Information, Communication & Society

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rics20

Technology use and norm change in online privacy: experimental evidence from vignette studies

Christine Horne & Wojtek Przepiorka

To cite this article: Christine Horne & Wojtek Przepiorka (2021) Technology use and norm change in online privacy: experimental evidence from vignette studies, Information, Communication & Society, 24:9, 1212-1228, DOI: 10.1080/1369118X.2019.1684542

To link to this article: https://doi.org/10.1080/1369118X.2019.1684542

INFORMATION, COMMUNICATION & SOCIETY
2021, VOL. 24, NO. 9, 1212–1228
https://doi.org/10.1080/1369118X.2019.1684542

Routledge
Taylor & Francis Group

Technology use and norm change in online privacy: experimental evidence from vignette studies

Christine Horne[a*] and Wojtek Przepiorka[b*]

[a]Department of Sociology, Washington State University, Pullman, WA, USA; [b]Department of Sociology, Utrecht University, Utrecht, Netherlands

ABSTRACT
We suggest that explaining privacy behaviors requires understanding not only individual attitudes, but also norms and trust. We propose: (1) the popularity of a potentially privacy-violating technology leads individuals to expect that others approve of privacy violations and simultaneously increases their trust in the technology provider; (2) the frequency of privacy violations by other similar providers leads individuals to expect that a specific provider will engage in privacy-violating behaviors and decreases trust in that provider; (3) trust in a specific provider and expectations that others approve of the provider violating users' privacy increase, and expectations that other similar providers are likely to violate privacy decrease, willingness to use a technology. We test our propositions using two vignette experiments in the context of a household energy app. Our results are generally consistent with our hypotheses. Our findings have implications for understanding privacy norms and highlight the potential consequences of major technology roll-outs.

ARTICLE HISTORY
Received 2 November 2018
Accepted 20 October 2019

KEYWORDS
Descriptive norms; trust; smart grid; vignette experiment; normative expectations

Introduction

Many providers of new information and communication technologies (ICT) build their business models on information shared by users (e.g., Craglia & Shanley, 2015; Dellarocas, 2003). At the same time, frequent media accounts describing privacy invasions by ICT providers have heightened concerns about privacy (e.g., Associated Press, 2019; Bode, 2018; Kelly, 2019; Kiger, 2016; Shaban, 2018; Vaidhyanathan, 2018). If providers want to be trusted with users' information and data, they must take users' privacy concerns seriously.

Substantial research on privacy focuses on the associations between privacy attitudes and behaviors (Baruh, Secinti, & Cemalcilar, 2017; Dienlin & Trepte, 2015). Research on innovation diffusion highlights the potential importance of others' behaviors (e.g., Rogers, 1962); work on technology adoption emphasizes both social influence and aspects of people's confidence in a technology (e.g., Venkatesh, Morris, Davis, & Davis, 2003).

CONTACT Christine Horne ✉ chorne@wsu.edu Department of Sociology, Washington State University, 204 Wilson-Short Hall, Pullman, WA, 99164
*Both authors contributed equally to this work.
Supplemental data for this article can be accessed at https://doi.org/10.1080/1369118X.2019.1684542

Consistent with these literatures, we suggest that understanding privacy behaviors requires understanding not only individual attitudes, but also norms and trust (Cheshire, 2011; Feri, Giannetti, & Jentzsch, 2016; Joinson, Reips, Buchanan, & Schofield, 2010; Nissenbaum, 2010; Waldman, 2018). *Norms* are rules governing behavior that are socially enforced (Horne, 2018). When a norm is in place, people expect that others will react negatively to violations. Such normative expectations have significant effects on behavior and may lead people to comply with the norm rather than act according to their own preferences (Bicchieri, 2017). *Trust* is an ingredient in social and economic exchange relationships in which actors engage in behaviors that have the potential for gain, but also for losses that may occur as a result of others' actions (e.g., Fehr, 2009; Gambetta, 1988; Levi & Stoker, 2000; Riegelsberger, Sasse, & McCarthy, 2005). When people believe that someone is trustworthy, they are more willing to make some kind of advance (e.g., purchase a product or download an app), expecting that the other party has the ability and intention to meet that advance. In other words, when people view another party as trustworthy, they think the other party is competent, its work is high quality, and it cares about people's interests.

We argue that the widespread roll-out and use of new ICT (referred to as 'technology' or 'apps' throughout the paper) changes individuals' expectations, in turn, affecting their behavior. More specifically we argue that, when a technology could be used by a provider to violate individuals' privacy, individuals rely on others' use of that technology to infer that those others approve of privacy violations. Moreover, others' use of ICT may act as an endorsement of the technology and its provider, thereby affecting expectations regarding the trustworthiness (competence and intent) of the provider. Thus, the popularity of a technology that could be used to violate privacy tells people both that others approve of privacy violations and that such violations are not worrisome. Finally, privacy violations by other providers may also affect individuals' expectations (Feri et al., 2016). If many similar providers engage in privacy violations, then people are likely to think that a particular provider will do so as well and will have less trust in that provider. These expectations have implications for behavior. Normative expectations about how much others approve of privacy violations and expectations that a particular provider is trustworthy increase willingness to use a technology, whereas behavior expectations that a specific provider will violate privacy decrease willingness.

We test our hypotheses using two online vignette experiments in the context of a smart meter app for household energy management. The first study is based on a convenience sample of US residents. To assess the generalizability of the results obtained in our first study, we conduct our second study with a representative sample of the US adult population (Auspurg & Hinz, 2015). Our results provide substantial support for our hypotheses.

Energy context

Privacy research often focuses on contexts such as social media, business, and crime (e.g., Brayne, 2014; Earl, 2012). But ICT is used in other, less visible domains. Of particular significance is the increasing integration of ICT into critical infrastructures – sectors that are so vital 'that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof'

(US Department of Homeland Security, n.d.). In these contexts, understanding privacy concerns can have significant implications for national welfare.

One such critical infrastructure is the electricity delivery system. In its transition to a sustainable, reliable, efficient 'smart grid,' the system is integrating increasing amounts of ICT. Households (referred to as 'consumers' throughout the paper) are seen by many as key actors in the emerging smart grid (e.g., Bakke, 2016; Frickel, Wühr, Horne, & Kallman, 2017). But, consumers' engagement presupposes their willingness to participate in industry programs and provide information on their energy consumption. Initiatives that rely on consumers sharing private information and data with their utilities should not take voluntary participation for granted (see, e.g., Bode, 2018; Kiger, 2016 for media accounts of consumers' concerns about privacy in the electricity context and Balta-Ozkan, Boteler, & Amerighi, 2014 for evidence that consumers are wary of technologies that track in-home activities). If such initiatives fail to get consumers on board, because they neglect privacy concerns or turn out to be ineffective, a unique opportunity to maximize the benefits gained from consumer-generated information may be missed. Thus, understanding of norm and trust dynamics has implications for the productive engagement of consumers in the electricity delivery system and the future smart grid.

Previous research and hypotheses

Privacy research has a long history. Early work established privacy as a concern across time periods and cultures (e.g., Altman, 1977; Moore, 1984; Murphy, 1964; Shils, 1966; Westin, 1970). Much of the recent research on privacy focuses on individual privacy attitudes (Baruh et al., 2017; Nissenbaum, 2010; Norberg, Horne, & Horne, 2007) and on the costs and benefits of making private information public and keeping it private (Acquisti, Taylor, & Wagman, 2016; Dienlin & Metzger, 2016; Krause & Horvitz, 2010; Petronio, 1991). Some work has begun to look beyond individual attitudes and cost–benefit considerations to consider social influences. For example, Nissenbaum (2010) argues that privacy norms are contextual. They vary depending on factors such as the type of information and the roles of the people involved (for a review of research on social factors relevant for understanding privacy see Anthony, Campos-Castillo, & Horne, 2017; see also Rimal & Lapinski, 2015).

Can insights from the norms literature help us understand the likely consequences of ICT proliferation and media reports of privacy breaches/violations? The literature on norms is voluminous. Norms are of interest to scholars in anthropology, psychology (Cialdini, 2007), sociology (Hechter & Opp, 2001; Mollborn, 2017) philosophy (Bicchieri, 2017), communications (Rimal, Limaye, Roberts, Brown, & Mkandawire, 2013), law (Posner, 2000), political science (Mackie, 1996), economics (Fehr & Schurtenberger, 2018), and elsewhere. It is beyond the scope of this paper to fully incorporate or assess the nuances in these disparate literatures. Instead, we take a focused approach that draws on a few specific concepts. In particular, we draw on the literature on descriptive and injunctive norms (Cialdini, 2007; Cialdini & Trost, 1998).

Descriptive norms capture people's perceptions of what most others typically do – those behaviors that are popular or widespread (Cialdini, 2007; see also Rimal et al., 2013 on collective norms). Research on innovation diffusion and technology acceptance highlights the potential importance of others' behaviors on adoption and acceptance of new technologies (e.g., Rogers, 1962; Venkatesh et al., 2003). Thus, the literature on descriptive norms is potentially useful for helping to understand the implications of widespread use of ICT. Injunctive norms (henceforth norms) are rules that prescribe or proscribe behavior and are socially enforced (Coleman, 1990; Horne, 2018). When a norm is in place, people expect that violations will be punished and/or compliance will be rewarded (Bicchieri, 2017). Normative expectations refer to people's expectations about how much others approve or disapprove of a behavior (see also Ajzen, 1991 on subjective norms and Rimal & Lapinski, 2015 on perceived norms). These *normative expectations* indicate the existence of a norm. Such expectations are relevant for individuals' decisions about what to do in a particular situation (Willer, Kuwabara, & Macy, 2009; Xenitidou & Edmonds, 2014).

Recent research shows that descriptive norms (the popularity of a behavior) can affect normative expectations because people use others' behavior as a source of evidence about what those others approve (Diekmann, Przepiorka, & Rauhut, 2015; Horne, Tinkler, & Przepiorka, 2018; Willer et al., 2009; for research in the privacy context see Hofstra, Corten, & Tubergen, 2016). For example, if many others use a particular app, the individual is likely to infer that others approve of using the app. We build on this insight to argue that typical behaviors by one type of actor can also provide evidence of norms regulating *other* actors. In our case, when many people use a technology, such as a new app, their actions can be seen as expressing approval of not only using the app but also the actions of the company that provides it. The implication is that when a company provides a technology that could be used to violate users' privacy, people who use that technology are signaling that they approve of the technology and of potential privacy violations by the company. App popularity (descriptive norms) affects normative expectations about how much others approve of privacy violations. In other words:

> H1a: The more popular a technology that could be used to violate privacy, the more people will expect others to approve of privacy violations by the technology provider.

Descriptive norms also affect people's perceptions of quality; the popularity of a behavior affects people's perceptions of the likely consequences of engaging in that behavior. For example, when many people eat at a particular restaurant, people may assume that one can have confidence in it (Cialdini, Reno, & Kallgren, 1990; Dellarocas, 2003). Similarly, when an app is popular, the fact that many people are using it may act as an endorsement (e.g., Rogers, 1962). One can have confidence in the technology and its provider (Younts, 2008; Zelditch, 2001); the provider is trustworthy (Riegelsberger et al., 2005). Trustworthiness refers to a party's ability and intent to act in the interest of another party in return for an advance (e.g., good quality service or product in return for a monetary payment). Generalized trust (perceptions of the trustworthiness of the average person) predicts privacy attitudes and behavior (Heirman, Walrave, & Ponnet, 2013; Hofstra et al., 2016). Here we focus on people's trust in a specific entity – the technology provider (Joinson et al., 2010). Evidence that other people use a technology that could potentially be used to violate privacy may suggest that those others *trust* that the product the provider produces is high quality and that the provider will not act against users' interests. The popularity of a technology will lead people to view the provider as more trustworthy. Thus:

H1b: The more popular a technology that could be used to violate privacy, the more people will expect that the technology provider is trustworthy.

Thus far we have focused on the effects of app popularity. Now we turn to the effects of privacy violations. Despite regular reports on major privacy breaches and violations by well-known companies (e.g., Marsan, 2012), scholars know little about the consequences of such reports on user expectations and behaviors (Feri et al., 2016). Researchers have looked at how breaches of an individual's own privacy affect their dispositions and behavior (e.g., Awad & Krishnan, 2006; Bansal, Zahedi, & Gefen, 2007; 2010; 2016). Research also shows that privacy protections instituted by a company have implications for how much people trust that company (e.g., Metzger, 2006) and that privacy concerns and trust interact to affect disclosure of information (Joinson et al., 2010). This existing work tends to focus on the individual's own experience and on how actions by a particular company affect consumer trust in *that* company. Here we focus instead on how actions by *other* similar companies affect people's trust in a specific company. Rather than look at the effects of an individual's own experience, we focus on spillover effects that violations of *other* people's privacy by *other* companies may have on an individual's perceptions of a particular company.

We argue that media accounts of privacy violations by other, similar technology providers affect users' perceptions that a particular technology provider is untrustworthy and that it will violate their privacy. That is, we suggest that people use typical behaviors by other actors in a category as a source of information about what a particular actor in that category will do (Tirole, 1996). The implication is that if people have information that most providers of similar apps violate privacy, they will assume that a provider of a particular app is also likely to do so. Relatedly, they will have less trust in the company. Accordingly, we expect that:

H2a: The more frequently other providers of similar technologies engage in privacy violations; the more individuals will expect a particular technology provider to violate privacy.

H2b: The more frequently other providers of similar technologies engage in privacy violations; the less individuals will expect a particular technology provider to be trustworthy.

Normative expectations (of approval among other users), behavior expectations (of violations by other providers), and trustworthiness expectations (that a particular provider is trustworthy) in turn have implications for consumers' willingness to use a technology (from the particular provider). People who expect that others approve of privacy violations will be more willing to use a potentially privacy-violating technology because they will believe that doing so is socially acceptable; they are less likely to be blamed or feel shame if their privacy is violated (Bearden, Netemeyer, & Teel, 1989; Willer et al., 2009; see also Ajzen, 1991 on subjective norms; Chung & Rimal, 2016; Geber, Baumann, & Klimmt, 2017). In addition, people who expect that a company will violate their privacy will be less interested in using that company's technology (Waldman, 2018). Finally, people who perceive a company as more trustworthy will be more interested in using the company's products (Cialdini et al., 1990; Fehrler & Przepiorka, 2016; Przepiorka & Horne, 2018).

H3a: Expectations that others approve of privacy violations will increase people's willingness to use potentially privacy-violating technology.

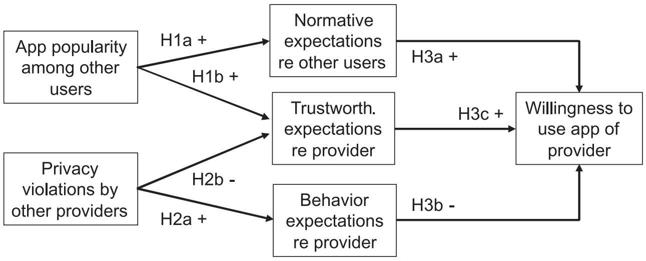
App popularity among other users
Privacy violations by other providers
H1a +
H1b +
H2b -
H2a +
Normative expectations re other users
Trustworth. expectations re provider
Behavior expectations re provider
H3a +
H3c +
H3b -
Willingness to use app of provider

Figure 1. Theoretical model. Normative expectations re other users = expectations about other users' approval of privacy violations by the specific provider; trustworth expectations re the provider = expectations about the trustworthiness of the specific provider; behavior expectations re provider = expectations about privacy violations by the specific provider.

H3b: Expectations that a specific provider will violate privacy will decrease people's willingness to use potentially privacy-violating technology from that provider.

H3c: Expectations that a specific provider is trustworthy will increase people's willingness to use potentially privacy-violating technology from that provider.

Figure 1 summarizes our theoretical argument.

Methods

We test our predictions using two online vignette experiments (Auspurg & Hinz, 2015). The vignettes described an app (i.e., technology) for household energy management. Many believe that the transition to the smart grid will require consumer engagement in monitoring and shifting their electricity use (Bakke, 2016; Frickel et al., 2017). Smart phone apps are a useful interface through which consumers can gain information about their energy use and utilities can engage customers in utility programs (Horne & Kennedy, 2017). But such interactions also create potential privacy threats for consumers (e.g., Quinn, 2009). Thus, understanding consumer willingness to use such technologies is a substantively important issue.

In addition, the energy app context is appropriate for testing our theory because the value of the app does not depend on how many other people are using it. A dating app, for example, is only valuable if many people use it (Shapiro & Varian, 1999). The popularity of a dating app will increase interest in using the app absent the mechanisms we describe here. Testing our theory requires a technology whose value is consistent regardless of number of users.

Participants

Our first study relies on a convenience sample recruited through Prolific – an online research hosting site similar to Amazon's Mechanical Turk, but designed for academic researchers (Peer, Brandimarte, Samat, & Acquisti, 2017). Participants go to the Prolific website and click on the study link. Once they complete the study, they are automatically directed back to the Prolific site for payment. In our study, half of the participants were male (50.6%). Mean age was 35.0 (S.D. = 11.9). Fifty-six per cent had a college degree.

Eighty-three per cent identified themselves as white. Fifty-nine percent identified themselves as liberal, 19.8% said they were conservative, and the rest indicated they were politically neutral (1 = very conservative; 7 = very liberal).

The second study was conducted with a nationally representative sample through YouGov. YouGov is a research company that maintains online panels of participants. It recruits participants, administers studies, and provides participants with coupons that can be redeemed for gift cards. Participants in the YouGov sample were mostly female (53.1%). Mean age was 46.4 (S.D. = 16.8). Thirty-nine per cent had completed at least two years of college education. Seventy-one per cent identified themselves as white. Twenty-eight per cent identified themselves as liberal and 30% said they were conservative (1 = very conservative; 5 = very liberal), with the rest indicating that they were moderate or not sure. The YouGov sample is older, less educated, and more conservative than the convenience sample. For the analyses with the YouGov data we used weights to achieve results that are nationally representative (reflecting makeup found in the 2012 American Community Survey).

Design and procedures

Both studies have a 2 × 2 between subject's factorial design crossing descriptive norms of household energy app use (popular vs unpopular) by frequency of privacy violations by other technology providers (frequent vs rare). The convenience sample included about 100 participants per condition for a total $N = 403$ participants. The representative sample included 300 participants per condition for a total $N = 1200$.[1]

Participants read the description of the app; each participant read only one version of the vignette. They then answered questions about their normative, behavioral, and trustworthiness expectations, as well as their willingness to use the app.

Experimental manipulations

We manipulated app popularity and frequency of privacy violations in a vignette. To manipulate app *popularity*, we described the app as either popular or unpopular and as being used by many or few other people. To operationalize privacy-violating behavior, we draw on existing research finding norms against analyzing and selling user information in the context of electricity consumption (Horne, Darras, Bean, Srivastava, & Frickel, 2015). We manipulate the *frequency* of such behavior (rare vs frequent) by stating that most or no other providers analyze and sell users' personal information. The text of the vignette reads:

> A company is providing a new app that helps people reduce their household energy consumption and thus save money and help the environment. It is possible that the app could be used by the provider to collect personal information about users.
>
> [*Most/No*] other providers of apps for reducing household energy consumption analyze users' personal information. [*Most/No*] other providers also sell the information they collect.
>
> This particular app is very [*popular/unpopular*]. [*Many/Few*] people are using it.

For a summary of the experimental conditions see Table 1.

Table 1. Experimental conditions.

	Rare	Frequent
Unpopular	No other providers … analyze … . No other providers … sell … . This particular app is very unpopular. Few people are using it	Most other providers … analyze … . Most other providers … sell … .. This particular app is very unpopular Few people are using it
Popular	No other providers … analyze … . No other providers … sell … . This particular app is very popular. Many people are using it	Most other providers … analyze … . Most other providers … sell … .. This particular app is very popular Many people are using it

Measures

After reading the vignette, participants answered questions about their *normative* expectations (how much they expected others to approve of privacy-violating behavior by the app provider: 1 = strongly disapprove; 10 = strongly approve), *behavior* expectations (their expectations regarding the likelihood that the particular company described in the vignette would engage in privacy violations: 1 = very unlikely; 10 = very likely), and their expectations regarding the *trustworthiness* of the company in the vignette (how

Table 2. Summary of procedures, manipulations and measures.

Step 1	Participants completed the consent form and were randomly assigned to an experimental condition.
Step 2	Manipulations: Participants read the vignette that manipulated ***popularity*** and ***frequency***.
Step 3	Measures: Participants answered questions about the vignette in the following order: (1) N***ormative*** expectations (intervening var) How much do you think most people would approve of the app provider analyzing and selling users' personal information to other companies? (2) B***ehavior*** expectations (intervening var) If you download the app, how likely is it that this app provider will analyze and sell your personal information? (3) T***rustworthiness*** expectations (intervening var) How trustworthy do you think the app provider is? (4) W***illingness*** to use the app (dependent var) How willing are you to download and use this app?
Step 4	Attention check: Participants answered a question about the purpose of the app What is the purpose of the app described in this study?
Step 5	Manipulation checks: Participants answered questions about: (1) ***app popularity*** How popular is the app described in this study? (2) ***frequency of privacy violations*** by other providers. Based on what you read, how common is it for household energy apps in general to analyze and sell information about people?
Step 6	Participants answered three Westin privacy attitude measures (used in the exploratory analyses in the online appendix)
Step 7	Participants answered sociodemographic measures for Prolific study only. YouGov provided sociodemographic characteristics of participants in the YouGov study.

trustworthy they thought the app provider was: 1 = not at all; 10 = very much). We also asked them how *willing* they were to use the app (1 = not at all; 10 = very).

At this point in the Prolific study, we asked about the sociodemographic characteristics described above. For the other study, YouGov provided data on sociodemographic characteristics; we also asked some questions to get at privacy attitudes (we use these measures in exploratory analyses reported in the online appendix).

Procedures, manipulations, and measures are summarized in Table 2.

Results

We first report the results from the convenience sample and thereafter the results from the nationally representative sample. For both studies, we report the results in terms of path models with unstandardized coefficient estimates (Figures 2 and 3). Moreover, both the unstandardized (*b*) and standardized coefficients (*β*) are mentioned in the text where appropriate alongside with corresponding standard errors (*SE*) and 95% confidence intervals (*CI*). Note that calculating standardized coefficients for categorical variables (e.g., binary treatment variables) is not meaningful. Coefficients and their standard errors are estimated by means of structural equation models (SEM) (Hayes & Preacher, 2014; Kline, 2010). The estimation of the standard errors is based on 5000 bootstrap replications in each case. For the Study 2 data, we use the *bsweights* command in Stata to account for the sample weights in the estimation process (Kolenikov, 2010). Tables with zero-order correlations, SEM estimation tables, as well as robustness checks with OLS regression models are reported in the online appendix. Our results do not change if OLS regression is used instead of SEM. Upon publication, the replication data for both studies are available at Harvard Dataverse.

Study 1: convenience sample

Table 3 reports participants' mean responses across experimental conditions.

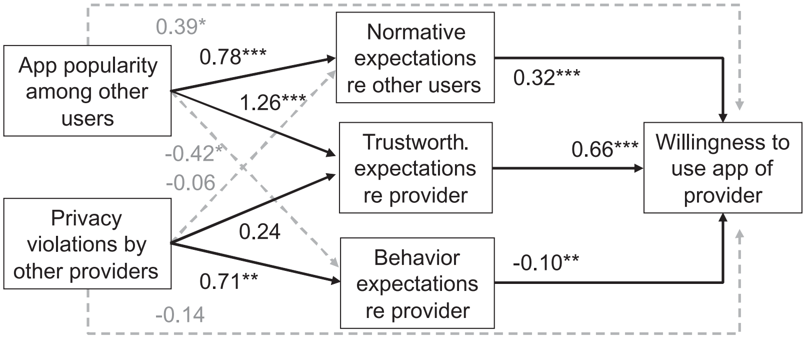
0.39*
App popularity among other users
0.78***
Normative expectations re other users
1.26***
0.32***
-0.42*
-0.06
Trustworth. expectations re provider
0.66***
Willingness to use app of provider
Privacy violations by other providers
0.24
0.71**
Behavior expectations re provider
-0.10**
-0.14

Figure 2. Path model of expectations and willingness (Study 1). Dashed, light-grey lines denote relations which are not part of our theoretical model (Figure 1). The results do not change if the SEM is fitted with coefficients pertaining to the theoretical model only. The figure shows unstandardized coefficients. The standardized coefficients are reported in the text where appropriate.

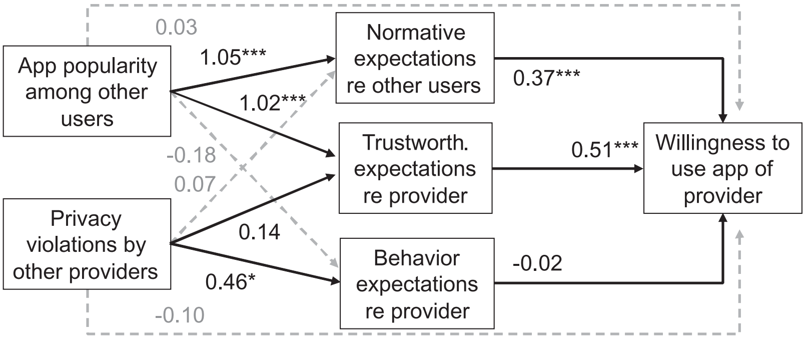
0.03
App popularity among other users
1.05***
1.02***
Normative expectations re other users
0.37***
-0.18
0.07
Trustworth. expectations re provider
0.51***
Willingness to use app of provider
Privacy violations by other providers
0.14
0.46*
Behavior expectations re provider
-0.02
-0.10

Figure 3. Path model of expectations and willingness (Study 2). Dashed, light-grey lines denote relations which are not part of our theoretical model (Figure 1). The results do not change if the SEM is fitted with coefficients pertaining to the theoretical model only. The figure shows unstandardized coefficients. The standardized coefficients are reported in the text where appropriate.

Figure 2 shows the unstandardized coefficient estimates of the structural equation model fitted to the Study 1 data. As predicted by Hypothesis 1a (see Figure 1), popularity has a statistically significant, positive effect on normative expectations ($b = 0.78$, $SE = 0.16$, 95% $CI = [0.46, 1.10]$).[2] As app popularity increased, people expected others to be more approving of privacy violations. Consistent with Hypothesis 1b, app popularity also has a statistically significant, positive effect on trustworthiness expectations – the more popular the app, the more participants trusted the app provider ($b = 1.26$, $SE = 0.19$, 95% $CI = [0.89, 1.63]$). These results support both Hypotheses 1a and 1b regarding the effects of app popularity. In contrast, although the results support Hypothesis 2a regarding the effect of violation frequency on behavior expectations, they are inconsistent with Hypothesis 2b that violation frequency will affect trust. Frequency of privacy violations has a statistically significant, positive effect on behavior expectations ($b = 0.71$, $SE = 0.21$, 95% $CI = [0.30, 1.12]$), but not on trustworthiness expectations ($b = 0.24$, $SE = 0.19$, 95% $CI = [-0.14, 0.61]$).

In line with our hypotheses, normative, behavioral, and trustworthiness expectations are all associated with willingness to use the app ($b = 0.32$, $SE = 0.06$, 95% $CI = [0.21, 0.43]$, $\beta = 0.26$; $b = -0.10$, $SE = 0.04$, 95% $CI = [-0.17, -0.03]$, $\beta = -0.10$; $b = 0.66$, $SE = 0.05$, 95% $CI = [0.55, 0.76]$, $\beta = 0.63$; respectively), with trustworthiness expectations having the strongest and behavior expectations the weakest association. These results support our Hypotheses 3a through 3c. However, the effect of app popularity is not completely mediated by expectations; a small but statistically significant direct effect of popularity on willingness to use the app remains ($b = 0.39$, $SE = 0.15$, 95% $CI = [0.09, 0.68]$). Results

Table 3. Mean and standard deviations of mediator and outcome variables across conditions (Study 1)

	Normative expectations		Behavior expectations		Trustworthiness expectations		Willingness to use app	
Exp. condition	*n*	*M (SD)*	*n*	*M (SD)*	*n*	*M (SD)*	*n*	*M (SD)*
Unpop. & rare	102	2.01 (1.76)	102	7.73 (2.36)	102	2.82 (1.88)	102	2.45 (2.03)
Popular & rare	99	2.80 (1.82)	99	7.58 (2.20)	99	4.15 (2.01)	99	3.88 (2.47)
Unpop. & freq.	101	1.97 (1.31)	101	8.66 (1.82)	100	3.13 (1.74)	101	2.32 (1.81)
Popular & freq.	101	2.73 (1.71)	101	8.01 (1.98)	101	4.32 (2.01)	101	3.88 (2.29)

Table 4. Mean and standard deviations of mediator and outcome variables across conditions (Study 2)

	Normative expectations		Behavior expectations		Trustworthiness expectations		Willingness to use app	
Exp. condition	*n*	*M (SD)*	*n*	*M (SD)*	*n*	*M (SD)*	*n*	*M (SD)*
Unpop. & rare	300	3.29 (2.87)	300	7.84 (2.55)	300	3.63 (2.55)	299	3.00 (2.65)
Popular & rare	300	4.35 (2.97)	300	7.55 (2.44)	300	4.62 (2.69)	300	3.83 (2.97)
Unpop. & freq.	300	3.29 (2.83)	300	8.19 (2.39)	300	3.68 (2.72)	300	2.94 (2.71)
Popular & freq.	299	4.46 (2.88)	300	7.68 (2.34)	300	4.63 (2.53)	300	3.84 (2.77)

do not change substantially if the data are analyzed by means of OLS regressions (see the online appendix).

Study 2: representative sample

The results for Study 2 are consistent with those of Study 1. Table 4 shows participants' mean responses across experimental conditions.

Figure 3 shows the unstandardized coefficient estimates of the structural equation model fitted to the Study 2 data. Consistent with Hypotheses 1a and 1b (Figure 1), app popularity has a statistically significant, positive effect on normative (approval) ($b = 1.05$, $SE = 0.23$, 95% $CI = [0.61, 1.50]$) and trustworthiness expectations ($b = 1.02$, $SE = 0.21$, 95% $CI = [0.62, 1.43]$). Consistent with Hypothesis 2a, frequency of privacy violations has a statistically significant positive effect on behavior (violation) expectations ($b = 0.46$, $SE = 0.20$, 95% $CI = [0.06, 0.86]$). But, again, results do not support the prediction in Hypothesis 2b that frequency of privacy violations affects trustworthiness expectations ($b = 0.14$, $SE = 0.21$, 95% $CI = [-0.27, 0.55]$).

And here too, trustworthiness expectations have the strongest association with willingness to use the app ($b = 0.51$, $SE = 0.04$, 95% $CI = [0.43, 0.58]$, $\beta = 0.56$), followed by normative expectations of approval ($b = 0.37$, $SE = 0.04$, 95% $CI = [0.29, 0.45]$, $\beta = 0.44$). The experimental conditions have no direct effect on willingness to use the app. These results support our Hypotheses 3a and 3c (about the associations between normative and trustworthiness expectations, and willingness). Unlike Study 1, Hypothesis 3b (about the association between behavior expectations and willingness) is not supported ($b = -0.02$, $SE = 0.03$, 95% $CI = [-0.08, 0.03]$, $\beta = -0.02$). These results do not change substantially if OLS regression is used to analyze the Study 2 data (see online appendix for details).

Summary of results

The results of the two studies are quite consistent and by and large support our theoretical argument. Our results show that descriptive norms affect normative (approval) and trustworthiness expectations, which, in turn, are associated with willingness to use a technology. The evidence for the association between behavior (violation) expectations and willingness is mixed. While the frequency of norm violations by other technology providers has an effect on behavior expectations in both our samples, the association between behavior expectations and willingness to use the app is only present in our convenience sample and is relatively small.

Discussion and conclusion

We find that the behaviors of technology users affect normative and trustworthiness expectations; behaviors of technology providers affect behavior expectations. When many people use a technology that could be used to violate privacy, individuals expect that others approve of privacy violations and have greater trust in the technology provider. When many other, similar providers violate privacy, people expect a particular provider to do so as well, but their trust in it is not affected. Normative (approval) expectations and trust in the provider, in turn are associated with people's willingness to use a technology.

Why is it that people place more weight on others' use of technology, and the inferences that they draw from others' behavior, than they do on evidence that many other companies violate users' privacy? First, information about app popularity, although indirect, provides people with information about the particular provider, whereas information about privacy violations by other companies, although direct, provides information about actors other than the actual provider. Information about a particular provider may be more salient than information about others. Second, research suggests that people do not have a good understanding of online privacy (Acquisti, Brandimarte, & Loewenstein, 2015). In the face of such uncertainty, other consumers' behaviors are a concrete source of information. If others use a technology, then that is good evidence that the downsides are not that big (Cialdini et al., 1990).

Our findings have implications for understanding the consequences of the increase in information and communications technologies. Our results suggest that the widespread use of a new technology affects privacy norms and trust. The more people use an ICT that could be used to violate privacy, the weaker privacy norms become. Even information about privacy violations by similar ICT providers seems to have little import in the face of evidence that others are using the technology. Thus, widespread use by peers is likely to increase an individual's use of ICT, even if they have privacy concerns.

A limitation of our study is that it does not measure behavior. Because we rely on vignette experiments, we can only get at individuals' intentions – their willingness to use a technology. Thus, it is possible that normative (approval) expectations, behavior (violation) expectations, and trust will have different associations with actual use. Future research should assess the association between privacy norms and privacy-related behavior.

Our study also relies on single-item measures, which may be less reliable than multi-item scales. Scales may do a better job of capturing multidimensional constructs and reduce measurement error (Price, 2017). In our case, although the construct of norms is multidimensional (entailing behavior, expectations and sanctioning), the particular variable we seek to measure (normative expectations about others' approval) is not; it is not even a construct but a measure of what a respondent thinks about a particular aspect of the scenario described in the vignette. This approach is consistent with measures used in other norms research (e.g., Horne, Dodoo, & Dodoo, 2018) and the approach recommended by noted norms scholars (e.g., Bicchieri, 2017). Single-item measures are also criticized for not being as sensitive as scales and therefore requiring larger sample sizes. Our measures used 10-point response scales, which provided sufficient variation given our sample size, (we performed a power analysis to determine the sample size we would need to detect the hypothesized effects) (see Methods section, endnote 1).

Finally, we focus on expectations regarding technology providers, not the technology itself. But people's expectations for a technology and for technological systems are also potentially important. Understanding trust in technology versus providers of a technology, as well as in technological systems, are areas for future research.

In sum, our study shows that the widespread adoption of ICT changes people's normative expectations about the social acceptability of privacy invasions and affects people's trust in technology providers. Thus, the roll-out of ICT may be affecting privacy norms and concerns without conscious attention to the issue. Technology providers should be aware that widespread use of such technologies may indicate a shift in privacy norms but does not necessarily mean that people personally accept privacy violations. As more and more systems rely on ICT, in order to be functional and effective, providers should take these privacy dynamics into account.

Notes

1. To determine the necessary size of the representative sample, we conducted a power analysis based on the results of the convenience sample study. We conducted a power analysis for a two-sample mean test based on the means and standard deviations in the respective treatment groups with no and with frequent occurrences of privacy violations among providers of similar apps (the factor that yielded the smaller treatment effect). Assuming a significance level of 5% for two-sided tests and a power of 80%, we obtain an estimated sample size of 151 participants per condition. However, this calculation was based on standard deviations estimated on the rather homogeneous online panel and hence likely too low. We therefore increased the standard deviations by one third to obtain an estimated sample size of 257 per condition. Finally, to be on the safe side, we rounded up the sample size to 300 participants per condition or 1200 participants in total.
2. Before conducting the studies reported here, we collected pilot data in which we used different vignette wording. The pilot data show that if people have reason to think that the technology provider is already violating users' privacy, then popularity of the app does not affect normative expectations. That is, popularity matters when people know it is *possible* for the technology provider to violate privacy, not when there is evidence that the provider has already done so.

Disclosure statement

No potential conflict of interest was reported by the authors.

Notes on contributors

Christine Horne is professor of sociology at Washington State University. She studies the emergence, enforcement, and application of social norms. Her work has been published in the American Sociological Review, Annual Review of Sociology, Social Psychology Quarterly, and Energy Policy.

Wojtek Przepiorka is assistant professor of sociology at Utrecht University. His research interests are analytical and economic sociology, game theory, organizational behavior and quantitative methodology. His work has been published in the American Journal of Political Science, American Sociological Review, and Social Forces.

Funding

This work was supported by National Science Foundation grant numbers 1441357, 1555980.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514.

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442–492.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, *50*(2), 179–211.

Altman, I. (1977). Privacy regulation: Culturally universal or culturally specific? *Journal of Social Issues*, *33*(3), 66–84.

Anthony, D., Campos-Castillo, C., & Horne, C. (2017). Toward a sociology of privacy. *Annual Review of Sociology*, *43*, 249–269.

Associated Press. (2019). 5-Stars online platform fined for privacy violations. *Washington Post*. April 5, 2019. Retrieved from https://www.washingtonpost.com/world/europe/5-stars-online-platform-fined-for-privacy-violations/2019/04/05/c04fae8a-57b5-11e9-aa83-504f086bf5d6_story.html?utm_term=.65a867511f25

Auspurg, K., & Hinz, T. (2015). *Factorial survey experiments*. Thousand Oaks, CA: Sage.

Awad, N. F., & Krishnan, M. S. (2006). The personalization privacy paradox: An empirical evaluation of information transparency and the willingness to be profiled online for personalization. *MIS Quarterly*, *30*(1), 13–28.

Bakke, G. (2016). *The grid: The fraying wires between Americans and our energy future*. NY: Bloomsbury.

Balta-Ozkan, N., Boteler, B., & Amerighi, O. (2014). European smart home market development: Public vies on technical and economic aspects across the United Kingdom, Germany, and Italy. *Energy Research and Social Science*, *3*, 65–77.

Bansal, G., Zahedi, F., & Gefen, D. (2007). The impact of personal dispositions on privacy and trust in disclosing health information online. AMCIS 2007 Proceedings. Paper 57.

Bansal, G., Zahedi, F., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern, and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138–150.

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? Trust and privacy concerns in disclosing private information online. *Information and Management*, *53*(1), 1–21.

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53.

Bearden, W. O., Netemeyer, R. G., & Teel, J. E. (1989). Measurement of consumer susceptibility to interpersonal influence. *Journal of Consumer Research*, *15*(4), 473–481.

Bicchieri, C. (2017). *Norms in the wild: How to diagnose, measure, and change social norms*. Oxford: Oxford University Press.

Bode, K. (2018). Your smart electricity meter can easily spy on you, court ruling warns. Motherboard. April 24, 2018. Retrieved from https://motherboard.vice.com/en_us/article/j5n3pb/your-smart-electricity-meter-can-easily-spy-on-you-court-ruling-warns

Brayne, S. (2014). Surveillance and system avoidance: Criminal justice contact and institutional attachment. *American Sociological Review*, *79*(3), 367–391.

Cheshire, C. (2011). Online trust, trustworthiness, or assurance? *Daedalus*, *140*(4), 49–58.

Chung, A., & Rimal, R. N. (2016). Social norms: A review. *Review of Communications Research*, *4*, 1–29.

Cialdini, R. B. (2007). Descriptive social norms as underappreciated sources of social control. *Psychometrika*, *72*(2), 263–268.

Cialdini, R. B., Reno, R. R., & Kallgren, C. A. (1990). A focus theory of normative conduct: Recycling the concept of norms to reduce littering in public places. *Journal of Personality and Social Psychology*, *58*(6), 1015–1026.

Cialdini, R. B., & Trost, M. R. (1998). Social influence: Social norms, conformity and compliance. In D. T. Gilbert, S. T. Fiske, & G. Lindzey (Eds.), *The handbook of social psychology* (pp. 151–192). New York, NY: McGraw-Hill.

Coleman, J. S. (1990). *Foundations of social theory*. Cambridge, MA: Belknap Press.

Craglia, M., & Shanley, L. (2015). Data democracy – increased supply of geospatial information and expanded participatory processes in the production of data. *International Journal of Digital Earth*, *8*(9), 679–693.

Dellarocas, C. (2003). The digitization of word of mouth: Promise and challenges of online feedback mechanisms. *Management Science*, *49*(10), 1407–1424.

Diekmann, A., Przepiorka, W., & Rauhut, H. (2015). Lifting the veil of ignorance: An experiment on the contagiousness of norm violations. *Rationality and Society*, *27*(3), 309–333.

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

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.

Earl, J. (2012). Private protest? Public and private engagement online. *Information, Communication, and Society*, *21*(3), 591–608.

Fehr, E. (2009). On the economics and biology of trust. *Journal of the European Economic Association*, *7*(2–3), 235–266.

Fehr, E., & Schurtenberger, I. (2018). Normative foundations of human cooperation. *Nature Human Behaviour*, *2*, 458–468.

Fehrler, S., & Przepiorka, W. (2016). Choosing a partner for social exchange: Charitable giving as a signal of trustworthiness. *Journal of Economic Behavior and Organization*, *129*, 157–171.

Feri, F., Giannetti, C., & Jentzsch, N. (2016). Disclosure of personal information under risk of privacy shocks. *Journal of Economic Behavior and Organization*, *123*, 138–148.

Frickel, S., Wühr, D., Horne, C., & Kallman, M. E. (2017). Field of visions: Interorganizational challenges to the smart energy transition in Washington state. *Brooklyn Law Review*, *82*(2), 693–724.

Gambetta, D. (1988). Can we trust trust? In D. Gambetta (Ed.), *Trust: Making and breaking cooperative relations* (pp. 213–237). Oxford: Basil Blackwell.

Geber, S., Baumann, E., & Klimmt, C. (2017). Where do norms come from? Peer communication as a factor in normative social influence on risk behavior. *Communication Research*. doi:10.1177/0093650217718656

Hayes, A. F., & Preacher, K. J. (2014). Statistical mediation analysis with a multicategorical independent variable. *British Journal of Mathematical and Statistical Psychology*, *67*(3), 451–470.

Hechter, M., & Opp, K.-D. (Eds.). (2001). *Social norms*. New York: Russell Sage Foundation.

Heirman, W., Walrave, M., & Ponnet, K. (2013). Predicting adolescents' disclosure of personal information in exchange for commercial incentives: An application of an extended theory of planned behavior. *Cyberpsychology, Behavior, and Social Networking*, *16*(2), 81–87.

Hofstra, B., Corten, R., & van Tubergen, F. (2016). Understanding the privacy behavior of adolescents on Facebook: The role of peers, popularity and trust. *Computers in Human Behavior*, *60*, 611–621.

Horne, C., Darras, B., Bean, E., Srivastava, A., & Frickel, S. (2015). Privacy, technology, and norms: The case of smart Meters. *Social Science Research*, *51*, 64–76.

Horne, C., Dodoo, N. D., & Dodoo, F. N.-A. (2018). The conditionality of norms: The case of bridewealth. *Social Psychology Quarterly*, *81*(4), 319–339.

Horne, C., & Kennedy, E. H. (2017). The power of social norms for reducing and shifting energy use. *Energy Policy*, *107*, 43–52.

Horne, C., Tinkler, J., & Przepiorka, W. (2018). Behavioral regularities and norm stickiness: The cases of transracial adoption and online privacy. *Social Research: An International*, *85*(1), 93–113.

Joinson, A. N., Reips, U.-D., Buchanan, T., & Schofield, C. B. P. (2010). Privacy, trust, and self-disclosure online. *Human-Computer Interaction*, *25*(1), 1–24.

Kelly, M. (2019). Facebook could reportedly face multibillion-dollar FTC fine over privacy violations. *The Verge*, Feb 14, 2019. Retrieved from https://www.theverge.com/2019/2/14/18225440/facebook-multibillion-dollar-ftc-fine-privacy-violations

Kiger, P. J. (2016). Why some people are refusing 'smart' utility meters in their homes. How stuff works. Sept 27, 2016. Retrieved from https://electronics.howstuffworks.com/gadgets/home/utility-smart-meters-privacy-violation-conspiracy.htm

Kline, R. B. (2010). *Principles and practice of structural equation modeling*. New York, NY: Guilford Press.

Kolenikov, S. (2010). Resampling variance estimation for complex survey data. *The Stata Journal: Promoting Communications on Statistics and Stata*, *10*(2), 165–199.

Krause, A., & Horvitz, E. (2010). A utility-theoretic approach to privacy in online services. *Journal of Artificial Intelligence Research*, *39*, 633–662.

Levi, M., & Stoker, L. (2000). Political trust and trustworthiness. *Annual Review of Political Science*, *3*, 475–507.

Mackie, G. (1996). Ending footbinding and infibulation: A convention account. *American Sociological Review*, *61*, 999–1017.

Marsan, C. D. (2012, January 26). 15 worst Internet privacy scandals of all time. *NetworkWorld*. Retrieved from https://www.networkworld.com/article/2185187/security/15-worst-internet-privacy-scandals-of-all-time.html

Metzger, M. J. (2006). Effects of site, vendor, and consumer characteristics on web site trust and disclosure. *Communication Research*, *33*(3), 155–179.

Mollborn, S. (2017). *Mixed messages: Norms and social control around teen sex and pregnancy*. NY: Oxford University Press.

Moore Jr., B. (1984). *Privacy: Studies in social and cultural history*. Armonk, NY: M.E. Sharpe.

Murphy, R. R. (1964). Social distance and the veil. *American Anthropologist*, *66*, 1257–1274.

Nissenbaum, H. (2010). *Privacy in context: Technology, privacy, and the integrity of social life*. Stanford, CA: Stanford Law Books.

Norberg, P. A., Horne, D. R., & Horne, D. A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs*, *41*(1), 100–126.

Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psycholog,y*, *70*, 153–163.

Petronio, S. (1991). Communication boundary management: A theoretical model of managing disclosure of private information between married couples. *Communication Theory*, *1*(4), 311–335.

Posner, E. A. (2000). *Law and social norms*. Cambridge, MA: Harvard University Press.

Price, L. R. (2017). *Psychometric methods: Theory into practice*. New York: Gilford Press.

Przepiorka, W., & Horne, C. (2018). How can consumer trust in energy utilities be increased? The effectiveness of prosocial, pro-environmental, and service-oriented investments as signals of trustworthiness. *Organization and Environment*. Advance online publication. doi:10.1177/1086026618803729

Quinn, E. L. (2009). *Privacy and the new energy infrastructure*. Retrieved from https://ssrn.com/abstract=1370731

Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2005). The mechanics of trust: A framework for research and design. *International Journal of Human-Computer Studies*, *62*(3), 381–422.

Rimal, R. N., & Lapinski, M. K. (2015). A re-explication of social norms, ten years later. *Communication Theory*, *25*, 393–409.

Rimal, R. N., Limaye, R. L., Roberts, P., Brown, J., & Mkandawire, G. (2013). The role of interpersonal discussion in reducing structural disparities and psychosocial deficiencies. Experience from the Malawi BRIDGE project. *Journal of Communication*, *63*, 51–71.

Rogers, E. M. (1962). *Diffusion of innovation*. NY: Free Press.

Shaban, H. (2018). Amazon Alexa user receives 1700 audio recordings of a stranger through 'human error.' *The Washington Post*. Dec 20, 2018. Retrieved from https://www.washingtonpost.com/technology/2018/12/20/amazon-alexa-user-receives-audio-recordings-stranger-through-human-error/?utm_term=.98d420cbcefa

Shapiro, C., & Varian, H. R. (1999). *Information rules: A strategic guide to the network economy*. Boston, MA: Harvard Business School Press.

Shils, E. A. (1966). Privacy: Its constitution and vicissitudes. *Law and Contemporary Problems*, *31* (2), 281–306.

Tirole, J. (1996). A theory of collective reputations (with applications to the persistence of corruption and to firm quality). *Review of Economic Studies*, *63*(1), 1–22.

US Department of Homeland Security. (n.d.). Critical infrastructure sectors. Retrieved from https://www.dhs.gov/critical-infrastructure-sectors

Vaidhyanathan, S. (2018). Violating our privacy is in Facebook's DNA. The Guardian Dec 20, 2018. Retrieved from https://www.theguardian.com/commentisfree/2018/dec/20/facebook-violating-privacy-mark-zuckerberg

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.

Waldman, A. E. (2018). *Privacy as trust: Information privacy for an information age*. Cambridge, MA: Cambridge University Press.

Westin, A. F. (1970). *Privacy and freedom*. New York, NY: Atheneum.

Willer, R., Kuwabara, K., & Macy, M. W. (2009). The false enforcement of unpopular norms. *American Journal of Sociology*, *115*(2), 451–490.

Xenitidou, M., & Edmonds, B. (2014). The conundrum of social norms. In M. Xenitidou & B. Edmonds (Eds.), *The complexity of social norms* (pp. 1–8). New York, NY: Springer.

Younts, C. W. (2008). Status, endorsement, and the legitimacy of deviance. *Social Forces*, *87*(1), 561–590.

Zelditch Jr., M. (2001). Processes of legitimation: Recent developments and new directions. *Social Psychology Quarterly*, *64*(1), 4–17.