J Bus Ethics
DOI 10.1007/s10551-017-3553-z

ORIGINAL PAPER

Perceived Privacy Violation: Exploring the Malleability of Privacy Expectations

Scott A. Wright[1] · **Guang-Xin Xie**[2]

Received: 9 September 2016 / Accepted: 21 April 2017

Abstract Recent scholarship in business ethics has revealed the importance of privacy expectations as they relate to implicit privacy norms and the business practices that may violate these expectations. Yet, it is unclear how and when businesses may violate these expectations, factors that form or influence privacy expectations, or whether or not expectations have in fact been violated by company actions. This article reports the findings of three studies exploring how and when the corporate dissemination of consumer data violates privacy expectations. The results indicate that consumer sentiment is more negative following intentional releases of sensitive consumer data, but the effect of data dissemination is more complex than that of company intentionality and data sensitivity alone. Companies can effectively set, and re-affirm, privacy expectations via consent procedures preceding and succeeding data dissemination notifications. Although implied consent has become more widely used in practice, we show how explicit consent outperforms implied consent in these regards. Importantly, this research provides process evidence that identifies perceived violation of privacy expectations as the underlying mechanism to explain the deleterious effects, on consumer sentiment, when company actions are misaligned with consumers' privacy expectations. Ethical implications for companies collecting and disseminating consumer information are offered.

Keywords Consumer privacy · Data dissemination · Explicit consent · Intentionality · Personal data · Implied consent · Privacy infringement · Sensitive information · Social contract theory

Introduction

Companies collect and disseminate a massive volume of individual-level data, and public attention to this process has been steadily increasing in the mainstream media (Kroft 2014). In response, individuals, agencies, and policy-makers have become progressively more concerned about how their personal information is collected, stored, and exchanged (Acquisti et al. 2015; Phelps et al. 2000; Walker 2016). For example, the Federal Trade Commission (FTC) has requested enhanced legislation and transparency regarding the dissemination of consumer data (FTC 2014). Much of this information is intentionally purchased and sold in the burgeoning data brokerage and analytics industries, which is a common practice between and among companies. For example, Acxiom, one of the largest personal data brokers with over $1 billion in annual revenue, has an average of 1500 pieces of information on over 200 million Americans (Kroft 2014).

Companies intentionally disseminate consumer data with other entities for a variety of purposes beyond marketing (e.g., to facilitate financial transactions, enhance fraud protection, respond to service complaints, and comply with legal requirements). As an example, according to

Electronic supplementary material The online version of this article (doi:10.1007/s10551-017-3553-z) contains supplementary material, which is available to authorized users.

✉ Scott A. Wright
s.wright@providence.edu

Guang-Xin Xie
vincent.xie@umb.edu

[1] Department of Marketing, Ryan Center for Business Studies, Providence College, Providence, RI 02908, USA

[2] Department of Marketing, College of Management, University of Massachusetts, Boston, MA 02125-3393, USA

Published online: 06 May 2017

Google's online privacy policy, the company intentionally shares a wide array of consumer data with companies, organizations, and individuals outside of Google (2016). Although users may consent to such policies, according to a recent Pew Research Report (Madden 2014), 91% of adults agree that consumers have lost control over how their personal information is collected and used by companies. From the consumers' perspective, corporate dissemination of consumer data often goes unnoticed and without incident (Dommeyer and Gross 2003), but this practice—i.e., the dissemination of consumer information by companies to a third party (hereafter referred to as "data dissemination")—is common and occurs for a variety of different reasons. For example, many instances of data dissemination can be characterized as unintentional "security breaches." In 2013, Adobe announced that hackers had stolen nearly 3 million encrypted customer credit card records, as well as login data for an undetermined number of Adobe user accounts (Finkle 2013). Similarly, a significant proportion of data dissemination incidences are unintentional. For example, Facebook accidentally released the email addresses and phone numbers of an estimated 6 million users who had set their personal accounts to "private" (Facebook 2013). Importantly, these incidences have been increasing at an astonishing rate with over 3.8 billion consumer records having been released from January 2014 to January 2017 by companies spanning nearly all industries (e.g., media, health care, transportation, military, retail, and financial services; Quick et al. 2017).

Despite its prevalence and consequential nature, there is no empirical research documenting *how* data dissemination affects consumer sentiment toward releasing companies in terms of attitudes, trust perceptions, and other evaluative judgments. In particular, the practice of data dissemination varies across companies and industries. Yet, what remains uncertain is how consumers react to data dissemination, and the ethical implications regarding this topic. Moreover, the relevant literatures make no distinctions according to the type of data or the manner in which the data are shared. Perhaps the prevailing assumption may be that all data dissemination incidences provoke negative reactions. This would be consistent with previous research demonstrating a negative market effect following security breach announcements (Campbell et al. 2003; Kannan et al. 2007). However, many data dissemination incidences do not constitute security breaches, and some may actually benefit consumers. For example, according to Target's privacy policy, the company collects Flash cookies for fraud prevention purposes and reserves the right to intentionally share this information with fraud prevention agencies (Target 2016). Similarly, Disney acknowledges that the company intentionally shares consumer data to other companies so that they can, "send you offers and promotions about their products and services" (Disney 2015). Thus, still missing from prior research is an understanding of how various data dissemination incidences affect company perceptions, a theoretical explanation for variations in perception, and an understanding of the boundary conditions that influence these perceptions.

In what follows, we present three studies that empirically investigate the effect of data dissemination on consumer perceptions toward companies. In doing so, we make important contributions to the privacy literature. Foremost, the current research extends and empirically substantiates a contractual, norms-based view of privacy (Martin 2012, 2015, 2016). We contribute to this work by empirically demonstrating when company practices—in this case data dissemination—violate privacy expectations. Moreover, we explore how companies can effectively set and reaffirm privacy expectations through consent procedures.

Companies currently implement a number of practices to notify the public of their privacy practices and to establish privacy expectations. Consistent with social contract theory, these practices typically adhere to contextually dependent micro-norms while respecting societal principles (i.e., hypernorms) such as fidelity, security, voice, consent, notice, and exit (Donaldson and Dunfee 1994; Martin 2012). For instance, many companies enact opt-in/opt-out procedures when implementing email-marketing campaigns to satisfy societal principles of exit and to comply with legal requirements specified in the CAN-SPAM Act. More specifically, the act prohibits businesses from selling or transferring users' email addresses once they opt out, even in the form of a mailing list (FTC 2009). Similarly, companies frequently implement consent procedures. Despite these efforts, previous research consistently shows that, in response to current consent procedures, consumers frequently ignore or misunderstand these privacy policies (Milne and Culnan 2004; Milne et al. 2006). Yet companies frequently have consumers either explicitly agree to their privacy policies (i.e., "explicit consent") or indirectly grant consent (i.e., "implied consent") by interacting with the company, or its subsidiaries, in a way that facilitates the collection of personal data. Explicit consent is a conscious act of permission whereby individuals explicitly "agree" to the specific terms of a given contract, policy, or agreement (Janssen and Gevers 2005). For example, in order to apply for a credit card at the Bank of America, a consumer must check a box on the bank's webpage, indicating that "by submitting this application, you: (1) acknowledge that you have reviewed the credit card Terms and Conditions; and (2) agree to submit your application for this credit card subject to those Terms and Conditions" (see Web Appendix W1). Hence, the act of checking the box is an explicit act of consent to the terms and conditions. From a company's standpoint,

consent denotes agreement, but does not assure an understanding or commitment to privacy terms or conditions. Thus, consent alone does not ensure an alignment between consumers' privacy expectations and company practices.

Given the procedural difficulties often inherent in obtaining explicit consent, many companies have adopted *implied* consent techniques. Contrary to explicit consent, implied consent is passively obtained without an explicit act of "agreement" (Johnson and Goldstein 2003), which, to our knowledge, has not yet been studied in the privacy literature. In essence, "implied consent" occurs when individuals take an action (e.g., accessing a Web site, downloading an app, or purchasing a product) that presupposes consent to specific privacy practices, policies, or other agreements, but without formally providing verbal or written permission (Veatch 2007, p. 40). For example, when accessing the CNN Web site (CNN.com), a banner provides notice of implied consent, "…by using this site, you agree to the Privacy Policy and Terms of Service." Similarly, when consumers create a new user account on Redfin.com, the company assumes consent with the following, "by joining you agree to our Terms of Use and Privacy Policy" (Redfin.com). Thus, both forms of consent require a form of action. For explicit consent, the action is a conscious act of permission to the privacy policy, agreement, or business practice, whereas, for implied consent the action is ancillary and an indirect form of agreement.

In the current research, we illustrate the importance of aligning privacy expectations with company actions to avoid perceived privacy infringements and the malleability of expectations. To substantiate our alignment account (see Fig. 1), we explore the important role of consent type (i.e., explicit vs. implied) in matching privacy expectations with company actions. Consistent with a contractual expectation account of privacy (Martin 2012, 2015, 2016), we find that consent type proves vital in determining consumers' perceptions of privacy violation and their reactions following notifications of data dissemination. Contrary to *implied consent*, when explicit consent is salient, privacy expectations are made clear and unambiguous, thus properly aligning expectations with company actions. The role of consent type suggests important theoretical links between privacy expectations, company actions, and perceptions of privacy violation—thus substantiating and extending this theoretical account within the context of data dissemination.

In sum, we offer a substantive shift in theorizing regarding the influence of data dissemination on company perceptions and the process underlying its influence from the consumer's standpoint. Importantly, the current research challenges the notion that consumer reactions, following an incident of data dissemination, are universally negative without examining the contexts of data dissemination incidences, thus increasing the importance that companies, policy-makers, and researchers should apportion to privacy norms, their associated expectations, and business actions that may violate these norms. Although widely used in practice, we also provide evidence that implied consent may not sufficiently establish consumers' privacy expectations, thus leaving companies vulnerable to the negative effect of misaligned privacy expectations and business practices.

Thus, this research offers several important implications. Foremost, as per our findings, companies should reconsider the extensive use of implied consent techniques. Although ease of use and high compliance rates may make implied consent particularly alluring, our findings demonstrate a significant deficiency in setting privacy expectations. Second, this research underscores the importance of continually monitoring, and re-affirming, consumers' privacy expectations and taking corrective actions to attenuate any incongruity between consumer expectations and company actions. Such monitoring should be undertaken by industry regulators, policy-makers, government agencies, and individual companies. Doing so could precipitate drastic improvements narrowing the imbalance between privacy expectations and the actions that may violate these expectations. Lastly, this research highlights the attention companies should apportion to the types of data they collect and the mechanisms by which these data are disseminated. For example, much care should be given to the collection and handling of sensitive consumer data as consumers may react with condemnation should they become aware that such data had been intentionally disseminated.

Theoretical Background

The privacy literature suggests that people, in general, are motivated to control the disclosure of their personal information (Altman 1975). Some information is deemed inherently personal, and people want the information inaccessible to most, if not all, others (Nowak and Phelps 1997). In other words, privacy is considered one's natural "right to be left alone" (Peslak 2005, p. 329). Meanwhile, people are also motivated to disclose some personal information as an act of establishing individual identities or fostering social bonds, and they will willingly share sensitive personal information with others, even when the recipients are unknown (Acquisti et al. 2015; Mothersbaugh et al. 2011). In short, the predominant view is that privacy violations are determined by the individual's perceived control over "when, how, and to what extent information about them is communicated to others" (Pollach 2005, p. 222).

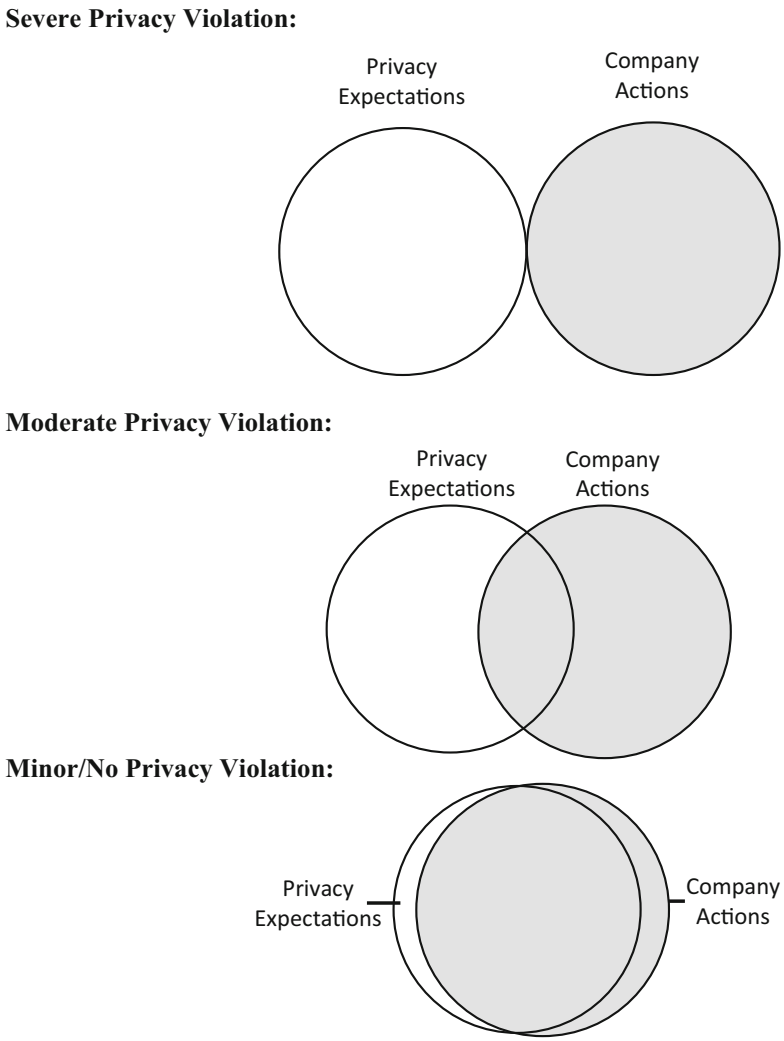


Fig. 1 Degree of perceived privacy violation as a function of the alignment between privacy expectations and company actions

A growing body of theoretical scholarship has recently proposed that the privacy expectations surrounding consumer privacy are often dictated by contextually dependent norms (Martin 2012, 2015, 2016). This approach highlights the importance of a "negotiated agreement" between consumers and companies (Martin 2016). That is, consumers do not universally expect their personal information to be inaccessible or under complete control for the sake of facilitating marketplace exchanges. Instead, when consumers exchange their personal information with companies, they form expectations regarding the management of their data that adhere to privacy norms.

Building upon prior theorizing, we predict that data dissemination incidences may violate these privacy expectations. In essence, Martin (2012) argues that privacy violations depend upon "negotiated information norms" within a particular community or situation (p. 520). We agree that these contractual expectations are often contextual in nature and can in fact be influenced by company actions (Nissenbaum 2004). For example, Nissenbaum (2004) argues that the appropriateness of how consumer information is gathered, stored, and disseminated depends on the particular consumer, the nature of the information itself, and the relationship between the consumer and the company. Thus, the manner by which the company shares the data could prove important and result in a misalignment between privacy expectations and company actions. In particular, data dissemination could be intentional or unintentional. That is, intentional data dissemination is arranged by the company and premeditated, whereas unintentional data dissemination lacks forethought and design.

The effect of intentionality is intriguing and non-obvious. There is anecdotal evidence that unintentional data dissemination may be perceived more negatively than intentional data dissemination. Unintentional data dissemination may signal haphazardness, disregard, or outright incompetence. For example, in 2005 Ameritrade Inc. informed 200,000 current and former customers that a computer backup tape containing their personal

information had been "lost" (Fredrix 2005). Similarly, unintentional data dissemination could indicate shortcomings in data security. According to California Data Breach report 2012–2015 (Harris 2016), about 17% of data breaches are caused by errors, predominantly mis-delivered emails and in-advertent exposure on the Internet.

Yet, there is also evidence suggesting the opposite effect—i.e., more negative reactions following intentional, rather than unintentional, data dissemination. For example, the moral psychology literature shows that individuals tend to rate intended harms as less moral than equivalent unintended harms (Pizarro et al. 2003). Specifically, compared to an accidental act, individuals assign more blame when the act is intentional. Research in the business domain has demonstrated a similar connection between intentionality and company perceptions (Newman et al. 2014). For instance, when a company communicated their actions to engage in a fair trade agreement (i.e., a beneficial act), consumers rated the company more favorably when the action was intentional rather than unintentional, and were more interested in purchasing the company's products (Newman et al. 2014). This finding is consistent with research showing that knowledge about intentions affects people's beliefs about the extent to which they are responsible for a particular outcome (Lombrozo 2010). Following this line of logic, individuals may be more likely to hold the company accountable when the companies' actions to disseminate personal information are intentional.

The effect of intentionality may further depend on the type of data. It is well established that beliefs and behavioral responses to privacy threats depend on the sensitivity level of disseminated information (Milne and Gordon 1993; Phelps et al. 2000; Sheehan and Hoy 2000). Consumers generally consider financial and medical data to be most sensitive, and at the aggregate level, purchasing/behavioral data as less sensitive (Sheehan and Hoy 2000; Phelps et al. 2000). Much of this is gathered via digital devices that generate a great deal of highly personalized data (Walker 2016). Sensitive data are particularly influential in terms of consumer judgment and company perceptions because such data, if exploited, could result in personal or financial harm (Ohm 2015). Prior research shows that data security breaches involving sensitive information result in negative effects on companies' market value, whereas breaches involving non-confidential information have no such effect (Campbell et al. 2003). Thus, based on the prior literature, we predict an interactive effect between company intentionality and data sensitivity. More specifically, we make the following prediction:

H1 Intentional (vs. unintentional) data dissemination will elicit more (vs. less) negative consumer attitudes toward the company. The effect of perceived intentionality will be stronger (vs. weaker) when the data are more (vs. less) sensitive.

Consistent with our theoretical account, we propose that the predictions described in H_1 will be driven by the perceived violation of contractual privacy expectations. That is, we anticipate that intentionally disseminating sensitive consumer data will result in a substantial misalignment between privacy expectations and company actions, which will evoke negative consumer perceptions of the company. Moreover, we anticipate that this effect will be explained by a perceived violation of consumers' privacy expectations:

H2 Perceived violation of contractual privacy expectations will mediate the negative effect of an intentional dissemination of sensitive data on consumer attitudes toward the company.

Using Consent to Align Privacy Expectations

Data dissemination, intentional or not, has become a serious public concern. In response, companies have made efforts to communicate their data policies to consumers and to obtain consumer consent allowing data dissemination. For example, many companies ask consumers to read or agree to various privacy or data security policies (e.g., click 'agree' on a "privacy policy" webpage). These actions adhere to models of notice and choice, also known as "awareness" and "control" (Milne 2000), which emphasize the use of privacy policies to notify consumers of firm practices (Cranor 2012; Milne and Culnan 2004). However, consumers and companies have different expectations with regard to protection of consumer information (Milne and Bahl 2010). For example, Martin (2016) found that consumers tend to expect more stringent online security protection than the companies' privacy policies actually promise. In other words, consumers assume that companies have an obligation to keep their data safe and secure to a greater extent than the companies often deliver.

To communicate privacy expectations effectively, among other reasons (e.g., legal requirements), companies often have consumers consent to their privacy policies. As previously noted, these often come in two forms—explicit or implied consent. Explicit consent is a conscious act of permission whereby individuals directly "agree" to the specific terms, whereas implied consent is passively obtained without an explicit act of "agreement" (Johnson and Goldstein 2003). In this context, one could classify implied consent as a default option. Consistent with this conceptualization, Huh et al. (2014, p. 748) define the implied (or default) option as "the choice option that consumers consider first and adopt as the status quo before considering other choice options." Although consumers are often unaware of their influence

(Smith et al. 2013), implied (or default) options have been shown to have dramatic effects on consumer behavior (Johnson et al. 2002; Johnson and Goldstein 2003). Across a wide variety of contexts, consumers disproportionately select defaults unless they are certain about their preferences or engage in effortful deliberation (Huh et al. 2014). Although implied consent may be particularly effective in obtaining consumer consent, consumers are often unlikely to expend significant effort attending to and deliberating the terms set by the privacy policy (Johnson and Goldstein 2003). This could have serious implications on aligning privacy expectations with company actions. More specifically, consumers may react more negatively given shallow processing of the terms and incompatible privacy expectations.

We predict that implementing an explicit consent could be particularly effective especially when its terms are made salient. Information is deemed "salient" when it is presented in a prominent manner, thus drawing attention and subsequent processing (Tom et al. 1987). According to commitment and signaling theory (Baca-Motes et al. 2013), increasing the saliency of a commitment has a substantial effect on subsequent behavior. Similarly, according to existing privacy research (Tom et al. 1987), individuals are more likely to purchase from companies when privacy information is made salient compared to when this information is not salient. To this end, repeating an explicit consent agreement following notification of data dissemination is likely to make the terms salient, to reinforce privacy expectations, and to serve as a reminder of the consumer's agreement condoning the action. Conversely, in the case of implied consent, increasing information saliency, through repetition, is less likely to influence consumer reactions because the default option is not determined by the consumer and no additional action was required for consent. Based on this line of reasoning, we propose the following:

H3a For explicit consent, consumer attitudes toward a company will be less (vs. more) negative if consent is made salient (vs. not salient) following an intentional dissemination of sensitive data.

H3b For implied consent, consumer attitudes toward the company are less likely to be influenced by consent saliency.

Empirical Studies

Building upon a privacy norms perspective (Martin 2012, 2015, 2016), this research carries out three studies to examine consumer attitudinal reactions to data dissemination. In particular, we empirically substantiate and extend this theoretical account. Consistent with prior research in this area (Martin 2012, 2016), we use a series of vignettes to test our hypotheses. Specifically, our Study 1 objective is to demonstrate the malleability of privacy expectations and the contextual nature of privacy violations. Thus, Study 1 documents how perceptions vary according to intentionality and data sensitivity. Study 2 provides process evidence supporting our alignment account and identifies perceived expectancy violations as the underlying process. Important to our theoretical model, in Study 3 we explore the theoretical importance of aligning privacy expectations and factors that alter, and re-affirm, expectations. We find that the type of consent (explicit vs. implied) and consent saliency interact to influence expectations and subsequent perceptions. Please see Fig. 2 for a conceptual model summarizing our proposed hypotheses.

Study 1: How Context Determines Perceived Privacy Violations

Consistent with a contextual-based account of privacy (Nissenbaum 2004), Study 1 examines the interactive effect of data dissemination intentionality and data sensitivity on consumers' attitudes toward a company following a notification of data dissemination. When the data are highly sensitive, we anticipate that consumers will perceive intentional dissemination as a purposeful violation of privacy expectations, resulting in more (vs. less) negative attitudes toward the company. The effect of perceived intentionality will be less impactful when the disseminated data are non-sensitive.

Method

Participants and Design

A total of 197 US adults (133 females; $M_{age} = 36.6$) from an online panel participated in this study and received a small stipend. In an online experiment, the survey software randomly assigned participants to one of four conditions in a 2 (perceived intentionality: intentional vs. unintentional) $\times$ 2 (data sensitivity: sensitive vs. neutral) between-subjects design.

Procedure

Participants began by naming a real company with which they had shared personal data (e.g., for billing purposes, communications, or to receive promotions). Responses covered a variety of industries. Next, participants read a news article (see Web Appendix W2) reporting that the named company had shared customer information to client companies in order to improve their target marketing (i.e.,

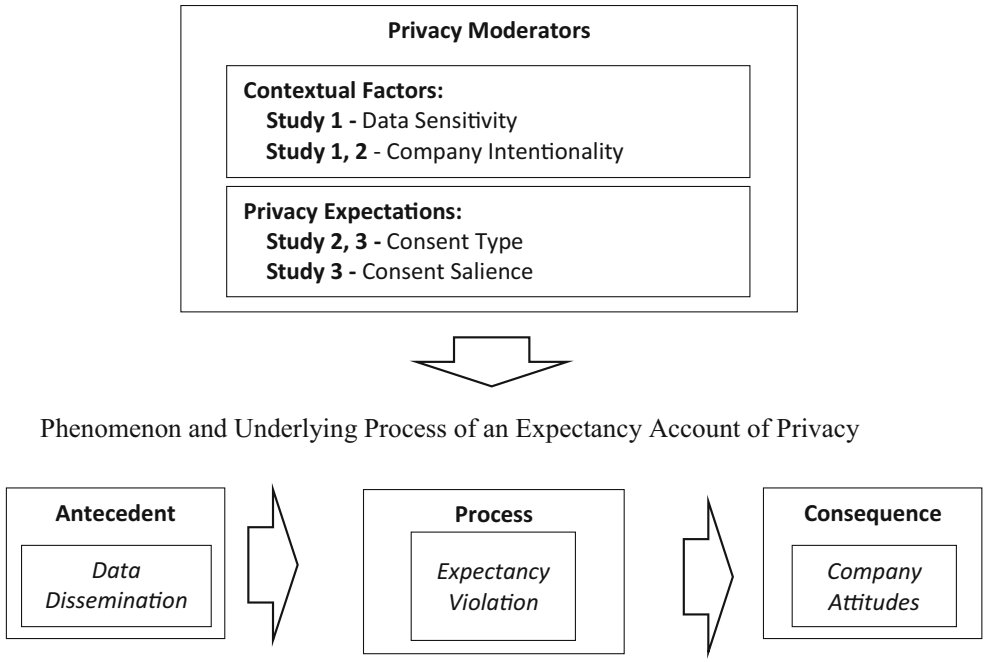


Fig. 2 Conceptual overview

intentional), or the named company accidentally shared customer information to client companies (i.e., unintentional). The personal information included customers' household incomes, credit card numbers, and phone numbers (i.e., sensitive), or favorite TV shows, email addresses, and ages (i.e., neutral). The types of personal information were selected based on a previous study demonstrating their relative sensitivity (Ackerman et al. 1999, p. 3). After reading the article, participants reported their attitudes toward the company on a three-item scale anchored from 1 (*bad, unfavorable, negative)* to 7 (*good, favorable, positive*; unidimensional, $\alpha = .96$).

Participants also answered two randomly presented manipulation check measures, each with three items. One measured the company's intentionality on a scale anchored from 1 (*unintentional, accidental, unplanned)* to 7 (*intentional, deliberate, planned*; unidimensional, $\alpha = .95$). The other measured information sensitivity as being "sensitive," "private," and "confidential" (*1: not at all; 7: very;* unidimensional, $\alpha = .97$). Lastly, participants reported their basic demographic information such as age and gender.

Results

Manipulation Checks

A 2 (intentionality) × 2 (sensitivity) between-subjects ANOVA on perceived information sensitivity revealed a significant main effect of the sensitivity manipulation. As expected, perceived sensitivity was significantly higher in the sensitive data condition ($M = 6.42$, SD = 1.04) than in the neutral data condition ($M = 3.82$, SD = 1.45, F (1, 193) = 206.93, $p < .001$). Further, perceived sensitivity was significantly higher than the scale midpoint (4) in the sensitive data condition (t (97) = 22.89, $p < .001$), whereas the mean in the neutral data condition was statistically equivalent to the scale midpoint (t (98) = −1.20, $p = .23$). The effect of the intentionality manipulation was not significant ($p = .84$), nor the interaction ($p = .15$).

A 2 (intentionality) × 2 (sensitivity) between-subjects ANOVA on perceived intentionality revealed a significant main effect of the intentionality manipulation (F (1, 193) = 125.66, $p < .001$). As expected, perceived intentionality was significantly higher in the intentional data dissemination condition ($M = 5.46$, SD = 1.74) than that in the unintentional data dissemination condition ($M = 2.74$, SD = 1.70, t (1, 195) = 11.11, $p < .001$). Further, perceived intentionality was significantly higher than the scale midpoint (4) in the intentional data dissemination condition (t (97) = 8.32, $p < .001$), whereas the mean in the unintentional data dissemination was statistically lower than the midpoint (t (98) = −7.39, $p < .001$). The effect of the sensitivity manipulation was not significant ($p = .19$), nor the interaction ($p = .16$). Thus, the manipulations were effective and there was no evidence of confounding.

Consumer Attitudes

Prior research has demonstrated the importance of organizational context in terms of privacy expectations

(Nissenbaum 2015, 2009; Martin and Shilton 2015, 2016). Subsequently, we tested our Study 1 predictions while controlling for industry. First, we adopted the industry coding schema developed by Luo et al. (2013) to categorize the self-reported companies into one of the following six industries: e-commerce (33% of responses), retail (27.4% of responses), finance (8.1% of responses), telecom/entertainment (7.6% of responses), electronics (6.6% of responses), and miscellaneous (17.3% of responses) (see "Appendix" for example responses). Next, we submitted consumer attitudes to a multiple regression analysis with perceived intentionality (0 = unintentional, 1 = intentional), data sensitivity (0 = sensitive, 1 = neutral), their interaction, and industry as predictors. Thus, the model is:

$$\begin{aligned}&\text{Attitude-toward-the company}\\&= \beta_0 + \beta_1(\text{perceived intentionality})\\&\quad + \beta_2(\text{data sensitivity}) + \beta_{3-7}(\text{industry dummies})\\&\quad + \beta_8(\text{perceived intentionality} \times \text{data sensitivity}) + \varepsilon_s\end{aligned}$$

The analysis revealed a main effect of perceived intentionality ($\beta_1 = .62$, t (188) = 2.72, $p < .01$) that was qualified by the predicted two-way interaction between perceived intentionality and data sensitivity ($\beta_8 = -.60$, t (188) = −1.95, $p = .05$). No other effects were significant (all $ps > .05$). In support of H_1, when the data were sensitive, participants' attitudes toward the company were less negative if the incident was unintentional ($M = 3.33$, SD = 1.55) relative to intentional ($M = 2.38$, SD = 1.43, t (96) = −3.12, $p = .002$). When the data were neutral, the company's intentionality did not affect attitudes (t (97) = −.65, $p = .52$). Means for each measure are listed in Table 1.

Discussion

Building on previous research arguing that privacy expectations are highly contextual (Brenkert 1981; Nissenbaum 2004), this study provides the first empirical evidence of company actions that violate privacy expectations and, consistent with this perspective, identifies intentionality and data sensitivity as important contextual factors.

As expected, Study 1 supports H_1 in that the negative effect of disseminating sensitive consumer data was greater when the incident was intentional, rather than unintentional. That is, consumers' overall attitudes toward the company were more negative when the company intentionally, rather than unintentionally, disseminated sensitive consumer data. Importantly, the study identified real companies, as given by participants, and the effect of perceived intentionality was not significant when the data were non-sensitive in nature. This pattern of results was observed across a wide variety of companies and persisted while explicitly controlling for industry. However, it is not clear yet if this negative effect is ascribed to violations of privacy expectations. Therefore, Study 2 was designed to provide insights in this respect. We aimed to investigate whether the psychological mechanism underlying this effect on consumer attitudes toward the company is explained by expectancy violations and our misalignment account.

Study 2: Measuring Perceived Expectancy Violations

Study 2 extends Study 1 by investigating the underlying mechanism explaining the effect of data dissemination on attitudes. In general, information exchange forms an implicit agreement between the company and the customer based on privacy expectations (Heide et al. 2007). Thus, we predict that the negative effect of intentionally disseminating sensitive data may be mitigated if consumers grant the company an explicit consent beforehand condoning the action. The role of consent is crucial to our theoretical account because it substantiates information exchange as a "negotiated agreement" that is superseded by the explicit terms of a consent agreement. Moreover, we propose consent as an effective means of aligning privacy expectations with company actions. Without consent, we expect to replicate the effects demonstrated in Study 1. According to our theoretical account, perceived violation of privacy expectations should serve as the underlying mechanism driving negative attitudes toward the company (H_2).

Method

Participants and Design

A total of 160 participants (61 females, $M_{age} = 32.5$) from an online panel participated in this study for a small stipend. A 2 (perceived intentionality: intentional vs. unintentional) × 2 (consent: present vs. absent) between-subjects design was used in this online experiment. The "absent" condition is in essence a control condition in which no consent information is presented.

Procedure

To control for the potential effect of preexisting brand associations, participants read about a fictitious telecommunications company, Forket Inc. Similar to Study 1, participants were informed that the company intentionally (i.e., started a new data dissemination project with client companies) or unintentionally (i.e., accidentally exposed

Table 1 Results for Study 1: the influence of company intentionality and data sensitivity on consumer perceptions

Measure	Sensitive information		Neutral information	
	Intentional ($n = 47$)	Unintentional ($n = 51$)	Intentional ($n = 51$)	Unintentional ($n = 48$)
Attitude toward the company (post-release)	2.38 (1.43)	3.32 (1.55)	2.69 (1.29)	2.85 (1.15)
Company intentionality	5.81 (1.71)	2.73 (1.80)	5.14 (1.71)	2.75 (1.61)
Data sensitivity	6.53 (.93)	6.31 (1.14)	3.68 (1.47)	3.98 (1.42)

Raw means and SDs (in parentheses) are reported in each cell

customer data to its client companies) disseminated sensitive customer data, including household income, credit card number, and phone number (see Web Appendix W3). In the explicit consent condition, participants were instructed that they had given consent to the company as new customers (i.e., signed a document consenting to the company's use of any and all consumer data for business, transactional, and analytical purposes). In the control condition, participants received no information regarding consent.

These manipulations were chosen based on a pretest ($N = 102$; 62 females; $M_{age} = 34.16$) where participants were exposed to the stimuli using the same experimental design featured in the main study. Pretest participants assessed the perceived intentionality of the company using the intentionality manipulation check described in Study 1 along with the perceived explicitness of the consent according to the following item, "You had given the company an expressed consent regarding how they handled your customer information" (1: strongly disagree; 7: strongly agree). According to the pretest results, the intentional data dissemination was in fact perceived as more intentional ($M = 6.73$, SD = .81) compared to the unintentional data dissemination ($M = 2.20$, SD = 1.26, t (100) = 21.66, $p < .001$). Importantly, in the explicit consent condition participants were more likely to agree that they had expressed consent ($M = 4.06$, SD = 2.11) compared to participants in the no consent condition ($M = 3.17$, SD = 2.04, t (100) = 2.16, $p = .03$). Thus, the manipulations were carried forward to the main study (see Web Appendix W3).

Measures In addition to attitudes toward the company ($\alpha = .96$), participants in our main study also indicated the extent to which the company violated contractual privacy expectations measured according to seven 7-point Likert scales (1: strongly disagree; 7: strongly agree). Consistent with a contractual approach to privacy (Martin 2012, 2016), the multi-item measure was adapted from multiple scales measuring the perceived violation of psychological contracts (Robinson 1996; Robinson and Morrison 2000; Rousseau 1989). Importantly, this scale was intended to capture both cognitive and emotional reactions when consumers perceive contractual violations of privacy expectations. For example, participants indicated how strongly they agreed or disagreed with the following statements, "I feel that Forket has violated a contract between us," "I feel betrayed by Forket," and "I feel that Forket has violated an understanding between us" (unidimensional, $\alpha = .96$; see Web Appendix W4 for scale items).

Results

Expectancy Violation

A 2 (intentionality) × 2 (consent) ANOVA on participants' perception that privacy expectations had been violated revealed a main effect of intentionality (F (1, 156) = 4.65, $p = .03$). Participants' perception of an expectancy violation was greater when the information was disseminated intentionally ($M = 5.88$, SD = 1.19) rather than unintentionally ($M = 5.45$, SD = 1.23, t (158) = −2.24, $p = .03$). The analysis also revealed the expected two-way interaction (F (1, 156) = 6.84, $p = .01$). When explicit consent was not granted, perceptions of an expectancy violation were higher when the data dissemination was intentional ($M = 6.20$, SD = .89) relative to unintentional ($M = 5.31$, SD = 1.31, t (82) = −3.63, $p < .001$). When consent was granted, by contrast, consumer perceptions of an expectancy violation did not vary by intentionality (t (74) = .30, $p = .76$). There was no main effect of the consent type (F (1, 156) = .89, $p = .33$).

Consumer Attitudes

A 2 (intentionality) × 2 (consent) between-subjects ANOVA on consumer attitudes toward the company revealed a significant two-way interaction (F (1, 156) = 10.21, $p = .002$) and no main effects. When explicit consent was not granted, consumer attitudes followed the same pattern demonstrated in Study 1, where evaluations were less negative when the data dissemination was unintentional ($M = 2.30$, SD = 1.10) relative to intentional ($M = 1.43$, SD = .95, t (82) = 3.88, $p < .001$). When consent was granted, by contrast, consumer attitudes did not vary by intentionality (t (74) = −1.07, $p = .29$). Means for each measure are listed in Table 2.

Mediation

We hypothesized that perceived violation of contractual privacy expectations mediates the negative effect of an intentional dissemination of sensitive data on consumer attitudes toward the company (H2). To test this mediated moderation, we employed Model 8 in Hayes (2013) with 5000 resamples. First, the model regressed mean-centered perceived expectancy violation on to intentionality, consent, and their interaction. The intentionality × consent interaction predicted perceived expectancy violations ($\beta = .99$, $t = 2.62$, $p = .01$). Second, the model regressed company attitudes on perceived expectancy violations, intentionality, consent, and the interaction of the last two factors. Perceived expectancy violations predicted company attitudes ($\beta = -.77$, $t = -14.93$, $p < .001$). Third, and most importantly, conditional indirect effects analysis, using bootstrapping, revealed that perceived expectancy violation mediated the effect of intentionality on company attitudes when consent was absent, with a 95% CI excluding zero (95% CI, −1.04 to −.36). However, perceived expectancy violation did not mediate the effect of intentionality on company attitudes when consent was present (95% CI, −.34 to .52). Figure 3 depicts the mediation model.

Discussion

In Study 2, we replicate the findings demonstrated in Study 1 using a unique sample, company, and disclosure notification. In addition, we provide empirical evidence that the contextual effects of intentionality and data sensitivity are in fact driven by perceived violations of privacy expectations. According to prior research (Martin 2012, 2016; Nissenbaum 2004), data exchanges form implicit agreements between parties with expectations of data security, privacy, voice, and exit, which can be overridden in the case of explicit agreements. Thus, as we find, an explicit agreement condoning data dissemination aligns consumer privacy expectations with company actions and negates the effect of intentionality. It is worth noting that the experimental design assumed that consumers must have given their consent, without examining specific technical procedures such as whether the consent was "good enough." Study 3 addresses this limitation and further explores how the specific consent procedures, and not consent in and of itself, influence consumers' privacy expectations and perceived privacy violations accordingly. That is, we extend our investigation of privacy expectations within this theoretical framework to provide a more differentiated link between privacy expectations and perceptions of privacy violation.

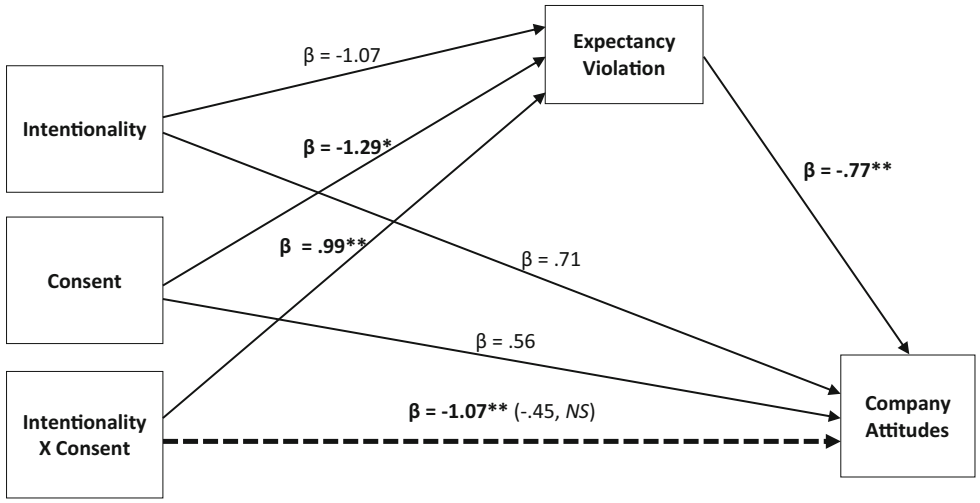
Study 3: Using Consent and Saliency to Form and Re-Affirm Privacy Expectations

The purpose of Study 3 is to empirically test the theoretical link between contractual expectancies and privacy, as theorized in previous research (Martin 2012, 2015, 2016). According to Martin (2012), privacy expectations are negotiated informational norms within a particular community or situation. We manipulate privacy expectations through consent type and saliency. Consistent with H3, given that explicit consent requires a conscious act of permission to the consent terms, we anticipate that privacy expectations regarding data dissemination will be much clearer when its terms are made salient following an occurrence of data dissemination. Thus, consumer attitudes will be less negative when privacy expectations align with company actions. Conversely, when company practices violate privacy expectations, which is common (Martin 2016), and consumers do not realize they are committed to the privacy policies, reactions following a notification of data dissemination should be unchanged by consent salience. Thus, Study 3 builds upon our Study 2 findings in three important ways. First, rather than informing participants of consent, we have them complete the consent procedures. Second, by incorporating consent type we explore the complexity indicative of real consent procedures. Lastly, we further substantiate our process account (i.e., the underlying mechanism) through consumer perceptions of expectancy violation and through consent saliency.

Table 2 Results for Study 2: the influence of company intentionality and consent on consumer perceptions

Measure	Consent		No consent	
	Intentional ($n = 37$)	Unintentional ($n = 39$)	Intentional ($n = 40$)	Unintentional ($n = 44$)
Attitude toward the Company (post-release)	2.29 (1.62)	1.96 (1.03)	1.43 (.95)	2.30 (1.10)
Perceived expectancy violation	5.53 (1.37)	5.61 (1.12)	6.20 (.89)	5.31 (1.31)
Data sensitivity	5.71 (1.96)	5.55 (2.15)	5.88 (2.00)	6.01 (1.55)

Raw means and SDs (in parentheses) are reported in each cell



*$p < .05$

**$p < .01$.

Fig. 3 Study 2: mediated moderation model

Method

Participants and Design

A total of 227 US adults (156 females, $M_{age} = 36.44$) from an online panel participated in this study for a small stipend. A 2 (Consent type: implied vs. explicit) × 2 (Consent salience: high vs. low) between-subjects design was used in this online experiment.

Procedure

Participants were informed of our interest in their reaction toward a real mobile application that allows users to save and watch NBC programming on mobile devices. Before reviewing the application, participants indicated their initial attitudes toward NBC using the same attitude toward the company scale described in Study 1.

Next, all participants were presented with a detailed description of the application and asked how likely they would be to download this application (1: definitely no, 7: definitely yes). Both consent types used the same 544-word privacy policy, which was adapted from the online privacy policy of NBA.com, suggesting that the company may share customer information with their clients (see Web Appendix W5). Participants in the explicit consent condition read, "Before downloading the application you must read and consent to the following privacy policy," and were presented with two options: (1) to agree to the consent terms and type their initials or (2) to disagree to the consent terms. Conversely, participants in the implied consent condition were told, "Please note that by downloading the application you consent to NBC Networks' privacy policy," and asked whether they would like to review the policy or not. Thus, the policy was presented only to participants who expressed an interest in reviewing it. The total time spent reviewing the consent information was recorded by the online survey software.

Participants then were informed that the company had started a new data dissemination project with client companies across multiple industries twelve months later. The type of data shared was highly sensitive in nature. Rather than using the types of sensitive data identified in prior research (Ackerman et al. 1999, p. 3), we selected data based on a pretest ($N = 82$; 45 females; $M_{age} = 39.3$) where participants examined the sensitivity of 31 types of personal information on three-item scales (*sensitive/private/confidential*; 1: not at all; 7: very). The results support that billing/home address ($M = 4.89$, SD = 1.91), online search/browsing history ($M = 5.10$, SD = 1.80), and cell/home phone number ($M = 5.27$, SD = 1.83) were considered sensitive personal information compared to the neutral point (4) on the scales ($ps < .05$) and thus carried forward to the main study.

Depending on saliency conditions, the consent was either repeated or not repeated following the data dissemination notification. In the high salience condition, participants were reminded that they had consented to the privacy policy allowing the company to collect and share their personal information with third parties and presented with the same 544-word privacy policy. By contrast,

participants in the low salience condition proceeded directly to the attitude measures.

All participants then reported their attitudes toward NBC using the same attitude scale presented at the onset of the study followed by the same expectancy violation measures described in Study 2. Participants also completed two manipulation check measures. The first assessed perceived intentionality and asked, "Did NBC intentionally (i.e., purposefully) release your personal information to its client companies?", whereas the second asked, "Did you provide an explicit consent to NBC's privacy policy?" Responses were measured according to seven-point scales anchored at *definitely no—definitely yes*. Lastly, participants indicated several demographics and were debriefed that the scenario and privacy policy were created for the purpose of this thought experiment.

Results

Given that the purposeful dissemination of consumer information following explicit documentation prohibiting such an act is in strict violation of the FTC Act (FTC 2011), only participants who agreed to the explicit consent were retained for the main analyses. That is, participants assigned to the explicit consent condition, who answered "No" to the consent terms ($n = 40$) were removed from the analysis, whereas all other participants were retained. Thus, a final sample of 187 participants (124 females, $M_{age} = 35.20$) was retained for analysis. All of the scales used in Study 3 were unidimensional and highly reliable (all $\alpha > .89$).

Manipulation Checks

A 2 (consent type) × 2 (consent salience) between-subjects ANOVA on the perceived explicitness of the consent revealed a significant main effect of consent type (F (1, 183) = 29.34, $p < .001$) and no additional effects (all $ps > .50$). As expected, the consent was perceived as significantly more explicit in the explicit consent condition ($M = 5.86$, SD = 1.69) compared to the implied consent condition ($M = 4.11$, SD = 2.37, t (185) = 5.51, $p < .001$).

Similarly, a 2 (consent type) × 2 (consent salience) ANOVA on the perceived intentionality of the information release revealed no main or interaction effects (all $ps > .30$). As expected, intentionality was not significantly different between the consent type conditions, nor the consent saliency conditions. In addition, the release was perceived as intentional, given that the mean response was statistically above the scale midpoint (4) ($M = 4.79$, SD = 2.29, t (186) = 4.72, $p < .001$).

Consumer Attitudes

Given participants evaluated the company on the same scale before and after information release, we submitted attitude toward the company to a repeated-measures ANOVA, with attitudes as a within-subjects factor and consent type and consent salience as independent variables. This analysis revealed a significant main effect of the within-subjects factor (F (1183) = 159.71, $p < .001$). As expected, attitudes prior to the data dissemination notification were more favorable ($M = 5.25$, SD = 1.39) than attitudes following the notification ($M = 3.60$, SD = 1.80, t (186) = 12.93, $p < .001$). The analysis also revealed a marginal interaction effect between the within-subjects factor and consent salience (F (1183) = 3.00, $p = .09$). Whereas attitudes prior to the data dissemination notification were equivalent ($p > .9$) across the saliency conditions, attitudes following the data dissemination notification were more favorable when the consent was highly salient ($M = 3.86$, SD = 1.87) compared to when the consent was not highly salient ($M = 3.39$, SD = 1.79, F (1183) = 3.05, $p = .08$). More importantly, the analysis also revealed the predicted consent type × consent salience interaction (F (1183) = 4.61, $p = .03$) and no additional main or interactive effects (all $ps > .19$).

In the explicit consent condition, participants' attitudes toward the company, following the data dissemination notification, were more favorable when the consent was highly salient ($M = 4.16$, SD = 1.68) compared to when the consent was not salient ($M = 3.09$, SD = 1.55, F (1183) = 4.57, $p = .03$). Conversely, in the implied consent condition, participants' attitudes toward the company did not vary when the consent was salient ($M = 3.55$, $SD = 1.72$) versus not salient ($M = 3.69$, SD = 2.06, F (1183) < 1.0, *NS*). Means for each measure are listed in Table 3.

Expectancy Violation

Consistent with Study 2, we speculated that perceptions of expectancy violation would mediate the effect of increasing the salience of privacy expectations on consumer attitudes when consent was explicit, but not when consent was implied. To test this mediated moderation, we employed Model 8 in Hayes (2013) with 5000 resamples. The model regressed post-notification company attitudes on perceived expectancy violations, consent type, consent salience, and the interaction of the last two factors. Perceived expectancy violations predicted company attitudes ($\beta = -1.08$, $t = -10.38$, $p < .001$). More importantly, the results of a conditional indirect effects analysis, using bootstrapping, revealed that perceived expectancy violation mediated the effect of saliency on company attitudes when the consent

was explicit, with a 95% CI excluding zero (95% CI, .03–.87). However, perceived expectancy violation did not mediate the effect of saliency on company attitudes when consent was implied (95% CI, −.31 to .38).

Discussion

According to the Study 3 results, the negative effect of data dissemination on consumer sentiment is lessened when explicit consent is made salient following data dissemination notifications. Why was this effect observed? Consistent with our alignment account, repeating an explicit consent following a notification of data dissemination helps to reinforce a preexisting agreement that the intentional exchange of consumer information was condoned. The mediation model replicated that in Study 2, lending further support to a contractual expectancy violation account of data dissemination. That is, implementing consent procedures designed to set and reinforce privacy expectations proved effective in attenuating negative consumer perceptions. According to our theoretical account, this occurred because contextual factors encouraged consumers' privacy expectations to match the companies' actions. It is important to reiterate that the actions themselves remained the same, along with the type of data that were disseminated.

Interestingly, repeating the consent terms does not have an effect when the consent is implied. One potential explanation is that while easy to implement, consumers may not attend to implied consent information. This is consistent with previous research showing consumers are either unlikely to read privacy policies or unlikely to comprehend them (Milne and Culnan 2004; Milne et al. 2006). This is also supported by the Study 3 results indicating that participants in the implied consent condition spent considerably less time reading the privacy policy ($M = 5.75$ s, SD = 16.06 s) compared to participants in the explicit consent condition ($M = 28.07$ s, SD = 25.10 s, t (185) = 7.42, $p < .001$).

General Discussion

Prior privacy research has explored the importance of privacy expectations in determining the social norms that consumers expect companies to follow when managing their personal data (Martin 2012, 2015, 2016). The current research builds upon this prior theorizing to explore when privacy expectations may be violated within the context of data dissemination—an extremely consequential and increasingly common phenomenon. Three studies show that when companies disseminate consumer information, they often violate contractual privacy expectations with their customers—consequently, damaging consumers' company perceptions. This data dissemination effect occurred across a variety of companies, industries, shared data, and disclosure notifications. However, this effect is not universal to all information types and is contingent upon multiple factors—both within and outside the company's purview. For example, consumers react more negatively when the information is sensitive and the action is intentional (Study 1). Beyond documenting a novel means by which information dissemination impacts consumers' evaluations, we also demonstrate process evidence in support of our theoretical account (Studies 2 and 3). Consistent with prior research, we propose that when consumers exchange information with a company, they maintain certain privacy expectations regarding its storage, usage, and dissemination. Thus, the act of information exchange forms contractual privacy expectations. We further posit that contextual factors (e.g., intentionality and data sensitivity) can influence the alignment of privacy expectations with company actions (even when other contextual factors remain constant). More specifically, intentionally disseminating sensitive consumer information violates these privacy expectations. Consistent with our alignment account, the effect of data dissemination on company reputation was mediated by consumers' perception that contractual expectations had been violated in a way that benefited the company. In other words, the act of intentionally disseminating sensitive consumer data

Table 3 Results for Study 3: the influence of consent type and saliency on consumer perceptions

Measure	Explicit consent		Implied consent	
	Repeated ($n = 34$)	Not repeated ($n = 39$)	Repeated ($n = 63$)	Not repeated ($n = 51$)
Attitude toward the company (pre-release)	5.52 (1.32)	5.25 (1.23)	5.06 (1.51)	5.31 (1.41)
Attitude toward the company (post-release)	4.16 (1.68)	3.09 (1.55)	3.55 (1.72)	3.69 (2.06)
Perceived expectancy violation	4.11 (1.43)	4.74 (1.57)	4.25 (1.68)	4.31 (1.45)
Company intentionality	5.29 (1.73)	5.41 (2.10)	4.87 (2.30)	5.18 (2.16)
Perceived consent explicitness	5.68 (1.67)	6.03 (1.71)	4.08 (2.43)	4.14 (2.32)
Time spent reviewing consent (s)	24.39 (24.53)	31.28 (25.47)	6.54 (15.35)	4.78 (16.99)

Raw means and SDs (in parentheses) are reported in each cell

violated the contractual privacy expectations on which it was formed.

Finally, our results show that companies can take actions to better align privacy expectations with company actions, thus minimizing this data dissemination effect. In particular, disseminating non-sensitive data (Study 1) or securing consent prior to the data sharing notification (Studies 2 and 3) mitigates the effect. Indeed, according to the Study 3 findings the type of consent (implied vs. explicit) is also an important factor, especially when the consent is made salient. In particular, explicit consent methods prove particularly effective when made highly salient following a data dissemination notification. Despite these findings, lay intuition and common business practice offer implied consent as an equivalent alternative to explicit consent—minus the procedural difficulties inherent in securing explicit consent. The current research challenges this notion by arguing that while explicit consent is often met with increased scrutiny and potential non-compliance during its proposal, this additional scrutiny may prove invaluable following a notification of data dissemination. Collectively, then, this research provides an important advancement in our understanding of the manner by which consumers react to data dissemination, in particular, and violations of contractual privacy expectations, more generally. The results underscore the importance of aligning privacy expectations with company actions. Importantly, whether or not consumers perceive a company action as violating privacy expectations depends on how, and the extent to which, consumers construe the "negotiated agreement" between the company and the consumer which varies by contextual factors (e.g., consent type, type of data, intentionality) that serve to align (or misalign) privacy expectations with company actions.

Theoretical Contributions

This research offers two major theoretical contributions to the business ethics literature pertaining to consumer privacy. Foremost, this research illustrates the malleability of privacy expectations and perceived privacy violations. In doing so, this is the first research to examine the concept of intentionality in relation to privacy infringements. Indeed, the effect of intentionality is not straightforward. Consumers may consider intentional data dissemination as business centric, dubious, and even malicious at times. If so, they could react more negatively, relative to unintentional data dissemination. However, purposeful data dissemination can be well intended (e.g., to customize products, target advertising) and fully disclosed (as written in the privacy policy, e.g., Facebook, CNN, Google). In such cases, consumers may react favorably to intentional data dissemination. By contrast, when data dissemination is unintended, consumers may infer that some mistakes, errors, or lapses in good judgment occurred on the company's part, which can trigger more negative reactions relative to intentional data dissemination. The recent Target example suggests that an incident of external hacking can expose the company's technical or operational failures, which has resulted in a significant public outcry. In response, Target has spent a substantial amount of financial resources in crisis management and organizational restructuring, which has diminished the company's market valuation (Garcia 2015). In this research, we address these competing plausible outcomes empirically. Intentionality is a particularly intriguing construct for two main reasons. First, each year millions of consumers are affected by intentional and unintentional data dissemination alike, so studying this construct is practically important. Second, given that the data itself are the same in both cases, logically speaking, it is interesting to find different consumer reactions for when those data are intentionally rather than unintentionally disseminated. Conceptually, the findings lend further support to a contextually dependent approach to understanding information exchange and privacy in general (Martin 2012; Nissenbaum 2004).

Further, we adopt techniques from the psychological contract literature to measure the perceived violation of contractual privacy expectations (Acquisti, Brandimarte, and Loewenstein 2015). This contribution is particularly important given the criticism that identifying implicit contracts, their terms, and the actions that violate these expectancies is practically infeasible (Dunfee 2006). From a managerial standpoint, although data dissemination is common in the marketplace, the literature has documented little systematic research examining consumers' reactions to data dissemination and boundary conditions to these effects. Moreover, the existing literature primarily documents negative market effects of data dissemination (Campbell et al. 2003; Kannan et al. 2007). Departing from this perspective, this research formally examines when and how data dissemination influences consumers' perceptions. Vital managerial insights include the implication that companies can avoid violating privacy expectations without impeding information dissemination by aligning expectations with company actions. Overall, this research develops our understanding of how data dissemination shapes consumer sentiment and behavior in this era of Big Data (Nunan and Di Domenico 2015).

This research also contributes to the business ethics literature. Building upon Martin's (2012, 2015, 2016) contractual, norms-based view of privacy, we articulate the ethical importance of aligning privacy expectations with company actions. At the moment, companies seem preoccupied with collecting and utilizing consumer data for their

own advances while enacting privacy procedures (e.g., implied consent) designed to protect themselves from legal liability. While this approach often benefits the companies and stakeholders utilizing the data, it seems contrary to a number of normative ethical theories. For instance, according to teleological or consequentialist theories, ethical actions are those that benefit the greatest number of individuals (Micewski and Troy 2007). Yet, on an annual basis, millions of consumers are negatively impacted by current privacy practices and notification procedures (Kroft 2014; Quick et al. 2017). Similarly, our results suggest that consumers construe misalignments in privacy expectations as violating privacy norms and social contracts (Martin 2016). Thus, the current work illustrates the importance of aligning privacy expectations so as to avoid unethical business practices and perceived privacy violations.

The Consequences of Consent

Consumer consent is another intriguing aspect of privacy infringement due to information asymmetry. Privacy policies are often worded carefully by legal professionals to avoid liability on the side of the company. Consumers, however, do not necessarily fully read or understand the policies. What's more, most, if not all, consent is required for consumers to complete a transaction. Put differently, companies frequently require consumers to give consent, but granting consent does not necessarily imply that privacy expectations have been properly established. Given that consumers do not always know how their personal data will be used, the effects of "consent" are questionable from a privacy perspective. Exploring consumer consent with the type of data disseminated enhances our understanding of the "contextual dependency" of privacy. We find that consumer reactions to data dissemination depend on whether or not consumers provided prior consent condoning the company's actions and the extent to which they have internalized this consent. These findings are consistent with, and contribute to, an extensive body of literature on default options (Huh et al. 2014; Smith et al. 2013).

Contrary to popular practice, implied consent, which incorporates a default of agreement, proves to be particularly ineffective following data dissemination notifications–even when made salient. In the case of implied consent, our findings suggest that although these individuals may "agree" to the terms, they may have very little awareness and commitment to these terms. Thus, counterintuitively, companies may want to leverage explicit consent techniques if they hope to minimize the negative reactions common to perceived privacy infringements. Doing so helps reduce the risk of perceived privacy violations in two important ways. First, as evidenced by our Study 3 time measures, individuals expend more time elaborating upon the privacy terms when presented with an explicit, rather than implied consent. This increases the odds that consent terms will be read, comprehended, and internalized. We also find that repeating these consent terms helps to re-affirm privacy expectations. Companies could easily communicate consent information on a routine basis, following a privacy practice change, or in response to a particular incident permissible as per the consent terms. In sum, the results lend strong empirical support to our alignment account and illustrate the importance that companies should place on aligning privacy expectations with business practices.

Managerial Implications

Our findings suggest a number of potential managerial implications. Much of the "Big Data" discussions among business professionals focus on how to gather and utilize customer data more effectively. To date, however, very few studies have examined how practitioners should manage and sustain relationships with individuals who provide companies with their personal information. We present one of the first empirical studies to shed light on this critical issue. The most straightforward implication is that once companies engage in data dissemination or an unintentional incident has occurred, companies should clearly communicate the incident to those affected. Moreover, if hacked or released by mistake, it is crucial for the company to characterize the incidence as "unintentional" when communicating with affected consumers, the constituencies, and the public. This is consistent with our Study 1 and 2 results showing that consumers tend to be more forgiving when they are informed that the data dissemination incident is unintentional, despite the dissemination of personally sensitive information.

This research also highlights the importance of monitoring and maintaining privacy expectations. That is, companies should continually monitor what privacy expectations their consumers hold and take actions to mitigate any misalignments between privacy expectations and company actions. We explored this process through consent, but companies could potentially align privacy expectations with company actions through any number of mechanisms, including clarifications to the privacy policies themselves (Martin 2015), enhanced regulation and standardization of innovative technologies (Zhou and Piramuthu 2015), or by mitigating internal abuses and inconsistencies (Lowry et al. 2014). Furthermore, companies can use the measures described in Study 3 to explore which company actions have or may potentially violate privacy expectations. This contributes to a growing body of ethics literature recommending enhanced transparency and communicative channels between companies and

consumers (Kang and Hustvedt 2014; Russo-Spena et al. 2016; Stohl et al. 2015).

Study 3 also explored the practice of implied consent. Undoubtedly, being particularly nonintrusive and convenient, implied consent possesses some unique utility. Yet, our findings suggest that there may be a significant downside to this utility. That is, consumers tend to consider agreement by means of inaction, as is the case in implied consent, differently than agreements by means of action, as is the case in explicit consent. This finding casts doubt on the effectiveness of this increasingly popular practice (i.e., implied consent) in aligning privacy expectations. Marketers should be more cautious by implementing a clear consent policy requiring thoughtful deliberation and explicit agreement. For example, companies can provide a short highlight or summary in addition to the full-scale privacy policy. They may also consider highlighted text to urge consumers to read privacy policy more closely and, in some cases, may provide small incentives (e.g., loyalty program points) to encourage consumers to give more informed consent. Recent legislative changes highlighting the privacy rights of consumers (Kelly 2017) may further provoke consumers to attend more deliberately to consent procedures, privacy policies, and privacy more generally, but companies should do more to encourage consumers to take an active role in understanding how their data will be managed and disseminated.

Limitations and Further Research

The present research is subject to several limitations that suggest directions for further theoretical and empirical extension. For one, the stimuli do not consider all possible scenarios. With regard to intentionality, specifically, it is plausible that companies are required to disseminate data for legal compliance. By contrast, companies may unintentionally disseminate customer data due to insufficient security, which is not always forgivable. Future research should explore the role of specific attributions in conjunction with perceived intentionality. In a similar vein, the explicit versus implied consent may take a variety of forms in practice. Some consent procedures require users to agree to a lengthy and obscure privacy policy, which in fact many users do not read. The effectiveness of such explicit consents can be questionable, from a consumer standpoint. More empirical work is necessary to elucidate the complex intricacies of consent.

It is also important to consider consumer reactions over time. In this research, we collected cross-sectional data. Although the findings indicate that data dissemination often results in negative consumer responses and that these reactions are bounded by company and information specific factors, further research might investigate in greater detail the effect of data dissemination as a function of time. For instance, at certain points of time consumers may think more deliberately about data dissemination, when the actual consequences of data dissemination become critical for consumers to react. Such a study would require a longitudinal design that records consumers' reactions at multiple times.

In addition, future studies should address the broader issue concerning managerial remedies designed to restore consumer perceptions following a data dissemination notification. An effective response may be to provide customer privileges with an assurance that the violation will not re-occur in the future (e.g., by providing an opt-out option). Financial compensation may also be an effective remedy, while the amount of compensation may need to exceed a minimum threshold; otherwise, financial restitution may backfire and magnify the negative effect.

Of course, our findings may extend beyond this particular context and aid our understanding of other default options and privacy violations. These may be fruitful future research topics. Although our findings certainly highlight the importance of consent type in terms of privacy expectations, future research may also serve to build upon these findings to further determine what constitutes "unsatisfactory consent" as discussed in the consent literature (e.g., Easton et al. 2007; Veatch 2007). That is, there may be ample avenues to determine other contextual factors that may influence privacy expectations in terms of consent length, timing (e.g., just-in-time notices), or other substantive interventions. Such research would certainly be useful given an abundant body of the literature suggesting consumers insufficiently process and comprehend standard consent notices (Milne and Culnan 2004; Milne et al. 2006).

Concluding Remarks

In conclusion, advances in information technology allow businesses to record, store, and exchange a wide array of consumers' personal information. The dissemination of these data among companies and corporations may be beneficial or detrimental to consumers. How this process is managed is of great concern to consumers, marketing managers, and the public. That is exactly why the concept of aligning privacy expectations with company actions is particularly relevant to developing appropriate business practices and public policies. Given that relatively little research has examined this process, future work is poised to build on this research to further our understanding of individual and company-level consequences of privacy and privacy infringement.

Compliance with Ethical Standards

Conflict of interest The authors declare that they have no conflict of interest.

Appendix

Study 1: Example Companies by Industry

Industry	Companies
E-commerce	Ebay
	Amazon
	Cardpool.com
Retail	Target
	Walmart
	Costco
Finance	Bank of America
	USAA
	Citibank
Electronics	Apple
	Samsung
	Best Buy
Telecom/entertainment	Comcast
	Bravo
	AT&T
Miscellaneous	US Air Force
	Kroger
	Mary Kay

References

Ackerman, M. S., Cranor, L. F., & Reagle, J. (1999). Privacy in e-commerce: Examining user scenarios and privacy preferences. In *Proceedings of the 1st ACM conference on electronic commerce* (pp. 1–8).

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

Altman, I. (1975). *Environment and social behavior: Privacy, personal space, territory, and crowding*. Monterey, CA: Brooks/Cole.

Baca-Motes, K., Brown, A., Gneezy, A., Keenan, E. A., & Nelson, L. D. (2013). Commitment and behavior change: Evidence from the field. *Journal of Consumer Research, 39*(5), 1070–1084.

Brenkert, G. G. (1981). Privacy, polygraphs and work. *Business and Professional Ethics Journal, 1*(1), 19–35.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448.

Cranor, L. F. (2012). Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications and High Technology Law, 10,* 273.

Disney (2015). Privacy policy. https://disneyprivacycenter.com/privacy-policy-translations/english/#DIMGQuestion4. Accessed May 25, 2016.

Dommeyer, C. J., & Gross, B. L. (2003). What consumers know and what they do: An investigation of consumer knowledge, awareness, and use of privacy protection strategies. *Journal of Interactive Marketing, 17*(2), 34–51.

Donaldson, T., & Dunfee, T. W. (1994). Toward a unified conception of business ethics: Integrative social contracts theory. *Academy of Management Review*, *19*(2), 252–284.

Dunfee, T. W. (2006). A critical perspective of integrative social contracts theory: Recurring criticisms and next generation research topics. *Journal of Business Ethics, 68*(3), 303–328.

Easton, R. B., Graber, M. A., Monnahan, J., & Hughes, J. (2007). Defining the scope of implied consent in the emergency department. *The American Journal of Bioethics*, *7*(12), 35–38.

Facebook (2013). Important message from Facebook's white hat program. https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766. Accessed December 19, 2015.

Federal Trade Commission. (2009). The CAN-SPAM Act: A compliance guide for business. https://www.ftc.gov/system/files/documents/plain-language/bus61-can-spam-act-compliance-guide-business.pdf. Accessed December 1, 2016.

Federal Trade Commission. (2011). FTC charges deceptive privacy practices in Google's rollout of its buzz social network. http://Ftc.Gov/Opa/2011/03/Googleshtm. Accessed December 1, 2016.

Federal Trade Commission. (2014). Data brokers: A call for transparency and accountability. Www.Ftc.Gov/System/Files/Documents/Reports/Data-Brokers-Call-Transparency-Accountabilityreport-Federal-Trade-Commission-may-2014/140527databrokerreport.Pdf. Accessed December 1, 2016.

Finkle, J. (2013). Adobe data breach more extensive than previously disclosed. *Reuters,* http://www.reuters.com/article/us-adobe-cyberattack-idUSBRE99S1DJ20131029. Accessed December 19, 2015.

Fredrix, E. (2005). Ameritrade loses backup tape containing 200 K client files. http://usatoday30.usatoday.com/tech/news/computersecurity/infotheft/2005-04-20-ameritrade-files-lost_x.htm. Accessed December 1, 2016.

Garcia, A. (2015). Target settles for $39 million over data breach. http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement. Accessed September 1, 2016.

Google. (2016). Privacy policy. http://www.google.com/policies/privacy. Accessed December 1, 2016.

Harris, K. D. (2016). California Data Breach Report 2012-2015. https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf. Accessed May 25, 2016.

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York: Guilford Press.

Heide, J. B., Wathne, K. H., & Rokkan, A. I. (2007). Interfirm monitoring, social contracts, and relationship outcomes. *Journal of Marketing Research, 44*(3), 425–433.

Huh, Y. E., Vosgerau, J., & Morewedge, C. K. (2014). Social defaults: Observed choices become choice defaults. *Journal of Consumer Research, 41*(3), 746–760.

Janssen, A., & Gevers, S. (2005). Explicit or implied consent and organ donation post-mortem: Does it matter. *Medicine and Law, 24*(3), 575–583.

Johnson, E. J., Bellman, S., & Lohse, G. L. (2002). Defaults, framing and privacy: Why opting in-opting out. *Marketing Letters, 13*(1), 5–15.

Johnson, E. J., & Goldstein, D. (2003). Do defaults save lives? *Science, 302*(5649), 1338–1339.

Kang, J., & Hustvedt, G. (2014). Building trust between consumers and corporations: The role of consumer perceptions of transparency and social responsibility. *Journal of Business Ethics, 125*(2), 253–265.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce, 12*(1), 69–91.

Kelly, E. (2017). Congress tackles major privacy, surveillance issues. *USA Today* https://www.usatoday.com/story/news/politics/2017/04/12/congress-tackles-major-privacy-surveillance-issues/100335168. Accessed April 16, 2017.

Kroft, S. (2014). The data brokers: Selling your personal information. *CBS News.* http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/. Accessed October 5, 2015.

Lombrozo, T. (2010). Causal–explanatory pluralism: How intentions, functions, and mechanisms influence causal ascriptions. *Cognitive Psychology, 61*(4), 303–332.

Lowry, P. B., Posey, C., Roberts, T. L., & Bennett, R. J. (2014). Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse. *Journal of Business Ethics, 121*(3), 385–401.

Luo, X., Raithel, S., & Wiles, M. A. (2013). The impact of brand rating dispersion on firm value. *Journal of Marketing Research, 50*(3), 399–415.

Madden, M. (2014). Public perceptions of privacy and security in the post-Snowden era. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions. Accessed December 1, 2016.

Martin, K. (2012). Diminished or just different? A factorial vignette study of privacy as a social contract. *Journal of Business Ethics, 111*(4), 519–539.

Martin, K. (2015). Privacy notices as tabula rasa: An empirical investigation into how complying with a privacy notice is related to meeting privacy expectations online. *Journal of Public Policy & Marketing, 34*(2), 210–227.

Martin, K. (2016). Understanding privacy online: Development of a social contract approach to privacy. *Journal of Business Ethics, 137*(3), 551–569.

Martin, K., & Shilton, K. (2015). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology, 67*(8), 1871–1882.

Martin, K., & Shilton, K. (2016). Putting mobile application privacy in context: An empirical study of user privacy expectations for mobile devices. *The Information Society, 32*(3), 200–216.

Micewski, E. R., & Troy, C. (2007). Business ethics–deontologically revisited. *Journal of Business Ethics*, *72*(1), 17–25.

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., & Bahl, S. (2010). Are there differences between consumers' and marketers' privacy expectations? A segment-and technology-level analysis. *Journal of Public Policy & Marketing, 29*(1), 138–149.

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., Culnan, M. J., & Greene, H. (2006). A longitudinal assessment of online privacy notice readability. *Journal of Public Policy & Marketing, 25*(2), 238–249.

Milne, G. R., & Gordon, M. E. (1993). Direct mail privacy-efficiency trade-offs within an implied social contract framework. *Journal of Public Policy & Marketing, 12*(2), 206–215.

Mothersbaugh, L. D., Foxx, W. K., II, Beatty, S. E., & Wang, S. (2011). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*(1), 76–98.

Newman, G. E., Gorlin, M., & Dhar, R. (2014). When going green backfires: How firm intentions shape the evaluation of socially beneficial product enhancements. *Journal of Consumer Research, 41*(3), 823–839.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review*, *79*, 101–139.

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford, CA: Stanford Law Books.

Nissenbaum, H. (2015). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics*. doi:10.1007/s11948-015-9674-9

Nowak, G. J., & Phelps, J. (1997). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Interactive Marketing, 11*(4), 94–108.

Nunan, D., & Di Domenico, M. (2015). Big data: A normal accident waiting to happen? *Journal of Business Ethics*. doi:10.1007/s10551-015-2904-x

Ohm, P. (2015). Sensitive information. *Southern California Law Review, 88*(5), 1125–1196.

Peslak, A. R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics, 59*(4), 327–345.

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.

Pizarro, D., Uhlmann, E., & Salovey, P. (2003). Asymmetry in judgments of moral blame and praise the role of perceived metadesires. *Psychological Science, 14*(3), 267–272.

Pollach, I. (2005). A typology of communicative strategies in online privacy policies: Ethics, power and informed consent. *Journal of Business Ethics, 62*(3), 221–235.

Quick, M., Hollowood, E., Miles, C., & Hampson, D. (2017). World's biggest data breaches. Informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks. Accessed April 16, 2017.

Robinson, S. L. (1996). Trust and breach of the psychological contract. *Administrative Science Quarterly, 41*(4), 574–599.

Robinson, S. L., & Morrison, E. W. (2000). The development of psychological contract breach and violation: A longitudinal study. *Journal of organizational Behavior, 21*(5), 525–546.

Rousseau, D. M. (1989). Psychological and implied contracts in organizations. *Employee Responsibilities and Rights Journal, 2*(2), 121–139.

Russo-Spena, T., Tregua, M., & De Chiara, A. (2016). Trends and drivers in CSR disclosure: A focus on reporting practices in the automotive industry. *Journal of Business Ethics,* 1–16.

Sheehan, K. B., & Hoy, M. G. (2000). Dimensions of privacy concern among online consumers. *Journal of Public Policy & Marketing, 19*(1), 62–73.

Smith, N. C., Goldstein, D. G., & Johnson, E. J. (2013). Choice without awareness: Ethical and policy implications of defaults. *Journal of Public Policy & Marketing, 32*(2), 159–172.

Stohl, C., Etter, M., Banghart, S., & Woo, D. (2015). Social media policies: Implications for contemporary notions of corporate social responsibility. *Journal of Business Ethics*. doi:10.1007/s10551-015-2743-9

Target. (2016). Privacy policy. http://www.target.com/spot/privacy-policy. Accessed May 25, 2016.

Tom, G., Barnett, T., Lew, W., & Selmants, J. (1987). Cueing the consumer: The role of salient cues in consumer perception. *Journal of Consumer Marketing, 4*(2), 23–27.

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

Walker, K. L. (2016). Surrendering information through the looking glass: Transparency, trust, and protection. *Journal of Public Policy & Marketing*, *35*(1), 144–158.

Zhou, W., & Piramuthu, S. (2015). Information relevance model of customized privacy for IoT. *Journal of Business Ethics, 131*(1), 19–30.