Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements

Kamleitner, Bernadette; Mitchell, Vince

Published in:
Journal of Public Policy and Marketing JPP&M

DOI:
10.1177/0743915619858924

Published: 01/01/2019

Document Version
Publisher's PDF, also known as Version of record

AMERICAN MARKETING ASSOCIATION

Journal of Public Policy & Marketing
2019, Vol. 38(4) 433-450


Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/0743915619858924
journals.sagepub.com/home/ppo

Your Data Is My Data: A Framework for Addressing Interdependent Privacy Infringements

Bernadette Kamleitner and Vince Mitchell

Abstract

Everyone holds personal information about others. Each person's privacy thus critically depends on the interplay of multiple actors. In an age of technology integration, this interdependence of data protection is becoming a major threat to privacy. Yet current regulation focuses on the sharing of information between two parties rather than multiactor situations. This study highlights how current policy inadequacies, illustrated by the European Union General Data Protection Regulation, can be overcome by means of a deeper understanding of the phenomenon. Specifically, the authors introduce a new phenomenological framework to explain interdependent infringements. This framework builds on parallels between property and privacy and suggests that interdependent peer protection necessitates three hierarchical steps, "the 3Rs": realize, recognize, and respect. In response to observed failures at these steps, the authors identify four classes of intervention that constitute a toolbox addressing what can be done by marketers, regulators, and privacy organizations. While the first three classes of interventions address issues arising from the corresponding 3Rs, the authors specifically advocate for a fourth class of interventions that proposes radical alternatives that shift the responsibilities for privacy protection away from consumers.

Keywords

consumer rights, data protection failure, digital technology, interdependent privacy infringements, personal data ownership

It is a little-discussed yet indisputable fact that privacy is not just personal, but interdependent. People are socially intertwined (Jetten, Haslam, and Alexander 2012) and bond with each other by sharing information (Petronio 2000). Consequently, everyone holding information about us, be it companies or other consumers, can compromise our privacy by passing on personal information that we might not have volunteered ourselves. Privacy is, therefore, a multiactor phenomenon. As technology advances to facilitate passive information sharing over an expanding range of devices (Bélanger and Crossler 2011; Fu et al. 2017; Williams, Nurse, and Creese 2016), consumers who hold and collect information about others, such as their family or colleagues, pose an increasing threat to these others' privacy. This threat is likely to increase in scope and complexity worldwide (Walker 2016). It affects marketers, who often are in charge of data collection, and it affects policy makers, who have yet to devote their full attention to the privacy infringements that arise from the use of data by private individuals. Presently, the issue of interdependent privacy constitutes a regulatory loophole even for the current best in class, the European Union General Data Protection Regulation (EU GDPR).

To illustrate the problem, let us introduce the case of Jane, which we will refer to throughout. Jane stands for any consumer who wants to download an app requesting access to data that may concern others. In the case of Jane, she wants to download a weather app. When she clicks "install," she not only gets the app's promised services, but also says "yes" to its request to access all her contacts as part of the download. With this small act, Jane essentially agrees to share the personal data of people other than herself.

That this can have momentous consequences has become evident in the case of Cambridge Analytica. The company received the personal information of more than 71 million people from only 270,000 consumers who installed its app-based personality quiz on Facebook (Bowcott and Hern 2018). On average, everyone taking that quiz infringed on the privacy of 263 others. The increasing integration of technology

Bernadette Kamleitner is Professor of Marketing, Department of Marketing, WU Vienna University of Economics and Business, Austria (email: bernadette.kamleitner@wu.ac.at). Vincent Wayne Mitchell is Professor of Marketing, University of Sydney Business School, University of Sydney, Australia (email: vince.mitchell@sydney.edu.au).

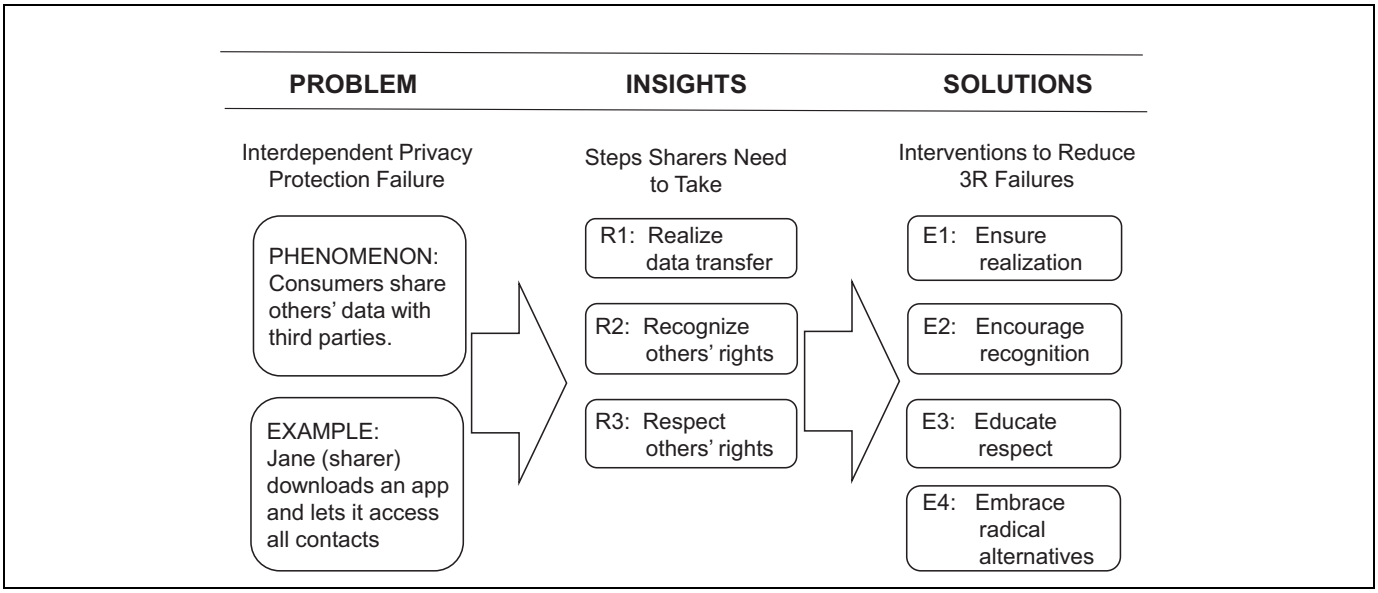

Figure 1. A summary of the problem and solution framework and its conceptual core, the 3R insight framework.

into everyday activities and homes will ensure that problems like this multiply across the globe. When downloading apps, people often volunteer access to data that others might rightly claim, such as contacts, pictures, or conversation logs. When plugging in "always-on" listening devices, such as Amazon Echo or smart TVs, people even agree to the passive monitoring of all their social surroundings.

Given these developments, interdependent privacy protection is a pressing issue. To date, there are only a few scholarly contributions on the phenomenon (e.g., Biczók and Chia 2013; Litt and Hargittai 2014; Morlok 2016; Pu and Grossklags 2016) and the scope of potential damages (Harkous and Aberer 2017; Olteanu et al. 2017). For example, Litt and Hargittai (2014) show that gender and digital media experience relate to the online sharing of pictures involving others and that this may come at a social cost. Similarly, Pu and Grossklags (2016) find that privacy concerns also affect how users value their friends' personal information. While addressing several interesting facets of the phenomenon, these studies hold only partial insights into why and how interdependent privacy infringements happen and do not address how these can be reduced or affected by marketers and regulators.

This article attempts to provide such insights. We draw on the conceptual similarity with the multiactor phenomenon of property and engage in a multicase analysis of interdependent infringements of both privacy and property rights by other consumers. From this analysis we derive a hierarchical framework, the "3R" framework, that helps explain why consumers may fail to protect others' personal data. In addition, we develop four classes of interventions that can help prevent or circumvent these failures. These interventions pertain to all stakeholders, include elements of self-regulation and regulation, and serve as a toolbox for all those interested in, or responsible for, interdependent privacy protection. Figure 1 summarizes the main problem, the framework of empirical insights, and the resulting interventions.

This article provides the first encompassing analytical, solution-focused, and policy-related analysis of interdependent privacy protection across fields. The novel 3R framework expands prior privacy work by focusing on multiactor, rather than dyadic, information transfers. It takes a novel approach by intertwining privacy and property conceptually and thus allows for fresh insights on both phenomena. Importantly, it also helps explain why interdependent privacy protection frequently fails in digital contexts and why current data protection efforts fall short in preventing interdependent privacy breaches.

We begin by examining the interdependence of privacy and the failure of current policies to adequately address the issue. We then identify what can be learned from conceptualizing personal data as property before discussing the methods used to develop the 3R framework. Next, we provide a detailed analysis of the four intervention classes that arise from the framework. To better illustrate the scope of regulatory gaps and the policy interventions, we use examples of EU and U.S. jurisdictions. The article ends with a discussion of how to draw on the framework's hierarchical properties to prioritize available interventions and our conclusion that sustainable interdependent privacy protection necessitates radical alternatives.

Theoretical Background

Privacy as an Interdependent Phenomenon

The need to belong is a fundamental human need (Baumeister and Leary 1995). Health and happiness rely on connection to, and interaction with, others (Jetten, Haslam, and Alexander 2012; Johnson 2003; Lambert et al. 2013). The conduit that allows for social interaction is communication (i.e., the sharing

of information both online and offline; Sinclair and Grieve 2017). Although the information people share with each other also includes their own personal details, the fact that people know things about each other gives rise to the notion of privacy as an interdependent phenomenon (Biczók and Chia 2013; Harkous and Aberer 2017; Pu and Grossklags 2016). The interdependence of privacy means that everyone holding information about a person can compromise his or her privacy, potentially without even noticing (e.g., a slip of the tongue, posting a picture online, accidentally transferring files containing intimate information; for multiple examples of interdependent privacy breaches, see Table 1). This means that there are potentially many more actors who invade privacy than try to protect privacy. Once shared, it is easy to lose control over even the most intimate data (Acquisti, Brandimarte, and Loewenstein 2015).

In an analog world, where everybody holds information about others (Petronio 2000), peer-privacy protection appears to work according to "implicit norms about what, why, and to whom information is shared within specific relationships" (Martin 2016, p. 551). People implicitly negotiate what information they divulge (Petronio 2015) and are mostly willing to respect others' privacy (for insights along these lines, see Afifi and Caughlin [2006] and Vangelisti and Caughlin [1997]). However, with new information and communication technologies, these negotiations are largely absent.

This is particularly problematic because, with new technologies, the scope for interdependent privacy infringements is significantly larger. In online settings, where people use devices to automatically and effortlessly collect and disclose information digitally (Kamleitner and Mitchell 2018), peer-privacy protection frequently fails (Litt and Hargittai 2014; Symeonidis et al. 2016). Although consumers are wary about others sharing their information online, and may even suffer from the social costs of having their trust in others broken (Litt and Hargittai 2014), they nonetheless regularly click accept to requests for data about others (Morlok 2016; Pu and Grossklags 2016), effectively infringing others' privacy. For example, when people collaborate on folders in cloud services, such as Google Drive, a collaborator's behavior contributes significantly to his or her own privacy risks (Harkous and Aberer 2017) and data volunteered by others make it difficult for people to keep their location private (Olteanu et al. 2017, p. 829). To illustrate, when people sign into a website with their social media account, they are potentially sharing the data of people in their network. Four out of five internet users dislike traditional registration forms, and 73% prefer to log in with their social media accounts (Bishoff 2016). When an app uses Facebook authorization, it can ask for up to 40 different permissions, ranging from access to photos to timeline posts to friends' lists. As a result, Facebook can track what consumers have done on over 8.4 million websites with the Facebook like button (Martineau 2018).

Interdependent Privacy and Current Regulations

The phenomenon of interdependent privacy infringements arises through the intertwined nature of human beings in society. It is, thus, a universal phenomenon that stretches across legal jurisdictions and becomes more important as humans and things become more technologically connected, meaning that more actors could gain and provide access to information at the tap of a screen.

Despite this, current laws and regulations across various territories reflect little awareness of the implications of interdependent privacy breaches. The prevalent use case in policy formulation has tended to simplify informational privacy as a phenomenon encompassing two actors: the discloser (the consumer or company) and the receiver (the company). This perspective appears to inform most privacy regulations (DLA Piper 2019), including those of the EU and the United States. Consistent with this perspective, regulators primarily focus on what organizations, rather than individual consumers like Jane, do with data. This allows for loopholes when it comes to privacy infringements as acts of social interdependence.

We illustrate this widespread regulation gap with an analysis of current best-in-class data protection regulation, the EU GDPR, which became fully enforceable in May 2018. Notably, the relevance of the GDPR stretches beyond the EU and is, for example, relevant to U.S. companies that sign up for Privacy Shield, the U.S. scheme for companies that want to comply with GDPR. It is applicable to any company worldwide that holds the data of EU citizens or that processes data of any world citizen in the EU.

A central Article in the GDPR is Article 6, which spells out the lawful grounds for processing personal data. Overall, Article 6 entails six such lawful grounds. First among them is paragraph 1a, which specifies consent by the data subject as a lawful ground. Article 7 further specifies what it means to obtain informed consent from, and requires notification of, the original data owner together with easy withdrawal of consent. This assumes that it is always clear who is the original owner. It does not acknowledge that humans are socially intertwined and may have others' information. For example, some personal data on Jane's phone, such as conversations and pictures, may be claimed by her friends, yet it is Jane, not her friends, who gives consent for use of the data. Article 7 also overlooks that personal data of one individual may be held and thus shared by multiple individuals with organizations. For example, when an app asks for access to a person's contacts, the app does not obtain consent from the original data owner. Neither of these issues is well-captured by the GDPR or any other regulation known to us. Indeed, in Article 2, the GDPR specifically excludes processing of personal data for household or purely personal purposes. This signals some awareness of the social necessity of information sharing but simultaneously further blurs the issue.

The answer to the question of who is responsible for obtaining consent when Jane, as a consumer of a weather app, shares personal data about others is unclear. Should the onus be on

Table 1. Illustrative Cases of Interdependent Infringements of Others' Personal Data Due to Failures to Realize, Recognize, and Respect.

#	Failure to	Synopsis	Context
1	Realize	Sharer installs recipient's always-on device (e.g., Amazon Echo) and does not bother to switch it on and off. Others come to visit sharer and hold an intimate conversation while the device remains switched on and listens in.	Digital
2	Realize	Sharer is on Facebook and takes part in a quiz programmed by recipient. Without reading, sharer ticks agree to the terms and conditions that give access to sharer's profile data. This includes access to her friends' profiles.	Digital
3	Recognize	Sharer proudly posts pictures of "his" child going to the potty for the first time on social media.	Digital
4	Recognize	Sharer wants a crossword app. When downloading the app, a window pops up. Sharer reads that the app wants access to all contacts (i.e., personal details of others). Without a second thought, sharer presses "accept and install."	Digital
5	Recognize	Investigative journalist R tricks politician O's secretary S to reveal information about politician O by ostensibly asking S for his own life story.	Analog
6	Respect	Sharer hacks other's Google Drive account and sells pictures of her to the highest bidder R.	Digital
7	Respect	Sharer knows that a communication app collects others' data when accessing contacts and call logs but installs the app like all her friends.	Digital
8	Respect	Other breaks up with sharer. Sharer takes revenge and uploads private pictures of other onto website R.	Analog
9	Respect	Other tells sharer that she has been diagnosed with leukemia. Both likely know that this information is meant to be for the sharer's ears only. One day, sharer is drunk and lets slip the news about the diagnosis to recipient.	Analog
10	Respect	Sharer goes shopping and is offered a discount by a shop if he participates in a referral program. Sharer really wants this discount and provides other's contacts.	Analog
11	Respect	Criminal R asks sharer for other's personal data at knife point. Sharer provides this information.	Analog
12	Recognize	Other and sharer prepare a presentation for class. Being in the same program, they have similar-looking USB flash drives. They save the presentation on other's stick, which also contains personal pictures and PDFs of other's birth certificate. Sharer pockets the stick. When R needs a stick later, sharer quickly volunteers other's stick thinking it is his own.	Analog and digital
13	Respect	Sharer finds the diary of her roommate O. Sharer sells the diary to researcher (R) who is purchasing diaries for a research project.	Analog
14	Realize	Architect O asks colleague S to comment on her latest design and provides S with access to a folder on a cloud service. S downloads editing app (R), which requires access to all accounts and files (including on cloud services).	Digital
15	Realize	Sharer opens an email containing spyware programmed by R. This spyware sends all files on sharer's device to R. Sharer is a lawyer specializing in patents. Other's patents are on sharer's device.	Digital
16	Realize	Neighbors sharer and other meet in the supermarket. Sharer is shopping for recipient. Other stands in line before sharer and accidentally leaves behind a purchased can of tuna. Sharer mindlessly puts other's tuna into his bag and brings the entire bag to his recipient.	Analog
17	Recognize	Sharer copies a book written by other. As a service to her classmates, she shares the PDF copy with them.	Digital
18	Recognize	Recipient visits a webpage for free music. She does not recognize that this is an illegal download service and downloads songs by other artists.	Digital
19	Recognize	Other lends a book to sharer. Sharer eventually puts it into a box with random items. When sharer moves house, he decides to hold a garage sale. Recipient buys the whole box with random items from sharer.	Analog
20	Recognize	Sharer, other, and recipient are in a meeting. Sharer asks other for a pen. Next, recipient needs a pen. Sharer hands recipient other's pen. Without further thought, recipient pockets the pen when leaving the meeting.	Analog
21	Respect	Bestselling author other has just finished a new book. Sharer learns about this, hacks other's computer, and sells the book file to recipient.	Digital
22	Respect	Sharer and other jointly write a paper, with sharer taking the lead. Sharer submits the paper to journal recipient under his own name only.	Digital
23	Respect	Sharer and other jointly build a boat. One day, sharer meets recipient, who offers to buy the boat. Sharer agrees.	Analog
24	Respect	S is a burglar. She breaks into the home of other and steals a laptop. She later sells it to recipient on the black market.	Analog

Notes: Sharers, others, and recipients could be people or organizations.

Jane to ensure that she only passes on information that she has permission to give, or should it be the responsibility of the organizations that receive and request the data to ensure that they obtain consent from all original data subjects? The common policy assumption appears to be that if consumers have the data, then they have the right to share it.

However, this approach is challenged by human rights regulation. Article 8 of the European Convention on Human Rights provides a right to respect for one's "private and family life, his home and his correspondence" (European Court of Human Rights 2019). Drawing on this right, German courts prosecuted an individual for sharing others' data on WhatsApp.[1] One could argue that this ruling offers an alternative regulatory mechanism for addressing the sharing of others' data. However, consider that (1) most consumers use privacy-invasive apps such as WhatsApp, (2) potentially even more invasive "always-on" smart technologies are on the rise, and (3) consumers have no way of finding out which information about them is tracked by an app or gadget. If consumers are tasked with ensuring consent for all information they (are made to) share, then every person would need to prosecute their friends and family.

Thus, even the newest and most comprehensive data protection policy has its limits when faced with the interplay of the deeply social and interdependent nature of privacy and new technological realities that can turn everyday activities into privacy infringements. Given the opaque data protection policies, the interdependence of consumers' privacy not only constitutes a threat to the individual but also exposes companies and those drawing on third-party data to the risk of lawsuits (Kamleitner et al. 2018). This is relevant to marketers, who tend to be involved in, or even in charge of, customer insights and the underlying data collection practices. To help determine how to best allocate responsibilities and enhance interdependent privacy protection, a better understanding of the underlying phenomenon and its dynamics is needed. Our starting point for this endeavor is the conceptual similarity between personal data and property.

Personal Data and Property

Debates on the right to and nature of privacy indicate the existence of parallels between privacy and property (Cohen 2000; Laudon 1996; Schoeman 1984; Warren and Brandeis 1890). On the one hand, personal information, a key element to privacy, is often treated like property. Like any other good, personal data is traded in a market that has been valued at over US$200 billion (Levine 2014). People also feel a sense of ownership for both property (Etzioni 1991; Pierce, Kostova, and Dirks 2003) and personal information (Kehr et al. 2015; Spiekermann and Korunovska 2017). In fact, perceptions of information ownership are a central premise in the leading theory on privacy management, communication privacy management theory (Petronio 2010; Petronio 2000). On the other hand, interference with possessions, such as a car or house, may be viewed as an intrusion of privacy (Benn 1971) because these possessions count as part of the self and hold information about us (Belk 2013).

The primary difference between privacy and property lies in their targets. Privacy has been framed as a right to one's own information and personal space, and property as a right to one's own possessions. (To bring these differences and similarities to life, see multiple cases of privacy and property infringement in Table 1.) The crossover between these rights becomes particularly pronounced in the case of information goods, such as software, books, or music (Bakos, Brynjolfsson, and Lichtman 1999; Galbreth, Ghosh, and Shor 2012; Varian 2003). These goods fall under the remit of property but, mostly through technology, are as easily shared, transferred, and multiplied as personal data (Kamleitner and Mitchell 2018). In addition, as cases 12 and 13 in Table 1 show, personal data is often stored on tangible possessions. When these possessions become infringed, this likely entails a simultaneous personal data infringement.

Personal data and property rights both allow individuals to exclude others from trespassing onto what is "theirs" (Purtova 2015; Warren and Brandeis 1890). However, as the cases in Table 1 illustrate, others often have access to what is somebody else's. For example, Jane has access to others' personal data, which she saves in her contact list. Effectivly protecting personal data and property from infringement requires cooperation by those who have access to a person's goods (Kirk, Peck, and Swain 2018; Rudmin 1991; Rudmin 2016) or information (Benn 1971; Petronio 2000; Schwartz 1968). Privacy and property rights are interdependent, and their protection requires multiple actors.

Common social rules reflect and recognize this potential weak spot. Learning to respect what is others', including their secrets (Farrell, DiTunnariello, and Pearson 2014), is an essential part of humans' moral development (DeScioli, Rosa, and Gutchess 2015; Gibbs et al. 2013) and people generally condemn the disrespecting of others' possessions and personal information as morally wrong. To illustrate, let us revisit Jane and imagine that a stranger on the street asked her for her mother's contact details. Although this does not threaten her own privacy, Jane might think this an intolerable intrusion into her mother's privacy and protect it rather than help infringe it.

In the case of property, respect for others' property is common and tends to go unquestioned. This might explain why our current knowledge on interdependent infringements is scarce, though urgently needed, as demonstrated in the fictitious case of Jane and the real-world example of Cambridge Analytica. Although we have few insights into the dynamics of interdependent personal data infringements such as these, there are prior insights on related types of infringements. Specifically, there is research on what makes people engage in property crime (Andrews and Bonta 2014; Kanazawa and Still 2000; Tyler 2006) and on the illegal digital sharing of information goods such as music (Rochelandet and Le Guel 2005; Sinha and Mandel 2008; Wingrove, Korpas, and Weisz 2011). In a

[1] See the full court judgement at http://www.lareda.hessenrecht.hessen.de/lexsoft/default/hessenrecht_lareda.html#docid:7876045.

nutshell, insights on these phenomena suggest that people infringe when they stand to gain from the infringement and when there is a favorable cost–benefit ratio or, in some cases, when they want to harm others.

Though informative, these insights do not readily transfer to interdependent privacy infringements such as the one committed by Jane when she shared the personal data of her contacts with the installation of a weather app. Jane is bound to feel close to at least some of her contacts. It is thus unlikely that she wants to harm them all. Moreover, her only gain was easy access to information about the weather, and there are multiple alternative avenues to gain this information. It is thus unlikely that Jane infringed on her contacts' personal data because of the benefits of infringement. There must be more to interdependent infringements than current research reveals. Therefore, in the next section we revisit the basic phenomenon of infringements due to interdependence (for concrete examples, see Table 1).

The Phenomenon of Infringements Due to Interdependence

Interdependent infringement means that personal data or property is accessed by a party who the owner of that good or information did not intend to have access. Infringements become interdependent when this happens through another party that does have (legitimate) access. This requires at least three actors. First, it requires one or multiple infringed parties. In the example of Jane this would be all her contacts. We call this party the "others." Second, it requires someone like Jane, that is, one or multiple people with (legitimate) access to the others' data or goods who pass on what is the others' without involving them. We call this type of actor the "sharer." Finally, it requires one or multiple parties that obtain access to what is the others' through the sharer. This would, for example, be the weather app company that obtains others' personal data through Jane and her contact list. We call these actors the "recipients." Table 1 illustrates such situations. A situation qualifies as an infringement when the others have not consented to recipients receiving their goods. Because the good is transferred through the sharer, the sharer is key to whether the transfer happens at all, and, if so, whether the others have the opportunity to consent.

Beyond the described exceptions of self-interest and malicious intent, we know little about why the sharer would enable an infringement of what is others'. Therefore, it is difficult to allocate blame or successfully prosecute such cases of interdependent infringements. Similarly, developing strategies to preempt or reduce them is challenging without deeper knowledge. It is these issues that we consider when next creating a conceptual framework of interdependent protection failures.

Methods

To ensure the required conceptual richness, we examine, assimilate, and contrast both interdependent privacy and property infringements. Because cases like Jane's constitute the primary regulatory loophole, our focus is on cases in which the sharer and the other(s) are (multiple) individuals. Moreover, we particularly focus on the role technology may play in this, contrasting cases in which the context of infringement is mediated by digital technologies, such as in the case of Jane's weather app, and those that are analog in nature, such as Jane providing her mother's data to a stranger on the street (see Table 1).

Methodological Approach

We conduct an instrumental, multicase study, which allows us to learn through assimilation and contrast (Stake 2006). To facilitate insights on whether infringing consumers should be held responsible, we focus on the phenomenon as experienced by the person of the sharer (Creswell and Creswell 2017) and enrich our analyses with aspects of phenomenology (Goulding 2005; Schutz 1967).

Data Collection and Sources

The criterion we used for case inclusion was that cases must entail an instance of factual infringement. Over the span of a year, we collected evidence of such instances from a variety of sources, including stories of infringement from forums on property and privacy, identified by using simple Google searches on problems of sharing/infringing/trespassing (for similar procedures, see Kozinets [2006]); the media; and numerous formal and informal discussions with experts on property law and privacy, scholars from a range of disciplines, students at all levels, audience members of public lectures given by the authors, family members and friends, and even strangers who had infringement stories to tell (for a similar openness to sources see, e.g., Fournier [1998]). Much of this data collection happened as part of our everyday private and professional lives and included self-observation data that came from personal concurrent and retrospective introspection (Gould 1995; Wallendorf and Brucks 1993; Woodside 2004). In all instances in which we obtained data through conversations, we told informants that we are interested in stories or occurrences in which one person passed on another person's property or data.

To allow for the inclusion of examples of different levels of data richness and maintain our focus on the binding phenomenon of infringement, we "formalized" (Herriott and Firestone [1983], as cited in Stake [2006]) the design of cases and condensed each example case into a synopsis. Because our focus was on the breadth of the phenomenon (for an illustration of this breadth, see Table 1), we refrained from adding cases that were very similar in their basic setup.

Analysis Strategy

To analyze and theorize acts of interdependent privacy (and property) infringement, we focused on the phenomenon of infringement as experienced by the sharer and adapted the

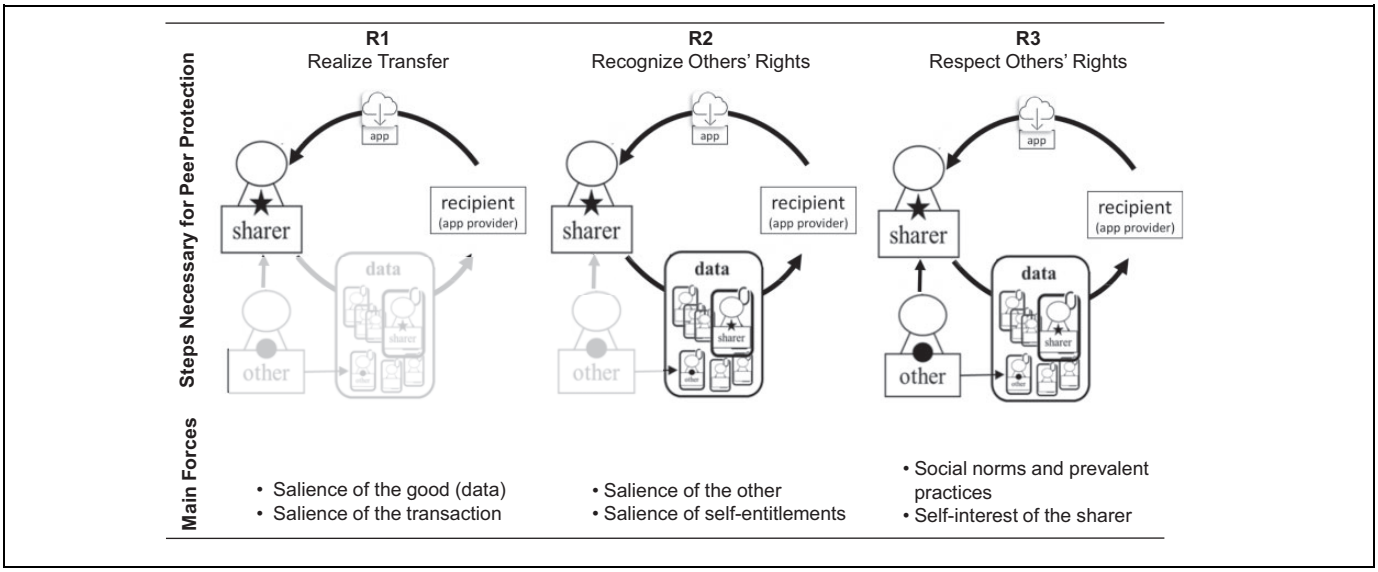

Figure 2. The 3Rs of interdependent privacy and property protection: The example of an app download.
Notes: Other(s) and sharer(s) could be one or multiple people; recipient(s) could be one or many persons and companies.

seven-step process suggested by Colaizzi (1978). We first read all the cases we had collected and identified their primary themes and then engaged in cross-case analysis to extract significant components and pivotal occurrences that explain our phenomenon (Fischer and Otnes 2006). To gain a deeper understanding of why infringement rather than protection took place, we reversed the logic and asked what would have been necessary to protect the good from infringement. Following Stake's (2006) approach to multicase studies, we ultimately posed the question "What helps us understand the phenomenological similarity (i.e., infringement)?" rather than "What helps us understand each of these cases?"

Next, we searched for deeper meanings and structures embedded in the extracted elements and repeated this process to develop common components and sequences. By mining and reducing the data in a search for patterns and underlying processes (Tsoukas 2009), we moved from specific phenomena to a more abstract theory. Finally, we engaged in several rounds of rewriting (Morse 1994) to reduce the insights into a concise structure that explains the behavior.

To allow for easy orientation along the key constructs and observations, the case base featured in Table 1 is structured along the domains of personal data (cases 1–11) and other possessions (cases 14–24) and also features exemplary cases in which both can be infringed simultaneously (cases 12–13). In addition, Table 1 indicates whether technology played a role in an infringement and whether an analog or digital transfer took place.

The 3R Interdependent Privacy Protection Framework

We observed acts of infringement ranging from property theft to an inadvertent slip of the tongue to the passing on of Facebook friends' data. Despite this variability, our analyses suggest that the interdependent protection of what is others' is contingent on potential sharers going through three consecutive and hierarchically dependent steps. We call these the 3Rs of Realizing (R1), Recognizing (R2), and Respect (R3). Figure 2 illustrates these 3Rs based on the introductory case of Jane. Note that the multiactor nature of privacy means that there potentially are many others and many recipients not visually represented in Figure 2. We discuss the findings against the backdrop of prior literature on privacy and property and do so in the order needed for interdependent personal data protection. We illustrate them with a selection of cases featured in Table 1, indicate in Table 1 which of the 3Rs may be most pertinent and provide first ideas about relevant antecedents and causes of these steps. We mainly use online infringements of personal data as key cases but use other cases to highlight specific points.

R1: Realization of Transfer

The first step toward protecting what is others' is for the sharer to realize that (s)he is about to transfer the good. If the sharer fails to realize that (s)he is passing something on to the recipient(s), the sharer necessarily also fails to realize that it is not his or hers to give. This may appear obvious, but it relies on the presence of two enabling conditions: salience of the good and salience of the transaction (see Figure 2). As cases 1, 2, 14, 15, and 16 illustrate (see Table 1), these conditions are not necessarily met in either privacy or property.

Salience of the transfer. The transfer of tangible goods entails effort and active involvement by the sharer and can be visually tracked. In contrast, the transfer of data and intangible goods requires little physical effort and no easily observable traces are associated with it. Personal data is hard to trace (Acquisti,

Brandimarte, and Loewenstein 2015), and once their data are shared, consumers cannot always know what is happening to them (Almuhimedi et al. 2015). This impedes realization of transfer. So too does the attention people tend to pay to specific transfer settings. In digital contexts, consumers have become used to pressing install without paying attention to notices and permissions (De Santo and Gaspoz 2015; Jensen, Potts, and Jensen 2005; see cases 2 and 14). Notably, lack of salience is characteristic of information but can also happen for goods, such as in case 16, where the good is hidden among other goods.

Salience of the good. A key difference between property and personal data is visibility and tangibility, which foster a good's salience and help actors realize what happens to it (for some analyses of the nature of data as a good, see Bélanger and Crossler [2011], Kamleitner and Mitchell [2018], and Schoeman [1984]). This can be observed in case 2, where an app requests access despite it being not clear to the sharer what the app actually wants to access. Kamleitner and Mitchell (2018) describe how the complexity of data makes it hard for people to truly comprehend data as a good. In turn, this makes it difficult for people to assign meaning to and evaluate data. Research has argued that consumer education campaigns aiming to enhance data and, thus, privacy protection are prone to failure precisely because data are not perceived as personally relevant and meaningful (Johnston, Warkentin, and Siponen 2015). In the domain of property, lack of salience of the good is most likely to play out digitally with the sharing of intangible (i.e., information) goods (e.g., case 14 in Table 1).

Our results and the existing literature align in suggesting that the context most conducive to failure at R1 is that of technology-mediated information collection and transfer (for a deeper analysis of the specifics of digital data transfers, see Christl and Spiekermann [2016] and Kamleitner and Mitchell [2018]). Giving permissions to apps and always-on devices means that people increasingly collect information about others without realizing either that they have just agreed to a transfer of data or what good they have shared. Online, both data about others and information goods may not so much be given as "leaked" (i.e., given away inadvertently or casually; Morlok 2016; Sarigol, Garcia, and Schweitzer 2014).

R2: Recognition of Others' Rights

Provided that sharers realize that they have transferred a good, they next need to recognize others' rights to this good. Figure 2 illustrates this second stage by veiling the other through a shaded box. Sharers can only effectively protect others from infringement if they recognize that their act of sharing concerns others. People intuitively classify the world along the question of "Whose is it?" from an early age (Blake and Harris 2011; Palamar, Le, and Friedman 2012) and are even biologically hardwired to do so (DeScioli, Rosa, and Gutchess 2015). Comprehending what is others facilitates harmonious social interactions and paves the way for shared understandings (Friedman and Ross 2011; Rudmin 1991). Yet sharers may not always consider or recognize others' rights to a good. Ownership attributions can shift in response to, for example, who held it first or who invested how much (Brown, Pierce, and Crossley 2014; Friedman 2010; Kanngiesser, Gjersoe, and Hood 2010; Kim and Kalish 2009; Nancekivell and Friedman 2014; Neary, Friedman, and Burnstein 2009). Analyzing our cases in this light reveals not only that R2-Recognition is a necessary second condition for peer protection but also that Recognition depends on similar antecedents as R1-Realization—that is, salience and understanding. This can manifest in two ways.

Salience of the other. First, people may infringe on others' rights because they do not even consider the possibility of others holding a stake—that is, because the *other is not salient*. For example, when downloading an app, a sharer may not even consider how much right to the information stored on one's phone others may hold (e.g., case 4). Apps ask for "the" or "your" contacts, files, and logs and do not make others salient. Sharers may fail to consider ownership when an app or service talks about "the" data (Kamleitner and Mitchell 2018). When there is no salient connection between the other and the good, sharers are unable to attribute ownership to the other.

Salience of self-entitlements. Second, there is the potential issue of self-entitlement blinding people to the possibility of rights being held by others (such as in case 3). If sharers primarily perceive a salient connection between themselves and the good, they may (wrongly) attribute all rights to themselves. Whether this happens largely depends on the degree of perceived control, knowledge, and investment a sharer has exerted on a good (Pierce, Kostova, and Dirks 2003). For many tangible goods, only one person can use and control them at a time (for the effect of perceived control on perceptions of ownership, see, e.g., Peck, Barger, and Webb [2013]). Ownership attributions for tangible goods are thus relatively clear cut. In contrast, intangible goods and personal data can be used by more than one person at a time. In fact, they may be used by a potentially infinite number of users without the awareness of the other or the sharer (Kamleitner and Mitchell 2018; Williams, Nurse, and Creese 2016). Personal information also tends to be readily at one's fingertips regardless of whether others use it. Consequently, the salience of one's own entitlements to specific information (goods) can quickly unfold, and it can diminish considerations of others. This is illustrated in case 5, which describes how a person was tricked into revealing something about another person without even noticing. These forces can be pronounced when it comes to the digital transfer of information. People self-collect the information (goods) on their devices, and because they own these devices, it is easy to overlook others' entitlements to this information (good) (see, e.g., cases 3, 18, and 19 in Table 1).

To conclude, our analyses suggest that failure of recognition is likely to be a threat to privacy when the other is not particularly visible in the information shared and when the sharer feels entitled to the information. These hold for disembodied, technology-based data transfers, such as in the case of a

crossword app (case 4), but are rarely the case in analog settings where the other's identity tends to be a salient part of the information transfer (e.g., case 9). Although the recognition of others is more likely in analog settings, others' claims can and sometimes are overlooked (for this possibility, see cases 3, 5, 20, and 21 in Table 1).

R3: Respecting Others' Rights

The final stage needed to prevent interdependent privacy and property infringements is the respect stage. Although respect can be defined in many ways (Rogers and Ashforth 2014), we apply a regulatory lens and refer to it as the fair and lawful treatment of others (Simon 2007). This means not risking infringing that which is recognized as belonging to another. In the respect stage, sharers recognize that others hold justified rights to the good and now face the decision of whether to respect others' rights. This can be done by (1) refraining from the transfer or (2) obtaining consent from the other. In the case of personal data, sharers can also resort to (3) modifying or anonymizing others' data prior to transfer.

Reigning norms and self-interest. At this step, two generic antecedent forces emerge from our analyses: reigning norms and self-interest. By and large, people disrespect others' rights either because they consider it socially acceptable to do or because they stand to gain from it. Our analyses suggest that the respective dominance of these forces varies as a function of technology integration. In analog settings, deeply ingrained norms of respect for what is others' prevail (Goodwin 1991; Kelvin 1973; Rudmin 1991), and people do not generally give away possessions or information with which others have entrusted them (Millar, Turri, and Friedman 2014; Petronio 2015; Schwartz 1968). If they do so, our analysis suggests that this is because they knowingly put their own interests above those of others, with the extreme case being criminal intent (e.g., cases 6 or 22 describing hacking incidents).

In technology-mediated digital settings, both self-interest and norms appear to be decisive forces for disrespecting what belongs to others. Consistent with notions such as privacy calculus (e.g., Kehr et al. 2015), which is a much-used paradigm for personal data sharing, people may sometimes weigh the benefits to themselves against their own and others' costs (e.g., potentially in cases 7 or 10). This is also known (Henning-Thurau, Henning, and Sattler 2007) and observed to hold for information goods, such as films, where utility-driven, economic motives dominate infringment decisions (Rochelandet and Le Guel 2005).

In addition, people appear to infringe because society accepts or trivializes disrespect in digital spheres while maintaining norms of protection and respect in analog settings. An example of the power of disrespecting norms in the case of privacy rights is people giving in to peer pressure and knowingly installing privacy-invasive apps (e.g., case 7). In digital settings, sharers may simply think that providing permission to others' data is not important because everyone is doing it (Boyd and Marwick 2011; Raab and Koops 2009). An example in the case of property rights is the juxtaposition between the socially unacceptable action of shoplifting CDs versus the widely accepted action of illegally downloading music (Freestone and Mitchell 2004; Wingrove, Korpas, and Weisz 2011).

To conclude, the forces of self-interest and social norms of trivialization can induce people to knowingly disrespect others' rights at the R3-Respect stage. In analog settings, such norms are an inherent part of human socialization, but in technology-mediated settings, they are less pronounced. We next use insights on the 3Rs to derive examples of concrete possibilities for interventions that reduce interdependent privacy breaches.

Implications of the 3Rs for Personal Data Protection

The 3R framework gives an alternative perspective on why current data protection policy and regulation might fail. We next use this perspective to identify classes of interventions that aim to prevent failures of the 3Rs. We call these the "4Es," and they comprise E1-Ensuring Realization, E2-Encouraging Recognition, E3-Educating for Respect, and E4-Embracing radical alternatives (see Figure 1). Table 2 illustrates specific interventions that fall under these respective classes. Intervention classes E1 through E3 involve interventions that improve consumers' ability to take responsibility for others' data. These interventions directly relate to our findings and tackle the corresponding issues that arise from the respective steps of the 3R framework. In essence, they incrementally improve interdependent privacy protection within current dominant practices and legislations, which tend to allocate responsibility to consumers.

Going beyond E1 through E3, and reflecting new technological possibilities, we suggest a fourth class of interventions (E4) that can advance current practices. These interventions embrace radical alternatives that shift the onus of privacy protection away from consumers. They are technology-based (for prior suggestions of enlisting technology to combat privacy issues, see Walker [2016]) and help circumvent consumer failures at the 3Rs and move responsibilities on to intermediaries. Our suggestions (summarized in Table 2) provide a toolbox of interventions that can inform all those interested in, or responsible for, reducing interdependent privacy breaches.

All these interventions require different stakeholders to act (i.e., policy makers and regulators, marketers and industry self-regulation, and consumer advocacy groups). To illustrate how and by whom policy interventions could be implemented, we provide examples from the EU and GDPR. In this regulatory area, most implications are for the Data Protection Authority (DPA) in each EU country. In the EU, DPAs handle reports of data breaches, mediate issues such as data subject access requests, and work to educate their countries about best practices in keeping digital data secure (European Commission 2016). In addition, changes in legislation, which may affect the United States through its Privacy Shield agreement and

Table 2. Select Interventions per Intervention Class to Improve Interdependent Privacy Protection Across Stakeholders.

#	Intervention	Primary Stakeholders	Intervention Class			
			E1	E2	E3	E4
1	Indicate amount (e.g., 1,001 pictures) or monetary value of data being transferred	Industry	●			
2	Visualize the process of data transfer before/after obtaining permissions	Industry	●			
3	Change the language from "access to" to "give away"	Industry	●			
4	Indicate the amount of data apps require and rank them on app platforms accordingly	Industry, privacy organizations	●			
5	Add/require additional steps of decision control in the transfer process	Industry, regulators, DPAs	●	●		
6	Provide a preview of actual data (e.g., picture snapshots, contact names) being given away	Industry	●	●		
7	Personalize/identify others' data (e.g., "all your contacts including the email of John, the number you call most often")	Industry, DPA	●	●		
8	Add warnings or interdependent privacy requests such as "the data you provide access to may belong to others. Do you have distribution rights?"	Industry, DPA	●	●		
9	Automated permission links sent to others when the system recognizes others	DPA	●	●	●	
10	Alert to data tracking (e.g., when inputting a new friend's data in a phone, consumers could be asked to confirm that they have consent to share these data)	Industry, DPA	●	●	●	
11	Publicize lawsuits and harm resulting from interdependent privacy breaches	Privacy organizations, DPA	●	●	●	
12	Educate consumers via the power of stories	Consumers, DPA	●	●	●	
13	Information campaigns on interdependent privacy	DPA, privacy organizations	●	●	●	
14	Draw on the 3R framework for blame allocation	DPA, regulators	●	●	●	
15	Design or require products and tools that screen out, blur, or stop sensing when third parties may be implied	Industry, DPA				●
16	Promote or require greater use of personalized privacy assistants	Industry, DPA, privacy organizations				●
17	Establishment and regulation of personal data managers	DPA, regulators				●

Notes: E1 = Ensuring Realization; E2 = Encouraging Recognition; E3 = Educating Respect; E4 = Embracing Radical Alternatives Circumventing the 3Rs.

the Federal Trade Commission, need to be addressed through the European Commission. In other jurisdictions, which tend to have less data protection (DLA Piper 2019), other authorities could take responsibility.

Implications for non–policy makers are not restricted to a judicial territory and include industry-based efforts toward self-regulation. Relevant codes of practice could be developed by bodies such as the American Marketing Association, the Digital Marketing Institute, the Mobile Marketing Association, or the Software Developers Alliance. In addition, individual businesses and marketers could draw on the business opportunities offered by the privacy-friendly innovations we suggest. Finally, independent privacy organizations could educate and advocate for self-protection. We discuss each of the classes of interventions of our solution framework before offering suggestions on how to prioritize them. Table 2 highlights specific interventions and outlines which stakeholders could best implement them.

E1: Ensuring Realization

Current privacy regulation predominantly follows so-called "notice and choice" or "awareness" and "control" models (Milne and Rohm 2000). These are also key planks of the U.S. Fair Information Practice Principles (Federal Trade Commission 2012) and of the EU GDPR. The main policy tools to protect privacy in this model are notices and informed consent (Martin 2015). These are rooted in a dyadic understanding of privacy between company and consumer and rest on the fundamental premise of rational, self-determined consumers who can obtain and process all the data necessary to enact protection for themselves. Realization is thus a necessary precondition for "informed" consent (Martin 2015). As we and others have shown, this precondition is rarely met, and consumers ignore, miss, misinterpret, and fail to fully understand what they are consenting to (Borgesius 2015; Martin 2013; McDonald and Cranor 2008; Milne and Culnan 2004; Nissenbaum 2011).

We identified a lack of salience of the data and the transfer decision as primary forces causing such realization failures. Accordingly, we suggest interventions that enhance salience. While there are some regulatory efforts in this direction (e.g., the GDPR requires data collectors to specify what data are being collected and how they will be used, under the U.S. Consumer Privacy Bill of Rights, consumers can access their personal data in usable formats), current efforts are bound to

fall short of ensuring full realization. This is because personal data descriptions remain rather abstract and are rarely imbued with the meaning necessary for users to recognize data as a good (Kamleitner and Mitchell 2018). In addition, consent to data access and transfer is still given by the simple click of a button, which is not conducive to full awareness of the actual transfer and its scope. Other measures to ensure realization are therefore needed. Importantly, both personal and interdependent privacy protection depend on realization of a transfer. Any improvement in interdependent self-protection is bound to also reduce the problem of self-disclosure.

All of the interventions we suggest to ensure Realization (interventions 1–4 in Table 2) work by increasing the salience of data transfers and imbuing data with meaning. For example, in intervention 4, we suggest that app platforms could flag apps that ask for more data (of others) than technically needed, and in intervention 2, we propose to make transfers more salient by visualizing the process and possibly also the type of data. What stands out is that these interventions primarily involve self-regulation. Industry bodies, such as the Digital Marketing Institute or alliances of app software developers, could develop best-practice guidance that includes such interventions. So too could individual market players. For example, the Google Play store as well as individual customer apps could change the way data requests and transfers are visualized and worded (see intervention 3 in Table 2).

E2: Encouraging Recognition

The need to recognize that we hold others' data (R2) is unique to interdependent privacy, and thus, little existing policy makes explicit provision for it. As we have shown, it cannot be taken for granted that sharers recognize whose data they have and under what conditions they can use it. Recognition requires that the data hold salient traces of the others. Interventions we suggest to achieve this (see interventions 5–8 in Table 2) include automated warnings such as "The data you are giving away may belong to others. Do you have all necessary distribution rights?" or increased personalization of data, such as "All your contacts including the email of John." In addition, salience of others could be increased through enhanced decision control (Malhotra, Kim, and Agarwal 2004), such as by asking sharers to give consent for each different type of data. These suggestions could be implemented as best-practice suggestions developed by industry bodies or DPAs.

E3: Educating for Respect

Successful interdependent privacy management depends on actors negotiating the boundaries of their respective rights (Petronio 2015) and then adhering to these boundaries. To prevent breaches of interdependent privacy, social contracts are required to which consumers feel bound (for their general role in privacy, see Martin [2016]). These can ensure respect (R3) for what belongs to others. To do so, we suggest educating for respect (see interventions 9–14 in Table 2) and thus combating the reigning norms of trivialization we identified as causing disrespect. This could be achieved, for example, through general information campaigns (see itervention 13), but there is also the potential of policy intervention (see intervention 10). The GDPR and Privacy Shield could be altered to mandate automated permission links to be sent to others when the system recognizes that others' data is being shared to require and ensure active consent by the third party. This would close the consent loophole and affect the way people think about sharing others' data, but it would also place an additional burden on consumers.

Given that we identified self-interest as a cause for failure to respect what is others, we also suggest interventions that increase individuals' understanding of the potential for harm. To achieve this, we suggest drawing on the power of stories (Bruner 1990; Escalas 1998) that can demonstrate to consumers that they are stewards of others' data to whom blame can be allocated. The DPA and privacy organizations could heavily publicize real stories about data infringements, the infringed person's feelings and fate (intervention 12), and the consequences for the infringer (intervention 11). For example, stories from the Cambridge Analytica scandal are an opportunity to deeply engage consumers with this issue.

Finally, we suggest that the 3R framework can help improve harm-based approaches to policy. These are concerned with the allocation of blame and compensation when privacy infringements have caused actual harm. Such approaches are also part of the GDPR regulation that entails substantial fines for data protection breaches (up to 4% of global turnover or €20 million) and foresees a right for compensation under Article 82. In intervention 14, we suggest that the courts could specify which of the 3Rs were breached by sharers. If a sharer can genuinely show no realization of transfer, then the recipient is solely to blame. Our framework then would influence the type of information requested and relied on in legal proceedings.

E4: Embracing Radical Alternatives

Both notice and choice and harm-based approaches to personal data protection assume that sharers realize data transfer and recognize and respect when these data belong to others. Our first three classes of interventions can help make this a more realistic assumption but do not relieve potential sharers from the burden of going through all 3R stages whenever they or their devices handle others' data. Many consumers already have surrendered to technology and "readily and willingly exchange information under conditions and in circumstances that they do not adequately understand" (Walker 2016, p. 145). In response, we propose interventions that aim to mitigate the risks of personal data infringements in the first place. We call this class of interventions Embracing Radical Alternatives because it substantially deviates from mainstream policies, which still place an onus on the consumer. In contrast, these interventions (interventions 15–17 in Table 2) put responsibilities on intermediaries. They provide alternative protection mechanisms, which are not policy based, though their

operation would benefit from changes in policy. These mechanisms are market-based and enable and stimulate novel entrepreneurial opportunities. In addition, they heavily depend on the establishment of a technological infrastructure that acts on behalf of consumers, thus allowing technology to come to the aid of a problem technology created (Walker 2016).

In policy terms, this class of interventions best aligns with what can be called the "preventive approach." Key principles, which can also be found in the EU GDPR, are data minimization, privacy by design, and privacy by default. All of these preempt the possibility of consumers leaking personal data (Williams, Nurse, and Creese 2016); yet they may not suffice. After all, they need to be enacted by those who have an interest in data collection. For example, despite three years' notice, a third of European companies remained underprepared for the GDPR (Shepherd, Afifi-Sabet, and Hopping 2018), and Facebook had planned to use the GDPR to reduce its liabilities (Gul 2018; Reuters 2018).

Additional steps are needed, which can also represent a business opportunity. In intervention 15, we suggest working on innovations that help prevent the collection of others' data. One recent example would be a cone of silence that prevents smart speakers from listening in (Maloney 2019). Again, this would only tackle part of the issue, and control over the risks would lie with the sharer rather than the other. To move control to potential victims of interdependent infringement, we suggest delegating the responsibility for protecting one's own and others' data to technology (intervention 16) or technology-assisted professionals (intervention 17). The first refers to what can be called privacy-enhancing technologies or privacy assistants (see www.privacyassistant.org). These are technological agents that learn the privacy preferences of their users over time, semiautomatically configure a range of settings, and make many privacy decisions on behalf of consumers who can thus maintain control of their own privacy (see Jutla and Bodorik [2005]).

For instance, HAT (www.hubofallthings.com) can be used to log in to apps and to provide only the data with which users are comfortable. It is based on microserver technology that allows individuals to store personal data as in a bank vault. Furthermore, Wibson, a disruptive technology based on blockchain, helps people connect to data sources such as Facebook and monitor offers from data buyers to sell their personal data (e.g., location data). Companies offering similar services include digi.me, Ocean, and the U.S. start-up Datacoup. Provided there are unified data standards, these systems have the potential to become capable of tracing the whereabouts of data and instigating their sharing and deletion at the user's request. Ideally, they should also be programmable to allow dealing with data concerning others. Technological development is moving in that direction (Boden et al. 2017; Ross, McEvilley, and Oren 2018).

A second proposition is the personal data manager, who, assisted by software, can manage data for consumers, look after consumers' information on their behalf, and investigate when and where this information is being used (Kamleitner and Mitchell [2018] explain why this is necessary). Like personal financial asset managers who manage a range of assets, personal data managers could carry out privacy risk assessments, suggest actions to maximize personal data rewards, and be liable for their recommendations. Although current regulation allows for it, eventually this idea would require new legislation. In the EU, this would involve the European Commission and fall under the responsibility of the Commissioner for Justice, Consumers and Gender Equality. An initiative could result from lobbying activities by countries, industry bodies, or privacy advocacy organizations such as Privacy International, noyb.eu, or the European Union Agency for Fundamental Rights. Alternatively, there could be a citizen's initiative, which could be instigated by only seven voting-age EU citizens living in at least seven member states.[2] In the United States, the initiation of such a process might, for example, include the Department of Justice, the Privacy and Civil Liberties Oversight Board, the Center for Democracy and Technology, the Future of Privacy Forum, the Electronic Frontier Foundation, or the Privacy Rights Clearinghouse.

Privacy assistants and personal data mangers place the onus for realizing, recognizing, and respecting the transfer of the data of others to software and professionals rather than consumers. They are a response to Walker's (2016) conclusion that we currently surrender our data. With these interventions, we advocate for more surrendering, but only to those who have the knowledge and ability to protect the data. The implications of widespread use of human and software data agents are considerable. They would raise awareness among consumers of the issues of personal and interdependent privacy, improve the rate of identification of privacy breaches, and increase the number of claims for compensation issued.

From a regulation of personal data markets perspective, data managers would act as an extra monitoring mechanism. Given the huge information asymmetries in personal data markets, such a move has the potential to enhance fairness and consumers' market power. Because consumers already give their data to companies, we assume that consumers would consider these services a welcome relief from the burdens of privacy protection. The success of personal data managers, however, depends on the regulation of their statutory duties and their monitoring. There are also questions of equal access to such privacy protection across different social strata—how can regulators avoid a new form of discrimination where poor people cannot afford privacy protection? Perhaps personal data managers could be partly remunerated by the compensations obtained from the successful prosecution of data breaches. While there is money to be made from exploiting data, these radical alternative interventions show that business models can also be built on data protection. For marketers, this possibility offers liability threats when firms take on the roles of sharers or others and novel opportunities when they help develop the interventions suggested here.

[2] http://ec.europa.eu/citizens-initiative/public/basic-facts.

Prioritizing Interventions

All interventions can help protect interdependent privacy, and while some may appear obvious, they are not currently in place. The task of getting every consumer to realize, recognize, and respect others' data is substantial and complicated. This is partly because of the multiactor nature of the problem, which involves numerous relevant parties such as companies, app developers, direct marketing agencies, industry bodies, privacy organizations, regulators, and consumers. As a result, responsibility is spread among these actors, which means that there may be limited motivation to ensure the privacy of others. There is thus a need to consider how to prioritize these interventions. One way of doing so would be to take a stakeholder perspective and decide on which stakeholders to involve first. Because industry self-regulation is voluntary, adds cost, and reduces data flows, one could prioritize privacy organizations and regulators as the primary initial targets for change (for some suggestions of which stakeholders are best-suited to take care of which intervention, see Table 2).

Another useful and complementary perspective on prioritization considers the hierarchical nature of the 3R framework. Sharers cannot possibly ensure respect for other's rights without first realizing that they are transferring something to which others hold rights. This hierarchical contingency implies that interventions designed to educate consumers about respecting others' data simultaneously ensure realization and encourage recognition (see Table 2). From this perspective, interventions that teach respect should be prioritized.

A final crucial consideration is that avoiding failure at the 3Rs places a cognitive and emotional burden on consumers and takes their time. In an instant digital world where multiple people engage with multiple data-collecting devices, multiple others (e.g., on average Americans hold 634 phone contacts, Hampton et al. 2011) would need to be asked before installing any app that requests access to contacts. The potential for request overload is clear. As Walker (2016, p. 145) argues, "Requiring more data to be transparent will mean more information for consumers to process, further challenging their ability to make sound decisions and engage in protection behaviors." In response, where possible, we advocate for relieving consumers from the burden of protecting others and prioritizing the suggested radical alternatives of privacy assistants and data managers. That said, interested stakeholders would be ill-advised to place their trust in a single intervention. As a multiactor phenomenon that appears to result from several forces (see Figure 2), successful interdependent privacy protection requires a range of interventions and an awareness of the prevalence of failure at each stage.

General Discussion

Privacy has always been interdependent. However, an increasing integration of technology in data transfers affects the ease and scale with which interdependent privacy breaches happen and the consequences that they entail. "Always on," in-home, artificially intelligent or at least "smart devices," such as Apple's Siri; HomeKit; Microsoft's Cortana; Amazon's Alexa; Google's former home assistant, Allo; and smart TVs, are installed in more and more homes. Such devices are permitted to switch on at any time and can collect a wide range of data about any human or device in the room. "As IoT-related systems capture more of the entirety of a consumer's being in the form of data, it will be as if more of a person will be inside the Internet and is being passed around from machine to machine" (Weinberg, Milne, and Hajjat 2015, p. 6) and from consumer to consumer. The challenge of personal data protection is growing and necessitates a better understanding of the dynamics that induce the sharing of others' information. Our 3R framework provides such an understanding. It contributes to prior literature by adding a multiactor perspective, juxtaposing interdependent breaches of privacy and property, identifying hierarchical contingencies, highlighting the primary forces that give rise to them, and paving the way for different classes of interventions.

The privacy and consumer policy literature has hitherto focused on the sharing of one's own data. Our framework extends this literature and explicitly recognizes the interdependent nature of privacy (Petronio 2015) and ownership (Rudmin 1991). In addition, our conceptual blend of privacy and property paves the way for further transfers between these two domains. For example, it suggests that insights on the sharing economy might extend to the context of personal data sharing and vice versa.

We also contribute by highlighting anteceding forces of the 3Rs (Realization, Recognition, and Respect of others' data). Salience of all elements in a transaction plays a key role for Realization and Recognition. This explains why the problem is of such relevance in the less visible and intangible digital domain. Moreover, at the Respect stage, we find that social norms might play a much stronger role in privacy protection than prior literature suggests. And although our insights confirm a role for self-interest, which is central in many privacy frameworks such as privacy calculus (e.g., Kehr et al. 2015), they put its importance into perspective. Self-interest and economic considerations only emerge as antecedent forces in the final stage of the problem and appear no more important than social norms. Thinking beyond the immediate antecedents, the infringements, exemplified by Jane and Cambridge Analytica in our opening examples, may be a symptom of digital native cultures and socialization processes in an increasingly digital society. The 3R framework can help shed light on such symptoms. It also helps show that interdependent and personal privacy protection are rooted in the same initial requirement for realization of a transfer. Tackling interdependent privacy protection is thus also likely to increase self-protection.

To improve protection and reduce the prevalence of interdependent infringements, we moreover contribute by offering a set of novel interventions, the 4Es. We provide guidance on who may be best suited to use them and on how to prioritize them. The interventions listed in Table 2 amount to a versatile toolbox that all interested stakeholders can draw on, further adapt, and extend. In particular, we suggest a class of

interventions that holds the potential to disrupt data markets and privacy regulation, (partly) delegating data protection responsibilities to digital assistants or personal data managers. As intermediaries, personal data managers would interact with marketers on consumers' behalf. They would also become a potential influential and knowledgeable stakeholder voice for reform of future policy.

Finally, through our ongoing reference to the EU GDPR, we contribute specific policy insights. Our insights can help explore, challenge, and improve the adequacy of the recent EU GDPR legislation. For example, under Article 14 (1a–f), GDPR consumers do have the right to be informed "where personal data have not been obtained from the data subject," and under Article 17, they have the "right to be forgotten." Both articles presume that others, such as Jane's contacts, are aware of, or can access, all the details of all the organizations with which their data has been shared. Our results suggest that this is unlikely. This seems to be a major limitation in the current regulatory provision designed to protect personal data and exemplifies our first R (Realization) as a highly problematic issue for exercising even the new and best-in-class rights under the GDPR. Furthermore, in the EU, the DPA and eventually the courts need to add further clarity to GDPR Article 2, which specifically excludes processing of personal data for household or purely personal purposes. Regulators need to decide if having others' personal data on an individual's phone means that that individual has sharing rights to the data. If so—and this is another point that needs clarification—would this mean that the app provider does not need to obtain consent from the original data owner?

Conclusion and Future Research

The framework highlights the limitations of current regulation, which largely fails to reflect the interdependent and dynamic nature of privacy. Specifically, current approaches appear to underplay the key function of recognition and respect in privacy protection and are ill-suited to reducing the substantial burden of considering all 3Rs in the digital world. The resulting 4E interventions and their applicability to industry, regulators, and consumers could even disrupt data markets and privacy regulations as we currently know them. In building the framework, we do not claim to know all that goes on within it or all the ways it can be applied. Different and varied applications of the framework will allow for greater understanding of its potential uses, implications, and limitations. A key point, however, is that the framework is designed to focus on the sharer, because it is the sharer who has to realize, recognize, and respect others' data. This promotes several avenues for further academic research.

One important avenue is to identify the extent to which data-collecting systems such as apps, websites, or always-on devices ensure realization, recognition, and respect. This would allow researchers to determine the most problematic areas in practice (e.g., messenger apps vs. retail). Another relevant future direction would be to test the effectiveness of the proposed interventions, for example, through experiments that change the wording in permissions from "access" to "give away" or that provide information on the exact amount of data being shared. Future research should also explore the hierarchical relationships between the 3Rs—that is, how much realization is needed before recognition dawns? Alternatively, how much recognition is needed before respect follows? Our focus has been on the sharer as a private individual. However, organizations also may become infringers when they pass on their customer data to other organizations or are the recipients of others' data. To revisit a previous question, if a device tracks and passes on personal data, who then is responsible? The owner or user of the device? The manufacturer of the device? Or any other service provider that ensures that consumers obtain and use the device? There is research to be done to establish how well the 3R framework translates to organizations and how well it is suited to analyze the position of the recipient. Finally, there is work to be done to pinpoint who around the world might be (jointly) responsible for, or best suited to, changing data protection policy jurisdictions. Pressure groups, think tanks, and groups other than legislators can all bring about an urgently needed change that will prevent technological facilitation from corrupting a human strength—our interdependent, social nature—into an uncontrollable threat.

Acknowledgments

The authors thank Joann Peck, Martin Paul Fritze, and Michalis Kokkoris for their helpful feedback on a prior version of this paper. The authors also gratefully acknowledge constructive input from the members of the Sustainable Computing and Privacy Lab at WU, from participants of the International Workshop on Ownership in Vienna, and from the *JPPM* review team.

Editorial Team

Kristen Walker, George Milne, and Bruce Weinberg served as guest editors for this article.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Acquisti, Alessandro, Laura Brandimarte, and George Loewenstein (2015), "Privacy and Human Behavior in the Age of Information," *Science*, 347 (6221), 509–14.

Afifi, Walid and John Caughlin (2006), "A Close Look at Revealing Secrets and Some Consequences That Follow," *Communication Research*, 33 (6), 467–88.

Almuhimedi, Hazim, Florian Schaub, Norman Sadeh, Idris Adjerid, Alessandro Acquisti, Joshua Gluck, et al. (2015), "Your Location Has Been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging," in *Proceedings of the 33rd Annual ACM*

Conference on Human Factors in Computing Systems. Scottsdale, AZ: Association for Computing Machinery, 787–96.

Andrews, Donald Arthur and James Bonta (2014), *The Psychology of Criminal Conduct*. New York: Routledge.

Bakos, Yannis, Erik Brynjolfsson, and Douglas Lichtman (1999), "Shared Information Goods," *Journal of Law and Economics*, 42 (1), 117–56.

Baumeister, Roy F. and Mark R. Leary (1995), "The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation," *Psychological Bulletin*, 117 (3), 497–529.

Bélanger, France and Robert E. Crossler (2011), "Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems," *MIS Quarterly*, 35 (4), 1017–42.

Belk, Russell W. (2013). "Extended Self in a Digital World," *Journal of Consumer Research*, 40 (3), 477–500.

Benn, Stanley I. (1971), "Privacy, Freedom, and Respect for Persons," in *Nomos XIII: Privacy*, J. Roland Pennock and John W. Chapman, eds. New York: Atherton Press.

Biczók, Gergely and Pern Hui Chia (2013), *Interdependent Privacy: Let Me Share Your Data*. Berlin: Springer.

Bishoff, P. (2016), "Facebook, Twitter, Google+ or LinkedIn, Which Should You Log In With?" *Comparitech* (January 13), https://www.comparitech.com/blog/vpn-privacy/facebook-twitter-google-or-linkedin-which-should-you-log-in-with/.

Blake, Peter R. and Paul Harris (2011), "Early Representations of Ownership," *New Directions for Child and Adolescent Development*, 2011 (132), 39–51.

Boden, Margaret, Joanna Bryson, Darwin Caldwell, Kerstin Dautenhahn, Lilian Edwards, Sarah Kember, et al. (2017), "Principles of Robotics: Regulating Robots in the Real World," *Connection Science*, 29 (2), 124–29.

Borgesius, Frederik Zuiderveen (2015), "Informed Consent: We Can Do Better to Defend Privacy," *IEEE Security & Privacy*, 13 (2), 103–07.

Bowcott, Owen and Alex Hern (2018), "Facebook and Cambridge Analytica Face Class Action Lawsuit," *The Guardian* (April 10), https://www.theguardian.com/news/2018/apr/10/cambridge-analytica-and-facebook-face-class-action-lawsuit.

Boyd, Danah and Alice E. Marwick (2011), "Social Privacy in Networked Publics: Teens' Attitudes, Practices, and Strategies," in *A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society*, https://ssrn.com/abstract=1925128.

Brown, Graham, Jon L. Pierce, and Craig Crossley (2014), "Toward an Understanding of the Development of Ownership Feelings," *Journal of Organizational Behavior*, 35 (3), 318–38.

Bruner, Jerome S. (1990), *Acts of Meaning*. Cambridge, MA: Harvard University Press.

Christl, Wolfie and Sarah Spiekermann (2016), *Networks of Control. A Report on Corporate Surveillance, Digital Tracking*. Vienna: Facultas.

Cohen, Julie E. (2000), "Examined Lives: Informational Privacy and the Subject as Object," *Stanford Law Review*, 52 (5), 1373–1438.

Colaizzi, Paul F. (1978), "Psychological Research as the Phenomenologist Views It," in *Existential-Phenomenological Alternatives for Psychology*, Ronald S. Valle and Mark King, eds. Oxford, UK: Oxford University Press.

Creswell, John W. and J. David Creswell (2017), *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. Thousand Oaks CA: SAGE Publications.

De Santo, Alessio and Cédric Gaspoz (2015), "Influence of Users' Privacy Risks Literacy on the Intention to Install a Mobile Application," in *New Contributions in Information Systems and Technologies*, Vol. 353, A. Rocha, A. Correia, S. Costanzo, and L. Reis, eds. Cham, Switzerland: Springer, 329–41.

DeScioli, Peter, Nicole M. Rosa, and Angela H. Gutchess (2015), "A Memory Advantage for Property," *Evolutionary Psychology*, 13 (2), doi:10.1177/147470491501300205.

DLA Piper (2019), "*Data Protection Laws of the World*," (accessed July 2, 2019), www.dlapiperdataprotection.com.

Escalas, Jennifer Edson (1998), "Advertising Narrative. What are They and How do They Work," in *Representing Consumers: Voices, Views and Visions*, Barbara Stern, ed. London: Routledge, 267–89.

Etzioni, Amitai (1991), "The Socioeconomics of Property," *Journal of Social Behavior and Personality*, 6 (6), 465–68.

European Commission (2016), "Data Protection Authorities," (November 24), https://ec.europa.eu/justice/article-29/structure/data-protection-authorities/index_en.htm.

European Court of Human Rights (2019), "European Convention on Human Rights," (accessed February 2, 2019), https://www.echr.coe.int/Documents/Convention_ENG.pdf.

Farrell, Laura, Nancy Di Tunnariello, and Judy C. Pearson (2014), "Exploring Relational Cultures: Rituals, Privacy Disclosure, and Relational Satisfaction," *Communication Studies*, 65 (3), 314–29.

Federal Trade Commission (2012), "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers," report (March), https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

Fischer, Eileen and Cele Otnes (2006), "Breaking New Grounds: Developing Grounded Theories in Marketing and Consumer Behavior," in *Handbook of Qualitative Methods in Marketing*, Russell Belk, ed. Northampton, MA: Elgar, 19–30.

Fournier, Susan (1998), "Consumers and Their Brands: Developing Relationship Theory in Consumer Research," *Journal of Consumer Research*, 24 (4), 343–73.

Freestone, Oliver and Vincent-Wayne Mitchell (2004), "Generation Y Attitudes Towards E-Ethics and Internet-Related Misbehaviours," *Journal of Business Ethics*, 54 (2), 121–28.

Friedman, Ori (2010), "Necessary for Possession: How People Reason About the Acquisition of Ownership," *Personality and Social Psychology Bulletin*, 36 (9), 1161–69.

Friedman, Ori and Hildy Ross (2011), "Twenty-One Reasons to Care About the Psychological Basis of Ownership," *New Directions for Child and Adolescent Development*, 2011 (132), 1–8.

Fu, Kevin, Tadayoshi Kohno, Daniel Lopresti, Elizabeth Mynatt, Klara Nahrstedt, Shwetak Patel, et al. (2017), "Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things," in *Computing Community Consortium* (accessed July 2, 2019), http://cra.org/ccc/wp-content/uploads/sites/2/2017/02/Safety-Security-and-Privacy-Threats-in-IoT.pdf.

Galbreth, Michael R., Bikram Ghosh, and Mikhael Shor (2012), "Social Sharing of Information Goods: Implications for Pricing and Profits," *Marketing Science*, 31 (4), 603–20.

Gibbs, J.C., Karen S. Basinger, Dick Fuller, and Richard L. Fuller (2013), *Moral Maturity: Measuring the Development of Sociomoral Reflection*. Oxford, UK: Routledge.

Goodwin, Cathy (1991), "Privacy: Recognition of a Consumer Right," *Journal of Public Policy & Marketing*, 10 (1), 149–66.

Gould, Stephen J. (1995), "Researcher Introspection as a Method in Consumer Research: Applications, Issues, and Implications," *Journal of Consumer Research*, 21 (4), 719–22.

Goulding, Christina (2005), "Grounded Theory, Ethnography and Phenomenology: A Comparative Analysis of Three Qualitative Strategies for Marketing Research," *European Journal of Marketing*, 39 (3/4), 294–308.

Gul, Munawar (2018), "Social Media Giants, GDPR, and Billion-Dollar Lawsuits," *Tapscape* (June 29), https://www.tapscape.com/social-media-giants-gdpr-billion-dollar-lawsuits/.

Hampton, Keith, Lauren Sessions Goulet, and Kristen Purcell (2011), "*Social Networking Site Users Have More Friends and More Close Friends*," Pew Research Center (June 16), http://www.pewinternet.org/2011/06/16/part-3-social-networking-site-users-have-more-friends-and-more-close-friends/.

Harkous, Hamza and Karl Aberer (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*. Scottsdale, AZ: Association for Computing Machinery.

Henning-Thurau, Thorsten, Victor Henning, and Henrik Sattler (2007), "Consumer File Sharing of Motion Pictures," *Journal of Marketing*, 71 (4), 1–18.

Jensen, Carlos, Colin Potts, and Christian Jensen (2005), "Privacy Practices of Internet Users: Self-Reports Versus Observed Behavior," *International Journal of Human-Computer Studies*, 63 (1–2), 203–27.

Herriott, Robert E. and William A. Firestone (1983), "Multisite Qualitative Policy Research: Optimizing Description and Generalizability," *Educational Researcher*, 12 (2), 14–19.

Jetten, Jolanda, Catherine Haslam, and S. Haslam Alexander (2012), *The Social Cure: Identity, Health and Well-Being*. Hove, UK: Psychology Press.

Johnson, David W. (2003), "Social Interdependence: Interrelationships Among Theory, Research, and Practice," *American Psychologist*, 58 (11), 934–945.

Johnston, Allen, Merrill Warkentin, and Mikko Siponen (2015), "An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric," *MIS Quarterly*, 39 (1), 113–34.

Jutla, Dawn N. and Peter Bodorik (2005), "Sociotechnical Architecture for Online Privacy," *IEEE Security & Privacy*, 3 (2), 29–39.

Kamleitner, Bernadette and Vincent-Wayne Mitchell (2018), "Can Consumers Experience Ownership for All Their Personal Data? From Issues of Scope and Invisibility to Agents Handling Our Digital Blueprints," in *Psychological Ownership and Consumer Behavior*, Joann Peck and Suzanne B. Shu, eds. Cham, Switzerland: Springer, 91–118.

Kamleitner, Bernadette, Vincent W. Mitchell, Andrew Stephen, and Ardi Kolah (2018), "Your Customers May Be the Weakest Link in Your Data Privacy Defenses," *MIT Sloan Management Review* (May 22), https://sloanreview.mit.edu/article/your-customers-may-be-the-weakest-link-in-your-data-privacy-defenses/.

Kanazawa, Satoshi and Mary C. Still (2000), "Why Men Commit Crimes (and Why They Desist)," *Sociological Theory*, 18 (3), 434–47.

Kanngiesser, Patricia, Nathalia Gjersoe, and Bruce M. Hood (2010), "The Effect of Creative Labor on Property-Ownership Transfer by Preschool Children and Adults," *Psychological Science*, 21 (9), 1236–41.

Kehr, Flavius, Tobias Kowatsch, Daniel Wentzel, and Elgar Fleisch (2015), "Blissfully Ignorant: The Effects of General Privacy Concerns, General Institutional Trust, and Affect in the Privacy Calculus," *Information Systems Journal*, 25 (6), 607–35.

Kelvin, Peter (1973), "A Social-Psychological Examination of Privacy," *British Journal of Social and Clinical Psychology*, 12 (3), 24–61.

Kim, Sunae and Charles W. Kalish (2009), "Children's Ascriptions of Property Rights with Changes of Ownership," *Cognitive Development*, 24 (3), 322–36.

Kirk, Colleen, Joann Peck, and Scott D. Swain (2018), "Property Lines in the Mind: Consumers' Psychological Ownership and Their Territorial Responses," *Journal of Consumer Research*, 45 (1), 148–68.

Kozinets, Rob V. (2006), "Click to Connect: Netnography and Tribal Advertising," *Journal of Advertising Research*, 46 (3), 279–88.

Lambert, Nathaniel M., Tyler F. Stillman, Joshua A. Hicks, Shanmukh Vasant Kamble, Roy F. Baumeister, and Frank D. Fincham (2013), "To Belong Is to Matter: Sense of Belonging Enhances Meaning in Life," *Personality and Social Psychology Bulletin*, 39 (11), 1418–27.

Laudon, Kenneth C. (1996), "Markets and Privacy," *Communications of the Association for Computing Machinery*, 39 (9), 92–104.

Levine, Yasha (2014), "Surveillance Valley Scammers! Why Hack our Data When You Can Just Buy It?" *Pando* (January 8), https://pando.com/2014/01/08/surveillance-valley-scammers-why-hack-our-data-when-you-can-just-buy-it/.

Litt, Eden and Eszter Hargittai (2014), "A Bumpy Ride on the Information Superhighway: Exploring Turbulence Online," *Computers in Human Behavior*, 36 (July), 520–29.

Malhotra, Naresh, Sung Kim, and James Agarwal (2004), "Internet Users' Information Privacy Concerns: The Construct, the Scale, and a Causal Model," *Information Systems Research*, 15 (4), 336–55.

Maloney, Dan (2019), "Win Back Some Privacy with a Cone of Silence for Your Smart Speakers," *Hackaday* (January 17), https://hackaday.com/2019/01/17/win-back-some-privacy-with-a-cone-of-silence-for-your-smart-speaker/.

Martin, Kirsten (2013), "Transaction Costs, Privacy, and Trust: The Laudable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online," *First Monday*, 18 (12), https://firstmonday.org/ojs/index.php/fm/article/view/4838/3802.

Martin, Kirsten (2015), "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is

Related to Meeting Privacy Expectations Online," *Journal of Public Policy & Marketing*, 34 (2), 210–17.

Martin, Kirsten (2016), "Understanding Privacy Online: Development of a Social Contract Approach to Privacy," *Journal of Business Ethics*, 137 (3), 551–69.

Martineau, Paris (2018), "'Facebook Is Tracking You on over 8.4 Million Websites,"' *The Outline* (May 18), https://theoutline.com/post/4578/facebook-is-tracking-you-on-over-8-million-websites.

McDonald, Aleecia M. and Lorrie Faith Cranor (2008), "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, 4 (3), 543–68.

Millar, Charles, John Turri, and Ori Friedman (2014), "For the Greater Goods? Ownership Rights and Utilitarian Moral Judgment," *Cognition*, 133 (1), 79–84.

Milne, George R. and Mary J. Culnan (2004), "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices," *Journal of Interactive Marketing*, 18 (3), 15–29.

Milne, George R. and Andrew J. Rohm (2000), "Consumer Privacy and Name Removal Across Direct Marketing Channels: Exploring Opt-In and Opt-Out Alternatives," *Journal of Public Policy & Marketing*, 19 (2), 238–49.

Morlok, Tina (2016), "Sharing Is (Not) Caring: The Role of External Privacy in Users' Information Disclosure Behaviors on Social Networking Sites," in *Pacific Asia Conference on Information Systems*, Paper 75.

Morse, Janice M (1994), "Emerging from the Data: The Cognitive Processes of Analysis in Qualitative Inquiry," *Critical Issues in Qualitative Research Methods*, Janice M. Morse, ed. Thousand Oaks, CA: SAGE Publications, 23–46.

Nancekivell, Shaylene and Ori Friedman (2014), "Mine. Yours. No One's: Children's Understanding of How Ownership Affects Object Use," *Developmental Psychology*, 50 (7), 1845–53.

Neary, Karen R., Ori Friedman, and Corinna L. Burnstein (2009), "Preschoolers Infer Ownership from 'Control of Permission'," *Developmental Psychology*, 45 (3), 873–76.

Nissenbaum, Helen (2011), "A Contextual Approach to Privacy Online," *Daedalus*, 140 (4), 32–48.

Olteanu, Alexandra- Mihaela, Kévin Huguenin, Reza Shokri, Mathias Humbert, and Jean-Pierre Hubaux (2017), "Quantifying Interdependent Privacy Risks with Location Data," *IEEE Transactions on Mobile Computing*, 16 (3), 829–42.

Palamar, Max, Doan T. Le, and Ori Friedman (2012), "Acquiring Ownership and the Attribution of Responsibility," *Cognition*, 124 (2), 201–08.

Peck, Joann, Victor A. Barger, and Andrea Webb (2013), "In Search of a Surrogate for Touch: The Effect of Haptic Imagery on Perceived Ownership," *Journal of Consumer Psychology*, 23 (2), 189–96.

Petronio, Sandra (2000), "The Boundaries of Privacy: Praxis of Everyday Life," in *LEA's Communication Series. Balancing the Secrets of Private Disclosures*, Sandra Petronio, ed. Mahwah, NJ: Lawrence Erlbaum Associates, 37–49.

Petronio, Sandra (2010), "Communication Privacy Management Theory: What Do We Know About Family Privacy Regulation?" *Journal of Family Theory & Review*, 2 (3), 175–96.

Petronio, Sandra (2015), "Communication Privacy Management Theory," in *The International Encyclopedia of Interpersonal Communication*, Bruhn Jensen, ed. New York: John Wiley & Sons, 335–47.

Pierce, Jon L., Tatiana Kostova, and Kurt T. Dirks (2003), "The State of Psychological Ownership: Integrating and Extending a Century of Research," *Review of General Psychology*, 7 (1), 84–107.

Pu, Yu and Jens Grossklags (2016), "Towards a Model on the Factors Influencing Social App Users' Valuation of Interdependent Privacy," *Proceedings on Privacy Enhancing Technologies*, 2016 (2), 61–81.

Purtova, Nadezhda (2015), "The Illusion of Personal Data as No One's Property," *Law, Innovation and Technology*, 7 (1), 83–111.

Raab, Charles and Bert-Jaap Koops (2009), "Privacy Actors, Performances and the Future Of Privacy Protection," in *Reinventing Data Protection*, Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne, and Sjaak Nouwt, eds. New York: Springer, 207–21.

Reuters (2018), "Inside Facebook's Plan to Limit the Impact of GDPR Protections," (April 19), https://www.computerworld.com.au/article/640328/inside-facebook-plan-limit-gdpr-protections-european-users.

Rochelandet, Fabrice and Fabrice Le Guel (2005), "P2P Music Sharing Networks: Why the Legal Fight Against Copiers May Be Inefficient," *Review of Economic Research on Copyright Issues*, 2 (2), 69–82.

Rogers, Kristie M. and Blake E. Ashforth (2014), "Respect in Organizations: Feeling Valued as 'We' and 'Me'," *Journal of Management*, 43 (5), 1578–1608.

Ross, Ronald S., Michael McEvilley, and Janet C. Oren (2018), "Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems [including updates as of 1-03-2018]," No. Special Publication (NIST SP)-800-160), https://www.nist.gov/publications/systems-security-engineering-considerations-multidisciplinary-approach-engineering-0.

Rudmin, Floyd Webster (1991), "To Own Is to Be Perceived to Own: A Social Cognitive Look at the Ownership of Property," *Journal of Social Behavior and Personality*, 6 (6), 85–104.

Rudmin, Floyd Webster (2016), "The Consumer Science of Sharing: A Discussant's Observations," *Journal of the Association for Consumer Research*, 1 (2), 198–209.

Sarigol, Emre, David Garcia, and Frank Schweitzer (2014), "Online Privacy as a Collective Phenomenon," in *Proceedings of the Second ACM Conference on Online Social Networks*. New York: Association for Computing Machinery, 95–106.

Schoeman, Ferdinand David (1984), *Philosophical Dimensions of Privacy: An Anthology*. Cambridge, UK: Cambridge University Press.

Schutz, Alfred (1967), *The Phenomenology of the Social World*. Evanston, IL: Northwestern University Press.

Schwartz, Barry (1968), "The Social Psychology of Privacy," *American Journal of Sociology*, 73 (6), 741–52.

Shepherd, Adam, Keumars Afifi-Sabet, and Clare Hopping (2018), "GDPR News: GDPR Turns Six Months Old," *ITPro* (November

21), https://www.itpro.co.uk/data-protection/28029/latest-gdpr-news-uk.

Simon, Bernd (2007), "Respect, Equality, and Power: A Social Psychological Perspective," *Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie*, 38 (3), 309–26.

Sinclair, Tara J. and Rachel Grieve (2017), "Facebook as a Source of Social Connectedness in Older Adults," *Computers in Human Behavior*, 66 (C), 363–69.

Sinha, Rajiv K. and Naomi Mandel (2008), "Preventing Digital Music Piracy: The Carrot or the Stick?" *Journal of Marketing*, 72 (1), 1–15.

Spiekermann, Sarah and Jana Korunovska (2017), "Towards a Value Theory for Personal Data," *Journal of Information Technology*, 32 (1), 62–84.

Stake, Robert E. (2006), *Multiple Case Study Analysis*. New York: Guilford Press.

Symeonidis, Iraklis, Fatemeh Shirazi, Gergely Biczók, Cristina Pérez-Solà, and Bart Preneel (2016), "Collateral Damage of Facebook Apps: Friends, Providers, and Privacy Interdependence," in *Proceedings of the IFIP International Information Security and Privacy Conference*. Cham, Switzerland: Springer.

Tsoukas, Haridimos (2009), "Craving for Generality and Small-N Studies: A Wittgensteinian Approach Towards the Epistemology of the Particular in Organization and Management Studies," in *SAGE Handbook of Organizational Research Methods*, D. A. Buchanan and A. Bryman, eds. London: SAGE Publications, 285–301.

Tyler, Tom R. (2006), *Why People Obey the Law*. Princeton, NJ: Princeton University Press.

Vangelisti, Anita L. and John P. Caughlin (1997), "Revealing Family Secrets: The Influence of Topic, Function, and Relationships," *Journal of Social and Personal Relationships*, 14 (5), 679–705.

Varian, Hal R. (2003), "Buying, Sharing and Renting Information Goods," *Journal of Industrial Economics*, 48 (4), 473–488.

Walker, Kristen L. (2016), "Surrendering Information Through the Looking Glass: Transparency, Trust, and Protection," *Journal of Public Policy & Marketing*, 35 (1), 144–58.

Wallendorf, Melanie and Merrie Brucks (1993), "Introspection in Consumer Research: Implementation and Implications," *Journal of Consumer Research*, 20 (3), 339–59.

Warren, Samuel D. and Louis D. Brandeis (1890), "The Right to Privacy," *Harvard Law Review*, 4 (5), 193–220.

Weinberg, Bruce D., George R. Milne, and Fatima M. Hajjat (2015), "Internet of Things: Convenience vs. Privacy and Secrecy," *Business Horizons*, 58 (6), 615–24.

Williams, Meredydd, Jason R. Nurse, and Sadie Creese (2016), "The Perfect Storm: The Privacy Paradox and the Internet-of-Things," in *IEEE Workshop on Challenges in Information Security and Privacy Management at the 11th International Conference on Availability Reliability and Security (ARES)*, https://ieeexplore.ieee.org/document/7784629.

Wingrove, Twila, Angela L. Korpas, and Victoria Weisz (2011), "Why Were Millions of People Not Obeying the Law? Motivational Influences on Non-Compliance with the Law in the Case of Music Piracy," *Psychology, Crime & Law*, 17 (3), 261–76.

Woodside, Arch G. (2004), "Advancing from Subjective to Confirmatory Personal Introspection in Consumer Research," *Psychology & Marketing*, 21 (12), 987–1010.