Lutz, C., Hoffman, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. *Information, Communication & Society, 21*(10), 1472-1492 Doi: https://doi.org/10.1080/1369118X.2017.1339726

The Role of Privacy Concerns in the Sharing Economy

Christoph Lutz*
Assistant Professor
Nordic Centre for Internet & Society
Department of Communication & Culture
BI Norwegian Business School, Nydalsveien 37, 0484 Oslo (Norway)
christoph.lutz@bi.no

Christian Pieter Hoffmann
Professor
Institute of Communication and Media Studies
University of Leipzig, Burgstraße 21, 04109 Leipzig (Germany)
christian.hoffmann@uni-leipzig.de

Eliane Bucher
Assistant Professor/Researcher 2
Nordic Centre for Internet & Society
Department of Communication & Culture
BI Norwegian Business School, Nydalsveien 37, 0484 Oslo (Norway)
eliane.bucher@bi.no

Christian Fieseler
Professor
Nordic Centre for Internet & Society
Department of Communication & Culture
BI Norwegian Business School, Nydalsveien 37, 0484 Oslo (Norway)
eliane.bucher@bi.no

*Corresponding Author

Published in *Information, Communication & Society*. Please cite as:

Lutz, C., Hoffmann, C. P., Bucher, E., & Fieseler, C. (2018). The role of privacy concerns in the sharing economy. *Information, Communication & Society, 21*(10), 1472-1492. doi: 10.1080/1369118X.2017.1339726

Abstract

Internet-mediated sharing is growing quickly. Millions of users around the world share personal services and possessions with others—often complete strangers. Shared goods can amount to substantial financial and immaterial value. Despite this, little research has investigated privacy in the sharing economy. To fill this gap, we examine the sharing-privacy nexus by exploring the privacy threats associated with Internet-mediated sharing. Given the popularity of sharing services, users seem quite willing to share goods and services despite the compounded informational and physical privacy threats associated with such sharing. We develop and test a framework for analyzing the effect of privacy concerns on sharing that considers institutional and social privacy threats, trust and social-hedonic as well as monetary motives.

Keywords: sharing, social media, privacy, privacy paradox, privacy calculus

The Role of Privacy Concerns in the Sharing Economy

The Internet has long been a place for sharing—the sharing of ideas, knowledge and opinions. However, recent Internet services have extended the notion of sharing from immaterial to material goods and services—and thus created a vibrant new domain for both business and research. Despite its apparent popularity, the scientific exploration of the sharing phenomenon is still in its infancy. A number of authors have attempted to conceptualize the notion of sharing (Belk, 1985, 2010, 2014; John, 2013a, 2013b; Lamberton & Rose, 2012; Ozanne & Ballantine, 2010; Wittel, 2011). In his influential definition, Belk (2007) characterizes sharing as the "act and process of distributing what is ours to others for their use and/or the act or process of receiving or taking something from others for our use" (Belk, 2007, p. 126). In a similar vein, Hamari, Sjöklint and Ukkonen (2016, p. 2047) define "collaborative consumption" as "the peer-to-peer-based activity of obtaining, giving, or sharing the access to goods and services, coordinated through community-based online services".

In this article, we will focus on the sharing of material goods and services through online communities via contractual renting or leasing, as in the case of, for example, Airbnb. Sharing is associated with various benefits, ranging from bonding and solidarity (Belk, 2010; Benkler, 2004; Wittel, 2011) to financial profit, synergies (Belk, 2007; Gurven, 2006), status improvement (Gurven, 2006), and increased environmental sustainability (Botsman & Rogers, 2010; Belk, 2010). Sharing also comes with substantial risks: shared goods may be damaged or lost. Physical damage can cause emotional harm because, "knowingly or unknowingly, intentionally or unintentionally, we regard our possessions as parts of ourselves" (Belk, 1988, p. 139).

Belk's (1988) notion of the extended self indicates a critical risk associated with sharing: besides the risk of physical damage, sharing also increases the risk of (perceived) interpersonal contamination in the form of the violation of one’s personal space. For example, in the case of renting out an apartment, physical damage, pollution or contamination through odors, fluids, heat or other residues left behind by the person sharing the space may entail not only material loss but also a violation of personal integrity, as our homes are an essential locus of our extended selves (Belk, 1988; Goffman, 1971). Of course, the perceived risk of interpersonal contamination is more pronounced when we are less familiar with the person sharing a space or good (Belk, 2010)—which is a key characteristic of online sharing services.

The use of online services has long been associated with privacy threats—sharing personal data and information online renders Internet users vulnerable to both accidental and intentional harm caused by other users (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Malhotra, Kim, & Agarwal, 2004). High levels of user anxiety regarding privacy have been described as a key obstacle to the expansion of online transactions (Hoffman, Novak, & Peralta, 1999; McKnight, Choudhury, & Kacmar, 2002; Urban, Amyx & Lorenzon, 2009). Sharing services facilitate the sharing not only of personal data or information but also of physical products and services beyond one’s circle of trusted acquaintances. Therefore, based on Belk’s (1988) concept of the extended self, we propose that the privacy threats associated with the “sharing economy” extend beyond those associated with the use of more traditional online services, such as e-commerce or social media. Accordingly, users could be expected to shy away from the use of sharing services because of compounded privacy concerns (Belk, 2010; Kleine, Kleine, & Allen, 1995).

However, given the popularity of major sharing services, such as Airbnb, Couchsurfing, Uber or Getaround, we are faced with an apparent contradiction: users’ willingness to engage in the Internet-facilitated sharing of physical products and services with strangers, despite these compounded privacy threats. In this article, based on previous research on the privacy calculus, benefits of sharing as well as social influence, and inspired by the notion of the “extended self”

(Belk, 1988), we develop a nomological model of privacy concerns in the sharing context, which we test based on a survey of 374 users who are actively engaged in sharing as hosts on Airbnb. We derive conclusions on the effect of privacy concerns in the context of the sharing economy.

Literature Review

Privacy Concerns on the Internet

Since the emergence of commercial online services, user trust has been regarded as a prerequisite for the flourishing of online business (Hoffman et al., 1999; Milne, 2000; Jarvenpaa, Tractinsky, & Saarinen, 1999; McKnight et al., 2002). The importance of trust increases whenever settings are characterized by uncertainty and risk (McKnight & Chervany, 2002; Nissenbaum, 2001). In the case of online services, one such risk that necessitates trust on the part of users is associated with the disclosure and sharing of personal data (Dinev & Hart, 2006; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010).

Sharing personal data online makes users vulnerable to the potential loss of control over the spread and use of these data (Culnan & Armstrong, 1999). This vulnerability induces privacy concerns, which are based on assessments of the likelihood and extent of adverse consequences from information disclosures (Dinev & Hart, 2004; Malhotra et al. 2004). Frequently, the provision of at least some personal data is a precondition for the use of online services (Schoenbachler & Gordon, 2002; Wang, Beatty, & Fox, 2004). Rust, Kannan and Peng (2002, p. 455) find the following: “In fact, it may be quite impossible for customers to transact business on the Internet without revealing information about themselves that they may be unwilling to share”.

Major privacy concerns have been discussed as potential obstacles to the expansion of online business (Hoffman et al., 1999; McKnight et al., 2002; Urban et al., 2009). The more pronounced users' privacy concerns, the less likely they are to engage in an online transaction (Olivero & Lunt, 2004; Phelps, Nowak, & Ferrell, 2000; Phelps, D'Souza, & Nowak, 2001; Sheehan & Hoy, 1999). At the same time, privacy concerns do not generally preclude the sharing of personal data online. Lanier and Saini (2008) find that humans feel a need for seclusion, autonomy and self-control. However, as social beings, they also want to interact with one another. Therefore, while privacy concerns affect human behavior and limit self-disclosure, they do not prevent it (Dinev & Hart, 2006).

Large-scale surveys, such as the Eurobarometer (2011) study in Europe and the Pew surveys in the US (Madden & Rainie, 2015), have shown that a substantial number of citizens in Western countries report online privacy concerns. At the same time, numerous studies have shown that, despite these reported concerns, users extensively use online services and share personal information online (Gross & Acquisti, 2005; Tufekci, 2008). In fact, privacy protection mechanisms are regularly ignored (Madden & Rainie, 2015). The notion of a *privacy paradox* describes this apparent divergence between attitudes and behavior (Barnes, 2006).

Many studies have found that privacy concerns (attitudes) do not strongly affect online self-disclosure or protection behaviors (behaviors) (Chen & Rea, 2004; Milne & Culnan, 2004; Milne, Labrecque, & Cromer, 2009; Milne, Rohm, & Bahl, 2004). Others have noted that the relationship between privacy concerns and behavior is contingent on the context, the type of service or the privacy threat (e.g., Dienlin & Trepte, 2015; Utz & Krämer, 2009; Young & Quan-Haase, 2013). In this study, we will focus on privacy concerns in the context of the growing domain of sharing services. We argue that, compared with more traditional online services, sharing is associated with distinct forms of privacy concerns that should aggravate the level of privacy concerns, necessitating strong theoretical explanations for users' sharing behavior despite privacy concerns.

Privacy in the Sharing Economy

Early research on online privacy concerns focused on the specific context of e-commerce services (Milne & Boza, 1999; Olivero & Lunt, 2004; Rust et al., 2002). With these services, users disclose data to a service provider. In a computer-mediated environment, this disclosure introduces privacy concerns, as users must base their estimation of the provider's trustworthiness on a limited number of cues (Ashworth & Free, 2006; Friedman et al., 2000; Gefen, 2000; Hoffman et al., 1999; Jarvenpaa et al., 1999; Wang et al., 2004; Yoon, 2002). Privacy concerns regarding a service provider can be termed "institutional privacy threats". They are directed toward the agent who creates and provides the institutional setting for an online transaction.

The emergence of social media services has further fueled research interest in privacy concerns and data disclosure (Wilson, Gosling, & Graham, 2012; Zhang & Leung, 2015). Fundamentally, social media specialize in lowering the barriers to online self-disclosure and the (semi-)public sharing of data (Acquisti & Gross, 2006; Special & Li-Barber, 2012), which is especially true for social networking sites that facilitate connections between users based on personal profiles (Ellison et al., 2007; Krasnova et al., 2010). Some scholars have noted that social media may aggravate privacy concerns, as users disclose personal data on these platforms—not only to the service provider but also to other users (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). As such, institutional privacy concerns are amplified by social privacy concerns. Preliminary findings have shown that users tend to adapt more carefully to social privacy threats, such as stalking and cyberbullying, than to institutional privacy threats (boyd & Hargittai, 2010).

Both institutional and social online privacy concerns are based on the sharing of personal data or information on online platforms. However, in the case of sharing services (in the vein of the sharing economy), users also share material goods or physical personal property.

Therefore, sharing services are associated with additional and distinct privacy threats that pertain to physical privacy (Smith, Dinev, & Xu, 2011). On the one hand, physical privacy—i.e., the “right to be left alone” and a cornerstone of the legal definition of privacy (Warren & Brandeis, 1890)—describes individuals’ sense of having a private space that others cannot enter against their will. It is linked to the protection of one’s personal space from surveillance and intrusion. On the other hand, information privacy refers to personal (identifiable) information and its protection from unwanted uses. While physical and information privacy can be conceptually differentiated, both are intimately related, as the invasion of physical privacy is also commonly associated with a breach of information privacy.

For example, sharing a room with a stranger through Airbnb may result in violations of physical privacy, with guests invading the host’s physical personal space. Another scenario in the context of sharing is damage to personal property—resulting in both physical and emotional harm. At the same time, the host may find her information privacy disturbed by guests who learn about their host’s living conditions, personal interests and tastes, possibly uncovering intimate information in the apartment. Physical privacy concerns associated with sharing can be suitably conceptualized based on Belk’s (1988) notion of the extended self, as physical intrusions, damages and material losses all constitute infringements on the extended self. In the context of sharing, privacy concerns due to the threat of such infringements will likely be especially pronounced, as users tend to interact with strangers (Belk, 2010).

In summary, the privacy concerns that affect the use of sharing platforms likely go beyond those in e-commerce and social media contexts (cf., boyd & Hargittai, 2010; Young & Quan-Haase, 2013), where users face threats such as misuse or loss of data (Khadem, 2015), harassment, stalking and discrimination (Edelman & Luca, 2014; Edelman, Luca, & Svirsky, 2015). These additional concerns include physical privacy threats due to the disclosure and sharing of physical personal spaces.

H1: Online privacy concerns (both institutional and social) negatively affect users' sharing behavior.

H2: Physical privacy concerns negatively affect users' sharing behavior.

In the context of sharing services, online and physical privacy concerns are intertwined; neither can be avoided if a user decides to engage in sharing. Overcoming online privacy concerns is an initial requirement before physical sharing can occur. If users estimate the privacy risks of using the online platform to be high or if they have adverse experiences when using the online platform, we expect their level of concern regarding the physical act of sharing to rise. If, for example, in the course of sharing a room on Airbnb, users begin to mistrust the quality of the processes or assurances provided by the service or develop mistrust toward some of the users encountered online, we expect them to become more skeptical and careful when actually hosting guests.

H3: Online privacy concerns are positively associated with physical privacy concerns.

Explaining Sharing despite Privacy Concerns

Based on previous studies of online privacy and the APCO framework in particular (Smith et al., 2011), several possible explanations for users overcoming their privacy concerns to engage in online services can be distinguished. These explanations are based on (1) user trust, (2) the privacy/sharing calculus, and (3) social dynamics. In this segment, we will discuss all three of these theoretical perspectives and derive a nomological model of privacy concerns in the sharing context (see figure 1).

(1) User trust: Sharing services constitute a dynamic and complex social environment online. Based on the assumption of bounded rationality, Acquisti (2004) argues that Internet users seeking immediate gratification will struggle with obtaining and rationally processing the necessary information to calculate privacy risks. To navigate this environment, users may rely

on heuristics as cognitive support systems, which allows for flexible adaptation and speedy decision making. Conventionally, trust has been defined as “a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviors of another” (Rousseau, Sitkin, Burt, & Camerer, 1998, p. 395). These positive expectations emerge from specific beliefs in terms of the transaction partner’s trustworthiness (Bhattacherjee, 2002; McKnight et al., 2002). Categorizing specific service providers as trustworthy will allow users to rely on their services and enjoy their benefits without having to engage in elaborate risk calculation or extensive protection behaviors. Therefore, despite overall high levels of online privacy concerns, users may choose to interact with select institutions or organizations that they judge as trustworthy. User trust has been shown to be a key prerequisite for the establishment and growth of online services (Hoffman et al., 1999; Jarvenpaa et al., 1999).

H4: Trusting beliefs positively affect users’ sharing behaviors.

Overall, we expect that a high level of online and physical privacy concerns will lower users’ readiness to categorize services as trustworthy. In this vein, privacy concerns denote a skeptical, careful stance toward online services that will affect judgments regarding individual providers.

H5a–b: Online (a) and physical (b) privacy threats negatively affect users’ trusting beliefs.

A well-documented heuristic in forming trusting beliefs is based on fair information practices (i.e., the pro-active communication of security and privacy policies, guarantees, and further customer services). These are interpreted as signals of a service’s trustworthiness (Culnan & Armstrong, 1999; Wang et al., 2004). Fair information practices allow users to judge the trade-off between the risk they are willing to take and the expected benefits (Ashworth & Free, 2006; Kim, Ferrin, & Rao, 2008; Sheehan & Hoy, 2000). Yet while studies suggest that only few studies study the information provided, the mere presence of privacy assurances strengthens trusting beliefs by signaling a willingness to create transparency (McKnight & Chervany, 2002). Warranties, in particular, signal trustworthiness because opportunistic behavior will entail expenses for the transaction partner (Wells, Valacich, & Hess, 2011). Given that privacy assurances enhance both the perceived integrity and benevolence of a service and reduce risk perceptions, we expect them to have a positive effect on users' trusting beliefs and a negative effect on their online privacy concerns.

H6: Privacy assurances positively affect users' trusting beliefs.

H7: Privacy assurances negatively affect users' online privacy concerns.

(2) As we have seen, Internet users struggle to rationally asses the *risks and benefits of online transaction* (Acquisti, 2004). Based on a rational choice assumption, the "privacy calculus" thesis suggests that users attempt to weigh the identified or assumed (privacy) risks of a transaction against its benefits (e.g., Culnan & Armstrong, 1999; Dinev & Hart, 2006; Kokolakis, 2015; Lee, Park, & Kim, 2013; Smith et al., 2011). Thereby, a trade-off exists between the risk users are willing to take by disclosing personal data, on the one hand, and the benefits derived from this transaction, on the other hand (Ashworth & Free, 2006; Phelps et al., 2000; Sheehan & Hoy, 2000). Previous studies have found that a fair degree of reciprocity in the exchange of data, money, products and services reduces user concerns and increases their willingness to employ online services (Olivero & Lunt, 2004; Sheehan & Hoy, 2000).

One practical implication of the "privacy calculus" perspective is that an online service can counter privacy concerns among potential customers by stressing the benefits provided by the service (Ashworth & Free, 2006; Olivero & Lunt, 2004). However, pronounced privacy concerns will lessen the perceived benefits provided by a service. In the case of sharing services, two distinct benefits are especially salient: social-hedonic benefits, derived by meeting new, interesting people during the act of sharing, and monetary benefits (Bucher, Fieseler, & Lutz, 2016). In fact, the introduction of monetary benefits may have an especially strong effect on the privacy/sharing calculus, as it primes users to apply rationality and exchange frames to the transaction. Users are explicitly compensated for the risks they are willing to take on.

H8: Perceived social-hedonic benefits positively affect users' sharing behaviors.

H9: Perceived monetary benefits positively affect users' sharing behaviors.

H10a–b: Online privacy concerns are negatively associated with perceived social-hedonic (a) and perceived monetary benefits (b).

H11a–b: Physical privacy concerns are negatively associated with perceived social-hedonic (a) and perceived monetary benefits (b).

(3) A third possible explanation for users' sharing behavior despite privacy concerns is based on the *social dynamics of information and communications technology (ICT) adoption in general and of sharing services in particular*. Studies focusing on the individual-level adoption of new media have acknowledged that social influence has an impact on users' willingness and intentions to adopt new ICT. Therefore, technology adoption models incorporate "subjective norms" or "social influence", i.e., an individual's perception of important others' expectations that he or she should use new ICT, as antecedents of acceptance (Venkatesh & Bala, 2008; Venkatesh & Davis, 2000; Venkatesh, Morris, Davis, & Davis, 2003). Social cognitive theory also stresses the impact of social interaction and shared learning experiences on ICT use (Compeau & Higgins, 1995). Some studies have applied a social network approach to the investigation of technology diffusion (Dodds & Watts, 2005; Watts & Dodds, 2007). The results indicate that personal relationships are crucial for the acceptance and adoption of innovative new technologies (Goldenberg, Han, Lehmann, & Hong, 2009; Iyengar, Van den Bulte, & Valente, 2011).

In the case of sharing services, we expect the influence of social interactions or expectations on use intentions to be especially pronounced, as these platforms are community-based and heavily rely on word-of-mouth marketing. Therefore, if a user is embedded in a social environment that encourages sharing, he or she will tend to experience situational normality (Li, Hess, & Valacich, 2008; McKnight & Chervany, 2002) and accordingly perceive fewer privacy concerns. In addition, social norms of reciprocity may encourage users who benefit from sharing to overcome potential online or physical privacy concerns and to physically share themselves (Jenkins, Molesworth, & Scullion, 2014; Ozanne & Ballantine, 2010; Wittel, 2011).

H12: Social influence positively affects users' sharing behaviors.

H13a–b: Social influence negatively affects users' online (a) and physical (b) privacy concerns.

Given the community dynamics of sharing platforms, we expect that social encouragement will also enhance the perceived benefits of sharing: Studies have found that interpersonal agreement on the desirability of an outcome can intensify the perceived enjoyment derived from it (Raghunathan & Corfman, 2006). Accordingly, a social environment that encourages and supports sharing may lead to increased perceived benefits derived from it.

H14a-b: Social influence is positively associated with perceived social-hedonic (a) and perceived monetary benefits (b).

Figure 1 presents the resulting nomological model of privacy concerns in the sharing context, which we will test based on a quantitative survey of active users on the sharing platform Airbnb. The model considers three alternative explanations of sharing behavior despite privacy concerns, including monetary incentives, the implicit communal dynamics and potential reciprocity norms that are encountered in a sharing context. The model is the first to incorporate institutional, social and physical privacy concerns, thereby capturing the compounded privacy challenges of the sharing economy.

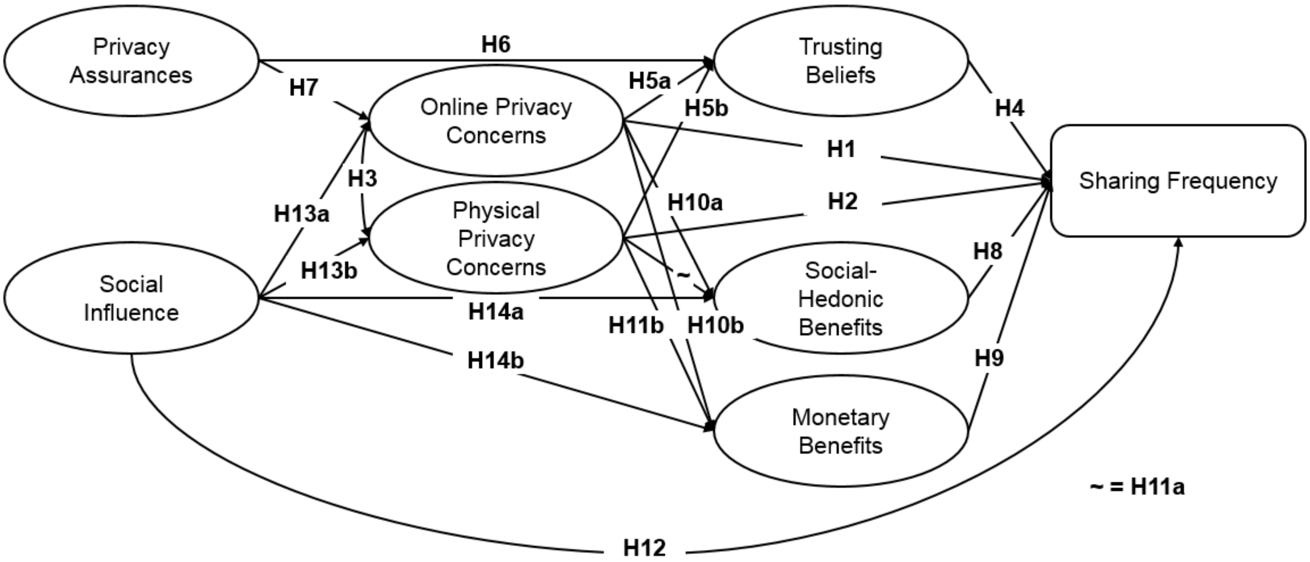


Figure 1. Relationship between privacy concerns and sharing beahvior

Methods

Sample

We base the analysis on a survey conducted on Amazon Mechanical Turk (MTurk) in mid-February 2016. Participants were offered a small monetary incentive, and completing the survey took approximately 15 minutes. A total of 389 respondents completed the survey, 374 of whom were included in the structural equation model and had no or very few missing values. The respondents' profiles and demographics are summarized in Table 1. The questionnaire was aimed at Airbnb hosts only to capture the physical privacy concerns associated with hosting strangers. Accordingly, we applied a filter question addressing previous experience as an Airbnb host.

Most participants in the sample are young or middle-aged. Very few elderly users are included the sample. The gender distribution is quite equal, but men are slightly overrepresented in the sample. The survey participants seem to be highly educated, and most are medium-income earners.

	Count	*%*	*Missing*	*Missing %*
Gender				
Male	192	49.4		
Female	182	46.8		
Total	374	96.1	15	3.9
Age				
19–30	163	41.9		
31–45	163	41.9		
46–64	30	7.7		
65 and older	3	0.8		
Total	359	92.3	30	7.7
Education				
No schooling completed	3	0.8		
High school graduate	29	7.5		
Some college	95	24.4		
Bachelor's degree or equivalent	183	47.0		
Master's degree or equivalent	58	14.9		
Doctorate or equivalent	7	1.8		
Other	1	0.3		
Total	376	96.7	13	3.3
Income				
Low	74	19.0		
Medium	256	65.8		
High	36	9.3		
Total	366	94.1	23	5.9

Table 1. Demographic Composition of the Sample

Method

We relied on structural equation modeling (SEM) to test the research model. We relied on robust maximum-likelihood estimation (MLR) in Mplus (Version 7) to account for non-normality and other possible distortion, such as the non-normal distribution of error terms and heteroscedasticity (Byrne, 2012).

Measurement

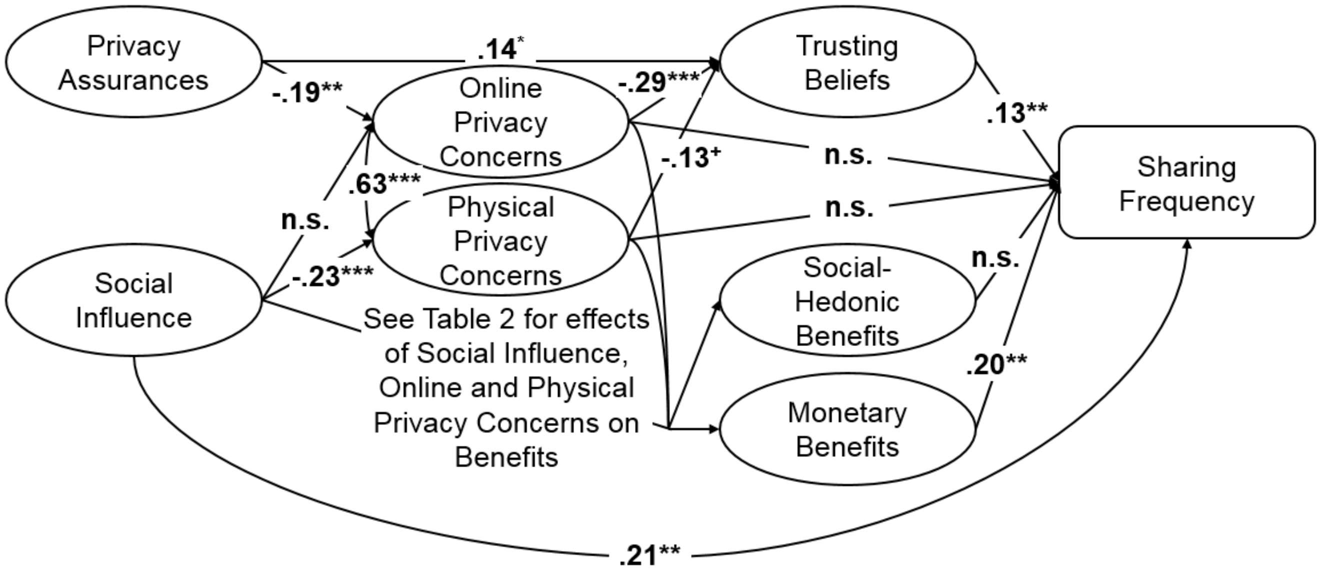
We used the following item to measure respondents' sharing frequency: "*How often have you rented out your place (apartment/house) since joining Airbnb?*" The answer categories range from “0 times” to “10 or more times”. The scales used to measure trusting beliefs (McKnight et al., 2002) and social influence (Venkatesh et al., 2003) were derived from well-established models. The measures for privacy assurances (Hoffmann, Lutz, & Meckel, 2014) and both social-hedonic and monetary benefits (Bucher et al., 2016) were also taken from previous studies. The measures for online and physical privacy concerns were based on previous studies (Stutzman, Capra, & Thompson, 2011; Malhotra et al., 2004), but they were adapted to cover both institutional and social privacy threats in the context of a sharing service.

Appendix A presents the questionnaire, with the wording and references of all the measures applied in this study. We relied on 5-point Likert scales ranging from “strongly disagree” to “strongly agree” for all items, except for privacy concerns. Here, respondents could assess their concern on a 5-point scale ranging from “no concern at all” (1) to “very high concern” (5). As Appendix B shows, the scales reveal good measurement properties in terms of internal consistency, reliability and validity. The measurement model thus satisfies the necessary conditions to report the structural model, i.e., it displays both convergent and discriminant validity (Bollen, 1989; Fornell & Larcker, 1981; Netemeyer, Bearden, & Sharma, 2003).

Results

Before turning to the structural model, we first present a few basic descriptive results: Most respondents have rented out their places between one and three times since joining Airbnb. The arithmetic mean for the sharing frequency variable is 3.77, and the median is 3 (standard deviation is 1.7). However, the sample includes a small proportion of “heavy sharers”: 23 individuals (or 6 percent of the sample) have rented out their place at least 10 times.

The descriptive analysis of the privacy concerns items (see the last column of Table B1 in Appendix B) reveals that users are moderately concerned about their privacy in the Airbnb context. On the 5-point scale used in the survey, the arithmetic means for the privacy concern items range from 2.56 (online privacy: concern about cyberstalking) to 3.25 (physical privacy: guests damaging or dirtying personal belongings). Overall, physical privacy concerns are more pronounced than online privacy concerns, with arithmetic means larger than 3 for each item, while means are below 3 for each online privacy concern item. The Airbnb users in the sample reveal moderate to high levels of trust in the company. However, a minority of approximately 7 percent considers Airbnb untrustworthy (i.e., scoring lowest on the trusting beliefs scale), and approximately 20 percent have little trust in the platform (i.e., scoring second lowest on the trusting beliefs scale).



See Table 2 for effects of Social Influence, Online and Physical Privacy Concerns on Benefits

Figure 2. Results of the SEM

Figure 2 shows the results of the SEM analysis by displaying the structural paths, and Table 2 summarizes the hypothesis tests. Rejecting H1 and H2, we find that both online and physical privacy concerns do not significantly influence respondents' sharing frequency. This absence of a significant effect is in line with previous findings on the privacy paradox. In line with H3, we detect a high correlation between online and physical privacy concerns, showing that the two forms are interrelated yet separate. In the context of sharing, online privacy threats are thus compounded by physical privacy concerns.

	Dependent	
Independent	Social-Hedonic Benefits	Monetary Benefits
Online Privacy Concerns	0.24**	-0.34***
Physical Privacy Concerns	-0.24**	0.28***
Social Influence	0.42***	0.42***

Standardized path coefficients are displayed both for Figure 2 and Table 2.
**** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$; $^+$ $p < 0.1$*

Table 2. Effects of social influence and privacy concerns on benefits

In line with the first explanation proposed for sharing behavior despite privacy concerns, we find that trust mediates the effect of privacy concerns on sharing frequency: Online privacy concerns significantly and negatively affect trusting beliefs, while physical privacy concerns only show a negative effect on the 0.1 level. Trust, in turn, has a significant positive effect on sharing. We also confirm that privacy assurances positively affect trusting beliefs (H6) and reduce online privacy concerns (H7). Overall, these results lend credence to an explanation for sharing behavior despite privacy concerns based on user trust.

As to the second proposed explanation based on a “privacy calculus”, we find that social-hedonic motives (H8) do not significantly affect sharing frequency, but monetary benefits do (H9). As to the effect of privacy concerns on perceived benefits, we find some mixed results: Contrary to our hypothesis (H10a), online privacy concerns are positively associated with perceived social-hedonic benefits, but, in line with H10b, they weaken users’ perceived monetary benefits. In other words, users with pronounced online privacy concerns find Airbnb sharing to be less financially rewarding but more socially and hedonically rewarding. Physical privacy concerns, in turn, negatively affect perceived social-hedonic benefits (H11a) but positively affect perceived monetary benefits (H11b). Thereby, users with more pronounced physical privacy concerns consider the monetary benefits of sharing with Airbnb more rewarding but consider the social-hedonic benefits less rewarding. In sum, we find that perceived benefits mediate the effect of privacy concerns on sharing frequency, yet this effect is more complex than initially proposed.

As to the third explanation proposed for sharing behavior despite privacy concerns, we find that social influence plays an important role in users' sharing decisions. We confirm H12, as social influence has a significant positive direct effect on sharing frequency. The more the people in the sharers' environment encourage and support their sharing, the more frequently these users will share. We also confirm that social influence leads to lower levels of both online (H13a) and physical privacy concerns (H13b). Social influence also strongly fosters the perceived social-hedonic (H14a) and monetary benefits (H14b) associated with sharing via Airbnb.

Hypothesis Number	**Rejected or confirmed**
H1: ONPRI -> - Sharing Frequency	Rejected
H2: PHPRI -> - Sharing Frequency	Rejected
H3: ONPRI -> + PHPRI	Confirmed
H4: TRUST -> + Sharing Frequency	Confirmed
H5: PRI -> - TRUST	Confirmed
H5a: ONPRI -> - TRUST	Confirmed
H5b: PHPRI -> - TRUST	Confirmed
H6: ASSUR -> + TRUST	Confirmed
H7: ASSUR -> - ONPRI	Confirmed
H8: SOC -> + Sharing Frequency	Rejected
H9: MON -> + Sharing Frequency	Confirmed
H10: ONPRI -> - BEN	Partly confirmed
H10a: ONPRI -> - SOC	Rejected
H10b: ONPRI -> - MON	Confirmed
H11: PHPRI -> - BEN	Partly confirmed
H11a : PHPRI -> - SOC	Confirmed
H11b : PHPRI -> - MON	Rejected
H12: INFL -> + Sharing Frequency	Confirmed
H13: INFL -> - PRI	Partly Confirmed
H13a: INFL -> - ONPRI	Rejected
H14b: INFL -> - PHPRI	Confirmed
H14: INFL -> + BEN	Confirmed
H14a: INFL -> + SOC	Confirmed
H14b : INFL -> + MON	Confirmed

Table 3. Overview of Hypotheses

Construct	**R^2**
Sharing Frequency	0.15***
Online Privacy Concerns	0.06*
Offline Privacy Concerns	0.05$^+$
Trusting Beliefs	0.20***
Social-Hedonic Benefits	0.23***
Monetary Benefits	0.25***
Chi Square	849.34
Degrees of Freedom (df)	539
CFI/TLI	0.950/0.944
RMSEA	0.039
SRMR	0.061

CFI = Comparative Fit Index; TLI = Tucker Lewis Index; RMSEA = Root Mean Square Error of Approximation; SRMR = Standardized Root Mean Square Residual.
*** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$; $^+$ $p < 0.1$

Table 4. R^2 and Fit Values of the Model

In summary, the overall model describes the data adequately, as the fit values show (Table 4). However, we are only able to explain 15 percent of the total variance in sharing frequency (Table 4).

Discussion and Conclusion

The sharing economy has attracted the attention of consumers, investors and researchers alike. User privacy and the handling of personal data have been constant concerns since the establishment of online business. Early studies on the emergence of e-commerce have focused on institutional privacy threats, i.e., the service provider’s handling of user data (Hoffman et al., 1999; Milne, 2000; Jarvenpaa et al., 1999; McKnight et al., 2002). Observers have warned that ever-rising consumer concerns may hinder the growth of online business, as users’ willingness to use online services has been found to be negatively related to their online concerns (Sheehan & Hoy, 1999; Phelps et al., 2000, 2001; Olivero & Lunt, 2004).

The emergence of social media has further intensified the debate on online privacy, as these platforms specialize in facilitating the sharing of personal data and the publication of information by lay users (Ellison et al., 2007; Krasnova et al., 2010). Accordingly, with social media, institutional privacy concerns are compounded by social privacy concerns, i.e., concerns about privacy threats that are caused by other users rather than the service provider (Raynes-Goldie, 2010; Young & Quan-Haase, 2013). Based on Belk's (1988) notion of the extended self, we argue that the sharing economy poses an entirely new challenge to users' privacy, as sharing platforms extend beyond the digital domain and threaten users' physical privacy.

As community-based online platforms, sharing services are associated with both institutional and social online privacy concerns. Because these platforms facilitate the sharing of physical resources, they extend users' privacy concerns to the physical domain. Accordingly, sharing services are likely burdened with compounded privacy threats and concerns. However, these services enjoy avid and ever-growing use. In the context of e-commerce and social media services, research has found a paradoxical disparity between users' privacy concerns and their online behaviors, such as a lack of privacy protection and a willingness to engage in extensive data sharing (Chen & Rea, 2004; Milne & Culnan, 2004; Milne et al., 2004, 2009). Based on these findings, we develop and test a nomological model that considers three distinct explanations for users' sharing behavior despite compounded privacy concerns.

Our study provides a number of theoretical and practical implications. First, we establish the existence of compounded privacy concerns in the sharing context, as we find evidence of both online and physical privacy concerns as well as a significant correlation between both. Second, we find a "sharing paradox" in line with previous findings on the privacy paradox, as we find that neither online nor physical privacy concerns directly affect sharing behaviors. Third, our research model provides support for three distinct theoretical explanations for sharing behavior despite compounded privacy concerns that are based on user trust, the privacy calculus and social influence.

We find that user trust mediates the effect of privacy concerns on sharing behaviors. Users' trusting beliefs in specific service providers thereby facilitate sharing, while privacy concerns inhibit the development of these trusting beliefs. Service providers may engage in practices that facilitate trust, such as the provision of privacy assurances. We thus show the importance of combining insights on online trust with the privacy discourse to provide an explanation for the apparent disparities between user attitudes and behaviors. We argue that trusting beliefs serve as a heuristic that facilitates specific online transactions while circumventing general attitudes.

We also find some support for the notion of users engaging in a mental calculus, weighing transaction risks against benefits. This rational choice argument holds that users decide to overcome or ignore privacy concerns to reap benefits that are deemed more valuable than the associated privacy risks (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Kokolakis, 2015; Lee et al., 2013; Smith et al., 2011). In the context of sharing services such as Uber or Airbnb (as opposed to non-commercial sharing in the vein Belk, 2014), both social-hedonic and monetary benefits may sway users to overcome their concerns and engage in sharing. We find that, among the active sharers on Airbnb in our sample, only monetary benefits drive user behaviors and mediate the effect of privacy concerns. More specifically, we find that online privacy concerns decrease perceived monetary benefits, while physical concerns actually increase them. This somewhat surprising finding may be attributed to the value of the property shared, as sharers of valuable properties may have especially high physical concerns and may also receive larger monetary reimbursements. As such, more pronounced physical concerns may actually be associated with higher monetary benefits. However, this hypothesis goes beyond the scope of our examination and should be considered in future studies.

Finally, we find that social dynamics are especially important in the analysis of sharing behaviors. In fact, we find that social influence drives sharing in three ways. First, social influence directly facilitates sharing frequency. Second, social influence reduces privacy concerns. Third, social influence strongly increases the perceived benefits of sharing. While the first can be explained using technology acceptance models (Venkatesh & Bala, 2008; Venkatesh & Davis, 2000; Venkatesh et al., 2003) and the second is in line with findings on perceived situational normality (Li et al., 2008; McKnight & Chervany, 2002), we find the third finding to be especially noteworthy. The notion of sharing is heavily based on community norms of reciprocity and mutual support (Belk, 2007, 2014). Our findings demonstrate that these norms are of crucial importance, even for commercial services. While monetary benefits play an important role in our model, the perception of these benefits is actually contingent on social encouragement and approval (cf., Raghunathan & Corfman, 2006). As such, service providers would do well to invest in community management, and they should rely heavily on word-of-mouth promotion.

Another practical implication of our research is that service providers should not discount privacy concerns, despite an apparent “sharing paradox”. Our data show that users—even experienced sharers—have privacy concerns, particularly physical privacy concerns. Notably, our study does not illuminate the concerns of users who avoid using the platform in the first place. Additionally, our nomological model shows that privacy concerns have an effect on sharing intensity, although this effect is mediated through either trust or perceived benefits. The privacy assurances of sharing services thus need to go beyond well-established mechanisms of online privacy assurance and address potential physical privacy concerns. Recent media coverage of privacy issues with regard to sharing services such as Airbnb and

Uber indicates increasing public attention to these matters (e.g., Constable, 2014; Reisinger, 2014).

Our research presents some *limitations*, which may inspire future research on the topic. First, we conducted a cross-sectional survey with a relatively low number of participants and a specific target group (Airbnb hosts). Thus, our findings should be applied to other sharing contexts with care, especially in the case of non-commercial sharing. Future research should investigate additional sharing contexts, such as car and tool sharing. It should perform longitudinal analyses with a broader spectrum of the sharing population. Second, for the sake of brevity, our questionnaire did not assess a large number of platform characteristics (such as ease of use, technological reliability and design) or affordances. Moreover, we could not assess contextual characteristics, such as users' cultural backgrounds or their social milieus. Future research could delve deeper into both user and platform characteristics to achieve a more holistic understanding of privacy in the sharing economy.

Despite these limitations, our study not only highlights the compounded privacy challenges that are associated with the sharing economy but also establishes the existence of a "sharing paradox" and provides several explanations for the apparent disparities between user attitudes and behaviors. Our nomological model of privacy concerns in the sharing context considers institutional, social and physical privacy threats; it differentiates the benefits previously discussed in the sharing literature; and it examines the social dynamics that are associated with online sharing.

References

Acquisti, A. (2004). Privacy in electronic commerce and the economics of immediate gratification. *Proceedings of the 5th ACM Conference on Electronic Commerce* (pp. 21-29). New York: ACM.

Acquisti, A., & Gross, R. (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook," in *Privacy Enhancing Technologies*, Berlin: Springer Verlag, pp. 36-58.

Ashworth, L., & Free, C. (2006). Marketing Dataveillance and Digital Privacy: Using Theories of Justice to Understand Consumers' Online Privacy Concerns. *Journal of Business Ethics, 67*(2), 107-123.

Barnes, S. B. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9). Retrieved from: http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312

Belk, R. (1985). Materialism: Trait aspects of living in the material world. *Journal of Consumer Research, 12*(3), 265-80.

Belk, R. (1988). *Possessions and Self*. John Wiley & Sons, Ltd.

Belk, R. (2007). Why not share rather than own? *The Annals of the American Academy of Political and Social Science, 611*(1), 126-140.

Belk, R. (2010). Sharing. *Journal of Consumer Research, 36*(5), 715-734.

Belk, R. (2014). You are what you can access: Sharing and collaborative con-sumption online. *Journal of Business Research, 67*(8), 1595-1600.

Benkler, Y. (2004). Sharing Nicely: On Shareable Goods and the Emergence of Sharing as a Modality of Economic Production. *Yale Law Journal*, *114*(2), 273-358.

Bhattacherjee, A. (2002). Individual Trust in Online Firms: Scale Development and Initial Test. *Journal of Management Information Systems, 19*(1), 211-241.

Bollen, K. A. (1989). *Structural Equations with Latent Variables*. Hoboken, NJ: Wiley Interscience.

Botsman, R., & Rogers, R. 2010. *What's Mine Is Yours*, New York: Harper Business.

boyd, D., & Hargittai, E. 2010. Facebook Privacy Settings: Who Cares? *First Monday, 15*(8). Retrieved from http://firstmonday.org/article/view/3086/2589

Bucher, E., Fieseler, C., & Lutz, C. (2016). What's mine is yours (for a nominal fee)–Exploring the spectrum of utilitarian to altruistic motives for Internet-mediated sharing. *Computers in Human Behavior*, *62*, 316-326.

Byrne, B. M. (2012). *Structural Equation Modeling with Mplus: Basic Concepts, Applications, and Programming*. New York, NY: Routledge.

Chen, K., & Rea, A. I. (2004). Protecting Personal Information Online: A Survey of User Privacy Concerns and Control Techniques. *Journal of Computer Information Systems, 44*(4), 85-92.

Compeau, D. R., & Higgins, C. A. (1995). Application of Social Cognitive Theory to Training for Computer Skills. *Information Systems Research, 6*(2), 118-143.

Constable, K. (2014). Think Twice Before Giving AirBnB Your ID. *Huffpost British Columbia*, 3 March . Retrieved from http://www.huffingtonpost.ca/kris-constable/airbnb-privacy-security-id-jumio_b_4887509.html

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Proce-dural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science, 10*(1), 104-115.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology, 45*(3), 285-297.

Dinev, T., & Hart, P. (2004). Internet Privacy Concerns and Their Antecedents: Measurement Validity and a Regression Model. *Behavior and Information Technology, 23*(6), 413-423.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80.

Dodds, P. S., & Watts, D. J. (2005). A Generalized Model of Social and Biological Contagion. *Journal of Theoretical Biology*, *232*(4), 587–604.

Edelman, B. G., & Luca, M. (2014). Digital Discrimination: the Case of Airbnb.com. *Harvard Business School NOM Unit Working Paper* (14-054). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2377353

Edelman, B., Luca, M., & Svirsky, D. (2015). Racial Discrimination in the Sharing Economy: Evidence from a Field Experiment. *Harvard Business School NOM Unit Working Paper* (16-069). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2701902

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The Benefits of Facebook 'Friends': Social Capital and College Students' Use of Online Social Network Sites. *Journal of Computer*‐*Mediated Communication*, *12*(4), 143-1168.

Eurobarometer (2011). Special Eurobarometer 359. *Attitudes on Data Protection and Electronic Identity in the European Union*. June 2011. https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/report_eb_743_eid_just_jrc_en_full_report_final.pdf

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research, 18*(1), 39–50.

Friedman, B., Khan, P. H., & Howe, D. C. (2000). Trust Online. *Communications of the ACM, 43*(12), 34-40.

Gefen, D. (2000). E-Commerce: The Role of Familiarity and Trust. *Omega, 28*(6), 725-737.

Goffman, E. (1971). The Territories of the Self. *Relations in Public*, 28-61.

Goldenberg, J., Han, S., Lehmann, D. R., & Hong, J. W. (2009). The Role of Hubs in the Adoption Process. *Journal of Marketing, 73*(2), 1-13.

Gross, R., & Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks. *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society* (pp. 71-80). New York, NY: ACM.

Gurven, M. (2006). The Evolution of Contingent Cooperation. *Current Anthropology* (47), 185-192.

Hamari, J., Sjöklint, M., & Ukkonen, A. (2016). The Sharing Economy: Why People Participate in Collaborative Consumption. *Journal of the Association for Information Science & Technology, 67*(9), 2047-2059.

Hoffman, D. L., Novak, T. P., & Peralta, M. A. (1999). Information Privacy in the Marketspace: Implications for the Commercial Uses of Anonymity on the Web. *Information Society, 15*(2), 129-139.

Hoffmann, C. P., Lutz, C., & Meckel, M. (2014). Digital natives or digital immigrants? The impact of user characteristics on online trust. *Journal of Management Information Systems, 31*(3), 138-171.

Iyengar, R., Van Den Bulte, C., & Valente, T. W. (2011). Opinion Leadership and Social Contagion in New Product Diffusion. *Marketing Science, 30*(2), 195–212.

Jarvenpaa, S. L., Tractinsky, N., & Saarinen, L. (1999). Consumer Trust in an Internet Store. *Journal of Computer-Mediated Communcation, 5*(2), 34-67.

Jenkins, R., Molesworth, M., & Scullion, R. (2014). The Messy Social Lives of Objects: Inter-Personal Borrowing and the Ambiguity of Possession and Ownership. *Journal of Consumer Behaviour, 13*(2), 131-139.

John, N. A. (2013a). The social logics of sharing. *The Communication Review*, *16*(3), 113-131.

John, N. A. (2013b). Sharing and web 2.0: The emergence of a keyword. *New Media & Society*, *15*(2), 167-182.

Khadem, N. (2015). Turbulence for Airbnb over privacy concerns. *The Sydney Morning Herald*, 17 February 2015. Retrieved from http://www.smh.com.au/business/turbulence-for-airbnb-over-privacy-concerns-20150216-13g8tm.html

Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A Trust-Based Consumer Decision-Making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents. *Decision Support Systems*, *44*(2), 544–564.

Kleine, S.S., Kleine III, R.E., & Allen, C.T. (1995). How Is a Possession ‘Me’ Or ‘Not Me’? Characterizing Types and an Antecedent of Material Possession Attachment. *Journal of Consumer Research*, *22*(3), 327-343.

Kokolakis, S. (2015). Privacy attitudes and privacy behaviour: A review of cur-rent research on the privacy paradox phenomenon. *Computers & Security*, online first. doi:10.1016/j.cose.2015.07.002

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology*, *25*(2), 09–125.

Lamberton, C. P., & Rose, R. L. (2012). When Is Ours Better Than Mine? A Framework for Understanding and Altering Participation in Commercial Sharing Systems. *Journal of Marketing*, *76*(4), 109-125.

Lanier, C. D., & Saini, A. (2008). Understanding Consumer Privacy: A Review and Future Directions. *Academy of Marketing Science Review*, *12*(2), 1-45.

Lee, H., Park, H., & Kim, J. (2013). Why do people share their context infor-mation on Social Network Services? A qualitative study and an experi-mental study on users' behavior of balancing perceived benefit and risk. *International Journal of Human-Computer Studies, 71*(9), 826-877.

Li, X., Hess, T. J., & Valacich, J. S. (2008). Why do We Trust New Technology? A Study of Initial Trust Formation with Organizational Information Systems. *Journal of Strategic Information Systems, 17*(1), 39-71.

Madden, M., & Rainie, L. (2015). Americans' Attitudes about Privacy, Security and Surveillance. *Pew Internet & American Life Project Report*. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research, 15*(4), 336-355.

McKnight, D. H., & Chervany, N. L. (2002). What Trust Means in E-Commerce Customer Relationships: an Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce, 6*(2), 35-59.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and Validating Trust Measures for E-Commerce: an Integrative Typology. *Information Systems Research, 13*(3), 334-359.

Milne, G. R. (2000). Privacy and Ethical Issues in Database/Interactive Marketing and Public Policy: A Research Framework and Overview of the Special Issue. *Journal of Public Policy & Marketing, 19*(1), 1-6.

Milne, G. R., & Boza, M.-E. (1999). Trust and Concern in Consumers' Perceptions of Marketing Information Management Practices. *Journal of Interactive Marketing, 13*(1), 5-24.

Milne, G. R., & Culnan, M. J. (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, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, *43*(3), 449-473.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' Protection of Online Privacy and Identity. *Journal of Consumer Affairs*, *38*(2), 217–232.

Netemeyer, R. G., Bearden, W. O., & Sharma, S. (2003). *Scaling Procedures. Issues and Applications*. London: Sage Publishing.

Nissenbaum, H. (2001). Securing Trust Online: Wisdom or Oxymoron? *Boston University Law Review*, *81*(3), 101-131.

Olivero, N., & Lunt, P. (2004). Privacy versus Willingness to Disclose in E-Commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control. *Journal of Economic Psychology*, *25*(2), 243-262.

Ozanne, L. K., & Ballantine, P. W. (2010). Sharing as a Form of Anti-Consumption? An Examination of Toy Library Users. *Journal of Consumer Behaviour, 9*(6), 485-498.

Phelps, J. E., D'Souza, G., & Nowak, G. J. (2001). .Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation. *Journal of Interactive Marketing*, *15*(4), 2-17.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, *19*(1), 27-41.

Raghunathan, R., & Corfman, K. (2006). Is Happiness Shared Doubled and Sadness Shared Halved? Social Influence on Enjoyment of Hedonic Experiences. *Journal of Marketing Research*, *43*(3), 386-394.

Raynes-Goldie, K. (2010). Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook. *First Monday, 15*(1). doi:10.5210/fm.v15i1.2775

Reisinger, D. (2014). Uber's 'God View' under Scrutiny as Spotlight Intensifies on Its Practices. *Cnet*, 19 November. Retrieved from http://www.cnet.com/news/god-view-under-spotlight-as-uber-investigation-intensifies/

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so Different after All: A Cross-Discipline View of Trust. *Academy of Management Review, 23*(3), 393-404.

Rust, R. T., Kannan, P. K., & Peng, N. (2002). The Customer Economics of Internet Privacy. *Journal of the Academy of Marketing Science, 30*(4), 455-464.

Schoenbachler, D. D., & Gordon, G. L. (2002). Trust and Customer Willingness to Provide Information in Database-driven Relationship Marketing. *Journal of Interactive Marketing, 16*(3), 2-16.

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, Complaining, Abstaining: How Online Users Respond to Privacy Concerns. *Journal of Advertising, 28*(3), 37-51.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of Privacy Concern Among Online Consumers. *Journal of Public Policy & Marketing, 19*(1), 62-73.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information Privacy Research: an Interdisciplinary Review. *MIS Quarterly, 35*(4), 989-1016.

Special, W. P., & Li-Barber, K. T. (2012). Self-Disclosure and Student Satisfaction with Facebook. *Computers in Human Behavior, 28*(2), 624-630.

Stutzman, F., Capra, R., & Thompson, J. (2011). Factors Mediating Disclosure in Social Network Sites. *Computers in Human Behavior, 27*(1), 590-598.

Tufekci, Z. (2008). Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. *Bulletin of Science, Technology & Society, 28*(1), 20-36.

Urban, G. L., Amyx, C., & Lorenzon, A. (2009). Online Trust: State of the Art, New Frontiers, and Research Potential. *Journal of Interactive Marketing*, *23*(2), 179-190.

Utz, S., & Krämer, N. (2009). The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms. Cyberpsychology. *Journal of Psychosocial Research on Cyberspace*, *3*(2), Article 1.

Venkatesh, V., & Bala, H. (2008). Technology Acceptance model 3 and a Research Agenda on Interventions. *Decision Sciences*, *39*(2), 273-315.

Venkatesh, V., & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies. *Management Science*, *46*(2), 186-204.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, *27*(3), 425-478.

Wang, S., Beatty, S. E., & Foxx, W. (2004). Signaling the Trustworthiness of Small Online Retailers. *Journal of Interactive Marketing*, *18*(1), 53-69.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. Harvard Law Review, *4*(5), 193-220.

Watts, D. J., & Dodds, P. S. (2007). Influentials, Networks, and Public Opinion Formation. *Journal of Consumer Research*, *34*(4), 441–458.

Wells, J. D., Valacich, J. S., & Hess, T. J. (2011). What Signal Are You Sending? How Website Quality Influences Perceptions of Product Quality and Purchase Intentions. *MIS Quarterly*, *35*(2), 373–396.

Wilson, R. E., Gosling, S. D., & Graham, L. T. (2012). A Review of Facebook Research in the Social Sciences. *Perspectives on Psychological Science*, *7*(3), 203-220.

Wittel, A. (2011). Qualities of Sharing and Their Transformation in the Digital Age. International Review of Information. *Ethics*, *15*(9), 3-8.

Yoon, S.-J. (2002). The Antecedents and Consequences of Trust in Online-Purchase Decisions. *Journal of Interactive Marketing*, *16*(2), 47-63.

Young, A. L., & Quan-Haase, A. (2013). Privacy Protection Strategies on Facebook: The Internet Privacy Paradox Revisited. *Information, Communication & Society, 16*(4), 479–500.

Zhang, Y., & Leung, L. (2015). A Review of Social Networking Service (SNS) Research in Communication Journals from 2006 to 2011. *New Media & Society*, *17*(7), 1007-1024.

Appendix

Appendix A: Questionnaire

Sharing Motives: Monetary (Bucher et al., 2016)	***I share because it pays well.***
	Earning extra money is an important factor when sharing.
	Sharing is a good way to supplement my income.
	Sharing allows me to make money from something I own.
Sharing Motives: Social-Hedonic (Bucher et al., 2016)	*Sharing is a good way to meet new people.*
	Through sharing, there is a good chance that I will meet like-minded people.
	Sharing makes me feel like part of a community.
	Sharing is a good way to find company.
	Sharing is fun.
	I share because it is an adventure.
Privacy Assurance (Hoffmann et al., 2014)	*The service explains why it needs specific personal data.*
	The privacy policy is easy to find.
	The privacy policy is easy to understand.
	The terms and conditions are easy to find.
Social Influence (based on Venkatesh et al., 2003)	*People who are important to me think that I should use Airbnb.*
	My friends have been helpful in the use of Airbnb.
	In general, my friends have supported the use of Airbnb.
Online Privacy Concerns (first four items adapted from Stutzman et al., 2011, and last four items newly developed and partly based on Malhotra et al., 2004)	Please indicate your level of concern about the following potential privacy risks that arise when you share your personal information on Airbnb.
	Other users engaging in identity theft
	Other users hacking into my account
	Other users stalking me (cyberstalking)
	Other users publishing my personal information without my consent
	Airbnb insufficiently protecting personal data (information leakage)
	Airbnb tracking and analyzing personal data
	Airbnb selling personal data to third parties
	Airbnb sharing personal data with government agencies
Physical Privacy Concerns (adapted from Stutzman et al., 2011)	Please indicate your level of concern about the following potential privacy risks that arise when you host someone at your place via Airbnb.
	Guests damaging or dirtying my personal belongings (e.g., furniture)
	Guests snooping through my personal belongings (e.g., pictures)
	Guests entering areas that they should not access (e.g., bedroom)
	Guests using items that they should not use (e.g., bedclothes, pillows, personal hygiene products)
Trusting Beliefs (based on McKnight et al., 2002)	*Airbnb is interested in my well-being, not just its own.*
	Airbnb is competent and effective in providing its services.
	I would characterize Airbnb as honest.
	Airbnb is trustworthy.
	I would characterize Airbnb as reliable.

Table A. Questionnaire of the survey

Appendix B: Measurement Model

Construct	Item	Standardized loading	t-values	R^2	α	C.R.	AVE	Descriptive statistics
Sharing Motives: Monetary (MON)	mon1	0.686	18.130***	0.470	0.86	0.86	0.61	Mean: 4.23 Median: 4.00 Std. deviation: 0.80
	mon2	0.766	19.105***	0.587				
	mon3	0.808	26.069***	0.654				
	mon4	0.861	33.808***	0.741				
Sharing Motives: Social-Hedonic (SOC)	soc1	0.831	36.772***	0.690	0.90	0.90	0.61	Mean: 3.61 Median: 4.00 Std. deviation: 1.06
	soc2	0.792	23.898***	0.626				
	soc3	0.766	22.296***	0.587				
	soc4	0.752	24.289***	0.566				
	soc5	0.773	24.403***	0.597				
	soc6	0.756	25.204***	0.572				
Privacy Assurance (ASS)	ass1	0.714	19.566***	0.510	0.83	0.83	0.56	Mean: 3.85 Median: 4.00 Std. deviation: 0.90
	ass2	0.847	31.343***	0.717				
	ass3	0.736	20.849***	0.542				
	ass4	0.684	13.884***	0.464				
Social Influence (INFL)	infl1	0.647	13.788***	0.418	0.81	0.79	0.56	Mean: 3.71 Median: 4.00 Std. deviation: 0.94
	infl2	0.753	21.707***	0.566				
	infl3	0.837	28.663**	0.701				
Online Privacy Concerns (ONPRI)	onpri1	0.796	30.630***	0.634	0.92	0.92	0.59	Mean: 2.81 Median: 3.00 Std. deviation: 1.14
	onpri2	0.815	34.657***	0.664				
	onpri3	0.770	29.957***	0.593				
	onpri4	0.793	29.237***	0.629				
	onpri1	0.804	35.847***	0.646				
	onpri2	0.747	28.369***	0.559				
	onpri3	0.713	22.229***	0.508				
	onpri4	0.690	21.264***	0.476				
Physical Privacy Concerns (PHPRI)	phpri1	0.757	23.241***	0.573	0.89	0.89	0.67	Mean: 3.24 Median: 3.00 Std. deviation: 1.12
	phpri2	0.839	38.676***	0.704				
	phpri3	0.854	39.342***	0.730				
	phpri4	0.817	30.244***	0.668				
Trusting Beliefs (TRUST)	trust1	0.717	22.745***	0.514	0.935	0.94	0.75	Mean: 3.24 Median: 3.50 Std. deviation: 1.14
	trust2	0.891	54.429***	0.793				
	trust3	0.892	50.105***	0.795				
	trust4	0.895	52.203***	0.801				
	trust5	0.906	65.846***	0.821				
Criterion		≥ 0.5	min*	≥ 0.4, < 0.9	≥ 0.7	≥ 0.6	≥ 0.5	

α = Cronbach's Alpha; C.R. = composite reliability; AVE = average variance extracted.
Average, median and standard deviation calculated per item and then averaged across items for each construct; N=374.

Table B. Measurement model

	AVE	**MON**	**SOC**	**ASS**	**INFL**	**ONPRI**	**PHPRI**
MON	0.61						
SOC	0.61	0.03					
ASS	0.56	0.30	0.15				
INFL	0.56	0.14	0.16	0.21			
ONPRI	0.59	0.06	0.00	0.07	0.04		
PHPRI	0.67	0.00	0.04	0.03	0.05	0.40	
TRUST	0.75	0.10	0.01	0.06	0.02	0.17	0.12

Squared correlations between the constructs are shown; AVE = average variance extracted.

Table C. Discriminant validity test (Fornell Larcker criterion)