−0.2608	0.0848
(3) IPN → RS → DOI	−0.089	0.076	−0.2724	0.0155
(4) IPN → RE → RC → DOI	−0.034	0.056	−0.1592	0.0659
(5) IPN → RE → RS → DOI	−0.002	0.016	−0.0350	0.0330
(6) IPN → RC → RS → DOI	**−0.084**	**0.060**	**−0.2247**	**−0.0004**
(7) IPN → RE →RC → RS → DOI	**−0.059**	**0.041**	**−0.1619**	**−0.0023**

Coefficients were computed based on serial multiple mediation analysis including all controls and using bootstrapping with 10,000 samples and a 95% bias-corrected confidence interval (LLCI = Lower Limit / ULCI = Upper Limit of Confidence Interval) (Hayes 2018). Significant indirect effects are marked in bold.

Table 3 Overview of participants' free-text statements

Participants who disclosed others' personal information ("Allow Access")

Code	Number of statements		Exemplary statements
	IPN absent (N = 31)	IPN present (N = 13)	
Gain more followers without much effort	21	9	*"It would be easier to find people that I know."* *"Because it's gonna help me add more contacts."*
Trust in Instagram	5	1	*"I think Instagram is safe enough to be trusted."*

Participants who did not disclose others' personal information ("Don't Allow Access")

Code	Number of statements		Exemplary statements
	IPN absent (N = 135)	IPN present (N = 151)	
Own privacy concerns towards Instagram	71	75	*"I don't like sharing my personal information to large companies."* *"I don't know how safe my data is with Facebook."* *"I try to avoid anything that barges into my privacy (more than social media already does)."*
Feature does not create added value	44	54	*"[…] I don't want to sync my contacts because I don't really care for that."* *"I don't have any interest in following people from my contact list."*
Respect for contacts' privacy rights	8	33	*"It does not seem right to share other peoples' data without their consent."* *"I have no right (or intend) to share personal data of my contacts with a company that makes money out of it."* *"Because the data in question does not belong to me."* *"I don't want to compromise my contacts' private info."*
Privacy protection towards contacts	15	15	*"I don't want every contact on my phone to see or find my Instagram account."* *"[…] I'd rather keep my Instagram private and prefer to not be able to be found by everyone in my contact list."*

therefore not sorted into any category. Table 3 gives an overview of participants' motives with exemplary statements.

As for participants who disclosed others' personal information by allowing Instagram access to their contacts, the most stated reason was the wish to gain more followers without much effort. For example, one participant stated: *"Because it helps to find people from my contacts without having to ask them for their username."* Others seemed to have potential privacy concerns in mind, but found Instagram to be *"safe enough to be trusted"*, or the prompt to be *"relatively trustworthy"*.

Participants who chose to not allow Instagram access to their contacts stated several motives not to do so. While around one third stated that they *"just don't need that feature"* or have *"no interest in it"*, privacy protection seemed to play a role in several ways. On the one hand,

146 participants stated that they had concerns regarding their own privacy towards Instagram (e.g., *"I don't know how safe my privacy is with Facebook"*, or *"I value my privacy more than having followers"*). On the other hand, several participants expressed the wish to protect their privacy towards their contacts by stating, for example, that they *"don't want every contact on [their] phone to see or find [their] Instagram account"*, or that they *"rather keep [their] Instagram private"*. Lastly, and most interesting to our research, 41 participants (control group: 8, treatment group: 33) stated that they chose to not allow Instagram access to their address book due to their respect for their contacts' privacy rights. Participants' motives reflected our construct *RS*, for example, *"I have no right […] to share personal data of my contacts […]"* or *"I don't want to compromise my contacts' private info"*, which at the same time implicates their *RE* and *RC*. The qualitative results hence further confirm our theoretical model.

Discussion

The disclosure of our own personal information through others increasingly threatens our privacy, specifically in the context of online platforms. Leading privacy researchers have hence called for a more versatile, multilevel understanding of privacy that acknowledges the complexity of sophisticated digital environments in order to be able to explore concepts such as, for example, interdependent privacy (e.g., Bélanger & James 2020; Cao et al., 2018; Lowry, Dinev, et al., 2017). Whereas prior works on interdependent privacy have yielded important insights into the phenomenon of interdependent privacy, what has been missing is a deeper understanding of why and how users decide to either protect or violate others' privacy when interacting with online platforms, as well as an investigation of effective remedies. Our study revealed that an additional step of decision control in the form of an interdependent privacy salience nudge can decrease the likelihood that a user discloses others' information by 62%. Moreover, our results indicate a serial mediation through users' *RE*, *RC*, and *RS* when forming the decision to disclose others' personal data. Our study holds important implications for the emerging field of research on interdependent privacy in both theory and practice, which we will elaborate on in the following.

Contributions to interdependent privacy literature

We believe that our study contributes to interdependent privacy research in three particular ways. Our first contribution lies in the investigation of the interdependent privacy nudge itself. To our knowledge, this is one of the first works to explore the efficacy of an interdependent privacy salience nudge in a user study. Our interdependent privacy salience nudge was designed to increase the salience of the data and the data transfer as well as the salience of potential co-owners of the data. To do so, we implemented an opt-in mechanism, framing, as well as transparent privacy-related information as nudging mechanisms in alignment with prior literature (Kamleitner & Mitchell, 2019; Schöbel et al., 2020). Our experimental results show that the implementation of our nudge yielded a 62% decrease in participants' disclosure of others' personal information. This suggests a need for more transparent and salient communication of interdependent privacy implications on online platforms.

A second, broader contribution of this study relates to the theoretical mechanisms through which our interdependent privacy salience nudge decreases individuals' disclosure behavior. Manipulating the salience of the data transfer and the salience of the other, our data indicates that users' protection of others' privacy rights unfolds through a complete serial mediation of three consecutive stages as theorized by Kamleitner and Mitchell (2019). Our results hence empirically validate the 3R framework. However, while Kamleitner and Mitchell (2019) have proposed *RE*, *RC*, and *RS* to be three consecutive and hierarchically dependent steps, we found that the interdependent privacy salience nudge directly increases both *RE* and *RC*, and that there is a significant mediation path IPN → RC → RS → DOI. These findings deviate from the 3R framework, in that *RC* can be increased without relying on *RE* as a prerequisite. Our results advance our understanding of how interventions, such as our *IPN*, can act as effective remedies against interdependent privacy violations.

Our third contribution is of methodological nature and lies in the development and validation of a measurement instrument to capture users' *RE*, *RC*, and *RS* when disclosing others' information. Our measurement instrument allows to zoom into the micro-level processes of users' decision-making and might be useful for future studies in this field.

Implications for practice

Our findings suggest implications for both policy-makers and online platform user interface designers. Current regulations, such as the European Union GDPR, do not sufficiently consider interdependent privacy infringements (Kamleitner & Mitchell, 2019; Symeonidis et al., 2018). This presents a loophole for online platform providers to intrude individuals' privacy rights through their peers. While online platforms ask the user for their consent (e.g., "Allow Access") when sharing others' information, the numerous data subjects that are involved in the data transfer are neither notified nor given the possibility to opt out. As demonstrated in our vignette scenario, around one fifth of Instagram users would give Instagram access to their address book in a real-world scenario, hence disclosing potentially hundreds of names, phone numbers, email addresses, and the like. Our results reveal useful insights for regulators, as they show the potential

of providing users with design elements that increase the salience of the data transfer and the salience of the other. While, in a privacy-wise ideal world, users would not be allowed to share others' personal data without each of their co-owners' consent, this is not feasible in today's interconnected environment. However, we show that enabling users to make an informed decision about the disclosure of others' personal information can reduce interdependent privacy violations significantly. The significant indirect effect path (IPN → RE → DOI) reveals that social online platforms have potential for improvement in transparently communicating their practices for data collection and usage in general, since users seem to not be aware of the fact that data as a good is being transferred to the platform when, e.g., synchronizing contacts, let alone that this data belongs to other individuals. The introduction of the GDPR, which demands for mandatory opt-in mechanisms when giving access to one's own information, has proven to improve the transparency and visual representation of organizations' privacy policies (Linden et al., 2020). We argue that a future refinement of the GDPR should include mandatory and informative opt-in mechanisms when disclosing others' data, and hope that our work can inform future policy-making.

As for online platform providers, prior research has demonstrated that users' privacy concerns impact their choice of and behavior on online platforms (Gal-Or et al., 2018; Liu et al., 2021; Tsai et al., 2011) to the point where businesses might be able to leverage privacy protection as a selling point. The evaluation of our interdependent privacy salience nudge can serve as a starting point for the design of user interfaces where users can make informed decisions regarding interdependent privacy.

Limitations and directions for future research

Despite the aforementioned theoretical and practical contributions of this research, our study is subject to several limitations, which open up a series of exciting venues for future research. Whereas our interdependent privacy salience nudge can serve as a starting point, we acknowledge that a more detailed evaluation of the individual nudging mechanisms (e.g., the default mechanism, the warning sign, or privacy-related information) is vital for the design of real-world interdependent privacy interventions. Prior research revealed that user-oriented information security and privacy interventions face issues such as information overload and habituation (Reeder et al., 2018; Vance et al., 2018), which have to be carefully navigated when aiming to support both individual and interdependent privacy decisions.

Our second limitation is of methodological nature. It has been argued that a research design where mediators are measured (such as the one chosen in our study) as opposed to manipulated, is problematic to justify causality (Pirlott & MacKinnon, 2016). Since participants self-select to levels of the mediating variables, they are not randomly distributed across mediator levels, and the relationship between the mediators and the dependent variable can be correlational. Our ability to infer that our three mediators indeed caused *DOI* is hence limited, and our measurement of *DOI* might be subject to alternative explanations.

Furthermore, scholars might wish to extend our study by assessing the formation of our mediating variable *RS* in more detail. Kamleitner & Mitchell (2019) have suggested social norms and self-interest as important forces influencing *RS*, which has not been covered in our study. *RS* might also be subject to cultural factors: We conducted our study drawing on a sample of EU citizens, hence in countries with relatively similar cultural backgrounds. However, prior research has demonstrated the intercultural dynamics of privacy calculus on social networking sites (Krasnova et al., 2012). Accordingly, we encourage future research to further explore interdependent privacy protection across cultures.

Lastly, even though we designed our vignette experiment with the goal to represent a realistic scenario by employing an actual Instagram prompt as well as a sample of real-world Instagram users, our study relied on hypothetical and cross-sectional observations, and hence did not allow us to investigate users while they were actually deciding on interdependent privacy protection. To further strengthen the validity of our findings, we invite future research to apply complementary research methods, such as randomized field experiments.

Conclusions

This work investigates the formation of users' interdependent privacy decisions, and how such decisions can be supported by design elements such as an interdependent privacy salience nudge. We empirically validate Kamleitner and Mitchell (2019)'s 3R Framework of Interdependent Privacy Protection by revealing a serial mediation effect of our interdependent privacy salience nudge on users' disclosure of others' information through their realization of the data transfer *(RE)*, recognition of other's ownership *(RC)* as well as respect for others' rights *(RS)*. This answers our research question RQ1, and sheds light on the steps that individuals have to take in order to be able to behave in an interdependent privacy-protecting manner. Addressing RQ2, we show that an interdependent privacy salience nudge employing an opt-in mechanism, framing, and transparent privacy-related information can support interdependent privacy protection on online platforms, with participants in the treatment group being 62% less likely to disclose others' personal information. This effect is reflected in users' qualitative statements, with participants expressing that "*it does not seem right to share other peoples' data without their consent*". Our study represents a starting point for future research on how to design usable and effective interventions for privacy protection in interdependent contexts.

Appendix

Tables 4 and 5

Table 4 Measurement items

Construct	Items
Realization of data transfer (RE) (self-developed based on Kamleitner & Mitchell 2019) ($\alpha = 0.875$)	*When deciding on how to proceed with the previous Instagram prompt, I was aware that syncing my contacts would imply…* RE1: …that I give Instagram access to data (such as names, email addresses or phone numbers). RE2: …that I share data (such as names, email addresses or phone numbers) that I own with Instagram. RE3: …that I transfer data (such as names, email addresses or phone numbers) from my belongings to Instagram. RE4: …that I make data (such as names, email addresses or phone numbers) available to Instagram that they have not had before.
Recognition of others' ownership (RC) (self-developed based on Kamleitner & Mitchell 2019) ($\alpha = 0.948$)	RC1: …that I give access to personal information of others. RC2: …that I give access to data that has been shared with me by others. RC3: …that I share data that belongs to others. RC4: …that I share the information of others in addition to my own.
Respect for others' rights (RS) (self-developed based on Kamleitner & Mitchell 2019) ($\alpha = 0.958$)	RS1: …that I treat others' privacy rights unfairly. RS2: …that I disrespect others' privacy rights. RS3: …that I treat others' personal data unlawfully. RS4: …that, before sharing others' personal data, I should have obtained their consent.
Privacy concerns towards Instagram (Pavlou et al., 2007; Smith et al., 1996) ($\alpha = 0.889$)	PC1: I am concerned about my privacy when browsing Instagram. PC2: I am concerned that Instagram is collecting too much information about me. PC3: It bothers me when Instagram asks me for personal information. PC4: My personal information could be misused when transacting with Instagram. PC5: My personal information could be accessed by unknown parties when transacting with Instagram. PC6: I have doubts as to how well my privacy is protected on Instagram.
Normative beliefs (Primack et al., 2008)	NB1: Among your peers, how socially acceptable is it to share others' information (e.g., names, phone numbers or email addresses) with platforms such as Instagram?

7-point Likert-type scales ranging from strongly disagree (1) to strongly agree (7) were used.

Table 5 Results from the serial multiple mediation analysis (coefficients and model summary information)

	M1 (RE)			M2 (RC)			M3 (RS)			Y (DOI)		
Antecedent	b	SE	p	b	SE	p	b	SE	p	b	SE	p
X (IPN)	0.397	0.134	0.0034	0.400	0.163	0.0146	0.282	0.174	0.1065	–0.475	0.420	0.2583
M1 (RE)	-	-	-	0.702	0.067	0.0000	0.018	0.082	0.8292	–0.429	0.146	0.0033
M2 (RC)	-	-	-	-	-	-	0.669	0.059	0.0000	–0.123	0.138	0.3708
M3 (RS)	-	-	-	-	-	-	-	-	-	–0.314	0.133	0.0185
Constant	5.134	0.481	0.0000	–0.163	0.668	0.8075	1.881	0.667	0.0051	4.354	1.578	0.0058
	$R^2=0.061$			$R^2=0.321$			$R^2=0.445$			Nagelkerke $R^2=0.409$		
	$F=2.98$; $p<.01$			$F=18.98$; $p<.001$			$F=28.52$; $p<.001$			Omnisbus model $\chi2=83.02$; $p<.001$		

All controls were included in the analysis as described in the section "Serial mediation analysis through the lens of the 3R framework" section

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., & Sleeper, M. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR), 50*(3), 1–41. https://doi.org/10.1145/3054926

Almuhimedi, H., Schaub, F., Sadeh, N., Adjerid, I., Acquisti, A., Gluck, J., Cranor, L. F., & Agarwal, Y. (2015). Your location has been shared 5,398 times! A field study on mobile app privacy nudging. *Proceedings of the 33rd annual ACM conference on human factors in computing systems,* Seoul. https://doi.org/10.1145/2702123.2702210

Alsarkal, Y., Zhang, N., & Xu, H. (2018). Your privacy is your friend's privacy: Examining interdependent information disclosure on online social networks. *Proceedings of the 51st Hawaii International Conference on System Sciences*, Hawaii.

Avgerou, C. (2013). Social mechanisms for causal explanation in social theory based IS research. *Journal of the Association for Information Systems, 14*(8), 3. https://doi.org/10.17705/1jais.00341

Barev, T. J., Janson, A., & Leimeister, J. M. (2020). Designing effective privacy nudges in digital environments: A design science research approach. In *International Conference on Design Science Research in Information Systems and Technology*. Kristiansand/Virtual.

Bélanger, F., & James, T. L. (2020). A theory of multilevel information privacy management for the digital era. *Information Systems Research, 31*(2), 510–536. https://doi.org/10.1287/isre.2019.0900

Benlian, A., Klumpe, J., & Hinz, O. (2020). Mitigating the intrusive effects of smart home assistants by using anthropomorphic design features: A multimethod investigation. *Information Systems Journal, 30*(6), 1010–1042. https://doi.org/10.1111/isj.12243

Biczók, G., & Chia, P. H. (2013). Interdependent privacy: Let me share your data. *International conference on financial cryptography and data security,* Okinawa.

Biczók, G., Huguenin, K., Humbert, M., & Grossklags, J. (2021, March). Call for Papers: Special issue on managing multi-party, interdependent privacy risks. *Computers & Security*

Cao, Z., Hui, K. L., & Xu, H. (2018). An economic analysis of peer disclosure in online social communities. *Information Systems Research, 29*(3), 546–566. https://doi.org/10.1287/isre.2017.0744

Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019). 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, Glasgow*

Casciano, R., & Massey, D. S. (2012). Neighborhood disorder and anxiety symptoms: new evidence from a quasi-experimental study.

Health & Place, 18(2), 180–190. https://doi.org/10.1016/j.healthplace.2011.09.002

Chen, J., Ping, J. W., Xu, Y., & Tan, B. C. (2015). Information privacy concern about peer disclosure in online social networks. *IEEE Transactions on Engineering Management, 62*(3), 311–324. https://doi.org/10.1109/Tem.2015.2432117

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika, 16*(3), 297–334. https://doi.org/10.1007/BF02310555

Dienlin, T., & Metzger, M. J. (2016). An extended privacy calculus model for SNSs: Analyzing self-disclosure and self-withdrawal in a representative US sample. *Journal of Computer-Mediated Communication, 21*(5), 368–383. https://doi.org/10.1111/jcc4.12163

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

European Parliament and Council (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union.*

Gal-Or, E., Gal-Or, R., & Penmetsa, N. (2018). The role of user privacy concerns in shaping competition among platforms. *Information Systems Research, 29*(3), 698–722. https://doi.org/10.1287/isre.2017.0730

Garcia, D. (2017). Leaking privacy and shadow profiles in online social networks. *Science Advances, 3*(8), e1701172. https://doi.org/10.1126/sciadv.1701172

Harwell, D., & Harris, S. (2021). *White House has spoken to Israeli officials about spyware concerns following Pegasus Project revelations*.The Washington Post. Retrieved 06.08.2021 from https://www.washingtonpost.com/technology/2021/07/29/pegasus-white-house-israel-concerns/

Hayes, A. F. (2018). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford Publications.

Humbert, M., Trubert, B., & Huguenin, K. (2019). A survey on interdependent privacy. *ACM Computing Surveys (CSUR), 52*(6), 1–40. https://doi.org/10.1145/3360498

Isaak, J., & Hanna, M. J. (2018). User data privacy: Facebook, Cambridge Analytica, and privacy protection. *Computer, 51*(8), 56–59. https://doi.org/10.1109/Mc.2018.3191268

Jia, H., & Xu, H. (2016). Autonomous and interdependent: Collaborative privacy management on social networking sites. *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, San Jose.

Kamleitner, B., & Mitchell, V. (2019). Your data is my data: a framework for addressing interdependent privacy infringements. *Journal of Public Policy & Marketing, 38*(4), 433–450. https://doi.org/10.1177/0743915619858924

Kamleitner, B., & Sotoudeh, M. (2019). Information sharing and privacy as a socio-technical phenomenon: Interview with Bernadette Kamleitner. *TATuP-Zeitschrift für Technikfolgenabschätzung in Theorie und Praxis, 28*(3), 68–71. https://doi.org/10.14512/tatup.28.3.68

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal, 25*(6), 607–635. https://doi.org/10.1111/isj.12062

Knijnenburg, B. P., Page, X., Wisniewski, P., Lipford, H. R., Proferes, N., & Romano, J. (2022). *Modern Socio-Technical Perspectives on Privacy*. Springer Nature. https://doi.org/10.1007/978-3-030-82786-1

Krasnova, H., Veltri, N. F., & Günther, O. (2012). Self-disclosure and privacy calculus on social networking sites: the role of culture. *Business & Information Systems Engineering, 4*(3), 127–135. https://doi.org/10.1007/s12599-012-0216-6

Li, H., Yu, L., & He, W. (2019). The impact of GDPR on global technology development. *Journal of Global Information Technology Management, 22*(1), 1–6. https://doi.org/10.1080/1097198x.2019.1569186

Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The privacy policy landscape after the GDPR. *Proceedings on Privacy Enhancing Technologies* (1), 47–64.

Liu, B. L., Pavlou, P. A., & Cheng, X. F. (2021, Oct). Achieving a balance between privacy protection and data collection: A field experimental examination of a theory-driven information technology solution. *Information Systems Research* (forthcoming). https://doi.org/10.1287/isre.2021.1045

Lowry, P. B., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546–563. https://doi.org/10.1057/s41303-017-0066-x

Lowry, P. B., Moody, G. D., & Chatterjee, S. (2017). Using IT design to prevent cyberbullying. *Journal of Management Information Systems, 34*(3), 863–901. https://doi.org/10.1080/07421222.2017.1373012

Marsch, M., Grossklags, J., & Patil, S. (2021). Won't you think of others?: Interdependent privacy in smartphone app permissions. *Proceedings of the ACM on Human-Computer Interaction, 5*(CSCW2), 1–35.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*(3), 551–569. https://doi.org/10.1007/s10551-015-2565-9

Mayring, P. (2014). *Qualitative content analysis: theoretical foundation, basic procedures and software solution.* Klagenfurt.

MacKenzie, S. B., Podsakoff, P. M., & Podsakoff, N. P. (2011). Construct measurement and validation procedures in MIS and behavioral research: Integrating new and existing techniques. MIS Quarterly, 293–334.

Moore, G. C., & Benbasat, I. (1991). Development of an instrument to measure the perceptions of adopting an information technology innovation. *Information Systems Research, 2*(3), 192–222.

Olteanu, A. M., Huguenin, K., Dacosta, I., & Hubaux, J. P. (2018). Consensual and privacy-preserving sharing of multi-subject and interdependent data. In *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS).*

Palan, S., & Schitter, C. (2018). Prolific.ac-A subject pool for online experiments. *Journal of Behavioral and Experimental Finance, 17,* 22–27. https://doi.org/10.1016/j.jbef.2017.12.004

Pavlou, P. A., Liang, H. G., & Xue, Y. J. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal-agent perspective. *MIS Quarterly, 31*(1), 105–136.

Pirlott, A. G., & MacKinnon, D. P. (2016). Design approaches to experimental mediation. *Journal of Experimental Social Psychology, 66,* 29–38. https://doi.org/10.1016/j.jesp.2015.09.012

Primack, B. A., Sidani, J., Agarwal, A. A., Shadel, W. G., Donny, E. C., & Eissenberg, T. E. (2008). Prevalence of and associations with waterpipe tobacco smoking among US university students. *Annals of Behavioral Medicine, 36*(1), 81–86. https://doi.org/10.1007/s12160-008-9047-6

Pu, Y., & Grossklags, J. (2015). Using conjoint analysis to investigate the value of interdependent privacy in social app adoption scenarios. *Proceedings of the International Conference on Information Systems,* Fort Worth, United States.

Pu, Y., & Grossklags, J. (2017). Valuating friends' privacy: Does anonymity of sharing personal data matter? *Thirteenth symposium on usable privacy and security* (SOUPS 2017), Santa Clara.

Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., & Egelman, S. (2018). An experience sampling study of user

reactions to browser warnings in the field. In *Proceedings of the 2018 CHI conference on human factors in computing systems*.

Schneider, C., Weinmann, M., & Vom Brocke, J. (2018). Digital nudging: guiding online user choices through interface design. *Communications of the ACM, 61*(7), 67–73. https://doi.org/10.1145/3213765

Schöbel, S., Barev, T., Janson, A., Hupfeld, F., & Leimeister, J. M. (2020). Understanding user preferences of digital privacy nudges–a best-worst scaling Approach. In *Proceedings of the 53rd Hawaii International Conference on System Sciences.*

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167–196. https://doi.org/10.2307/249477

Squicciarini, A. C., Shehab, M., & Paci, F. (2009). Collective privacy management in social networks. In *Proceedings of the 18th international conference on World wide web,* Madrid.

Statista (2021). *Most popular social networks worldwide as of July 2021, ranked by number of active users*. Retrieved 04.08.2021 from https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Symeonidis, I., Biczók, G., Shirazi, F., Pérez-Solà, C., Schroers, J., & Preneel, B. (2018). Collateral damage of Facebook third-party applications: a comprehensive study. *Computers & Security, 77,* 179–208. https://doi.org/10.1016/j.cose.2018.03.015

Thaler, R., & Sunstein, C. (2008). *Nudge: improving decisions about health, wealth and happiness Penguin*. Penguin Books.

Thomas, K., Grier, C., & Nicol, D. M. (2010). Unfriendly: Multi-party privacy risks in social networks. In *10th Privacy Enhancing Technologies Symposium*, Berlin.

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

Valentine, K. A., Li, N. P., Penke, L., & Perrett, D. I. (2014). Judging a man by the width of his face: The role of facial ratios and dominance in mate choice at speed-dating events. *Psychological Science, 25*(3), 806–811. https://doi.org/10.1177/0956797613511823

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly, 42*(2), 355–380. https://doi.org/10.25300/Misq/2018/14124

Wang, Y., Leon, P. G., Acquisti, A., Cranor, L. F., Forget, A., & Sadeh, N. (2014). A field trial of privacy nudges for facebook. In *Proceedings of the SIGCHI conference on human factors in computing systems*, Toronto.

Warkentin, M., Goel, S., & Menard, P. (2017). Shared benefits and information privacy: what determines smart meter technology adoption? *Journal of the Association for Information Systems, 18*(11), 3. https://doi.org/10.17705/1jais.00474

Westin, A. F. (1970). *Privacy and Freedom*. Ig Publishing.

Wirth, J., Maier, C., Laumer, S., & Weitzel, T. (2019). Perceived information sensitivity and interdependent privacy protection: a quantitative study. *Electronic Markets, 29*(3), 359–378. https://doi.org/10.1007/s12525-019-00335-0

Zhang, B., & Xu, H. (2016). Privacy nudges for mobile applications: Effects on the creepiness emotion and privacy attitudes. In *Proceedings of the 19th ACM conference on computer-supported cooperative work & social computing*, San Francisco.