Journal of Business Ethics
https://doi.org/10.1007/s10551-024-05649-4

ORIGINAL PAPER

Selling Who You Know: How We Justify Sharing Others' Data

Susanne Ruckelshausen[1] · Bernadette Kamleitner[1] · Vincent Mitchell[2]

Received: 29 September 2022 / Accepted: 22 February 2024

Abstract
Many apps request access to users' contacts or photos and many consumers agree to these requests. However, agreeing is ethically questionable as it also gives apps access to others' data. People thus regularly infringe each other's information privacy. This behavior is at odds with offline practices and still poorly understood. Introducing a novel application of the theory of neutralization, we explore how people justify the giving away of others' data and the emerging norms surrounding this behavior. To obtain a deeper understanding of the potentially ambiguous norms surrounding the behavior, we investigate how people justify, i.e., neutralize, the behavior from both offender and victim perspectives. Across four studies, offenders appear more likely to admit to moral wrongdoing than victims assume. This suggests moral disagreement between offenders and victims. The discrepancy appears to be reasonably robust across different samples, apps and whether the other is identified, but diminishes when people learn how easily others' data could be protected. These insights offer suggestions for businesses, consumers and public policy.

Keywords Justification · Sharing personal data · Interdependent privacy · Neutralizations · Responsibility taking · Victim and offender perspectives · Social norms

Introduction

Almost every person holds information about others. This means we can share information about each other, which, in turn, decreases the degree to which we can self-protect our privacy. Privacy interdependence is a substantial privacy threat (for some potential consequences, see Chaudhry et al., 2015; Humbert et al., 2019), and many large online businesses, like Meta, harvest this third-party data for profit (Nunan & Di Domenico, 2013; Sarigol et al., 2014). People who share others' data may sometimes consider the benefits for the other person when they make the decision to share data about others, for example when recommending others in a referral program. However, in many interdependent privacy situations the direct benefits to others are limited or unclear. This also holds for app-driven privacy infringements. In an age in which everyone has others' data on their mobile phones (e.g., contacts, photos and messages) and apps regularly request access to these data, this is an important ethical phenomenon. To illustrate, consider the Cambridge Analytica scandal: although only 270,000 users had installed the app-based quiz on Facebook, data were eventually harvested from 87 million users (Lapovsky, 2018).

Notably, giving away the data of others without their knowledge or permission is ethically questionable. In the analogue world, giving away the personal data of very many others is considered morally wrong (Petronio, 2015) and people commonly obtain permission before agreeing to share the contact details of a single person, let alone all their contacts. How can these same people then apparently justify the giving away of others' data to an app? This is particularly relevant, given that the scale of app-driven privacy infringements means consumers are likely to be both victims and offenders. While a lack of awareness has been highlighted as an issue (Kamleitner & Mitchell, 2019), 70% of a student sample and 65% of a UK Prolific sample decided to continue using a social media app even after they had been made aware (Kamleitner et al., 2018). This implies awareness on its own may have limited impact on reducing the behavior.

Susanne Ruckelshausen
Susanne.Ruckelshausen@wu.ac.at

Vincent Mitchell
vince.mitchell@sydney.edu.au

[1] Department of Marketing, Institute for Marketing and Consumer Research, Vienna University of Economics and Business (WU Vienna), Vienna, Austria

[2] Department of Marketing, University of Sydney Business School, Sydney, Australia

Published online: 23 May 2024

Addressing the question of how people justify giving away the data of others in an app, our research draws on the theoretical lens of the theory of neutralization (Kaptein & van Helvoort, 2019). This theory captures nuanced justifications that people use to neutralize, any guilt and blame after having engaged in deviant behavior. The way people justify themselves holds information about the degree to which they perceive a behavior to need justifying, i.e., how much this behavior is a norm violation. This offers a novel application of the theory of neutralization, namely, that people's justifications of an act can be used to investigate its normative acceptability. In situations where norms are ambiguous or evolving (such as the sharing of others' data through apps) and where individuals may feel uncertain about what is right or wrong, the way they justify a behavior can provide valuable insights into the emerging norms. In addition, responding to recent comments that the victim–offender overlap has not received sufficient attention in examining the explanation and control of misdemeanors (Berg & Schreck, 2022, p. 278), we empirically explore offenders' justifications, and the justifications victims expect them to adopt. This novel juxtaposition of perspectives allows a unique window into the interplay of norms surrounding the giving away of others' data in apps. Since justifications mirror actions, the dynamic interaction between the rationales offered by offenders and the perceptions of victims also suggests the direction the formation of norms is likely to take.

This research contributes to the literature in several ways. To the interdependent privacy literature (e.g., Demmers et al., 2022; Kamleitner & Mitchell, 2019; Pu & Grossklags, 2016; Woods & Böhme, 2022), we provide novel insights into the justifications and moral considerations behind the widespread and problematic behavior of app-driven privacy infringements. To the literature on neutralizations (Kaptein & van Helvoort, 2019; Sykes & Matza, 1957; Willison & Warkentin, 2013), we contribute in three ways. First, we add another important context for elucidating context-specific neutralizations. Second, we introduce a novel application showing how neutralizations can provide insights on norms and their formation. Third, we show how this theory can be applied to explore and contrast perspectives other than that of the offender, in our case the victim perspective (Berg & Mulford, 2020; Gottfredson & Hirschi, 1990). This novel twist allows for a better understanding of how neutralizations operate in circumstances where offenders are also victims at different times. We also show how this novel twist provides insights into the moral dynamics of the behavior and the formation of norms around it. Finally, and based on our qualitative insights, we also add to neutralization theory by allowing for the possibility that people may decide not to neutralize their privacy-infringing behavior.

The paper is structured as follows: We first briefly outline the key phenomenon of interest and why sharing others' data with an app ought to be considered wrong thus requiring justification. We next conceptually integrate the categories of neutralization and literature on norms and the victim–offender perspective before exploring the use of neutralizations empirically. An initial qualitative pilot study supports the merit of perspective taking and suggests the addition of a "responsibility acceptance" (non-neutralization) category. Three subsequent quantitative studies systematically vary victim–offender perspectives and details of the app-driven privacy infringement allowing us to explore the moral dynamics of the behavior. We conclude by outlining the theoretical and practical implications of our insights and by highlighting future research opportunities.

Theoretical Background

Interdependent Privacy Infringements

In general, interdependent privacy refers to situations in which the "actions of some individuals affect the privacy of others" (Humbert et al., 2019, p. 3). Digitalization has enormously boosted the potential of interdependent privacy infringements and an increasing number of scholars (for a review, see Humbert et al., 2019) are starting to address the topic (e.g., Biczók & Chia, 2013; Pu & Grossklags, 2016; Sarigol et al., 2014; Woods & Böhme, 2022) including its potential for harm (Harkous & Aberer, 2017; Olteanu et al., 2017).

In the context of apps, consumers regularly click accept to requests for data about others (Pu & Grossklags, 2016) and consequently, peer-privacy protection frequently fails (Symeonidis et al., 2016; Woods & Böhme, 2022). Although technically avoidable, this is true for almost all social media apps and happens for various other applications such as TripAdvisor, where the likelihood that the information of other people gets collected can be greater than 80% (Symeonidis et al., 2018).

Existing research has started to examine the user side of the phenomenon. The empirical evidence to date suggests that people tend to value their own information more highly than the information of others (e.g., Pu & Grossklags, 2016) and largely volunteer others' data without realizing they are doing so (Franz & Benlian, 2022; Kamleitner & Mitchell, 2019). Failure to realize that data, and any data transfer, are also about others explains a large part of the problem. For example, in a social media app download simulation, 95% of students and 71% of the general public were unable to correctly recall what data they volunteered to an app and 42% of students and 49% of the general public did not realize that permissions could involve contacts or pictures that could infringe on the data rights of people other than themselves (Kamleitner et al., 2018).

Clearly, awareness is an important part of the issue, but people have also been observed to continue giving away others' data even once they have been made aware. For example, Kamleitner et al. (2018) found that 65% of the general population and 70% of a student sample said they would keep an app despite knowing that it infringed on others' data. In a recent experimental simulation (Franz & Benlian, 2022), a salience nudge requesting to actively confirm others' consent (taken from Kamleitner & Mitchell, 2019) reduced the probability that people would disclose others' data by 62%. This is an impressive effect, but it still implies that 38% were prepared to wrongly claim (in a simulation with no consequences for themselves) that they had obtained the consent of all of their contacts (for other instances of the conscious giving away of others' data, see Demmers et al., 2022).

Despite the behavior of accepting an app's request to others' data being widespread, it is arguably morally wrong. At least that is what it would be if judged against the social norms of the offline world. Offline, implicit norms have been negotiated about "what, why, and to whom information is shared within specific relationships" (Martin, 2016, p. 551). When asked in person, people do not commonly pass on their friends' contact details without first obtaining their consent (Kamleitner & Mitchell, 2019; Petronio, 2000). This reigning social norm exists for a good reason. Costs or difficulties arising from the sharing of others' data in an app download context tend to be borne by others, which is why it has been linked to the economic concept of negative externalities (Biczók & Chia, 2013). In fact, the potential for harm from app-driven privacy infringements is massive as illustrated by the Cambridge Analytica case. Online, more data can be shared more quickly and there is more potential for third party use or abuse of others' data. In view of its long-term potential for harm, one might expect that people would condemn the practice of giving away others' data via apps.

One might also expect that it might be prohibited from a legal perspective. However, privacy and data protection laws vary from country to country. To illustrate the complexities, consider the key regulation about privacy in the European Union, the General Data Protection Regulation. Article 2 (2) (c) of the GDPR specifically excludes the processing of personal data by an individual solely for the purpose of personal or family-related activities (Bergauer, 2020). However, when controllers or processors facilitate personal data processing for such activities (for instance, providing software or tools), the GDPR still applies.[1] Additionally, the exception does not apply if the processing of personal data is driven by an underlying economic motive (Zukic, 2019). The first point to be determined is thus whether GDPR applies at all. If applicable in a particular case, the next question is whether one of the lawful grounds for data processing, i.e., consent by the data subject (Article 6) or legitimate interest, is present. If consent applies, then Article 7 specifies that informed consent requires notification of the original data owner together with easy withdrawal of consent. GDPR emphasizes explicit consent, which Faden and Beauchamp (1986) define as consent given by a subject with a substantial understanding of the transaction, in substantial absence of coercion by others, intentionally, and authorizing a certain course of action. Evidently, people do not provide explicit consent when others share their data without them being notified. That leaves the issue of implied consent, which occurs when individuals take an action that presupposes consent to specific privacy practices, policies, or other agreements without formally providing verbal or written permission (Veatch, 2007). However, when providing a colleague, friend or acquaintance with personal information, the lack of realization documented in prior research (Franz & Benlian, 2022; Kamleitner & Mitchell, 2019) combined with reigning social norms (Petronio, 2000) suggests that people do not commonly presuppose that their data will be handed on to third parties. In addition, it may not always be clear who the data owner is. For example, some personal data, such as conversations and pictures, may have joint ownership. Given these complexities, there is a potential legal threat to the individual private offender and companies who collect third-party data (Kamleitner et al., 2018). In this research, we aim to explore how people justify this morally and legally questionable behavior by drawing on the theory of neutralization and its ability to provide a glimpse of the presence of norms surrounding a behavior.

Theory of Neutralization

Neutralizations are explanations that people use to help "argue away, fully or partly, someone's responsibility" for a harmful behavior so that an offender experiences no or less guilt (Kaptein & van Helvoort, 2019, p. 4) and averts or reduces repercussions. Neutralizations have become one of the most commonly used concepts to understand and explain morally questionable behavior and people's propensity to repeat such behaviors (Serviere-Munoz & Mallin, 2013).

[1] This Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity and thus with no connection to a professional or commercial activity. Personal or household activities could include correspondence and the holding of addresses, or social networking and online

Footnote 1 (continued)

activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities. https://www.privacy-regulation.eu/en/recital-18-GDPR.htm

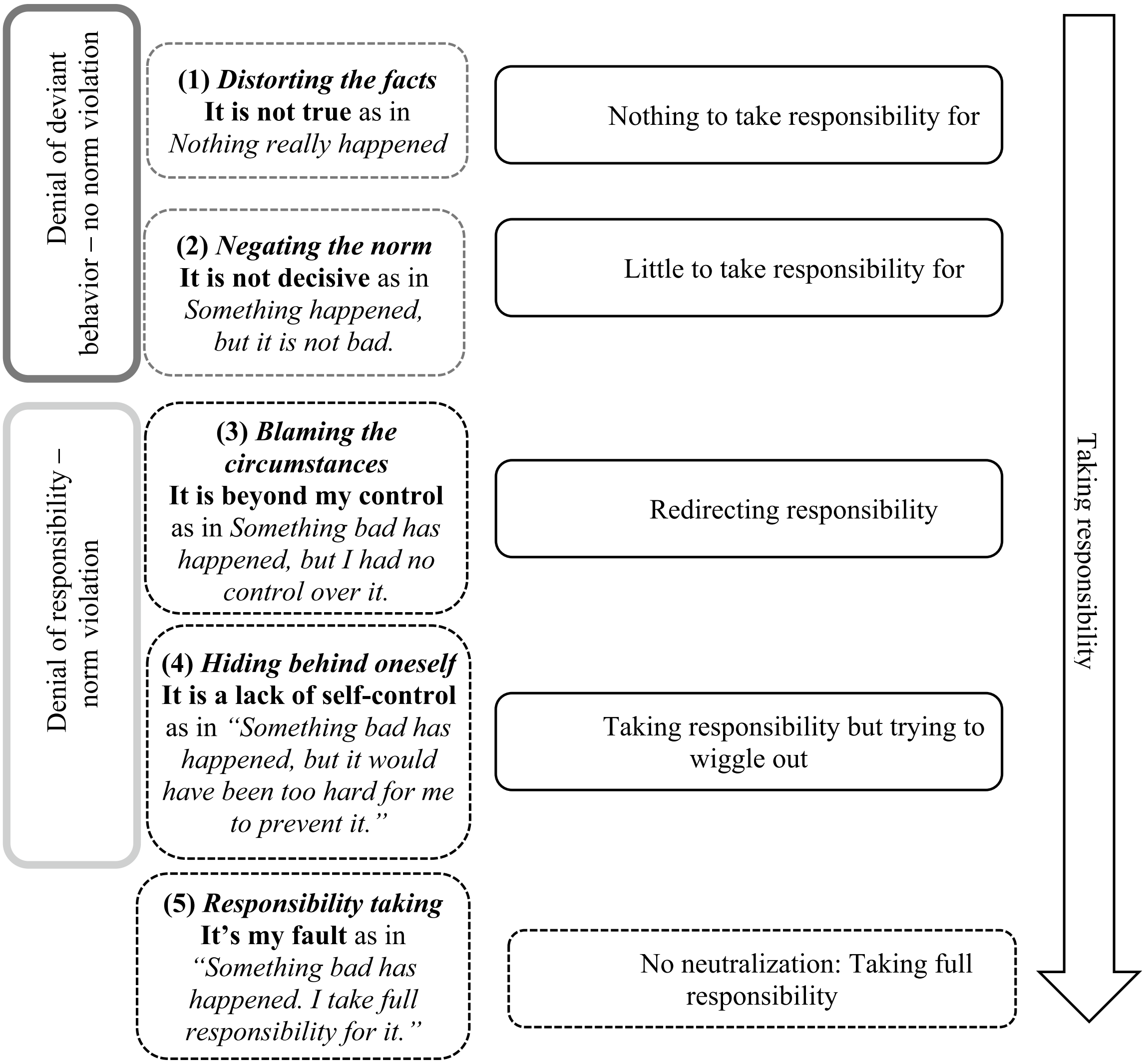

Denial of deviant behavior – no norm violation
(1) *Distorting the facts*
It is not true as in
Nothing really happened
(2) *Negating the norm*
It is not decisive as in
Something happened, but it is not bad.
Denial of responsibility – norm violation
(3) *Blaming the circumstances*
It is beyond my control
as in *Something bad has happened, but I had no control over it.*
(4) *Hiding behind oneself*
It is a lack of self-control
as in *"Something bad has happened, but it would have been too hard for me to prevent it."*
(5) *Responsibility taking*
It's my fault as in
"Something bad has happened. I take full responsibility for it."
Nothing to take responsibility for
Little to take responsibility for
Redirecting responsibility
Taking responsibility but trying to wiggle out
No neutralization: Taking full responsibility
Taking responsibility

Fig. 1 An extended list of categories of neutralization along a responsibility allocation continuum. *Note* Distribution of predominant categoriesDistribution of predominant categories of Adapted from Kaptein and van Helvoort (2019). The fifth category has been added in response to the results of our pilot study and in response to our novel application of neutralization theory, i.e., using justifications to infer the presence of (strict) norms

Developing the original five techniques first identified by Sykes and Matza (1957), other work has applied and adapted these to numerous contexts such as employees' unauthorized use of IT devices (Silic et al., 2017), app developers' ethical conceptions (Shilton & Greene, 2019) or the illegal sharing and downloading of files in a peer-to-peer context (Cohn & Vaccaro, 2006; Harris & Dumas, 2009; Odou & Bonnin, 2014). In an effort to deepen and consolidate the various applications of the theory of neutralization, Kaptein and van Helvoort (2019) have developed a comprehensive theoretical framework which organizes 60 specific techniques into four generic categories of neutralization. Figure 1 illustrates them.

These categories are formulated at a higher level of abstraction and can be applied across different contexts and types of transgressions including behaviors that may not even be considered wrong by many. Notably, categories differ in terms of how much they enable offenders to shift responsibility and blame away from themselves. Kaptein and van Helvoort (2019) consider these four categories of neutralizations from (1) to (4) as increasingly socially 'unsafe', meaning the closer one comes to admitting responsibility. The first two categories, (1) distorting the facts (it's not true) and (2) negating the norm (it's not decisive), depict the denying of a behavior being deviant or people's genuine belief that a behavior is morally acceptable.

The next two categories, (3) blaming the circumstances (it's beyond my control) and (4) hiding behind oneself (it's a lack of self-control), depict denying full responsibility while admitting to moral wrongdoing, i.e., to a norm violation.

Because the categories of neutralization are tied to the ease with which offenders can avoid taking responsibility (see Fig. 1), the Kaptein and van Helvoort (2019) study also provides insights about how much people feel that the behavior needs justifying. The categories thus also deliver insights into whether people feel that a behavior is morally wrong and violates a norm. In our research, we aim to make use of this little regarded implication of the framework.

Generally, literature on neutralizations has been interested in understanding how people manage to justify and even distance themselves from a norm violation. Kaptein and van Helvoort's (2019) framework, however, highlights that people's neutralizations are more than individual excuses. The categories of neutralization carry different moral weights and reflect the degree to which a behavior feels morally wrong, i.e., violates a norm. The categories of (1) distorting the facts and (2) negating the norm essentially correspond to the denial of moral wrongdoing. Individuals drawing on these categories deny the existence of a norm violation, either because they genuinely do not feel a norm has been violated or because they consider the norm is lax, debatable or not socially agreed upon. In contrast, categories (3) blaming the circumstances and (4) hiding behind oneself correspond to the admittance of a norm violation and simply differ on how a person tries to avert the blame. The categories of neutralization highlight the entanglement between justifications and norms. Importantly, the violation of norms gives rise to neutralizations, but neutralizations also provide a window on norms and their formation. In particular when norms are unclear or evolving and when uncertainty blurs moral consensus (such as in a novel moral problem), individuals' justifications provide insights on a behavior's moral acceptability that are prone to be more reliable than asking about norms directly. In other words, the process of neutralization itself can be indicative of the normative beliefs forming within a society.[2] A key merit of assessing justifications is that they hold more concrete details and are less abstract than so called norms. They are easier to grasp and thus report on concrete rather than abstract notions (Trope et al., 2007). Knowing how people justify a behavior is also useful in predicting individuals' future actions, e.g., ignore, repeat or (self-)punish the behavior, and in understanding how people will talk about the behavior from a moral perspective; after all much normative conversation centers on whether and how people justify their own or others' behaviors. In short, neutralizations allow insights on how the dialog about a (potentially) problematic behavior, its prevalence and its moral acceptability are prone to evolve over time. The moral acceptability of a behavior is, however, multi-faceted.

Moral Acceptability, Norms and the Sharing of Others' Data via Apps

Norms guide people's behaviors and inform them about what is or feels right or wrong. Those norms can be personal or social in nature and together they determine the moral acceptability of a behavior. Social norms are "a person's beliefs about the common and accepted behaviors of other people" (Schultz, 2022, p. 2) and essential enablers of human societies (Rossano, 2012). Social norms can either be descriptive or injunctive. Descriptive social norms specify what is done, i.e., provide guidance by highlighting what most others do, while injunctive norms constitute "rules or beliefs as to what constitutes morally approved and disapproved conduct" (Cialdini et al., 1990, p. 1015). Most people are intrinsically motivated to comply with social norms (Amiot et al., 2013) and noncompliance with injunctive (as opposed to descriptive) norms tends to be socially sanctioned (Lapinski & Rimal, 2005). In contrast to social norms, personal norms are internalized beliefs and values that guide an individual's behavior and emerge at the level of the individual (Schwartz, 1977). Although personal norms often reflect reigning social norms, compliance with personal norms is not based on "fear of social sanctions but the anticipation of having broken her/his personal norms" (Bamberg et al., 2007, p. 191). All norms tend to be context specific (Pedersen & LaBrie, 2008) and they can shift (Burke et al., 2010). In particular, social norms are constantly negotiated and dynamically evolve as people develop a joint understanding about new contexts (Yoshida et al., 2012).

Norms guide all human behavior including data and information sharing (Acquisti et al., 2011; Barth et al., 2006; Hoyle et al., 2020; Nissenbaum, 2004). However, in many respects app-driven privacy infringement is a new context. For one, it happens largely automatically and invisibly (Kamleitner & Mitchell, 2018). This makes the behavior hard to observe and comprehend. Yet, directly observing what others do and how others react to a behavior is an important basis for the establishment of social norms (Kenrick et al., 2003). Lack of observability also hampers blame attribution in case of harm. While sharing others' data may be legally questionable, it is often hard to prove that a specific harm has been brought about by a specific act of data sharing by a specific individual. People mostly cannot observe what others do. Upon reflection, however, most are bound to realize that they allowed apps to access others' data and other people will have provided access to their data (Kamleitner & Mitchell, 2019). The fact that people are both victims and offenders makes the establishment of norms and the corresponding forgiving and blaming complicated (Worthington Jr, 2009). It may either increase the uncertainty

[2] We thank an anonymous reviewer for summarizing our theorizing so succinctly.

around its moral acceptability or reduce the sense of norm violation (Cohen & Felson, 1979; Osgood et al., 1996).

Categories of Neutralization and Victim–Offender Perspectives

Remember that we suggest that the categories of neutralization people draw on are likely to provide information about whether they consider a behavior as morally defensible or violating a norm. Individuals' usage of categories (3) and (4) implies the admittance of a norm violation but it does not tell us what kind of norm(s) have been violated. Offenders are prone to experience guilt and justification pressure when violating either personal or social norms. Although personal norms carry more weight for an individual's immediate reaction, social norms inform about a behavior's acceptability, about "whether it is beneficial or easy to perform" (Bamberg & Möser, 2007, p. 17) and about whether offenders experience external blame on top of potential self-blame. Giving away others' data might be at odds with personal norms that respect others' privacy, yet those norms might relax over time if they are not supported by equally prohibitive social norms or legal sanction. The fact that most people are sharing others' data suggests that prohibitive injunctive social norms might be lacking. In fact, when we asked directly, 90% of a US sample said that there were no very clear norms around the behavior, yet over 80% saw it as morally wrong (see Figs. 4 and 5 in Appendix B).

But what does this presumable lack of clear social norms mean in practice? How do people translate this uncertainty into an overall moral assessment of the behavior? Do people fill the void in social norms with their personal norms, or do they interpret it to indicate moral acceptability? Answering these questions matters because it provides a window into the future prevalence of the behavior. If a lack of clear social norms is equated with normative permissiveness, there will be no social sanction and blame, even if offenders feel guilty for violating their own personal norms. The hurdle to reengage in the behavior is lower and eventually even the prohibitive personal norms may start to relax.

Personal and social norms combine to pave the way for a behavior's future prevalence. Notably, this future is shaped by how both offenders and victims think about and react to it. In the case of interdependent privacy infringements, the importance of offender and victim perspectives is particularly pronounced. After all, most people have had their data given away by others and have given away others' data themselves. Cultural theories have long taken the view that the victim–offender overlap is a product of conduct norms that endorse crime and violence (see Lauritsen & Laub, 2007). Looking only at the offender perspective provides a limited view on the behavior's moral acceptability. Consequently, we introduce perspectives (offender vs. victim) to the neutralization framework and build on the fact that people can justify their own behavior as well second-guess another's justifications. For example, when Susan learns that Fred shared her number, she may second-guess whether and how Fred would justify himself, e.g., by claiming that it wasn't ideal, but he only did what others do. This second-guess is likely to affect Susan's own behavior in the future. If she thinks that Fred didn't think it a big deal, she is likely to think it less of a big deal herself in the future (Gino & Galinsky, 2012). Both Susan's second-guess and Fred's actual justification reflect a blend of their personal and perceived social norms. However, the relative composition of this blend is likely to differ. Past literature has shown a gap between people's own attitudes and those they ascribe to others (Alicke et al., 1995; Anderson & Godfrey, 1987; Weiss et al., 2018). Research also suggests that victims and offenders do not draw on the same normative basis (McCarthy et al., 2021), with offenders being particularly likely to draw on their personal norms, which are a key source of guilt (Bamberg et al., 2007, Schwartz, 1977). By and large, offenders' neutralizations are prone to unveil both personal and social norms, but if justifications are voiced to oneself, personal norms are prone to be more decisive. In contrast, when victims second-guess offenders' neutralizations, they are prone to be based on social norms which is the common ground between victims and offenders.

Proposition 1 *There will be a difference between offenders' use of categories of neutralization and victims' second-guesses of their use. This difference provides insights on the overall social acceptability of the giving away of others' data.*

This dynamic interplay significantly shapes the development and evolution of emerging social norms related to interdependent privacy. In essence, we suggest that the ongoing interaction between offenders' justifications and victims' perceptions actively contributes to the negotiation and establishment of new societal standards in the realms of privacy and data sharing. The app-based sharing of others' data happens across a large range of apps and it arises in various interpersonal relationships. Given that social norms are often context specific (Pedersen & LaBrie, 2008) and that privacy behavior is a highly contextual phenomenon (Morando et al., 2014), these differences are likely to matter for the behavior's moral acceptability. If they do, such variations provide us with further insights on the origins and dynamics of the moral acceptability of interdependent privacy infringements. We explore two such variations: the type of app and whether the "other" is specified or not.

Some apps, such as messenger apps, are about connecting people. Other apps, such as information apps, are not. This difference plausibly affects how justifiable the sharing of others' data is deemed. Consumers may well assume that apps that connect people need others' data to properly function and this could render the sharing of others' data more acceptable. In fact, prior evidence suggests that people are particularly likely to devalue others' data when they believe that this data will improve the apps' functionality (Pu & Grossklags, 2017). We thus expect that sharing others' data may be considered less of a norm violation for communication apps than for other apps (e.g., information apps).

Proposition 2 *App type will affect the moral acceptability of sharing others' data with an app. This influence will become evident in the categories of neutralization that victims and offenders use.*

Interdependent privacy issues arise because people are socially related and there is reason to believe that knowing who exactly the other is makes a difference. Both the identification of victims and the social proximity between people affect moral judgements and decisions (Lee & Holyoak, 2020; Sah & Loewenstein, 2012). In app-based privacy infringements, specifying the other could be important in affecting the moral acceptability of the behavior for both victim and offender perspectives. Theoretically, different directions are plausible. On the one hand, findings in criminology show that putting a human face on a victim or meeting a victim helped offenders realize the extent of the consequences of their actions (Choi et al., 2011). In other words, offenders might feel more responsible toward specific others and this may translate into the use of higher categories of neutralization. On the other hand, offenders might feel more entitled to share information about specific others—in particular if they are close to them (Lerner & Mikula, 2013). It may thus be easier to justify the behavior when affecting close others. This would be equivalent to what has been found from a victim perspective. People were observed to allot less responsibility to offenders who were close to them (Hofmann et al., 2018) and to argue away moral blame when becoming the victim of the actions of a close other (Gino & Galinsky, 2012). We thus propose:

Proposition 3 *Specifying the other versus not specifying the other will affect offenders' use of categories of neutralization and victims' second-guesses of their use.*

Overview of Empirical Exploration

In four studies, we explore how offenders (are assumed to) neutralize the sharing of others' data once they learn that this is what they did when agreeing that an app can access the contacts on their phones. Our starting point for all studies is the offender's self-perspective, i.e., we query what category of neutralization offenders primarily draw on to explain their behavior. In all studies, we also explore victims' second-guesses about offenders' explanations. This contrast of perspective allows us to explore the overall moral acceptability of the behavior. To ensure the nuance of our insights, we explore the prevalence of categories of neutralizations across different situations and samples. Note that our interest in the prevalence of neutralization categories across different perspectives invites quantitative exploration. While the design we adopt closely resembles classical hypothesis testing, the spirit is not. We introduce variations to contexts as a way to probe how people currently make moral sense of contextual variations and firmly expect that specific results will change as norms evolve. Our exploratory insights thus serve as a map of the behaviors' current normative portrayal and as a benchmark for its future change.

We begin with a qualitative pilot study that reaffirms the fact that sharing others' data is morally in question. In addition, it highlights the complexity of neutralizations and the need to add a fifth "no neutralization" category to our framework. Further, it unearths the tendency of victims to take the perspective of the offender. Studies 1 and 2 next adopt a quantitative paradigm and examine what neutralization categories, including a no neutralization category, dominate and whether their relative prevalence varies across perspectives (proposition 1). Addressing proposition 2, study 1 also varies the type of app. Addressing proposition 3, study 2 additionally varies the salience of a specific "other". Study 3 finally adds additional information in response to questions arising from the prior studies. Specifically, it further enhances the realism of the study setting and it explores a potential angle to curb the behavior by making people aware that the act of sharing others' data is preventable by the press of a single button. Adding theoretical refinement, study 3 also assesses the complementary perspectives of victims' own moral judgements and offenders' second-guesses about these. Table 1 gives an overview of all three quantitative studies. Given our theoretical focus and the limitations of journal space, we only report on the categories of neutralization in our results. The methodological appendices A and B comprise the full set of items and additional analyses.

Pilot Study: A Qualitative Exploration of Responses to App-Driven Privacy Infringements

In this pilot study (reported in Appendix B), we explored 115 Austrian university students' spontaneous written reactions to a situation in which an app had been given access to another person's data. The goals of this initial study were (a) to explore whether participants would actually neutralize the behavior and consider it morally questionable and (b) to ensure that the generic descriptions of

Table 1 Overview of samples, variations and purpose for quantitative studies 1, 2, and 3

Study	Sample	Exploratory design variations		Purpose
		Perspectives	Additional features	
1	Representative Austria N = 293	Offenders' explanations vs. Victims' second-guesses	*Variation of app type:* communication app vs. information app	Explore the usage of neutralization categories across perspectives. Explore across apps that are (not) presumed to benefit from others' data in terms of functionality
2	Panelists U.S N = 348	Offenders' explanations vs. Victims' second-guesses	*Variation of other person:* specified other vs. unspecified other	Explore the usage of neutralization categories in the case of a specific app. Explore whether the identification of the other makes a difference
3	Representative Austria N = 267	Offenders' explanations vs. Victims' second-guesses Victims' explanations vs. Offenders' second-guesses	Salience of the preventable nature of the sharing of others' data by showing the consent interface	Explore what neutralization categories are used when people realize that a simple click prevents the sharing of others' data and add victims' own perspective

the categories of neutralization made sense against the backdrop of a natural discourse around the behavior. To this end, we varied whether participants adopted the role of an offender or a victim. In a lab environment, participants were randomly assigned to one of the two roles (offender vs. victim) and asked to write down their thoughts and feelings on a situation in which either they themselves had permitted a game app to access their friends' data (contact details, pictures and call logs) (offender) or in which a friend had permitted a game app to access their own data (victim). Two independent coders coded responses in terms of neutralization categories (see Fig. 1) and the presence of perspective taking.

Even though participants had not been directly asked to justify the behavior, there was evidence for the usage of all four neutralization categories, often within the same person, from both the victim and offender perspectives (for detailed results see Appendix B). The wording used to justify the behavior was often also remarkably close to the descriptions of the categories of neutralization. For example, *"At first it doesn't seem 'that bad'—but on reflection you get an uncomfortable feeling"* (female offender, aged 28) or *"Feels a bit like a loss of control. Friend is not to blame, because I also always just press 'install' without reading through the conditions"* (female victim, aged 25). Indicating a behavior with moral question marks, participants appeared to use signals from themselves and others to infer what appears acceptable (Lin & McFerran, 2016; Wenzel, 2005). Notably, multiple participants in the victim condition spontaneously put themselves in the shoes of the offender. They second-guessed offenders' thoughts and drew on what they appeared to assume was the social norm, e.g. *"I can't blame my friend, though, since everyone has done this before"* (female victim, aged 20).

The pilot study affirmed the ecological validity of our approach. It confirmed (a) that the app-driven sharing of others' data is considered morally questionable and spontaneously neutralized, (b) that people draw on multiple neutralizations and use wordings that resemble the neutralization categories, and offered the additional insight, (c) that people put into the position of a victim were prone to second-guess neutralizations on behalf of the offender. Going beyond our expectations, victims sometimes put themselves in the shoes of the offender to explicitly derive what they believe to be universally accepted norms. Finally, we also observed that the four categories of neutralization were unable to capture all the morally relevant responses. Sometimes offenders and victims did not resort to neutralization, but were willing to assume full responsibility. In our subsequent studies and in line with our novel application of the theory of neutralization as a window on a behavior's moral acceptability, we thus add a 'no neutralization' category (see Fig. 1).

Study 1: Categories of Neutralization Across Perspectives and App Types

In study 1, we examine the prevalence of neutralization categories. Specifically, we aim to assess category use by offenders and to learn about victims' corresponding second-guesses following proposition 1. To get a fuller picture of the overall moral acceptability of the behavior, we also varied the app type and examined whether the pattern of justifications used is sensitive to app type following proposition 2.

Sample and Procedure

We recruited 293 members of a representative sample of the Austrian working population via a professional online panel (53% female, 47% male, 0.3% diverse, mean age = 42.56, *SD* = 13.52). Study 1 employs a 2 (perspective: offender—self vs. victim—second-guessing offender) × 2 (app type: communication vs. information) between-subject design. Participants read about a scenario of interdependent privacy infringement before getting an opportunity to react to this situation (see Appendix A for study materials). In both conditions, an app (either a communication or information app) was said to have been granted permission to access data such as pictures and contacts. As a result, the app provider was able to access and use the data of others. Participants in the offender condition read that they gave away the data of a person close to them when installing an app. Participants in the victim condition read that a person close to them had given away their data when installing an app.

Following the scenario, participants were asked to indicate which statement best described the offender's thoughts (their own thoughts in the offender condition vs. their close other's thoughts in the victim condition) about giving away the victim's data. Participants could choose one of the following five options that represent the different categories of neutralization.

1. I do not think that anything happened at all.
2. Yes, something happened, but it really is not bad.
3. Yes, something happened that should not have happened, but it is not my fault as I did not have any real control over it.
4. Yes, something happened that should not have happened, but it really would have been difficult for me to prevent it.
5. Yes, something happened that should not have happened. I take full responsibility for it.

Additional exploratory variables that go beyond our key research question are featured in Appendix B (Table 3).

Results

Figure 2 depicts the distribution of neutralization categories across all exploratory conditions of studies 1 and 2. Darker shades indicate neutralization categories suggestive of the absence of a norm violation, while lighter shades suggest the presence of a norm violation. The top half of the figure features offenders' explanations, the bottom half features victims' second-guesses about these explanations. The boxed in area in the middle contains a summary of both studies split into perspectives.

Across conditions of study 1, we find that all categories of neutralization were used by at least part of the sample. Approximately half of the participants denied that any norm violation had occurred in response to the offender giving away the victim's data when downloading the app (53%). Of these, the majority denied that anything had happened at all (37% distorting the facts vs. 16% negating the norm). The other half of participants acknowledged the presence of a norm violation (47%) and the dominant way of doing so was to fully embrace responsibility and (self-)blame the offender (27%).

Comparing the pattern of answers across conditions puts these overall results into perspective. Overall, and speaking to the absence of a clear social norm violation, participants adopting the victim perspective tended to use the lower categories of neutralization, indicating they thought offenders were holding themselves less responsible than they actually were. This finding supports the reasoning behind proposition 1. In line with proposition 2, the imbalance between offender and victim perspectives persists across types of apps but becomes less pronounced in the case of a communication app, which reduces the propensity of responsibility taking by the offenders (see Fig. 2). Notably, while participants in the offender condition were sensitive to the context, participants in the victim condition were not. They were equally likely to excuse more (information app) and less (communication app) avoidable privacy infringements.

To determine the effects of both perspective and type of app, we conducted a multinomial logistic regression (see Table 2 for detailed results) with the no neutralization category serving as a reference category. In support of our overall observation of an effect of perspective, this factor approximated significance for the choice of all neutralization categories. Participants in the victim condition were significantly more likely to distort the facts (category 1) by indicating that the offender would think that nothing had happened (victim: 47% vs. offender: 29%) and to blame the circumstances (category 3) by maintaining that the offender had no real control over it (victim: 10% vs. offender: 3%). In contrast, participants in the offender condition indicated significantly more often they would take full responsibility for the transgression (category 5; offender: 37% vs. victim:

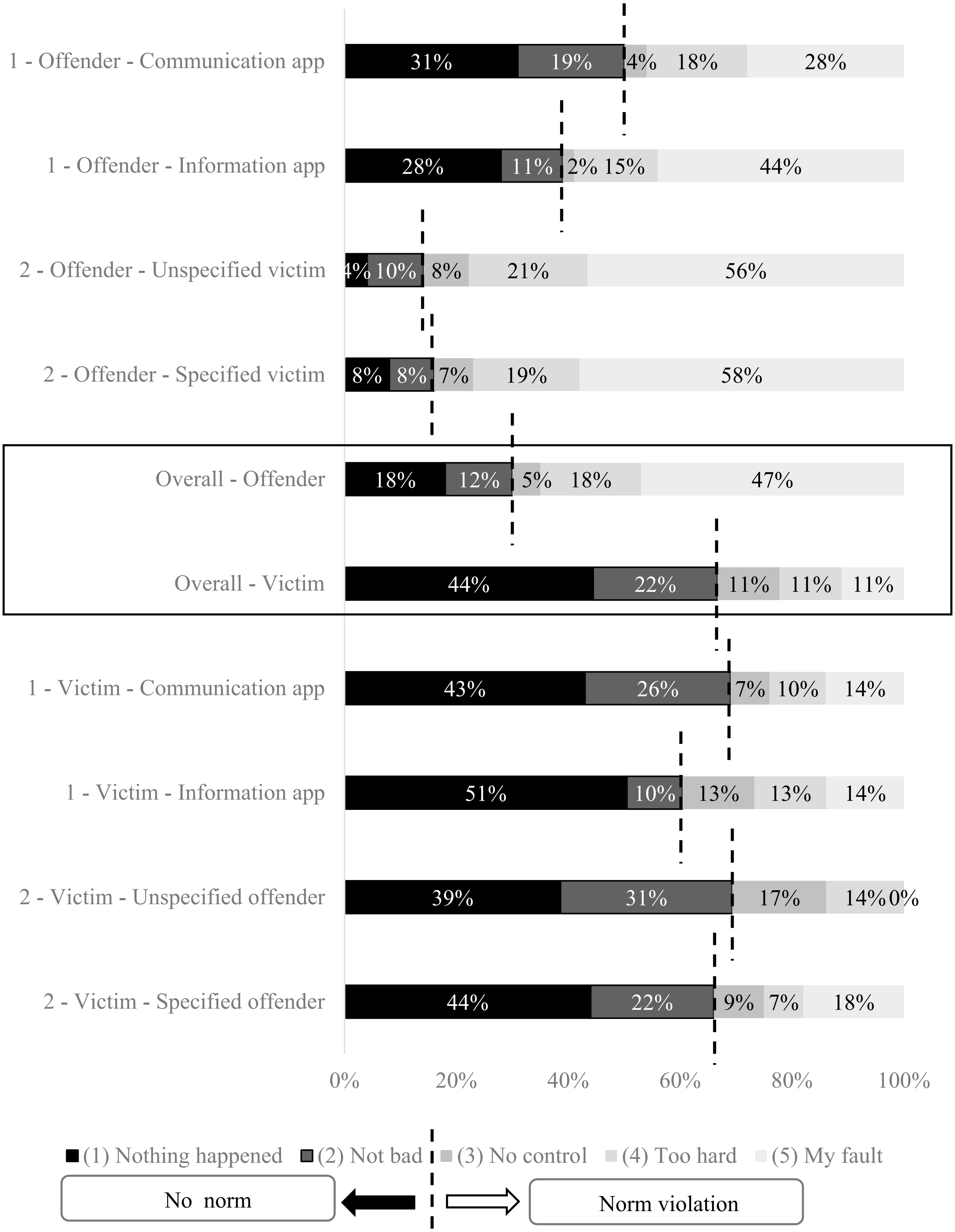


Fig. 2 Distribution of predominant categories of neutralization for each cell of studies 1 and 2. *Note* To facilitate a grasp of the bigger picture, results are sorted according to perspective rather than studies. The boxed area in the middle contains average responses per perspective across studies 1 and 2. *Note* Please note that in some cases percentages do not add up to 100 percent exactly due to rounding

14%, $\chi^2(1) = 18.93$, $p < 0.001$). Interestingly, neither an effect of app type nor an interaction effect between perspective and app type emerged. Having said that, Fig. 2 shows that this lack of significance is due to our theoretically motivated choice of reference category. In the case of the communication app, 28% of offenders were willing to take full

Table 2 Multinomial logistic regression of experimental variations on usage of neutralization categories in studies 1, 2, and 3

	Category 1 Nothing happened			Category 2 Not bad			Category 3 No control			Category 4 Too hard		
	B	Wald (df)	*p*	*B*	Wald (df)	*p*	*B*	Wald (df)	*p*	*B*	Wald (df)	*p*
Study 1 (N = 293)												
Perspective	−1.740	15.474 (1)	.000	−1.084	3.088 (1)	.079	−2.839	10.930 (1)	.001	−.967	2.976 (1)	.084
App type	−.141	.068 (1)	.794	.985	2.234 (1)	.135	−.588	.589 (1)	.443	−.182	.066 (1)	.797
Perspective * App type	.688	1.057 (1)	.304	.072	.008 (1)	.931	1.540	1.590 (1)	.207	.803	.892 (1)	.345
Study 2 (N = 348)												
Perspective	2.826	35.333 (1)	.000	2.157	18.667 (1)	.000	−2.079	5.101 (1)	.024	.248	.223	.637
Specification	−.675	1.109 (1)	.292	.241	.223 (1)	.637	.152	.076 (1)	.783	.172	.213	.644
Perspective * Specification	20.218	502.21 (1)	.000	19.725	556.46 (1)	.000	20.192	471.96 (1)	.000	20.082	–	–
Study 3 (N = 267)												
Perspective	−1.440	6.175 (1)	.013	−.952	2.151 (1)	.142	−.399	.395 (1)	.530	.037	.003 (1)	.954
Role	−2.457	14.005 (1)	.000	−1.253	3.595 (1)	.058	−1.723	5.503 (1)	.019	−1.001	2.142 (1)	.143
Perspective * Role	1.828	4.591 (1)	.032	.647	.523 (1)	.470	1.662	3.607 (1)	.058	1.362	2.868 (1)	.090

Category 5 (My fault) served as reference category

responsibility, while in the case of the information app this percentage increased to 44%. In essence, offenders were more likely to take responsibility when the app could be plausibly believed to fully function without accessing others' data.

Study 2: Categories of Neutralization Across Perspectives and (Un)specified Others

In study 1, we assessed what happens at the generic level of the problem description. We abstractly described the giving away of others' data to an app. We neither specified the exact app, nor the specific other or the exact permissions. In study 2, we deepened the exploration and went concrete. We used a mock-up news aggregator app and were clear about the permissions granted. In addition, we addressed proposition 3 and explored whether naming a concrete other affects people's use of neutralization categories.

Sample and Procedure

We recruited 348 American citizens via Prolific Academic. All participants owned a smartphone, passed attention checks, and completed the online questionnaire (49% female, 50% male, 1% other, mean age = 38.14, *SD* = 14.35). Participants were randomly assigned to one of the four experimental conditions of our 2 (perspective: offender—self vs. victim—second-guessing offender) × 2 (other: specified vs. unspecified) between-subject experimental design. The scenario was based on study 1 but instead of featuring an abstract reference to an app, participants read about and were shown a concrete news app called Spotlight News, which offers a personalized news alert service. A realistic screenshot detailed the permissions participants needed to grant.

Participants in the victim condition read that a person close to them (specified) or many other people (unspecified) had given away their data when installing Spotlight News and participants in the offender condition read that they gave away the data of a person close to them (specified) or many other people (unspecified) when installing Spotlight News. Prior to this scenario, participants in the specified other conditions were asked to name a concrete other person. To stress the manipulation, we inserted this specific name throughout the study via the piped text feature offered by Qualtrics. All key variables were assessed as in study 1 (see Appendix A, Table 4).

Results

Across conditions, 38% of the participants denied that any norm violation had occurred when the offender gave away the victim's data by downloading the app (category 1: 22% distorted the facts, category 2: 16% negated the norm) compared to 62% who acknowledged the presence of a norm violation. As in study 1, the dominant category (category 5: 37%) was to fully embrace responsibility and (self-)blame the offender followed by hiding behind oneself (category 4: 16%) and blaming the circumstances (category 3: 9%).

We regressed the categories of neutralization on the perspective, other specificity and their interaction, and again used category 5 as a reference category. Results reconfirmed the main effect of perspective and reasoning behind proposition 1 qualified by a significant interaction effect (see Table 2 for detailed results). Essentially, this interaction effect is partly in line with proposition 3. Offenders were twice as likely (4% vs. 8%) to adopt category 1 when the victim was specified compared to when the victim was not specified but there was no difference in offenders' use of categories 2, 3 and 4. In contrast, victims guessed that specified offenders as opposed to unspecified offenders would be less likely to draw on categories 2, 3 and 4. The most pronounced difference, however, emerged in victims' assumption of the use of the reference category 5. Some victims guessed that a specified offender they well knew would take full responsibility (18%) but no victim assumed that unspecified offenders would do so (0%; χ^2 (1) = 12.00, p = 0.001).

Key Insights of Studies 1 and 2

Figure 2 highlights three overarching insights. First, all categories of neutralization were used by at least part of the sample. The sharing of others' data was neither universally judged as wrong nor universally considered free from responsibility. In fact, the two opposite extremes were chosen most often: category 1 as in "nothing happened that anyone could be blamed for" and category 5 as in "something bad happened and there is no excuse". Perhaps surprisingly, participants least frequently chose category 3, blaming the circumstances as in "it was out of my control". Nearly no participants in the offender perspective resorted to this justification. Participants did not seem to see the app provider as the main culprit but to rather see this as a consumer-to-consumer issue.

Second, the perspective matters. The apparent disparity in category use across offender and victim perspectives hints at a normative disagreement between victims and offenders. Overall, offenders were more prepared to admit to wrongdoing and to take responsibility than victims second-guessed. This finding is remarkably robust across samples (Austria and USA) and contexts (types of apps and specificity of offenders). In line with our theorizing, this suggests that victims and offenders do not draw on the same normative basis (McCarthy et al., 2021). Victims substantially underestimated the extent to which offenders were willing to admit to wrongdoing. Arguably, most victims felt that offenders would not perceive the app-driven sharing of others' data as a norm violation and thus rendered the behavior socially acceptable. At the same time, sharing others' data was considered a violation of norms by most offenders.

Third, our contextual variations primarily affected participants adopting the offender's perspective. As the rather straight dotted line in the lower half of Fig. 2 illustrates, victims' second-guesses appeared insensitive to the pronounced contextual variations across and within studies 1 and 2. People likely feel uncertain about what the social norms are and infer that the app-driven sharing of others' data at least cannot be socially condemned.

Contrasting results across studies 1 and 2 yield additional contextual insights beyond app type and other specificity. Recall that another key difference between those studies was the concreteness of the scenario with study 2 providing a concrete app and an illustration of app permissions. The neutralization categories indicating the presence of a norm violation (3–5) were used more often than in study 1, in particular among offenders. While this may be a reflection of the different samples, it may also signal that a more concrete grasp of app-driven privacy infringements helps to highlight its moral doubtfulness.

Study 3: Examining Offenders' and Victims' Explanations of Each Other

Study 3 deepened the exploration in the following ways. First, it follows up on the possibility that a concrete and practical understanding of how the sharing happens may reduce its moral acceptability. We thus explored a situation in which participants understand that the sharing of others' data results from a single avoidable click. In study 3, all participants saw a pop-up window asking them to accept or refute an app's access to one's contacts.

Second, study 3 addressed another potential shortcoming of studies 1 and 2. Thus far, offenders were asked to assume that they had just given away others' data. Given the prevalence of the issue, this is an ecologically sound assumption. Yet, participants in the offender condition may not have considered this assumption to be an equally sound assumption when it comes to them personally. Offenders' preparedness to take responsibility could have been confounded with their belief that they would not have actually engaged in the behavior. The design of study 3 ensures that offenders actually agree to share others' data before being offered a chance to neutralize this behavior.

Finally, study 3 revisits the perhaps most puzzling finding of studies 1 and 2: victims' assumption that offenders would declare the behavior as normatively acceptable. This finding is concerning because it suggests that victims may fail to hold offenders responsible, allowing the problem to continue unabated. We directly address the substance of this implication by adding two additional perspectives, namely the victim's personal viewpoint, i.e., their propensity to hold the offender responsible, and the offender's second-guesses of the victim's viewpoint, i.e., offenders' expectations of potential repercussions.

Sample and Procedure

Overall, 267 participants were recruited from the same representative panel and following the same criteria as in study 1 (51% female, 49% male, 0.4% diverse, age 18 to 77 years, M = 42.43, SD = 12.81). Study 3 employs a 2 (role: offender vs. victim) × 2 (perspective: self vs. second-guessing other) between-subject design. All participants were asked to name

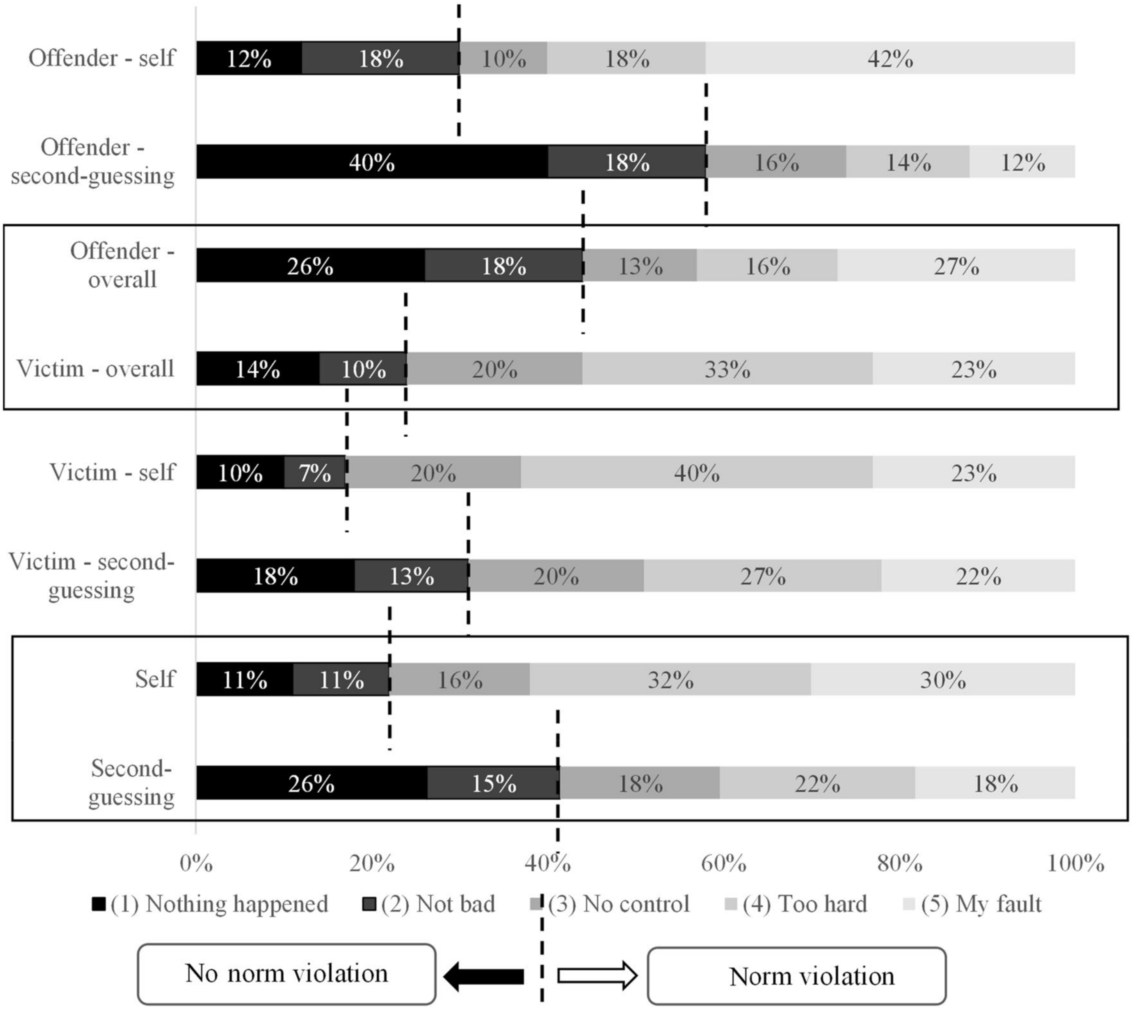


Fig. 3 Distribution of categories of neutralization per cell for study 3. *Note* Please note that in some cases percentages do not add up to 100 percent exactly due to rounding

a specific other before reading about a fictitious new messenger app called "ChitChat". Participants learned about the download process and saw a realistic pop-up message asking them to allow or deny the messenger app (ok vs. not allow) access to their contacts (see Appendix A for full materials). Participants in the offender condition had to click on one of these options. Participants in the victim condition were told that their specified close other (we inserted the specific name) had clicked "ok". We oversampled the offender condition to ensure a sufficiently large sample. Participants who clicked "not allow" (34%) were redirected to the victim condition and told that their close other had clicked "ok".[3] Next all participants were told that clicking "ok" means that either their data (victim) or their close others' data (offender) had been shared with the app. All participants next saw the same five statements as in study 1. Depending on condition, they either picked the statement that best reflected their own view of what had happened (self) or the statement that best reflected their guess of their close others' view (second-guessing). The wording was adjusted to fit to make it sound natural for all roles and perspectives.

Results and Discussion

Figure 3 summarizes results across conditions. The box in the middle summarizes responses (own neutralizations and second-guesses) of offenders and victims, respectively. The box at the bottom contrasts people's own responses with their second-guesses (regardless of role). To capture the relative importance of roles and perspectives, we again

[3] There was no significant difference in responses between those originally assigned to the victim condition and those redirected to it. We thus merged these subsamples (see Appendix B Figure 6 for a full split into subsamples).

ran a multinomial logistic regression predicting the categories of neutralization used (see Table 2) and followed up with chi^2-tests comparing specific distributions. Results replicate an earlier key observation. While a clear majority of participants (78%) considered the behavior a norm violation themselves, this verdict was significantly less frequent during second-guessing (58%; $\chi 2$ (1) = 10.91, $p = 0.001$). This finding is in line with the theorizing behind proposition 1 and shows that the difference in perspective emerges for both offenders and victims.

Another aim of study 3 was to examine the match between victims' second-guesses of offender justifications and their propensity to blame offenders. A chi^2-test contrasting the distributions of categories of neutralization across these conditions yielded no significant difference ($\chi 2$ (4) = 5.37, $p = 0.252$). However, if we only look at the fault line of norm violation, we find that participants in the victim-self condition were more likely to see the behavior as a norm violation than they second-guessed offenders would do so (categories 3–5: 83% self vs. 69% second-guessing, $\chi 2$ (1) = 4.19, $p = 0.041$). As Fig. 3 indicates, this difference was driven by neutralization category 4. Perspective made no difference to victims' propensity to hold the offender fully responsible (23% self vs. 22% second-guessing).

Study 3 thus reconfirms that participants in the offender-self condition are more likely to accept full responsibility than participants in any other condition. Given that all offenders in study 3 had freely decided to commit the offence, this finding suggests that the app-driven sharing of others' data feels personally wrong for many offenders. In addition, results show that victims consider the behavior overall less acceptable than their second-guesses about others might have indicated.

Study 3 also aimed to explore what happens when victims and offenders realize that the preventable click of a single button can make the difference to infringing privacy or not. Except for highlighting that it all hinges on a single click, study 3 had been equivalent to the communication app condition of study 1. Comparing these two studies suggests the following: realizing the power of a single click seems to increase offenders' propensity to accept full blame (42% vs. 28% in study 1) while reducing their propensity to claim that nothing happened (12% vs. 31%). We also see differences across studies in the victim second-guessing condition. Compared to study 1, victims were less likely to assume that offenders would think that nothing had happened (18% vs. 43%) and somewhat more likely to second-guess that offenders would take responsibility (22% vs. 14%). Realizing that the offender had chosen to click "ok" to share data rather than "not allow" seems to make a difference. This practical understanding seems to curb victims' willingness to excuse the behavior and may thus help the development of more prohibitive social norms.

There was, however, one condition that mapped exceedingly well onto victims' second-guesses in studies 1 and 2: offenders' second-guesses about victims' views, i.e., the only condition in which people may not have paid attention to the role of this single click. The distribution of categories of neutralization in this condition is virtually identical to the distribution of the overall victim condition in the prior studies (see Fig. 2). When second-guessing, offenders seem to have drawn on the same abstract (rather than practical) understanding of the sharing of others' data as "normal" that victims in studies 1 and 2 appear to have drawn on.

Discussion and Implications

Allowing apps access to contacts or photos amounts to sharing others' data and this potentially harmful behavior is morally and legally questionable. Prior research suggests that people infringe on others' information privacy even if they are aware of this implication (Kamleitner & Mitchell, 2019). However, despite the behavior being widespread, offenders are hard, if not impossible, to identify. This makes it difficult to determine the behavior's overall moral acceptability. In addition, most offenders are prone to be both offenders and victims and their moral verdict may differ across these roles. We therefore drew on offenders' neutralizations and victims' second-guesses of these neutralizations in order to capture the nuanced moral acceptability and evolving norms guiding and enabling the behavior. Building on this novel theoretical backbone, we conducted four exploratory studies (one qualitative and three quantitative) and reached the following key insights.

a. The app-driven sharing of others' data is morally ambiguous. The two opposite extremes 'nothing happened' and 'something bad and inexcusable happened' dominated the responses.
b. These opposing answers result from the juxtaposition of offenders' own perspective with victims' second-guesses about offenders' perspective. Offenders tended to take more responsibility than victims either allotted to them (study 3) or expected them to take (studies 1 and 2). One way to interpret these findings is to suggest an absence of clearly established social norms in light of more prohibitive personal norms.
c. Neutralizations vary across contexts, but these variations are remarkably small and mostly arose in the offender perspective. We deduce from this that people's personal norms are sensitive to contextual variations while their social norms are largely robust to context. While cultures could be reasonably expected to differ (Licht,

2008), the pattern of results is remarkably similar across our samples in Austria and US.

d. A practical understanding of the ease with which others' data can be protected as well as given away seems to increase the propensity to consider the behavior as a norm violation, in particular among victims.

Contributions to Theory

First, our insights align with prior literatures suggesting that people are struggling to understand online privacy (Kokolakis, 2017; Oetzel & Gonja, 2011), that digitalization is shifting norms (Bauman, 2013; Rosa, 2013), and that the online environment often negatively affects ethical judgements (Freestone & Mitchell, 2004) by creating an unreal environment free from offline norms (Runions & Bak, 2015). We find that these observations also extend to app-driven interdependent privacy. Prior literature suggests that when agreed social norms become violated, victims allot more responsibility to offenders than these offenders tend to be willing to take themselves (McCarthy et al., 2021). Our exploratory findings (see also Fig. 4 in Appendix B) suggest the absence of clear social norms for the app-based sharing of others' data. In this situation, we find the opposite: victims are less accusatory than offenders. A lack of clear social norms may explain this, but so does the fact that most victims are also offenders. Both considerations have scarcely been examined in current theorizing.

Second, we add a new theoretical lens, neutralizations, to existing thinking in the area of interdependent privacy. To the best of our knowledge, we are the first to focus on the moral dimension of the phenomenon. Traditionally, the study of neutralizations has centered on understanding individuals' justifications for deviating from these norms rather than delving into the norms themselves. We show how the very process of neutralization could serve as an indicator of the evolving social norms. Our results also shine a novel light on how much people respect others' data; something which Kamleitner and Mitchell (2019) consider the third and last step in a series of steps (the 3Rs; Realize, Recognize, Respect) that can lead to the sharing of others' data. Our research confirms their speculation that the disrespect of others' rights may represent a lack of inhibiting social norms.

Third, we expand on the literatures on neutralizations (Kaptein & van Helvoort, 2019; Sykes & Matza, 1957; Willison & Warkentin, 2013) and social norms (Acquisti et al., 2011; Barth et al., 2006; Hoyle et al., 2020; Nissenbaum, 2004). We find that people may be willing to admit to wrongdoing without making excuses and suggest the addition of a "no neutralization" category. This ensures that there is a fitting answer option for all situations in which a social or personal norm gets infringed. By assessing neutralizations at the level of categories, we also highlight that it may be possible to compare neutralizations across behaviors.

Finally, and perhaps most novel, we contribute to the neutralization literature by introducing perspectives. We draw attention to the possibility of victim–offender entanglement and highlight the merit of assessing second-guesses. Although this needs further investigation, we assume that the contrast between offenders' own justifications and victims' second-guesses about these justifications highlights the extent to which prohibitive personal and social norms exist and align. Whenever social norms are stricter than offenders' personal norms, we would expect victims to second-guess the use of higher categories of neutralization than offenders actually do. Whenever social norms are more relaxed than offenders' personal norms, we would expect the opposite. The interactive process of offenders' and victims' perceptions and the ongoing dialog between the two parties play a pivotal role in shaping and solidifying new societal norms surrounding interdependent privacy concerns.

Practical Implications

Our empirical findings pave the way for different courses of action and recommendations. First, they suggest a lack of moral consensus about the behavior. This makes it unlikely that the public will be prepared to press policy makers and app providers into bringing about change. Although the privacy-infringing behavior (currently) violates many individuals' own moral standards, it is likely to continue. This implies the need for clearer regulation and actual legal sanctions. Greater legal clarity about the lawfulness of this behavior and its legal ramifications for individuals and companies would assist in the development of norms and norm-breaking acknowledgments.

In the absence of clearer, stricter, and factually executed regulations, social norms are a key lever. These could be changed via some form of mass public education campaign such as has been successful at establishing preventative social norms around drinking and driving. Government is the primary stakeholder able to launch such a campaign together with information commissioners, which could also be supplemented by privacy NGOs.

While descriptive norms are often stronger to guide intention and behavior than injunctive norms (e.g., Elgaaied-Gambier et al., 2018), this is not helpful when thinking about the sharing of others' data which is widespread. Making people aware of its prevalence could serve to increase the behavior. Our results also suggest the absence of injunctive social norms. This leaves a focus on prohibitive personal norms that can matter more for actual behavior (Hornsey et al., 2007) than social norms (de Groot et al., 2021). We therefore propose interventions that stress personal norms and, for example, invoke the parallel to offline privacy.

Another approach could be the use of so-called dynamic norms which can include perceptions about expected future developments in relation to the behavior (Loschelder et al., 2019), e.g., "more and more people are protecting their friends' personal data". Yet another approach to combat a "nothing happened" mentality is fear of repercussions, although prior literature suggests that these appeals need to be particularly well crafted to work (for specific recommendations see Tannenbaum et al., 2015).

There are also implications for businesses. Not collecting data shared via others avoids any potential prosecution under GDPR and can be a business opportunity. Recent work suggests that promoting privacy friendliness can lead to robust positive changes in market shares and revenues (Eggers et al., 2022). In particular, our results suggest that businesses could get a competitive advantage by helping offenders avoid breaking their own norms, e.g., via pop-up messages on app permission reminding users of their responsibilities.

Notably, most people are both offenders and victims. Traditionally interventions focus on offenders. Our results suggest that the victim perspective gives policy makers, app providers and privacy activist groups another angle for action. Because of the high degree of victim–offender overlap, interventions could target the same person with different appeals. When targeting the victim perspective, messages could challenge the assumption that offenders will think nothing happened. Also, from study 3, we see that a practical understanding of the ease with which others' data can be protected as well as given away seems to increase the propensity to consider the behavior as a norm violation, particularly among victims. This could be made salient.

Although neutralizations vary across app contexts, these variations are remarkably small and mostly arose in the offender perspective. Nonetheless, the small differences could still have implications. Specifically, offenders were more likely to take responsibility when the app could plausibly be believed to fully function without accessing others' data. In particular for the communication app, messages might try to undermine offenders' defence that nothing happened.

Our results also suggest that making the other salient might play a role. Paradoxically, offenders were twice as likely (4% vs. 8%) to claim nothing happened when the victim was specified compared to when they were not specified. The most pronounced difference emerged in victims' use of category 5 (take full responsibility). Some victims thought a specified offender they knew well would take full responsibility (18%), but none thought that unspecified offenders would. Specifying the other after it happened thus appears to be of limited use and might even backfire.

Conclusions and Further Research

App-driven privacy infringements not only differ from sharing one's own data, but also from sharing others' data offline, which is much more conscious, traceable, punishable, and far less frequent. We argue that a deeper understanding of the moral acceptability of app-driven privacy infringements is an important piece in the puzzle. Yet, our results are a mere first step in exploring a facet of interdependent privacy and we consider some future directions that appear to show promise. One way forward is to extend theorizing and benefit from other theories that can address the learning of norms such as differential association (Matsueda, 2001) or social learning theory (Bandura & Walters, 1977).

Looking more broadly at the phenomenon, one of its most resounding characteristics is its embeddedness in layers of ambiguity. Since personal data are retained even when passed on (Kamleitner & Mitchell, 2018), and multiple copies may exist without a person knowing, there is uncertainty around the true culprit in case of subsequent harm, and it lowers potential levels of detection and reduces punishment for potential offenders (Freestone & Mitchell, 2004). A focus on variations in ambiguity of data ownership and potential punishments or consequences (Demmers et al., 2022; Kamleitner & Mitchell, 2018) is a promising avenue for future research.

This brings us to a final noteworthy observation, the fact that so many offenders indicated they would take responsibility. While this sounds positive, it does invite more questions. For example, it is possible that taking responsibility was considered an easy option with no repercussions. In light of this, future studies could also consider two independent axes when examining the sharing of others' data, namely the degree of responsibility taken and the degree of infringement.[4]

Finally, it is important to acknowledge that interdependent privacy breaches are a broader set of activities. The app-based sharing of others' data is but one of multiple instances of interdependent privacy issues. There are issues of social cost and benefit considerations which mostly manifest when people actively and visibly share others' data, e.g., when sharing others' pictures online (Litt & Hargittai, 2014). In addition, there are issues of co-created data, such as joint conversations or pictures taken together to consider. There are also considerations of (economic) personal benefits. Stretching the scope to consider the many facets of interdependent privacy paves the way for rich additional considerations. For example, referral programs are a great example of the active, conscious, limited and targeted giving away of others' data (typically an email address), which differs

[4] We thank an anonymous reviewer for this suggestion.

greatly from the passive mass transfer of all contacts data that describes app-based privacy infringements. Our insights are relevant to many contexts but there is much more to be learned about interdependent privacy.

Appendix A: Materials for Studies 1, 2 and 3

Materials for Study 1

Scenarios of the 2 (perspective: offender vs. victim) × 2 (app: communication vs. information) design

On the next page you will find a short scenario about downloading an app.

Try to put yourself in this situation as best as you can.

Imagine….

Offender—Information App [Communication App]

You recently downloaded an app.

It was an information app (e.g., a weather or news app) [communication app (e.g., WhatsApp or Telegram)].

When you downloaded the app, various permissions were requested (e.g., access to contacts and files, including photos). You agreed to all the requested permissions.

The app provider now has access to, among other things:

- All photos that are stored on your phone. These probably sometimes include a person close to you.
- All contacts stored on your phone. This includes contact details of a person close to you, such as their phone number and email address, but possibly also their date of birth.

Because you said "Yes", the app provider can now access the data of the person close to you.

Victim—Information App [Communication App]

A person close to you recently downloaded an app.

It was an information app (e.g., a weather or news app) [communication app (e.g., WhatsApp or Telegram)].

When downloading the app, various permissions were requested (e.g., access to contacts and files, including photos). The person close to you agreed to all the requested permissions.

The app provider now has access to, among other things:

- All photos stored on the cell phone of the person close to you. These probably sometimes include yourself.
- All contacts stored on the phone of the person close to you. This includes your own contact details such as your phone number and email address, but possibly also your date of birth.

Because the person close to you said "Yes", the app provider can now access your data.

Subsequent Questions—Offender Perspective

So now the app provider has the data of this person close to you through your phone.

Which of the following statements best describes your thoughts on this?

1. I do not think that anything happened at all.
2. Yes, something happened, but it really is not bad.
3. Yes, something happened that should not have happened, but it is not my fault as I did not have any real control over it.
4. Yes, something happened that should not have happened, but it really would have been difficult for me to prevent it.
5. Yes, something happened that should not have happened. I take full responsibility for it.

Subsequent Questions—Victim Perspective

So now the app provider has your data through the phone of the person close to you.

Which of the following statements best describes the thoughts of the person close to you about this in your opinion?

1. He/she thinks: I do not think that anything happened at all.
2. He/she thinks: Yes, something happened, but it really is not bad.
3. He/she thinks: Yes, something happened that should not have happened, but it is not my fault as I did not have any real control over it.
4. He/she thinks: Yes, something happened that should not have happened, but it really would have been difficult for me to prevent it.
5. He/she thinks: Yes, something happened that should not have happened. I take full responsibility for it. (Table 3)

Table 3 List of variables and scales study 1

Variable	Survey question	Scale
1) Psychological ownership (PO) for all smartphone data	How strongly do you feel a sense of ownership for the data on your phone? Please complete the following sentence "For me, the data on my phone is…"	7-point bipolar scale: 1 = "ANY data" to 7 = "MY data" (points in between were only numbered); adapted from Thürridl et al. (2020)
2) Close other	Think of a specific person close to you whose data is on your smartphone Who is this person? Give the person a (nick) name (this information also remains anonymous):	
3) Gender of the other person	What is the gender of the person?	1 = female 2 = male 3 = diverse
4) Closeness to other person	How close do you feel to this person?	Slider scale: 0 = "less close" to 100 = "especially close"
5) Usage of neutralizations	As described above	As described above
6) Perceived need to justify—Self (per condition)	Offender: Do you feel that you have to justify yourself to this person close to you because you gave away their data? Victim: Do you feel that the person close to you has to justify themself for giving away your data?	Slider bar with 9 possible positions; higher positions indicated stronger agreement
7) Perceived need to justify—Other	Offender: Do you feel that this person expects you to justify it? Victim: Do you feel that this person thinks they have to justify themself?	Slider bar with 9 possible positions; higher positions indicated stronger agreement
8) PO for the data given away	Offender: What do you think about the data on your phone concerning the person close to you (e.g., contact details of this person and photos on which this person is shown)? Please complete the following sentence "For me, this data on my phone is…" Victim: What do you think about this data on the phone of the person close to you (e.g., your contact details and photos on which you are depicted)? Please complete the following sentence "For me, this data is…"	7-point bipolar scale: 1 = "ANY data" to 7 = "MY data" (points in between were only numbered); adapted from Thürridl et al. (2020)
9) Ownership right	Who do you think should have a right to this data?	Slider scale; 0 = "only myself", 50 = "both equally", 100 = "only the person close to me"
10) Own bad conscience	Would you have a bad conscience if you shared your best friend's personal information with a third party without permission by downloading an app?	7-point scale; 1 = "no bad conscience at all" to 7 = "absolutely bad conscience"
11) Others' bad conscience	Do you think your best friend would have a bad conscience if he or she shared your personal information with a third party without permission by downloading an app?	7-point scale; 1 = "no bad conscience at all" to 7 = "absolutely bad conscience"
12) Empathy	How well could you put yourself into the situation described in the scenario?	7-point scale; 1 = "not at all" to 7 = "absolutely"

Table 3 (continued)

Variable	Survey question	Scale
13) Realism	How realistic do you perceive the situation to be?	7-point scale; 1 = "not at all realistic" to 7 = "absolutely realistic"
14) Frequency	How often do you think such a situation occurs?	7-point scale; 1 = "never" to 7 = "always"
15) Problematic nature	How problematic do you find such a situation?	7-point scale; 1 = "not at all problematic" to 7 = "absolutely problematic"
16) Gender	Your gender	1 = female 2 = male 3 = diverse
17) Age	Your age	
18) Income	Monthly income	1 = < 500€, 2 = 500€–1000€, 3 = 1001€–2500€, 4 = 2501€–5000€, 5 = > 5000€, 6 = no indication
19) Education	What is your highest completed level of education?	1 = mandatory school, 2 = middle school (no higher education qualification), 3 = apprenticeship, 4 = high school (higher education qualification), 5 = university/college

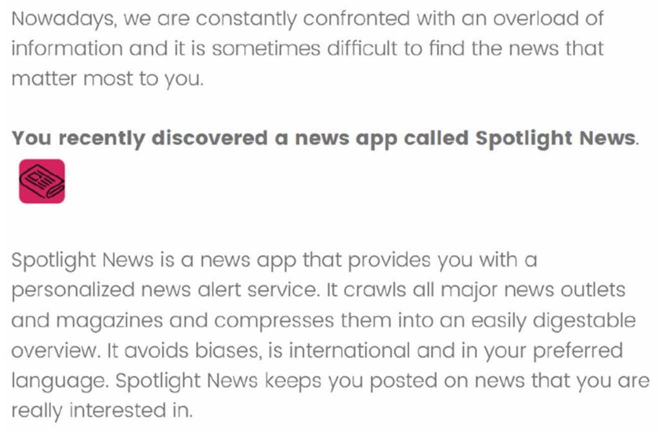
Materials for Study 2

Scenarios of the 2 (perspective: offender vs. victim) × 2 (victim/offender specification: specified vs. unspecified) design

On the next page you will find a short scenario about downloading an app.

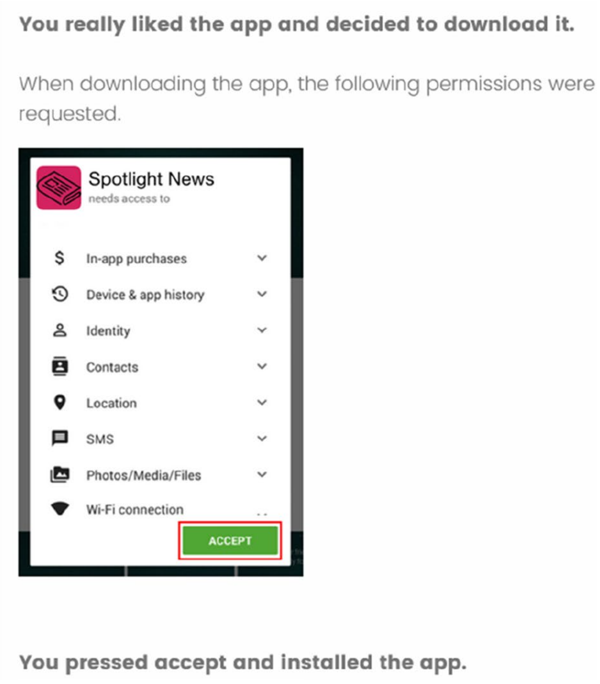
Try to put yourself in this situation as best as you can. Imagine….

1) Offender—Unspecified victim


Nowadays, we are constantly confronted with an overload of information and it is sometimes difficult to find the news that matter most to you.

You recently discovered a news app called Spotlight News.

Spotlight News is a news app that provides you with a personalized news alert service. It crawls all major news outlets and magazines and compresses them into an easily digestable overview. It avoids biases, is international and in your preferred language. Spotlight News keeps you posted on news that you are really interested in.


You really liked the app and decided to download it.

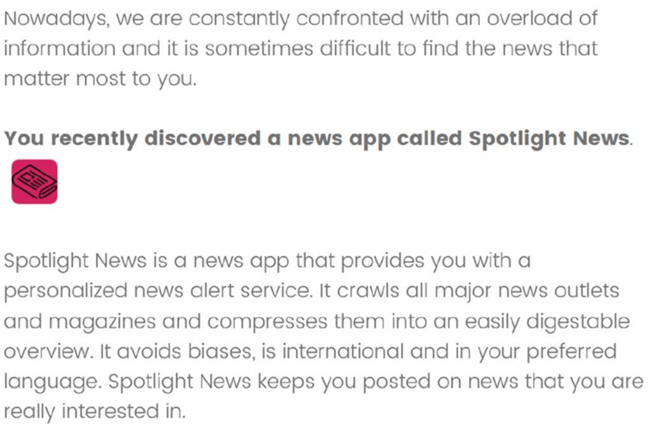
When downloading the app, the following permissions were requested.

You pressed accept and installed the app.

The app provider now has access to:

- All photos that are stored on your phone. These probably include pictures of other people
- All contacts stored on your phone. This includes contact details of other people, such as their phone number and email address, but possibly also their date of birth.

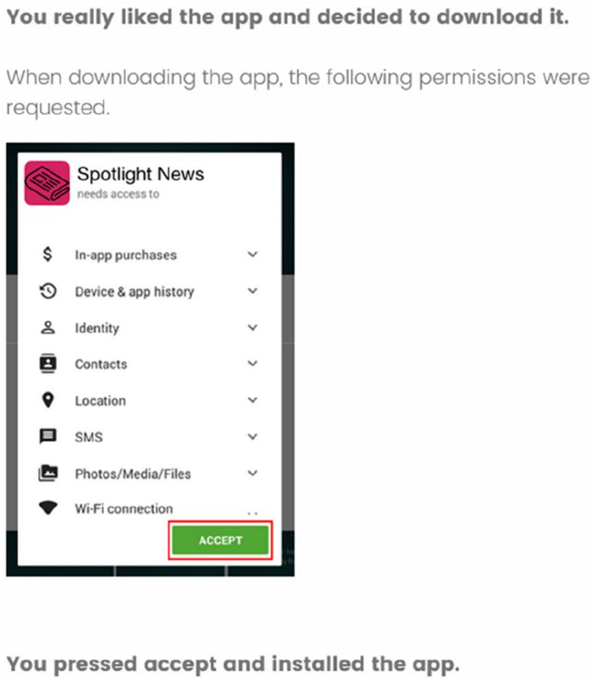
2) Offender—specified victim



Nowadays, we are constantly confronted with an overload of information and it is sometimes difficult to find the news that matter most to you.

You recently discovered a news app called Spotlight News.

Spotlight News is a news app that provides you with a personalized news alert service. It crawls all major news outlets and magazines and compresses them into an easily digestable overview. It avoids biases, is international and in your preferred language. Spotlight News keeps you posted on news that you are really interested in.



You really liked the app and decided to download it.

When downloading the app, the following permissions were requested.

You pressed accept and installed the app.

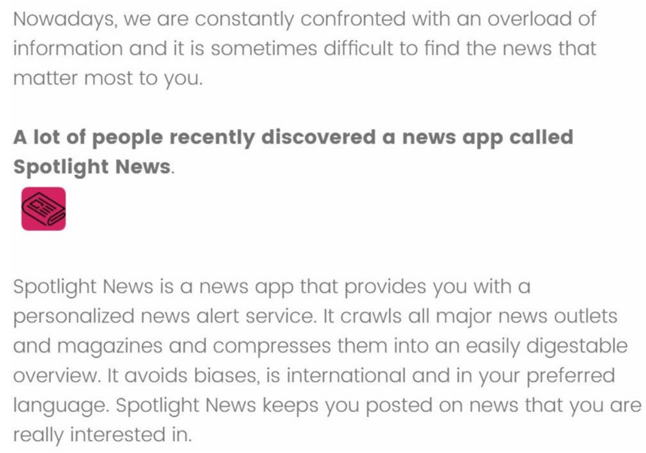
Because you pressed "Accept", the app provider can now access and use the data of those other people, even if they have not installed the app.

The app provider now has access to:

- All photos that are stored on your phone. These probably include pictures of [*name of other*]
- All contacts stored on your phone. This includes contact details of [*name of other*], such as their phone number and email address, but possibly also their date of birth.

Because you pressed “Accept”, the app provider can now access and use the data of [*name of other*'s] data, even if [*name of other*] has not installed the app.

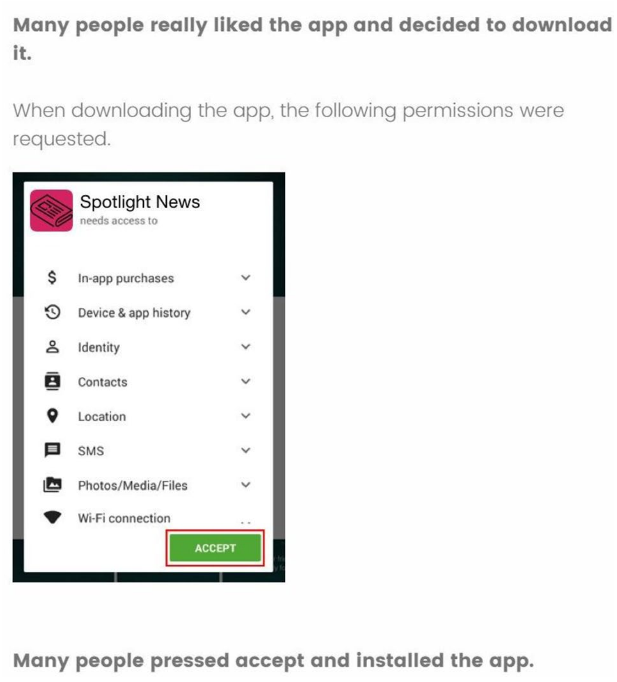
3) Victim—unspecified offender



Nowadays, we are constantly confronted with an overload of information and it is sometimes difficult to find the news that matter most to you.

A lot of people recently discovered a news app called Spotlight News.

Spotlight News is a news app that provides you with a personalized news alert service. It crawls all major news outlets and magazines and compresses them into an easily digestable overview. It avoids biases, is international and in your preferred language. Spotlight News keeps you posted on news that you are really interested in.



Many people really liked the app and decided to download it.

When downloading the app, the following permissions were requested.

Many people pressed accept and installed the app.

The app provider now has access to:

- All photos stored on the phones of other people. These probably include pictures of you as well.
- All contacts stored on the phones of other people. This includes your own contact details, such as your phone number and email address, but possibly also your date of birth.

Because other people pressed "Accept", the app provider can now access your data and use it, even if you have not installed the app.

4) Victim—specified offender:

Nowadays, we are constantly confronted with an overload of information and it is sometimes difficult to find the news that matter most to you.

[name

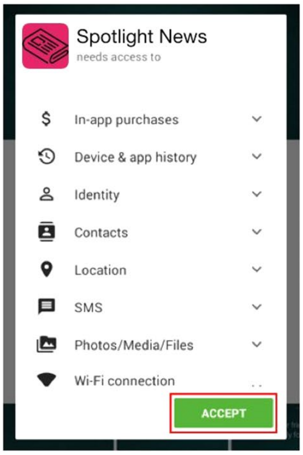
recently discovered a news app called Spotlight News.

Spotlight News is a news app that provides you with a personalized news alert service. It crawls all major news outlets and magazines and compresses them into an easily digestable overview. It avoids biases, is international and in your preferred language. Spotlight News keeps you posted on news that you are really interested in.

[name

really liked the app and decided to download it.

When downloading the app, the following permissions were requested.



pressed accept and installed the app.

The app provider now has access to:

- All photos stored on the phone of [name of other]. These probably include pictures of you as well.
- All contacts stored on the phone of [name of other]. This includes your own contact details, such as your phone number and email address, but possibly also your date of birth.

Because [name of other] pressed "Accept", the app provider can now access your data and use it, even if you have not installed the app (Table 4).

Materials for Study 3

Scenarios of the 2 (perspective: offender vs. victim) × 2 (second-guessing: no vs. yes) design

On the next page you will find a short scenario about downloading an app.

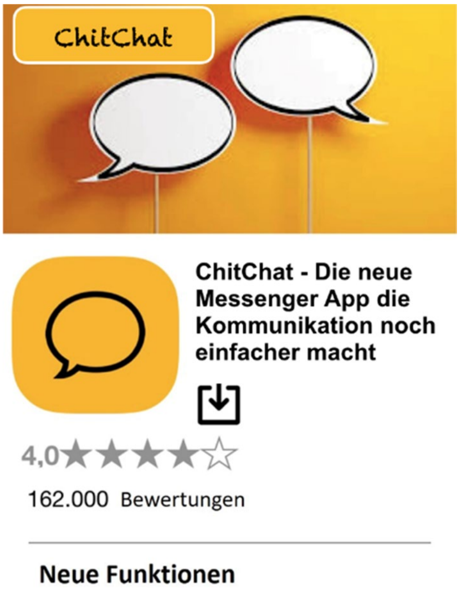
Try to put yourself in this situation as best as you can.

Imagine….

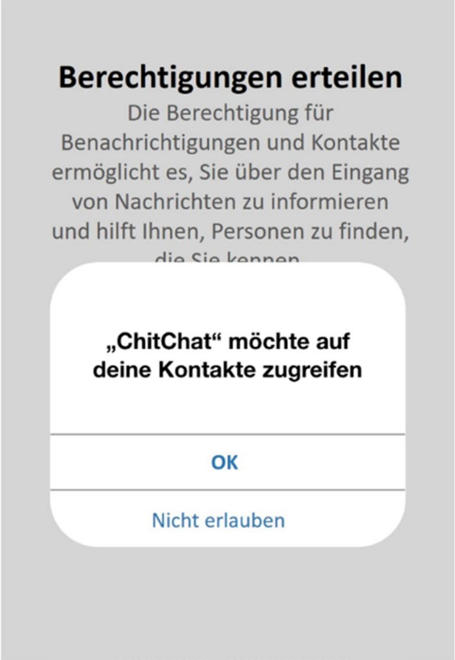
Choice Scenario

You have recently discovered a messenger app called "ChitChat". The app makes it even easier to communicate through new applications than through other apps in this field, so it's definitely an improvement for you.

This is the app. Please continue on the next page.


ChitChat
ChitChat - Die neue Messenger App die Kommunikation noch einfacher macht
4,0★★★★☆
162.000 Bewertungen
Neue Funktionen

Imagine you have downloaded the app. Before you can get started, another pop-up appears. Click as you normally would.



Berechtigungen erteilen

Die Berechtigung für Benachrichtigungen und Kontakte ermöglicht es, Sie über den Eingang von Nachrichten zu informieren und hilft Ihnen, Personen zu finden, die Sie kennen

„ChitChat" möchte auf deine Kontakte zugreifen

Offender Conditions (After Choice Scenario)

The app provider now has access to all contacts stored on your phone. This includes contact details of [name of other] like [name of other]'s phone number and email address, but possibly also [name of other]'s date of birth. Because you have given the app provider access, they may now have [name of other]'s contact information.

Victim Conditions (After Choice Scenario)

Imagine…[name of other] has also downloaded the app "ChitChat". [name of other] has given the app access to all contacts. The app provider now has access to all contacts stored on [name of other]'s phone. This includes your contact details such as your phone number and email address, but possibly also your date of birth. Because [name of other] has given access to the app provider, they can now have your contact details.

Victim Conditions (Without Choice Scenario)

[name of other] has recently discovered a messenger app called "ChitChat". The app makes it even easier to communicate through new applications than through other apps in this area and is therefore a clear improvement for [name of other].

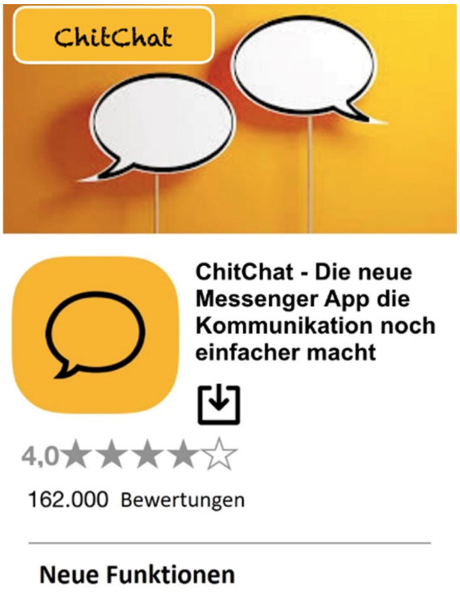
This is the app. Please continue on the next page.

Table 4 List of variables and scales – study 2

Variable	Survey question	Scale
1) Gender	Your gender	1 = female 2 = male 3 = diverse
2) Age	Your age	
3) Close other *(only in specified condition)*	Think of a specific person close to you whose data is on your smartphone Who is this person? Give the person a (nick) name (this information also remains anonymous):	
4) IOS (inclusion of other in the self, Aron et al., 1992) *(only in specified condition)*	Which of the following pictures best describes your relationship with this person (Other)?	Circles representing self and other that overlap to differing degrees
5) Closeness to the other person *(only in specified condition)*	How close do you feel to this person?	Slider scale; 0 = "not close at all" to 100 = "very close"
6) Empathy	Could you see yourself in a situation like this; downloading a new app allowing it access to all kinds of things on your phone?	Yes, no
7) Deinstallation	After some reflection, would [offender] deinstall the app?	Slider scale; 0 = "definitely keep" to 50 = "not sure" to 100 = "definitely deinstall"
8) Perceived need to justify – Self	Offender: Do you feel that you have to justify yourself to this person close to you because you gave away their data? Victim: Do you feel that the person close to you has to justify themself for giving away your data? (adapted)	Slider bar with nine possible positions; higher positions indicated stronger agreement
9) Perceived need to justify – Other	Offender: Do you have the feeling that this person expects you to justify it? Victim: Do you have the feeling that this person thinks they have to justify themself? (adapted)	Slider bar with nine possible positions; higher positions indicated stronger agreement
10) PO for the data given away	Offender: What do you think about the data on your phone concerning [other] (e.g., contact details and photos on which [other] is shown)? Please complete the following sentence "For me, this data on my phone is…" Victim: What do you think about this data on the phone of [other] (e.g., your contact details and photos on which you are depicted)? Please complete the following sentence "For me, this data is…"	7-point bipolar scale; 1 = "ANY data" to 7 = "MY data" (points in between were only numbered); adapted from Thürridl et al. (2020)
11) Ownership right	as in Study 1	as in Study 1
12) Existence of norms	Do you think there are generally accepted social norms about the sharing of others' data? (adapted)	5-point scale; 1 = "no norms at all" to 5 = "very clear norms"

Table 4 (continued)

Variable	Survey question	Scale
13) Social acceptance	In our society, how acceptable do you think it is to share others' data with apps without their explicit consent?	7-point scale; 1 = "Not at all acceptable" to 7 = "Absolutely acceptable"
14) Personal sense of morality	How do you feel about this personally? How morally right or wrong do you think it is to share other people's data with apps without their explicit consent?	7-point scale; 1 = "Absolutely morally wrong" to 7 = "Absolutely morally right"



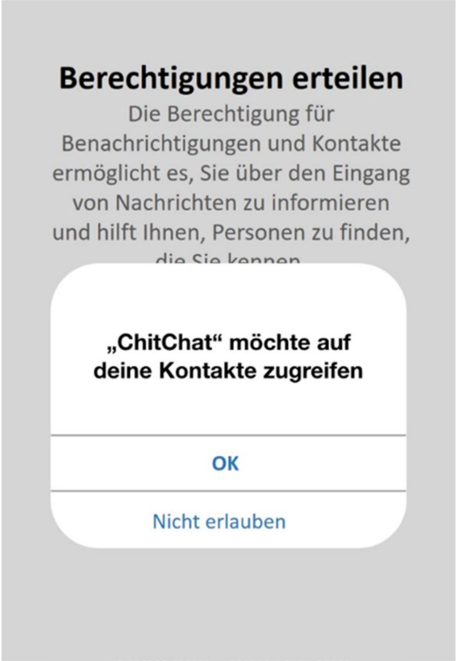
ChitChat - Die neue Messenger App die Kommunikation noch einfacher macht

4,0★★★★☆

162.000 Bewertungen

Neue Funktionen

Imagine [name of other] has downloaded the app and has agreed to the following permission.



Berechtigungen erteilen

Die Berechtigung für Benachrichtigungen und Kontakte ermöglicht es, Sie über den Eingang von Nachrichten zu informieren und hilft Ihnen, Personen zu finden, die Sie kennen

„ChitChat" möchte auf deine Kontakte zugreifen

OK

Nicht erlauben

The app provider now has access to all contacts stored on [name of other]'s phone. This includes your contact details such as your phone number and email address, but possibly also your date of birth. Because [name of other] has given access to the app provider, they can now have your contact details.

Non-second-Guessing Conditions

Table 5 List of variables and scales—Study 3

Variable	Survey question	Scale
1) Amount of apps	How many apps do you have on your phone	Slider scale 0 to 100
2) Close other	Think of a specific person who is close to you and you know well Give the person a (nick) name (this information also remains anonymous):	
3) Amount of apps close other	How many apps do you think that person has on their phone approximately?	Slider scale 0 to 100
4) Perceived need to justify	Offender—non-second-guessing: Do you feel that you have to justify yourself to this person close to you because you gave away their data? Victim—non-second-guessing: Do you feel that the person close to you has to justify themself for giving away your data? (adapted) Offender second-guessing: Do you have the feeling that this person expects you to justify it? Victim second-guessing: Do you have the feeling that this person thinks they have to justify themself? (adapted)	Slider bar with nine possible positions; higher positions indicated stronger agreement
5) PO for the data given away	Offender: What do you think about the data on your phone concerning [other] (e.g., contact details and photos on which [other] is shown)? Please complete the following sentence "For me, this data on my phone is…" Victim: What do you think about this data on the phone of [other] (e.g., your contact details and photos on which you are depicted)? Please complete the following sentence "For me, this data is…"	7-point bipolar scale; 1 = "ANY data" to 7 = "MY data" (points in between were only numbered); adapted from Thürridl et al. (2020)
6) Ownership right	as in Study 1	as in Study 1
7) Own bad conscience	Offender: Would you have a bad conscience if you shared your best friend's personal information with a third party without permission by downloading an app? Victim: Do you think [other] would feel bad if she or he shared your personal information with a third party without permission by downloading an app?	7-point scale; 1 = "no bad conscience at all" to 7 = "absolutely bad conscience"
8) Realism	Victims only: How realistic do you think it is that [other] would actually grant access to your contact details?	7-point scale; 1 = "Not at all realistic" to 7 = "Absolutely realistic"
9) Empathy	How well could you put yourself into the situation described in the scenario?	7-point scale; 1 = "not at all" to 7 = "absolutely"
10) Frequency	How often do you deal with the issue of privacy on your cell phone?	7-point scale; 1 = "Never" to 7 = "Constantly"
11) Importance	How important is privacy on your cell phone to you?	7-point scale; 1 = "Not at all important" to 7 = "Absolutely important"

Table 5 (continued)

Variable	Survey question	Scale
12) Familiarity	Have you ever heard of situations where the actions of private individuals interfere with the privacy of others. This is called "interdependent privacy"	"yes", "no", "not sure"
13) Problem	How important is privacy on your cell phone to you?	7-point scale; 1 = "Not at all problematic" to 7 = "Absolutely problematic"
14) Gender	Your gender	1 = female 2 = male 3 = diverse
15) Age	Your age	
16) Income	Monthly income	1 = < 500€, 2 = 500€–1000€, 3 = 1001€–2500€, 4 = 2501€–5000€, 5 = > 5000€, 6 = no indication
17) Education	What is your highest completed level of education?	1 = mandatory school, 2 = middle school (no higher education qualification), 3 = apprenticeship, 4 = high school (higher education qualification), 5 = university/college

So now the app provider has your data through the mobile of [name of other].

OR So now the app provider has the contact details of [name of other] through your phone.

Which of the following best describes **your thoughts** on this?

1. I do not think that anything happened at all.
2. Yes, something happened, but it really is not bad.
3. Yes, something happened that should not have happened, but it is not [name of other]/ my fault as [name of other]/I did not have any real control over it.
4. Yes, something happened that should not have happened, but it really would have been difficult for [name of other]/me to prevent it.
5. Yes, something happened that should not have happened. [name of other]/I bear(s) full responsibility for it.

Second-Guessing Conditions

So now the app provider has your data through the mobile of [name of other]./ So now the app provider has the contact details of [name of other]through your phone.

Which of the following best describes **[name of other]'s thoughts** on this?

1. I do not think that anything happened at all.
2. Yes, something happened, but it really is not bad.
3. Yes, something happened that should not have happened, but it is not my/your fault as I/you did not have any real control over it.
4. Yes, something happened that should not have happened, but it really would have been difficult for me/you to prevent it.
5. Yes, something happened that should not have happened. I/you bear full responsibility for it (Table 5).

Appendix B: Additional Findings

Pilot Study

Detailed methods and results pilot study ($N = 115$)

Sample and Procedure

A total of 115 Austrian university students ($M_{age} = 22.68$; $SD_{age} = 2.68$; 65% female, 35% male) participated in this study for course credits. In a lab environment, participants were randomly assigned to one of the two versions of a scenario (offender vs. victim) and asked to write down their thoughts and feelings on a situation in which either they

Table 6 Example quotes per neutralization category and perspective (offender vs. victim)

Categories	Example quotes	
Denying the norm violation		
Distorting the facts as in *"Nothing really happened."*	*Offender*	*I generally have no problem with it, since data, whether with consent or not, is passed on to third parties anyway.* (male offender, 22) *With some [applications] it even makes sense that they sometimes need access to private data (e.g., calendar and mobile device automatically connect to computer) […] that can also be very convenient.* (female offender, 21)
	Victim	*[…] I believe that they already have so much data and it makes little difference whether I agree or not.* (female victim, 21)
Negating the norm as in *"Something happened, but it is not bad."*	*Offender*	*[…] at the same time I know that these companies can't use such a large amount of data properly anyway.* (female offender, 22)
	Victim	*I have nothing to hide, no secrets, and I feel absolutely not watched or as a "transparent person".* (male victim, 22) *I would not be mad at my friend. Each of us already installed a dubious app at some point.* (female victim, 22)
Denying responsibility		
Blaming the circumstances as in *"Something bad has happened, but I had no control over it."*	*Offender*	*The problem nowadays is that no matter what you search or install, it is stored somewhere on the Internet without you being able to do anything about it.* (female offender, 26) *[…] without this consent the app often cannot be downloaded or often there is no choice.* (female offender, 21)
	Victim	*Nowadays, one has little or no control over which data is available to whom.* (female victim, 23) *[…] we ordinary people have nothing to say. The corporations make these rules.* (female victim, 21)
Hiding behind oneself as in *"Something bad has happened, but it would have been too hard for me to prevent it."*	*Offender*	*[…] I regret not to have read the small print exactly.* (female offender, 23) *The problem, however, is that no one actually reads the T&Cs.* (female offender, 21)
	Victim	*[…] one accepts the data release practically without questioning.* (male victim, 21) *[…], but that he handles his and also his data of the entire contact list so arbitrarily is very negligent and careless.* (male victim, 21)
Taking/Allocating responsibility		
Attribution of responsibility to the offender as in *"It is my fault."*	*Offender*	*[…] I would feel guilty towards my friends […]*(female offender, 21) *I have a bad conscience.* (female offender, 23)
	Victim	*[…] I find it irresponsible of my friend […]*(male victim, 22) *I feel left out and treated unfairly that someone has my data without my consent.* (male victim, 21)

themselves had permitted a game app to access their friends' data (contact details, pictures and call logs) (offender condition) or in which a friend had permitted a game app to access their own data (victim condition).

All responses were read by two independent coders who both identified text sections that aimed to explain or justify why the behavior had occurred and who was to be held responsible for it. After agreeing on the identified text sections both coders assigned codes (Stemler, 2000) of the five categories of our extended framework to each identified section: (1) denial of behavior—distorting the facts, (2) denial of behavior—negating the norm, (3) denial of responsibility—blaming the circumstances, (4) denial of responsibility—hiding behind oneself, and (5) assigning responsibility to the offender. Disagreements were resolved after subsequent discussions, which most commonly occurred when quotes had elements of more than one coding category.

Results Several general insights emerged and here we briefly discuss some patterns observed before concluding what these insights can tell us about the role of personal and social norms in the behavior of giving away others' data (see Appendix B Table 6 for more example quotes and their categorization).

(1) *Distorting the facts* There was evidence of participants denying that anything had happened at all. Essentially, quotes assigned to the category of distorting the facts

were rooted in a belief that privacy was dead anyway and that thus no (additional) injury could happen. Some participants in the offender condition perceived the giving away of others' data "*as almost normal or natural*" (female offender, 21) or did not perceive it as problematic as personal "*contact details have probably been shared in this way already*" (female offender, 22). This view was shared by some participants in the victim condition; as one participant put it "*through my activities on various social networks all my data is already known and buzzing around the net anyway*" (male victim, 22). These are interesting insights because they mean that even those who saw no problem in the practice did not necessarily consider it morally right. Having said that, some participants also thought that the giving away of others' data could have positive effects for both parties "*because it increases the user experience*" (male victim, 22).

(2) *Negating the norm* Some participants argued that, even though clearly something had happened, it was not bad. Thus, what happened could not be classified as a norm violation. One interesting justification was to suggest that sharing others' data only harms those who have something to hide. As the following quote makes clear, it was an argument that puts the responsibility on the victim rather than the offender: "*If you have nothing to hide, it doesn't matter—what I have to hide, I won't give away*" (male victim, 22). In addition, and addressing the social norm implications more directly, some participants in the victim condition argued that it would be hypocritical to blame the offender, as they themselves had been giving away others' data too – *"I can't blame my friend, though, since everyone has done this before"* (female victim, 20). Reflecting the large degree of victim–offender overlap, they relativized the norm violation as "everybody is doing it".

(3) *Blaming the circumstances* Many participants in both conditions additionally claimed that it was beyond the offender's control to prevent such a transgression. Thus, they acknowledged some norm violation, but shifted responsibility away from the offender and blamed the circumstances—"*Unfortunately, this often cannot be avoided, as one is practically forced to do so*" (male offender, 26). Participants blamed the app providers and the companies behind them—"*we ordinary people have nothing to say. The corporations make these rules*" (female victim, 21), and also legislators—"*I think that it should be forbidden to ask and implement such things in the first place*" (female victim, 21). These arguments suggest that participants felt that a norm was violated, but that offenders were forced to violate the norm. Taking the focus away from the offender–victim relationship, some participants felt obligated to exchange personal data as a substitute for money for the service the app provided—"*nothing is given for free, and in this case payment with information replaces payment with money*" (male offender, 21).

(4) *Hiding behind oneself* Quotes falling into this category of neutralization acknowledged the norm violation, but tried to justify the offender's behavior via referring to pardonable human failings, e.g., a lack of knowledge; "*So what it really means to release this data is something one is not so aware of*" (female offender, 22) or thoughtlessness; "*I think it's irresponsible to share your data thoughtlessly. People think far too little about what they reveal*" (female victim, 22). In line with the argument that this category is one in which people do take some responsibility, there was evidence of self-blame for these failings; "*Mad at myself for not reading any information about the app before downloading it*" (male offender, 20).

(5) *Attribution of responsibility to the offender* Far from trying to wriggle out, some participants in the offender condition blamed themselves. This was evidenced by exclamations such as "*I feel irresponsible towards my friends*" (female offender, 22), "*I have a bad conscience*" (female offender, 23) or "*I try to undo it*" (female offender, 40). Some participants in the victim condition also were willing to blame the offender as they felt deprived of their own personal decision to give away their data and felt that this situation threatened their relationship: "*I would be very angry and scold my friend very much […] I wouldn't trust him in this respect anymore*" (female victim, 23).

Study 1

See Tables 7, 8.

Table 7 Means and standard deviations (N = 293)

Condition	App								
	Communication			Information			Overall		
	Offender–offender	Victim–offender	Overall	Offender–offender	Victim–offender	Overall	Offender–offender	Victim–offender	Overall
	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)
PO for data on one's own smart phone	5.77 (1.30)	5.38 (1.74)	5.60 (1.51)	5.76 (1.54)	5.79 (1.35)	5.77 (1.45)	5.76 (1.43)	5.60 (1.54)	5.69 (1.48)
PO for the data given away	5.95^{a**} (1.22)	5.16^{a**} (1.61)	5.61 (1.45)	5.99^{a**} (1.43)	5.25^{a**} (1.65)	5.66 (1.57)	5.97^{c**} (1.33)	5.21^{c**} (1.62)	5.63 (1.51)
Perceived need to justify – Self	3.92^{a*} (2.94)	4.95^{a*} (2.61)	4.36 (2.84)	5.24 (2.82)	4.56 (2.80)	4.94 (2.83)	4.62 (2.95)	4.74 (2.71)	4.67 (2.84)
Perceived need to justify—Other	3.13^{a*} (2.69)	4.31^{a*} (2.65)	3.63 (2.73)	4.20 (2.91)	3.61 (2.44)	3.93 (2.71)	3.69 (2.85)	3.92 (2.55)	3.79 (2.72)
Ownership right	44.65 (35.52)	42.31 (30.66)	43.65 (33.43)	37.97 (34.00)	43.65 (32.53)	40.54 (33.36)	41.15 (34.79)	43.05 (31.59)	41.98 (33.37)
Own bad conscience	5.04 (1.44)	4.86 (1.64)	4.96 (1.52)	5.23 (1.64)	5.38 (1.63)	5.30 (1.63)	5.14 (1.55)	5.15 (1.65)	5.14 (1.59)
Others' bad conscience	4.27 (1.54)	4.02 (1.76)	4.16 (1.63)	4.58 (1.62)	4.45 (1.65)	4.52 (1.63)	4.43 (1.58)	4.26 (1.71)	4.35 (1.64)
Degree of closeness to the other person	90.71^{a*} (17.36)	83.88^{a*} (21.21)	87.79 (19.32)	92.87^{a*} (13.06)	85.39^{a*} (21.83)	89.49 (17.91)	91.84^{c**} (15.25)	84.71^{c**} (21.48)	88.70 (18.57)

M and *SD* represent mean and standard deviation respectively. All differences between perspectives per app, between apps overall, and between perspectives overall were tested

$^{*}p < .05$, $^{**}p < .01$

[a] Significant difference between perspectives per app

[b] Significant difference between apps overall

[c] Significant difference between perspectives overall

Table 8 Pearson and spearman correlations ($N = 293$)

Variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
1) PO for data on own phone												
2) Categories of Neutralization	$-.02_S$											
3) Perceived need to justify—Self	$-.02_P$	$.38^{**}_S$										
4) Perceived need to justify—Other	$-.06_P$	$.29^{**}_S$	$.70^{**}_P$									
5) PO for data given away	$.40^{**}_P$	$.19^{**}_S$	$.23^{**}_P$	$.12^{*}_P$								
6) Ownership right	$-.13^{*}_P$	$.01_S$	$-.06_P$	$.02_P$	$-.12^{*}_P$							
7) Own bad conscience	$.04_P$	$.34^{**}_S$	$.52^{**}_P$	$.38^{**}_P$	$.32^{**}_P$	$-.08_P$						
8) Other's bad conscience	$-.01_P$	$.25^{**}_S$	$.37^{**}_P$	$.32^{**}_P$	$.19^{**}_P$	$.01_P$	$.71^{**}_P$					
9) Closeness to the other	$.22^{**}_P$	$.13^{*}_S$	$.01_P$	$-.10_P$	$.26^{**}_P$	$.06_P$	$.07_P$	$.11_P$				
10) Gender	$.08_P$	$.05_S$	$.01_P$	$-.02_P$	$.12^{*}_P$	$-.08_P$	$.14^{*}_P$	$.08_P$	$.03_P$			
11) Age	$.01_P$	$-.01_S$	$.12^{*}_P$	$.15^{**}_P$	$.17^{**}_P$	$-.00_P$	$.16^{**}_P$	$.13^{*}_P$	$-.02_P$	$-.08_P$		
12) Income	$-.01_S$	. 01_S	$.03_S$	$.06_S$	. 07_S	$-.03_S$	$.03_S$	$.06_S$	$.02_S$	$-.13^{*}_S$	$.07_S$	
13) Education	$-.03_S$	$.01_S$	$.01_S$	$-.07_S$	$-.04_S$	$.12^{*}_S$	$.05_S$	$-.02_S$	$-.00_S$	$-.04_S$	$.02_S$	$.24^{**}_S$

$^{*}p < .05$, $^{**}p < .01$; $_P$ = Pearson $_S$ = Spearman. Categories of neutralization are treated as an ordinal variable here

Study 2

Additional exploratory study/items: Norms (See Tables 9 and 10).

In study 2, we added three items to directly measure the participants' opinions on the existence of norms about the sharing of others' data as well as well as how morally right or wrong participants personally feel this behavior. Variables

Table 9 Means and standard deviations ($N = 348$)

Perspective	Victim/offender specification								
	Specified			Unspecified			Overall		
	Offender	Victim	Overall	Offender	Victim	Overall	Offender	Victim	Overall
	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)
PO for the data given away	5.23^{a**} (1.65)	4.43^{a**} (1.84)	4.83^{b**} (1.79)	5.74^{a**} (1.60)	4.97^{a**} (1.75)	5.45^{b**} (1.70)	5.49^{c**} (1.64)	4.63^{c**} (1.82)	5.11 (1.77)
Perceived need to justify—Self	5.34 ^{a*} (2.71)	4.47^{a*} (2.79)	4.91 (2.78)	4.86 (2.79)	4.75 (2.71)	4.82 (2.80)	5.10 (2.80)	4.58 (2.75)	4.87 (2.78)
Perceived need to justify—Other	4.69 (2.90)	4.31 (2.65)	4.50 (2.78)	5.39^{a**} (2.87)	3.76^{a**} (2.61)	4.78 (2.87)	5.04^{c**} (2.89)	4.10^{c**} (2.64)	4.63 (2.82)
Ownership right	41.30 (24.67)	43.04 (27.89)	42.16^{b**} (26.25)	19.84 (23.71)	27.66 (25.74)	22.78^{b**} (24.71)	30.51^{c*} (26.42)	37.11^{c*} (28.02)	33.41 (27.29)
Likelihood to deinstall	83.31^{a**} (22.42)	68.68^{a**} (30.12)	76.02^{a} (27.39)	83.50^{a**} (23.39)	55.69^{a**} (28.20)	73.05^{b} (28.61)	83.31^{c**} (22.86)	63.67^{c**} (29.98)	74.68 (27.95)
IOS	5.00 (1.73)	5.41 (1.51)	5.20 (1.63)	–	–	–	–	–	–
Degree of closeness to other	83.36 (17.60)	83.00 (19.57)	83.18 (18.55)	–	–	–	–	–	–

M and *SD* represent mean and standard deviation respectively. All differences between perspectives per specifications, between specifications overall, and between perspectives overall were tested

$^{*}p < .05$, $^{**}p < .01$

[a] Significant difference between perspectives per specification

[b] Significant difference between specifications overall

[c] Significant difference between perspectives overall

Table 10 Pearson and spearman correlations (N=348)

Variable	1)	2)	3)	4)	5)	6)	7)	8)	9)	10)	11)
1) PO for data given away											
2) Categories of Neutralization	.23**$_S$										
3) Perceived need to justify—Self	.17**$_P$	.36**$_S$									
4) Perceived need to justify—Other	.15**$_P$	.37**$_S$	.56**$_P$								
5) Ownership right	−.47**$_P$	−.08$_S$	−.02$_P$	−.02$_P$							
6) IOS	−.02$_P$	.09$_S$	.09$_P$	.09$_P$	.12$_P$						
7) Closeness to the other	.03$_P$	.13$_S$	.12$_P$	.13$_P$	.05$_P$	.63**$_P$					
8) Likelihood to deinstall	.21**$_P$	.50**$_S$	.32**$_P$	.31**$_P$	−.07$_P$	.11$_P$	.14$_P$				
9) Existence of norms	.07$_P$	.16**$_S$	.24**$_P$	.31**$_P$	.04$_P$	.12$_P$	.03$_P$	.15**$_P$			
10) Social acceptance	−.13*$_P$	−.31**$_S$	−.25**$_P$	−.31**$_P$	.08$_P$	−.22**$_P$	−.14$_P$	−.37**$_P$	−.30**$_P$		
11) Personal morality	−.19**$_P$	−.33**$_S$	−.37**$_P$	−.27**$_P$	.19**$_P$	−.15*$_P$	−.07$_P$	−.37**$_P$	−.20**$_P$	.49**$_P$	
12) Gender	.07$_P$	.04$_S$	−.11*$_P$	−.04$_P$	−.06$_P$	.04$_P$	.16*$_P$	−.01$_P$	−.05$_P$	.08$_P$	.04$_P$
13) Age	.19**$_P$	.09$_S$	.24**$_P$	.20**$_P$	−.14*$_P$	.03$_P$	.11$_P$	.09$_P$	.00$_P$	−.15**$_P$	−.13*$_P$

*p < .05 **p < .01; $_P$=Pearson $_S$=Spearman, Categories of neutralization are treated as an ordinal variable here

(12 & 14) are depicted in Table 4. Results are depicted in Figs. 4 and 5.

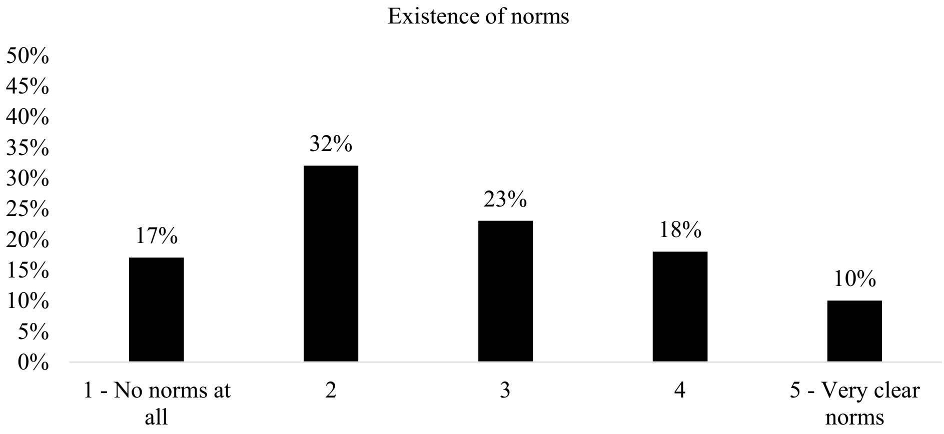


Fig. 4 Existence of norms about the sharing of others' data (N=348)

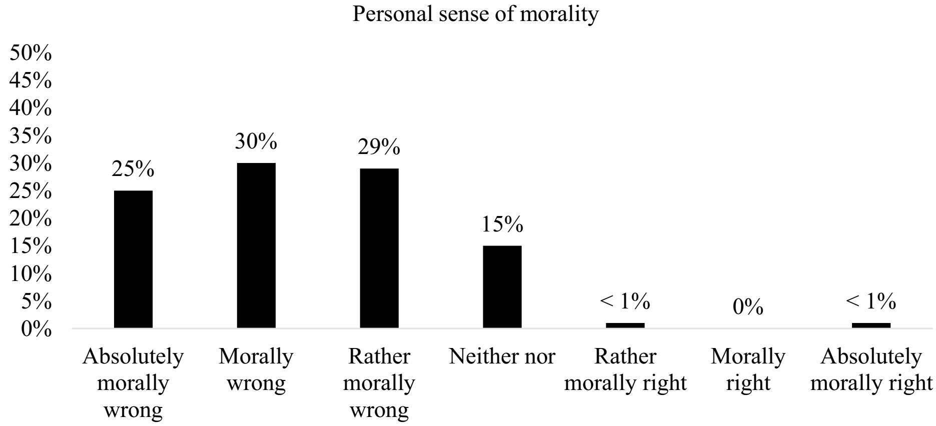


Fig. 5 Personal beliefs about the morality of the sharing of others' data (N=348)

Study 3

See Tables 11 and 12.

Table 11 Means and standard deviations ($N = 267$)

Perspective	Second-guessing								
	No			Yes			Overall		
	Offender	Victim	Overall	Offender	Victim	Overall	Offender	Victim	Overall
	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)	M (SD)
PO for the data given away	5.16 (1.83)	5.33 (1.78)	5.27 (1.79)	5.42 (1.69)	5.29 (1.77)	5.34 (1.74)	5.29 (1.76)	5.31 (1.77)	5.30 (1.76)
Perceived need to justify	5.28 (2.70)	4.35 (2.71)	4.70 (2.73)	4.68 (2.70)	4.71 (2.67)	4.70 (2.61)	4.98 (2.70)	4.53 (2.69)	4.70 (2.70)
Ownership right	41.84^{a**} (30.80)	28.49^{a**} (23.76)	33.55 (27.32)	38.88^{a*} (31.95)	26.74^{a*} (26.34)	31.24 (29.03)	40.36^{c**} (31.26)	27.60^{c**} (25.05)	32.38 (28.17)
Bad conscience	4.70 (1.87)	4.38 (1.83)	4.50 (1.84)	5.04 (1.78)	4.55 (1.56)	4.73 (1.66)	4.87 (1.82)	4.47 (1.70)	4.62 (1.75)

M and *SD* represent mean and standard deviation respectively. All differences between perspectives per second-guessing condition, between second-guessing conditions overall and between perspectives overall were tested

*$p < .05$, **$p < .01$

[a] Significant difference between perspectives per second-guessing condition

[b] Significant difference between second-guessing conditions overall

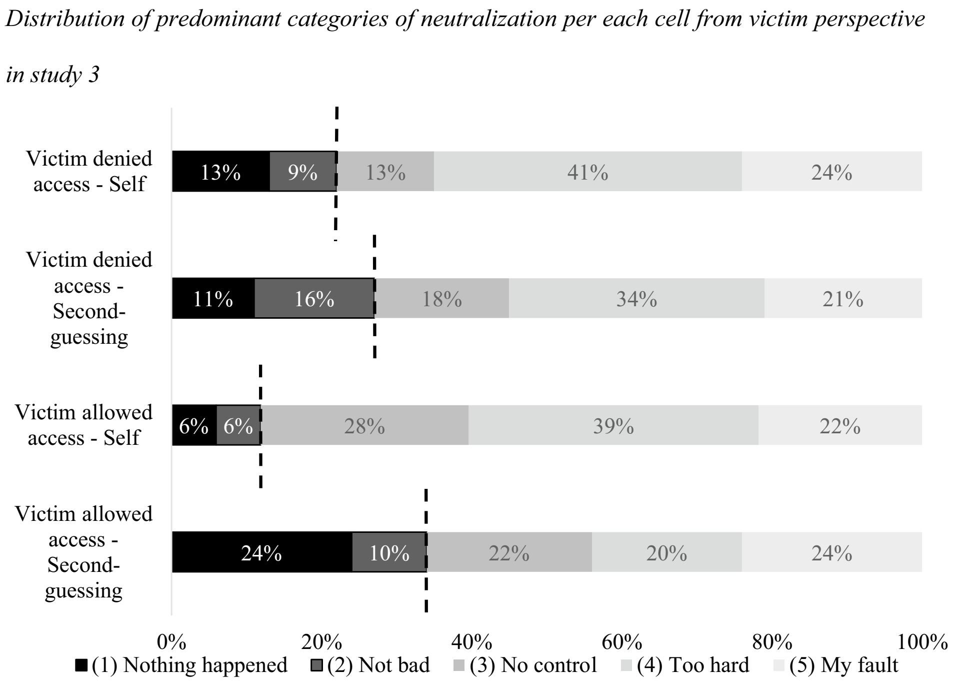
[c] Significant difference between perspectives overall

Table 12 Pearson and Spearman correlations ($N = 267$)

Variable	1)	2)	3)	4)	5)	6)	7)	8)	9)	10)	11)
1) PO for data given away											
2) Categories of Neutralization	.30**$_S$										
3) Perceived need to justify	.22**$_P$	.47**$_S$									
4) Ownership right	−.30**$_P$	−.07$_S$	−.00$_P$								
5) Bad conscience	.29**$_P$	.36**$_S$	.32**$_P$	−.01$_P$							
6) Realism	.06$_P$	−.05$_S$	−.01$_P$	−.01$_P$	−.16*$_P$						
7) Empathy	.29**$_P$	.16**$_S$	.08$_P$	.03$_P$	.17**$_P$	.20*$_P$					
8) Frequency	.27**$_P$	.18**$_S$	.13*$_{\mathrm{P}}$	.00$_P$	.31**$_P$	−.03$_P$	.32**$_P$				
9) Importance	.41**$_P$	.25**$_S$	.12*$_{\mathrm{P}}$	−.08$_P$	.40**$_{\mathrm{P}}$	−.13$_P$	.34**$_P$	.46**$_P$			
10) Problem	.46**$_P$	.31**$_S$	.19**$_P$	−.13$_P$	.51**$_P$	−.10$_P$	.33*$_P$	.33**$_P$	.62**$_P$		
11) Gender	.06$_P$	.06$_S$	−.13*$_P$	−.04$_P$	−.00$_P$	−.13$_P$	−.02$_P$	−.03$_P$	.05$_P$	.09$_P$	
12) Age	.16**$_P$	.12$_S$	.18**$_P$	−.04$_P$	.10*$_P$	−.07$_P$	.27**$_P$	.26**$_P$	.19**$_P$	.24**$_P$	−.17**$_P$

*$p < .05$ **$p < .01$; $_P$ = Pearson $_S$ = Spearman, Categories of neutralization are treated as an ordinal variable here

Fig. 6 Distribution of predominant categories of neutralization per each cell from victim perspective in study 3



Funding Open access funding provided by Vienna University of Economics and Business (WU).

Declarations

Conflict of interest There are no conflicts of interest to disclose.

Ethics approval The research involved human participants and all necessary ethics approvals we sought from the Vienna University of Economics and Business (WU Vienna)), Vienna, Austria.

Informed consent Informed consent was sought from all subjects who participated in the studies undertaken in this paper.

References

Acquisti, A., John, L. K., & Loewenstein, G. (2011). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research, 49*(2), 160–174. https://doi.org/10.1509/jmr.09.0215

Alicke, M. D., Klotz, M. L., Breitenbecher, D. L., Yurak, T. J., & Vredenburg, D. S. (1995). Personal contact, individuation, and the better-than-average effect. *Journal of Personality and Social Psychology, 68*(5), 804.

Amiot, C. E., Sansfaçon, S., & Louis, W. R. (2013). Investigating the motivations underlying harmful social behaviors and the motivational nature of social norms. *Journal of Applied Social Psychology, 43*(10), 2146–2157. https://doi.org/10.1111/jasp.12167

Anderson, C. A., & Godfrey, S. S. (1987). Thoughts about actions—the effects of specificity and availability of imagined behavioral scripts on expectations about oneself and others. *Social Cognition, 5*(3), 238–258.

Bamberg, S., & Möser, G. (2007). Twenty years after Hines, Hungerford, and Tomera: A new meta-analysis of psycho-social determinants of pro-environmental behavior. *Journal of Environmental Psychology, 27*(1), 17.

Bamberg, S., Hunecke, M., & Blöbaum, A. (2007). Social context, personal norms and the use of public transportation: Two field studies. *Journal of Environmental Psychology, 27*(3), 190–203.

Bandura, A., & Walters, R. H. (1977). *Social learning theory* (Vol. 1). Prentice Hall.

Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006). Privacy and contextual integrity: Framework and applications. In *2006 IEEE symposium on security and privacy (S&P'06)*.

Bauman, Z. (2013). *Liquid modernity*. Wiley.

Berg, M. T., & Mulford, C. F. (2020). Reappraising and redirecting research on the victim–offender overlap. *Trauma, Violence, & Abuse, 21*(1), 16–30.

Berg, M. T., & Schreck, C. J. (2022). The meaning of the victim–offender overlap for criminological theory and crime prevention policy. *Annual Review of Criminology, 5*, 277–297.

Bergauer, C. (2020). In Jahnel, Kommentar zur Datenschutz-Grundverordnung, Art. 2 DSGVO [Commentary on the General Data Protection Regulation, Article 2 GDPR].

Biczók, G., & Chia, P. H. (2013). Interdependent Privacy: Let Me Share Your Data. *Financial Cryptography and Data Security*, Berlin, Heidelberg.

Burke, M. A., Heiland, F. W., & Nadler, C. M. (2010). From "overweight" to "about right": Evidence of a generational shift in body weight norms. *Obesity, 18*(6), 1226–1234.

Chaudhry, A., Crowcroft, J., Howard, H., Madhavapeddy, A., Mortier, R., Haddadi, H., & McAuley, D. (2015). *Personal data: Thinking inside the box.* Proceedings of The Fifth Decennial Aarhus Conference on Critical Alternatives, Aarhus, Denmark.

Choi, J. J., Green, D. L., & Gilbert, M. J. (2011). Putting a human face on crimes: A qualitative study on restorative justice processes for youths. *Child and Adolescent Social Work Journal, 28*, 335–355.

Cialdini, R. B., Reno, R. R., & Kallgren, C. A. (1990). A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of Personality and Social Psychology, 58*(6), 1015.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 588–608.

Cohn, D. Y., & Vaccaro, V. L. (2006). A study of neutralisation theory's application to global consumer ethics: P2P file-trading of musical intellectual property on the internet. *International Journal of Internet Marketing and Advertising, 3*(1), 68–88.

Demmers, J., Weihrauch, A. N., & Mattison Thompson, F. H. (2022). Your data are (not) my data: The role of social value orientation in sharing data about others. *Journal of Consumer Psychology*. *32*(3), 500–508. https://doi.org/10.1002/jcpy.1255

De Groot, J. I., Bondy, K., & Schuitema, G. (2021). Listen to others or yourself? The role of personal norms on the effectiveness of social norm interventions to change pro-environmental behavior. *Journal of Environmental Psychology, 78*, 101688.

Eggers, F., Beke, F. T., Verhoef, P. C., & Wieringa, J. E. (2022). The market for privacy: Understanding how consumers trade off privacy practices. *Journal of Interactive Marketing*, 10949968221140061.

Elgaaied-Gambier, L., Monnot, E., & Reniou, F. (2018). Using descriptive norm appeals effectively to promote green behavior. *Journal of Business Research, 82*, 179–191.

Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent*. Oxford University Press.

Franz, A., & Benlian, A. (2022). Exploring interdependent privacy: Empirical insights into users' protection of others' privacy on online platforms. *Electronic Markets., 32*(4), 2293–2309. https://doi.org/10.1007/s12525-022-00566-8

Freestone, O., & Mitchell, V. (2004). Generation Y attitudes towards e-ethics and internet-related misbehaviours. *Journal of Business Ethics, 54*(2), 121–128.

Gino, F., & Galinsky, A. D. (2012). Vicarious dishonesty: When psychological closeness creates distance from one's moral compass. *Organizational Behavior and Human Decision Processes, 119*(1), 15–26.

Gottfredson, M. R., & Hirschi, T. (1990). *A general theory of crime*. Stanford University Press.

Harkous, H., & Aberer, K. (2017). " If You Can't Beat them, Join them" A Usability Approach to Interdependent Privacy in Cloud Apps. In *Proceedings of the seventh ACM on conference on data and application security and privacy* (pp. 127–138).

Harris, L. C., & Dumas, A. (2009). Online consumer misbehaviour: An application of neutralization theory. *Marketing Theory, 9*(4), 379–402.

Hofmann, W., Brandt, M. J., Wisneski, D. C., Rockenbach, B., & Skitka, L. J. (2018). Moral punishment in everyday life. *Personality and Social Psychology Bulletin, 44*(12), 1697–1711.

Hornsey, M. J., Smith, J. R., & Begg, D. (2007). Effects of norms among those with moral conviction: Counter-conformity emerges on intentions but not behaviors. *Social Influence, 2*(4), 244–268.

Hoyle, R., Stark, L., Ismail, Q., Crandall, D., Kapadia, A., & Anthony, D. (2020). Privacy norms and preferences for photos posted online. *ACM Transactions on Computer-Human Interaction (TOCHI), 27*(4), 1–27.

Humbert, M., Trubert, B., & Huguenin, K. (2019). A survey on interdependent privacy. *ACM Computing Surveys, 52*(6), Article 122. https://doi.org/10.1145/3360498

Kamleitner, B., & Mitchell, V.-W. (2018). Can consumers experience ownership for all their personal data? From issues of scope and invisibility to agents handling our digital blueprints. In J. Peck & S. B. Shu (Eds.), *Psychological ownership* (pp. 91–118). Springer.

Kamleitner, B., Mitchell, V.-W., Stephen, A. T., & Kolah, A. (2018). Your customers may be the weakest link in your data privacy defenses. *MIT Sloan Management Review*, May 22, 2018 https://sloanreview.mit.edu/article/your-customers-may-be-the-weakest-link-in-your-data-privacy-defenses/

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

Kaptein, M., & van Helvoort, M. (2019, 2019/10/03). A model of neutralization techniques. *Deviant Behavior, 40*(10), 1260–1285. https://doi.org/10.1080/01639625.2018.1491696

Kenrick, D. T., Li, N. P., & Butner, J. (2003). Dynamical evolutionary psychology: Individual decision rules and emergent social norms. *Psychological Review, 110*(1), 3–28.

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*, 122–134.

Lapinski, M. K., & Rimal, R. N. (2005). An explication of social norms. *Communication Theory, 15*(2), 127–147.

Lapovsky, I. (2018). *Facebook exposed 87 million users to cambridge analytica*. Wired. Retrieved 09/10/2021 from https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/

Lauritsen, J. L., & Laub, J. H. (2007). Understanding the link between victimization and offending: New reflections on an old idea. *Crime Prevention Studies, 22*, 55–75.

Lee, J., & Holyoak, K. J. (2020). "But he's my brother": The impact of family obligation on moral judgments and decisions. *Memory & Cognition, 48*, 158–170.

Lerner, M. J., & Mikula, G. (Eds.). (2013). *Entitlement and the affectional bond: Justice in close relationships*. Springer.

Licht, A. N. (2008). Social norms and the law: Why peoples obey the law. *Review of Law & Economics, 4*(3), 715–750.

Lin, L., & McFerran, B. (2016). The (ironic) Dove effect: Use of acceptance cues for larger body types increases unhealthy behaviors. *Journal of Public Policy & Marketing, 35*(1), 76–90. https://doi.org/10.1509/jppm.14.020

Litt, E., & Hargittai, E. (2014). Smile, snap, and share? A nuanced approach to privacy and online photo-sharing. *Poetics, 42*, 1–21.

Loschelder, D. D., Siepelmeyer, H., Fischer, D., & Rubel, J. A. (2019). Dynamic norms drive sustainable consumption: Norm-based nudging helps café customers to avoid disposable to-go-cups. *Journal of Economic Psychology, 75*, 102146.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*, 551–569.

Matsueda, R. L. (2001). Differential association theory. *Encyclopedia of Criminology and Deviant Behavior, 1*, 125–130.

Morando, F., Iemma, R., & Raiteri, E. (2014). Privacy evaluation: What empirical research on users' valuation of personal data tells us. *Internet Policy Review, 3*(2), 1–12.

McCarthy, R., Rivers, A. K., Jensen, A. P., Pawirosetiko, J. S., & Erickson, J. M. (2021). The victim-perpetrator asymmetry is stronger in situations where blame is being assigned. *Journal of*

Experimental Social Psychology, 96, 104164. https://doi.org/10.1016/j.jesp.2021.104164

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review, 79*, 119.

Nunan, D., & Di Domenico, M. (2013). Market research and the ethics of big data. *International Journal of Market Research, 55*(4), 505–520. https://doi.org/10.2501/IJMR-2013-015

Odou, P., & Bonnin, G. (2014). Consumers' neutralization strategies to counter normative pressure: The case of illegal downloading. *Recherche Et Applications En Marketing (english Edition), 29*(1), 103–121.

Olteanu, A. M., Huguenin, K., Shokri, R., Humbert, M., & Hubaux, J. P. (2017). Quantifying interdependent privacy risks with location data. *IEEE Transactions on Mobile Computing, 16*(3), 829–842.

Oetzel, M. C., & Gonja, T. (2011). The online privacy paradox: a social representations perspective. In *CHI'11 extended abstracts on human factors in computing systems* (pp. 2107–2112).

Osgood, D. W., Wilson, J. K., O'Malley, P. M., Bachman, J. G., & Johnston, L. D. (1996). Routine activities and individual deviant behavior. *American Sociological Review*, 635–655.

Pedersen, E. R., & LaBrie, J. W. (2008). Normative misperceptions of drinking among college students: A look at the specific contexts of prepartying and drinking games. *Journal of Studies on Alcohol and Drugs, 69*(3), 406–411.

Petronio, S. (2000). "The Boundaries of Privacy: Praxis of Everyday life," in EA's Communication Series. Balancing the Secrets of Private Disclosures, Sandra Petronio, ed. (pp. 37–49). Mahwah, NJ, US: Lawrence Erlbaum Associates Publishers

Petronio, S. (2015). *Communication privacy management theory*. Wiley.

Pu, Y., & Grossklags, J. (2016). Towards a model on the factors influencing social app users' valuation of interdependent privacy. *Proceedings on Privacy Enhancing Technologies, 2016*(2), 61–81.

Pu, Y., & Grossklags, J. (2017). Valuating {Friends'} privacy: Does anonymity of sharing personal data matter?. In *Thirteenth symposium on usable privacy and security (SOUPS 2017)* (pp. 339–355).

Rosa, H. (2013). *Social acceleration*. Columbia University Press.

Rossano, M. J. (2012). The essential role of ritual in the transmission and reinforcement of social norms. *Psychological Bulletin, 138*(3), 529–549.

Runions, K. C., & Bak, M. (2015). Online moral disengagement, cyberbullying, and cyber-aggression. *Cyberpsychology, Behavior, and Social Networking, 18*(7), 400–405.

Sah, S., & Loewenstein, G. (2012). More affected= more neglected: Amplification of bias in advice to the unidentified and many. *Social Psychological and Personality Science, 3*(3), 365–372.

Sarigol, E., Garcia, D., & Schweitzer, F. (2014). Online privacy as a collective phenomenon. In *Proceedings of the second ACM conference on Online social networks, Dublin, Ireland*. https://doi.org/10.1145/2660460.2660470

Schultz, P. W. (2022). Secret agents of influence: Leveraging social norms for good. *Current Directions in Psychological Science, 31*(5), 443–450.

Schwartz, S. H. (1977). Normative influences on altruism. In *Advances in Experimental Social Psychology* (Vol. 10, pp. 221–279). Academic Press.

Serviere-Munoz, L., & Mallin, M. L. (2013). How do unethical salespeople sleep at night? The role of neutralizations in the justification of unethical sales intentions. *Journal of Personal Selling & Sales Management, 33*(3), 289–306.

Shilton, K., & Greene, D. (2019). Linking platforms, practices, and developer ethics: Levers for privacy discourse in mobile application development. *Journal of Business Ethics, 155*(1), 131–146.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management, 54*(8), 1023–1037.

Sykes, G. M., & Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American Sociological Review, 22*(6), 664–670. https://doi.org/10.2307/2089195

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.

Symeonidis, I., Shirazi, F., Biczók, G., Pérez-Solà, C. & Preneel, B. (2016). Collateral damage of facebook apps: Friends, providers, and privacy interdependence. In *IFIP advances in information and communication technology* (S. 194–208). Springer. https://doi.org/10.1007/978-3-319-33630-5_14

Thürridl, C., Kamleitner, B., Ruzeviciute, R., Süssenbach, S., & Dickert, S. (2020). From happy consumption to possessive bonds: When positive affect increases psychological ownership for brands. *Journal of Business Research, 107*, 89–103.

Tannenbaum, M. B., Hepler, J., Zimmerman, R. S., Saul, L., Jacobs, S., Wilson, K., & Albarracín, D. (2015). Appealing to fear: A meta-analysis of fear appeal effectiveness and theories. *Psychological Bulletin, 141*(6), 1178–1204. https://doi.org/10.1037/a0039729

Trope, Y., Liberman, N., & Wakslak, C. (2007). Construal levels and psychological distance: Effects on representation, prediction, evaluation, and behavior. *Journal of Consumer Psychology, 17*(2), 83–95.

Veatch, R. M. (2007). Implied, presumed and waived consent: The relative moral wrongs of under-and over-informing. *The American Journal of Bioethics, 7*(12), 39–54.

Weiss, A., Burgmer, P., & Mussweiler, T. (2018). Two-faced morality: Distrust promotes divergent moral standards for the self versus others. *Personality and Social Psychology Bulletin, 44*(12), 1712–1724.

Wenzel, M. (2005). Motivation or rationalisation? Causal relations between ethics, norms and tax compliance. *Journal of Economic Psychology, 26*(4), 491–508.

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly, 37*(1), 1–20.

Woods, D. P., & Böhme, R. (2022). The commodification of consent. *Computers & Security, 115*, 102605. https://doi.org/10.1016/j.cose.2022.102605

Worthington Jr, E. L. (2009). *Forgiving and reconciling: Bridges to wholeness and hope*. InterVarsity Press.

Yoshida, E., Peach, J. M., Zanna, M. P., & Spencer, S. J. (2012). Not all automatic associations are created equal: How implicit normative evaluations are distinct from implicit attitudes and uniquely predict meaningful behavior. *Journal of Experimental Social Psychology, 48*(3), 694–706.

Zukic, E. (2019). Die Reichweite der Haushaltsausnahme der DS-GVO am Beispiel sozialer Online-Netzwerke und Bildaufnahmen. In *Datenschutzrecht Jahrbuch 2019* (pp. 61–93). Neuer Wissenschaftlicher Verlag-NWV.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.