J. of the Acad. Mark. Sci. (2017) 45:135–155
DOI 10.1007/s11747-016-0495-4

CONCEPTUAL/THEORETICAL PAPER

The role of data privacy in marketing

Kelly D. Martin[1] · **Patrick E. Murphy**[2]

Received: 13 April 2016 / Accepted: 30 August 2016 / Published online: 22 September 2016

Abstract This paper captures the current state of privacy scholarship in marketing and related disciplines. We examine theoretical perspectives and empirical findings about data and information privacy grouped according to privacy's role in society, the psychology of privacy, and the economics of privacy. Although a coherent subset of research themes provide deep understanding, theoretical and empirical findings show this narrow focus also has constrained our view of privacy to consumer, organizational, ethical, or legal silos. In response, we take a necessary step toward expanding the privacy domain across these borders, emphasizing the compelling synergies that span multiple interests. We conclude by highlighting future research themes that embody a multidimensional approach, which blends the many interconnected concerns that feature in contemporary privacy questions in marketing. Since internal and external stakeholders are affected in multiple and potentially unforeseen ways by data privacy issues, additional work in this space remains critical and needed.

Keywords Privacy · Big data · Ethics · Review article

Effects of widespread access to consumers' personal information are many, including vulnerability to fraud, privacy invasions, unwanted marketing communications, and highly targeted, obtrusive marketing communications that disrupt the rhythm of day-to-day activities. More often, though, the benefits to consumers deriving from information use initiatives are widely touted. Sophisticated use of consumer data allows for personalized product offerings and recommendations, price discounts, free services, and more relevant marketing communications and media content. Marketers, in theory, can pass along additional benefits to consumers because they are able to operate more efficiently with better information. These trends have led to a heightened focus on consumer privacy by academic researchers, social critics, and regulators, yet the costs and benefits to marketers and consumers are substantial and warrant further investigation. As such, we draw from the vast marketing literature on privacy and consumer data use (as well as from information systems, the law, ethics, and other disciplines) to capture what we know, and what remains to be understood in this space.

Our research motivation derives from observations that generally show that marketing practice using consumer data and analytics has advanced at a more rapid pace than has marketing academic scholarship. Specifically, we argue that in reality the meaningful questions have shifted from whether consumers are willing to disclose their private information to how consumers react now that their private information is widely accessible and available to a host of marketers and other interested parties. A respondent from a recent Pew survey on privacy commented:"I share data every time I leave the house, whether I want to or not. The data isn't [*sic*] really the problem. It's who gets to see and use that data that creates problems. It's too late to put that genie back in the bottle" (Rainie and Duggan 2016, p. 9).

Although there is no widely agreed upon definition of privacy (see Table 1), nor is it necessarily possible to define (argued by some privacy scholars [e.g., Solove 2008]), we agree with perspectives that assert its fuzzy definitional nature

✉ Kelly D. Martin
kelly.martin@colostate.edu

Patrick E. Murphy
Murphy.72@nd.edu

[1] College of Business, Colorado State University, Fort Collins, CO 80523-1278, USA

[2] Mendoza College of Business, University of Notre Dame, Notre Dame, Indiana 46556, USA

Table 1 Selected privacy concepts and definitions

Construct	Defintion	Source/Exemplary studies	Additional insights
Selected privacy definitions	State or condition of being free from being observed or disturbed by other people.	Oxford English Dictionary	Common lay definition of privacy in general.
	The right to be left alone.	Warren and Brandeis (1890)	Famous judicial definition, although a standalone U.S. Constitutional right does not exist.
	Privacy as a state of limited access to a consumer's information.	Westin (1967)	State of privacy can be defined as a goal worth attaining and preserving. Substates of privacy include anonymity, solitude, reserve, and intimacy.
	The selective control of access to the self.	Altman (1975)	One of the first definitions of privacy to feature centrally on the individual's ability to exercise some form of control.
	Claim to appropriate flows of personal information within distinctive social contexts.	Nissenbaum (2010)	Advocates for constraints on information flow depending on context, rather than a focus on determining whether the consumer setting or the information itself is private or public.
Consumer information privacy	Privacy as related to control of the dissemination and use of consumer information including, but not limited to demographic, search history, and personal profile information.	Foxman and Kilcoyne (1993); Nill and Aalberts (2014)	Privacy as relavent to people in the sphere of marketing. Violations of consumer privacy include, but are not limited to unwanted marketing communications, highly targeted advertisements, and surreptitious online tracking.
Privacy concerns	Proxy for measuring consumer privacy. Operationalized as consumers' beliefs, atttitudes, and perceptions about their privacy.	Malhotra et al. (2004); Smith et al. (1996)	Measured through the consumer privacy concern scale (Smith et al. 1996), also via an online focused version (Malhotra et al. 2004). Cast as antecedent, consequence, and moderating force in a number of early privacy studies.
Big data	Popular term referring to the extent to which vast information, often about individual consumers, is captured and used by various organizations to better understand and predict behavior.	Goodman (2016); Tirunillai and Tellis (2014)	Big data has become popular vernacular for use of consumer information and marketing analytics. While what constitutes "big" data remains somewhat questionable it is widely agreed that data becomes "big" on dimensions of volume, velocity, variety, and veracity (Gartner Report 2012).
Privacy paradox	The relationship between individuals' intentions to disclose personal information and their actual personal information disclosure behaviors.	Aguirre et al. (2015); Norberg et al. (2007)	Commonly used term to convey the disconnect between consumers' stated privacy preferences and their actual behavior. People commonly report being greatly concerned about privacy, yet divulge their sensitive personal information rather freely.
Privacy failure	Broad term for any organizational lapse that can compromise consumer information, including but not limited to a data breach, hacking intrusion, or company loss of information.	Malhotra and Malhotra (2011); Martin et al. (2016)	Most often investigated as event study impacts on the firm in question. Chronicled by company, industry, size and scope by reporting agencies such as privacyrights.org.
Privacy self-regulation	Common terminology for the ability of organizations to police their own privacy safeguards.	Bowie and Jamal (2006); Conitzer et al. (2012)	Much more strongly advocated among U.S. institutions as opposed to European countries. Mathmatical and economic studies sometimes model the parameters of self-regulation versus greater government intervention on consumer privacy questions.
Privacy as strategy	Terminology for the firm phenomena of using their consumer information protection approaches as competitive differentiation.	Casadesus-Masanell and Hervas-Drane (2015); Martin et al. (2016); Rust et al. (2002)	As consumer information use grows in parallel with consumer anxiety about such practices, the ability of firms to successfully compete on dimensions of privacy protection becomes attractive. The current study offers a set of tenets for doing so.

should not preclude studying privacy (i.e., Nissenbaum 2010). This paper draws from perspectives related to information privacy (e.g., Foxman and Kilcoyne 1993; Nill and Aalberts 2014) germane to organizations' access, use, dissemination, and protection of consumer personal data for marketing purposes. We begin with an overview of common theoretical perspectives that have laid the foundation for data privacy scholarship. This discussion details which conceptual

frameworks show the most potential to advance thinking. Integrated into this analysis, we extract several key emerging themes and disentangle their findings to highlight relationships among constructs within common theoretical approaches. In doing so, we offer a broad review of the privacy literature in marketing and related disciplines. Taking what we have learned collectively, we then transition our discussion to the imperative of conceptualizing privacy as meaningful to consumers, organizations, and regulators synergistically. We conclude with a future research agenda, emphasizing neglected questions and offering ideas for contributing to marketing scholarship in this critical domain.

Our research provides three key contributions beginning with a deep analysis of past privacy scholarship. Specifically, we ask, *what have we learned from the various theoretical foundations and empirical findings that underpin the vast privacy research literature*? Drawing from commonly used frameworks we find that, by-and-large, privacy theories have been applied in contexts specific to the consumer, the organization, or to broader ethical theory. We reconceptualize this organization into theory and findings related to the role of privacy in society, the psychology of privacy, and the economics of privacy (see Table 2 and Fig. 1). Through these various theoretical lenses, we deconstruct individual findings across research studies to understand commonly studied privacy relationships and effects. We use this review to advocate for a broader approach and describe how earlier research can be substantially enriched by a multidimensional focus on consumer, organizational, and ethical/legal relationships. This research imperative is grounded in our literature review, bringing together privacy scholarship across several decades and disciplines.

Our second contribution unfolds by addressing the question, *how might we synthesize consumer, organizational, and ethical/legal perspectives to develop a more holistic understanding of privacy in marketing*? To accomplish this task, we spend considerable effort on synthesizing these domains and building upon unanswered questions. For example, we investigate the salient themes involved with some firms' recent attempts to differentiate or position themselves on privacy relative to competitors. We explore this question more deeply as but one topical example of how understanding privacy intersections can greatly enrich marketing theory and practice.

Given all that we know about privacy across multiple disciplines, we finally offer an agenda for future research. We provide ideas about promising next questions and important research gaps in this space. We ask, *what questions remain about privacy at consumer, organizational, ethical, and legal intersections*? It is evident from past research that privacy scholarship has provided substantial insights on a range of topics. Yet, the speed at which privacy questions are arising warrants fresh thinking around issues especially salient to today's consumers and organizations. Hopefully, our future research ideas help steer scholarship in directions most meaningful to enhance data privacy theory and marketing practice.

Privacy in society

Privacy often is cast as an individual "right," and discussions about the "right to privacy" are common. Although Warren and Brandeis (1890) famously advocated for a right to be left alone, a standalone Constitutional right to privacy does not exist. The United States Bill of Rights embeds privacy protections into a number of Amendments (e.g., the First, Third, Fourth, and Fifth). Interestingly, protections that resemble a right to privacy have been observed across the courts and treated with great importance in the American justice system (Langenderfer and Miyazaki 2009). However, in the absence of a dedicated privacy right, federal regulators have been reluctant to enforce privacy protections across companies and governmental entities (Solove 2011). To date, questions surrounding whether and how the federal government ought to intervene (and if so, how to intervene effectively) remain challenging for key regulatory bodies such as the Federal Trade Commission (FTC). The FTC, which has emerged as the key governing body in the context of consumer information privacy issues, currently applies information privacy protections using two frameworks that include the Notice-and-Choice Model comprised of Fair Information Practice Principles (FIPPs), and the Harms-Based Model that pivots on whether physical or economic harm results to consumers from organizational misuse of (or more often, neglect or failure to protect) personal information (Ohlhausen 2014).

From 1970 until 1993, thirteen different privacy-related regulations were passed by Congress (Caudill and Murphy 2000). Since the mid-1990s, only the Children's Online Privacy Protection Act of 1998 and the Gramm-Leach-Bliley Act of 1999 that requires financial institutions to explain their information-sharing practices to their customers and to safeguard sensitive data have been passed. The FTC issues regular reports regarding privacy, but this is a nonbinding effort by the Commission to spur more responsible behavior by marketers. In the same vein, the White House (2012) published an extensive report that included a seven-point "Consumer Privacy Bill of Rights" linked to the FIPPs. In 2014, it followed those efforts by releasing a report focused on big data that emphasized student information privacy, company notification in the event of a data breach, and investigated big data in the context of price discrimination (White House 2014). Like the FTC efforts, the White House initiatives have focused attention, discussion, and funding, but have led to no new consumer privacy regulations.

Table 2 Theoretical perspectives of privacy: select consumer and organizational frameworks and findings

Theoretical framework	Key constructs	Definitions	Key findings	Example studies
Social Contract Theory	privacy norms and expectations; stakeholders; information control and disclosure	Organizations complete marketing transactions with consumers, doing so in a way that enhances future exchange, potentially creating conditions that lead to long-term relationships (Caudill and Murphy 2000). Social contract theory suggests a moral contract governs the basic tenets and agreements that exist between a society and an individual (Dunfee et al. 1999). Firms should adapt practices to meet stakeholder privacy norms (Maignan and Ferrell 2004).	Organizations can fail to uphold social contracts with consumers through privacy violations and privacy failures. Using the FTC's guidelines for information privacy provides a rubric against which to assess whether a firm upholds its privacy obligations (i.e., the social contract). Privacy policies are a necessary but not sufficient condition of the exchange. Consumers believe marketers have upheld their side of the social contract when the firm provides them greater value through personalized offerings or tangible monetary compensation.	Gabisch and Milne (2013); Martin (2015); Phelps et al. (2000)
Justice Theory	fairness; privacy processes; privacy outcomes; firm ethical behavior	Justice theory typically is dimensionalized across procedural and distributive aspects. Distributive justice was originally conceptualized to consider socially just distribution of goods across a society (Rawls 1971), but in marketing exchange more commonly refers to consumer perceptions of fairness resulting from the exchange. Procedural justice involves fairness perceptions related to the manner by which exchange outcomes were determined.	Procedures designed to protect consumer privacy represent the procedural justice dimension, whereas outcome of a privacy-relevant marketing exchange represent the distributive justice dimension. Fair information access and use practices typify procedural justice in this space. Policies perceived as fair can alleviate privacy concerns, promote trust and disclosure, and reduce falsifying behaviors. Distributive justice through beneficial outcomes also creates consumer benefits including customized offerings, personalization value, convenient customer-firm interactions, and access to free services. With high levels of distributive justice, consumers are more likely to relinquish some privacy and even accept mild privacy violations such as highly targeted advertising.	Ashworth and Free (2006); Culnan and Bies (2003); Vail et al. (2008)
Power-Responsibility Equilibrium Theory/Control Theory	withholding and protecting behaviors; information falsification; information sensitivity	The power-responsibility equilibrium model (PRE) stipulates that social power and social responsibility should be interconnected (Murphy et al. 2005), where the more powerful partner in a relationship has the societal obligation to promote an environment of felt equality (trust and confidence).	Consumers react defensively to perceived imbalances in power (i.e., threats to their information privacy). As such, they may fail to disclose information or falsify information they do provide to a firm. Findings suggest that marketer requests to consumers for private information are influenced by firm policy and legal regulation, and even the manner in which the organization requests the information. Robust corporate privacy policies as well as greater consumer perceived control can alleviate privacy concerns, however, the nature of information sought (e.g., low vs. high sensitivity) can further influence this relationship.	Lwin et al. (2007); Norberg and Horne (2014); Xu et al. (2012)
Social Exchange Theory	relationship type; willingness to disclose and disclosure consequences; reciprocity; trust	People rationally calculate costs, benefits, and competing alternatives prior to an exchange. Social exchange theory features a two-sided, mutually contingent and rewarding process involving a transaction or simple exchange (Emerson 1976). Social exchange theory argues that consumers will reveal personal information when perceived benefits outweigh perceived costs.	Consumers view the relinquishing of their personal information in the context of what the firm provides them in exchange. Social norms and reciprocity behaviors are shown to underpin such exchanges, where customers more freely divulge information, or endure targeted advertising, in exchange for benefits. Benefits include personalized marketing offerings, or even free services. Recent work shows consumers increasingly view enduring more frequent marketing communications and targeted ads as a quid pro quo for marketer provided services of value. Trust in the organization further enhances this effect.	Chellappa and Sin (2005); Schumann et al. (2014); White (2004)

Table 2 (continued)

Theoretical framework	Key constructs	Definitions	Key findings	Example studies
Reactance Theory	personalization; targeted advertising; click-through; control	Reactance represents an individual response to a consumption situation in which choice or decision freedom is constrained. The restricted choice becomes more attractive with the stipulation that the consumer reasonably expects free choice and freedom is important. If these conditions are met, consumer motivational arousal should occur to restore the freedom violations s/he perceives (Brehm 1966).	Complying with marketing goals such as purchase, information disclosure, or click-through improves when consumers perceive freedom of choice and/or control. When these attributes are constrained or unavailable, reactance can surface mitigating beneficial marketing outcomes. Trust, credibility, and the value of the marketer benefit can reduce reactance. Privacy concerns heighten reactance. Privacy research has demonstrated a level of reactance from marketer information approaches that compromise privacy (i.e., constrain freedom). Control appears to be a strong restorative factor, acting to empower the consumer and making her/him more receptive to marketing efforts.	Bleier and Eisenbeiss (2015a), b); Tucker (2014); White et al. (2008)
Behavioral Decision Theory	information disclosure; purchase behavior privacy valuation; contextual cues	Behavioral decision theory involves social psychological perspectives related to how consumers make decisions under complex circumstances (Kahneman 2003). Types of behavioral decision theory involve choice under risk and uncertainty, and decisions with information asymmetries. In consumer information privacy research, contextual cues influence risky, uncertain, and information asymmetric decisions with privacy implications such as whether to reveal information to a marketer.	Consumer perceptions and behaviors related to privacy are influenced by rational calculus across various dimensions. For example, perceived vulnerability and perceived control can determine privacy concerns related to access and use of personal information. Behavioral decision theory examines contexts where privacy concerns become more or less salient, such as when others have revealed information or when cues about marketer professionalism or question sequencing can influence decisions to reveal. Contextual cues and priming also can determine whether and to what extent consumers are willing to pay to protect their privacy.	Acquisti et al. (2013); Dinev and Hart (2004); Mothersbaugh et al. (2012)

Global privacy perspectives

The European Union (EU) Data Protection Directive (updated in 2015) represents a considerably more extensive set of consumer information privacy protections than any U.S.-based efforts. The EU Directive mandates a single set of data protection rules, holding companies accountable for privacy-relevant behaviors to a single regulating authority. Moreover, under the parameters of a "right to be forgotten," consumers in the EU may request removal of web links that no longer provide accurate personal information. After some negotiation as to how business and consumers would be affected by the EU directive, the EU-U.S. Privacy Shield was derived as follows: "The new arrangement will provide stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities" (European Commission 2016). Although U.S. companies reported much concern about stringent European regulations on them directly and indirectly by potentially creating discontent among American consumers, widespread requests to be forgotten, as one manifestation of the EU Directive, have not yet materialized to create harm for U.S. firms (Manjoo 2015). As such, the default mechanism toward promoting industry self-regulation in the context of consumer information privacy concerns remains the de facto approach embraced by both U.S. regulators and companies.

Global privacy research, including studies of how privacy preferences and practices vary cross-nationally, remains underdeveloped. Limited findings show that cultural values can influence people's privacy perceptions such that countries with tighter privacy regulations experience fewer privacy problems (e.g., Dolnicar and Jordaan 2007). Similarly, when firms lack privacy regulations, consumers report greater

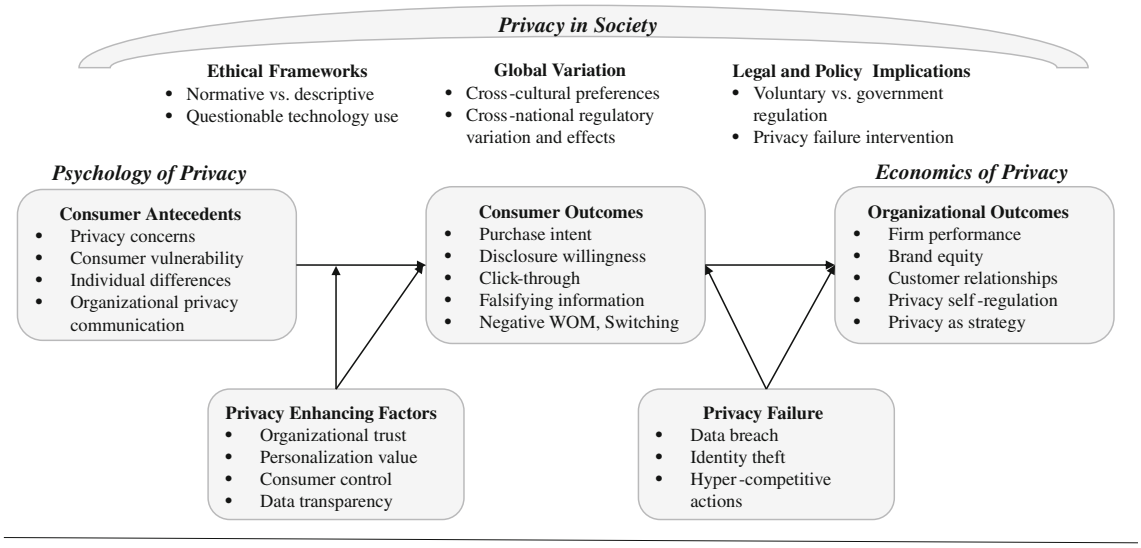

Fig. 1 Data privacy research in marketing: predominant constructs and relationships

dissatisfaction and desire for government intervention related to privacy (Milberg et al. 2000). Greater regulation can have a downside, however. In a natural experiment comparing pre- and post-policy implementation of the EU Data Protection Directive, researchers found that advertising effectiveness (measured through stated purchase intent) was significantly diminished in the EU after the policy. Yet, non-EU nations saw no change in effectiveness during the same time, showcasing the role of policy interventions on consumer marketing outcomes (Goldfarb and Tucker 2011b).

Clearly, additional global research examining privacy similarities and differences at both the consumer and the organizational level across international populations is needed. Much of our understanding about privacy across consumer, organizational, and legal/ethical domains is limited to U.S. and European samples. Although European consumers show a higher level of privacy concern, with subsequent regulation to protect such concerns by EU lawmakers, much formal knowledge about consumer privacy has a distinct Western flavor. Of course, an important missing space involves privacy issues in Eastern, more collectivist cultural societies such as India[1] and China. In general, our understanding of privacy concerns and approaches at the consumer and organizational level among BRIC countries, as well as in still-developing markets, is largely absent. Investigation of both cross-national and cross-cultural variation in privacy preferences and beliefs represents a needed area of future research.

The ethics of privacy

Over two decades ago, Bloom et al. (1994, p. 103) proposed two key questions which marketers ought to consider:

1. Should a company be allowed to acquire and store information about individuals without their knowledge or consent?
2. Should a company be allowed to disclose information about individuals to other parties without their knowledge or consent?

Although this debate remains unresolved in the literature (see Table 3), marketers nonetheless have responded as though they were granted access to personal information and permission to disclose, currently capturing, storing, and selling vast amounts of consumer data (Singer 2012). In their widely cited ethical evaluation of privacy in marketing, Foxman and Kilcoyne (1993, p. 106) advise: "marketers must make an active commitment to ethical behavior in this area if restrictive legislation is to be avoided." Although firms in the twenty-first century have largely staved off sweeping regulation of their information collection and use practices, researchers continue to consider how marketers should operate in this domain (Laczniak and Murphy 2006). Many stakeholders (i.e., businesses, consumers, policymakers, and advocacy groups) are invested in the parameters of information exchange and, as such, have a stake in the exchange rules and norms of consumer information access, protection, and use. Stakeholder norms surrounding privacy concerns, such

[1] An excellent example involves Indian citizens' widespread rejection of the Free Basics initiative by Facebook, which offered people limited access to the internet, including Facebook and select other websites. Mass protests occurred in the country to advocate for net neutrality and open access for all. This outcome surprised many experts who viewed the offer as an important step toward connectivity for the poor. Facebook has launched, or plans to launch Free Basics in more than 30 other developing and impoverished countries (BBC News).

Table 3 Consumer and organizational privacy perspectives: selected recent literature

Author(s)	Year	Outcomes	Influences	Key takeaways
Aguirre et al.	2015	vulnerability, click through	personalization value; overt/covert data collection; reliability and benevolence (i.e., trust-building cues)	Personalization leads to greater click-through when firms use overt (vs. covert) information collection. When covert information collection is made salient, consumers feel more vulnerable. Effects vary by trust and website credibility.
Bleier and Eisenbeiss	2015a	click-through intention	personalization depth and breadth; usefulness, reactance, privacy concerns, trust	In the context of online retargeting advertising, this research uses a pilot test (quasi-experimental field study) and a lab experiment to show that trust moderates personalization's influence on click-through. Personalization affects click through via privacy concerns, reactance, and usefulness.
Casadesus-Masanell and Hervas-Drane	2015	firm price setting; information disclosure practices	customer privacy preferences; competition	Theoretical model and advances propositions that analyze strategic interactions generated by consumer information provision and firm disclosure of that information to advertisers. Results suggest privacy can soften the intensity of competition when consumers are heterogeneous so that firms can effectively differentiate in their privacy policies and their willingness to pay is not so high that firms may operate profitably.
Martin	2015	consumer privacy expectations	privacy policy information content (information type, secondary use, personalization, storage, collection)	Through two studies with nearly 1000 consumers, this article examines the usefulness of privacy policy content in alleviating consumer concerns. Findings show privacy notices provide a necessary but not sufficient condition for meeting consumers' privacy expectations. Examines the specific reasons privacy notices fail to address consumer privacy expectations.
Sen and Borle	2015	privacy failure (data breach)	contextual risk factors (geographic location; industry; past breach)	Data breach risk can vary by industry. Investment in greater information technology (IT) security increases likelihood of a breach. Authors extend this thinking to suggest IT security not managed appropriately.
Nill and Aalberts	2014	online behavioral targeting	legal and ethical challenges	Online behavioral targeting (OBT) is the tracking of a consumer's online activities in order to develop a behavioral profile of the consumer. This article examines the tradeoffs that imply greater benefits for consumers, while simultaneously having the potential to violate their privacy to a larger degree. The article considers both legal and ethical implications.
Norberg and Horne	2014	consumer information falsification; disclosure	perceived control; elicitation style; disclosure experience; privacy concerns	This study attempts to understand the drivers and mitigators of consumer information falsification behavior when interacting with online firms. Companies' elicitation strategy (voluntary, required, validated) influences how consumers emotionally respond to and behaviorally cope with (through falsification) requests for information; falsification partially mediates pre-to-post disclosure control perceptions.
Romanosky et al.	2014	privacy failure lawsuits	nature of privacy failure (data breach); type of firm reparative action	Court dockets from 230 federal data breach lawsuits from 2000 to 2010 are examined. This research asks which breaches are being litigated and which breach lawsuits are settling? When individuals suffer financial harm, litigation is more likely, however providing free credit monitoring can mitigate litigation odds. Extrapolates results to privacy regulation versus privacy litigation question.
Schumann et al.	2014	acceptance of targeted advertising	reciprocity; relevance; advertising clutter; informativeness; website quality and utility	Through an experiment and two field studies, this research shows that users accept targeted advertising as a form of repayment to a firm for using its free services. Consumers view targeted advertising as a type of of online currency they can use to repay a website for benefits received, evidencing reciprocity. Find that reciprocity is more appealing to consumers than utilitarian arguments (i.e., use free services in exchange for targeted ads rather than: targeted ads provide you more value).
Tucker	2014	advertising outcomes in the form of click-throughs	targeted versus nontargeted ads; personalized versus nonpersonalized ads; privacy controls	This study used personalized versus nonpersonalized (and targeted versus nontargeted) ads for a nonprofit on Facebook; people responded more favorably to the personalized ads when they had the ability to control their privacy settings on Facebook. Participants were provided

Table 3 (continued)

Author(s)	Year	Outcomes	Influences	Key takeaways
				these controls midway through the study and subsequently, click through on personalized ads improved.
Gabisch and Milne	2014	consumer privacy expectations (information ownership, privacy control)	financial compensation; information ownership; information sensitivity	This paper asks who owns customer data, and whether consumers feel they have benefitted sufficiently from online personalization, customized services, etc. in exchange for their information. Two online experiments show that when compensated monetarily for their information, consumers are more likely to give companies the ownership of their data.
Acquisti et al.	2012	admission rates; propensity to disclose	proportion of affirmative responses (high versus low); question order and type	Research that demonstrates people are willing to disclose increasingly sensitive information when they believe others have done so. People disclose sensitive information more freely when queries are placed at the beginning of a questionnaire, as opposed to random or end placement, contrary to conventional wisdom. Priming with privacy concerns also changes the effect.
Brandimarte et al.	2012	willingness to disclose information	control over release of information; control over access to information	This article posits a control paradox, whereby consumers give up more information when they have stronger perceptions of control. Sometimes, they provide suboptimal levels of private information when they perceive greater control. These consumers may end up more vulnerable as a result of the measures designed to protect them.
Conitzer et al.	2012	firm initial and future price setting	willingness to pay for privacy	Research offers an empirical model and advances propositions that suggest a firm receives its highest profits when consumers can freely maintain anonymity, but that consumers benefit the most when anonymity is costly up to a point; third party privacy gatekeepers also worked to the detriment of consumers as they negotiated with firms to make anonymity free.
Goldfarb and Tucker	2012	willingness to reveal personal information	consumer age, over time (2001–2008)	Authors examine how consumer privacy regulations and protections have evolved along with firms' increasing intensity of data use. Using millions of consumer responses between 2001 and 2008 they find that users are less likely to reveal information over time (greater refusal rates), and older people are much less likely to reveal personal information.
Mothersbaugh et al.	2012	willingness to disclose online	online privacy concern; perceived control; perceived customization benefits; perceived risk; firm trust; information sensitivity	Information control and customization benefits increase willingness to disclose overall; online privacy concern did not decrease willingness to disclose; perceived risk and firm trust may suggest differential effects of disclosure antecedents across varying levels of sensitivity. Examines moderating role of information sensitivity on various willingness to disclose antecedents.
Xu et al.	2012	privacy concerns	privacy protecting strategies (personal and proxy agency control); perceived information control	This research examines different models for assuring consumer privacy in the context of location based services. Namely they consider whether self-protection, industry self-regulation, and government legislation, separately and in combination with consumer perceived control, influence privacy concerns. They find that customer perceived control is the mechanism through which these approaches can be effective.
Goldfarb and Tucker	2011a	ad recall; purchase intentions	website content ad matching, obtrusiveness; privacy concern; product category	Independently, matching ad to website content and ad obtrusiveness increase purchase intent. In combination, the two strategies are ineffective. The authors suggest that this result may be driven by consumer privacy concerns. Making privacy concerns salient may increase sensitivity to ads with manipulative intent.
Goldfarb and Tucker	2011b	purchase intentions	advertiser ability to target; context (EU, non EU)	In the context of the EU Privacy and Electronic Communications Directive, this article examines consumer privacy with targeted online advertising. Research finds that ad effectiveness decreased substantially (measured through stated purchase intent) in these countries after the Privacy Directive, whereas non-EU nations saw no significant change during the same timeframe.
John et al.	2011	information admission rates		Through four experiments, these researchers show that contextual information encouraged greater or less

Table 3 (continued)

Author(s)	Year	Outcomes	Influences	Key takeaways
			intrusiveness; questionnaire interface; privacy policy cueing	disclosure, including both intrusiveness and the professional/unprofessional look of a website. Interestingly, priming with a privacy statement decreases disclosure.
Malhotra and Malhotra	2011	firm performance	privacy failures (data breach); breach magnitude; firm size	Examining data breaches across firms, authors find that firm market value is negatively affected by a breach in both the short and long term, but more detrimental in the long term (contrary to past data breach research). According to this study larger companies suffer greater market value loss than smaller firms, and bigger ones suffer more from large breaches.
Romanosky et al.	2014	customer identity theft	privacy failure (data breach) disclosure laws	Panel data from U.S. FTC is used to study whether data breach disclosure laws actually reduce identity theft (2002–2009). On average, these statutes reduce identity theft caused by breaches by 6 %. Evidence of effectiveness of a particular privacy protecting law.
Tsai et al.	2011	purchase behavior	privacy information display (prominence, accessibility)	Participants in privacy information condition are more likely to purchase from websites offering medium or high levels of privacy, even when those sites charged higher prices (using experimenter money); control condition participants purchased from lowest priced vendor; overall, consumers may be willing to pay a premium for privacy.
Milne and Bahl	2010	privacy boundary preference	privacy boundary expectations; opt-in/opt-out; technology type; marketer vs. consumer	Compares privacy preferences between marketing managers and consumers to uncover synergies or disconnects. The authors find that consumers are more likely to choose closed boundaries than marketers, yet marketers wished exchange interactions were subject to permission boundaries; database marketers are much less aligned with consumers than general marketing managers; the restricted consumer segment is far less accepting of various technologies, yet the receptive group was even more accepting than the marketing managers to new technologies.
Culnan and Williams	2009	firm privacy protection	ethics and privacy practices embodied by the firm	This research argues that consumers inherently lack sufficient knowledge and control over the ways in which firms use their personal information; as such, companies have a moral obligation to customers to protect their privacy; conceptual analysis illustrates with case studies of TJX and ChoicePoint data breaches.
Wirtz and Lwin	2009	preventive and promotive behaviors surrounding willingness to disclose	fairness perceptions; trust; privacy concern	Privacy concern and trust are ways that firms can promote consumer information disclosure and relationship formation; privacy concern mitigates negative behaviors like falsifying information or negative WOM. Privacy concern reduction is reactive and trust is promotive as mechanisms that link justice theory dimensions and online behaviors.
Miyazaki	2008	consumer trust; purchase intent; recommendations	firm disclosure of cookie use; consumer online experience (high/low); privacy concern	Using website data from 2000 to 2007, the author finds that cookie use is increasing, but firm disclosure of this activity also is increasing. Consumer trust, purchase intent, and WOM decrease when cookie use is hidden, but disclosing cookie use can attenuate those effects. In a third study consumer online experience and privacy concern effects trust, usage intent, and WOM.
Vail et al.	2008	consumer confidence, security, and protection from privacy policies	privacy policy characteristics; typical versus atypical privacy policies	Privacy policy comprehension is low when consumers attempt to interpret a traditional privacy policy. Comprehension improves for nontraditional or atypical privacy policies, however, consumers simultaneously view these as being less trustworthy than more traditional, lengthy paragraph form.
White et al.	2008	reactance	email personalization; service utility	Highly personalized email communications that do not justify the basis for the strong personalization are more likely to create reactance in consumers. However, this effect differs by whether consumers perceive high utility of the product/service. High utility can alleviate personalization without justification effects, whereas low utility perceptions cannot.

Literature table begins at 2008 where recent marketing privacy reviews have left off (e.g., Lanier and Saini 2008)

as those related to consumer data collection and use, are gaining in prominence and firms violate such norms at their own peril (see Maignan and Ferrell 2004 for an excellent overview of the stakeholder perspective in marketing).

An important example, social contract theory stipulates that rules of consumer information sharing should account for the exchange purpose, risk, and potential harms to the consumer. A key backdrop against which social contract theory has been applied to privacy research in marketing involves the FTC's information principles. Although the FTC's domain is clearly the realm of public policy, the FIPPs have become a tangible representation of the firm's side of the social contract with consumers regarding the capture, use, sharing, and protection of their information. Research finds that although firms tend to fulfill obligations of notice and choice, other salient FIPP dimensions including information sharing or access, and security are underdeveloped (Sheehan 2005). Social contract theory research in the privacy space also finds that marketers need to go further in establishing perceptions of exchange fairness. Consumers are more likely to believe marketers have fulfilled their side of the social contract governing information exchange when they perceive greater personalization value from the exchange (Chellappa and Sin 2005), or when the firm financially compensates them for their information (Gabisch and Milne 2014). Consumer privacy literature positions fairness as key to marketers' ability to fulfill the social contract governing information exchange (Culnan and Bies 2003).

Related to social contract theory's view of fairness, justice theory often is dimensionalized across procedural and distributive aspects when applied to data privacy (Ashworth and Free 2006). Procedures implemented to protect information exchange fairness and consumer outcomes comprise the basic tenets of justice theory in this domain (Culnan and Armstrong 1999). Distributive justice theoretical outcomes include any benefits consumers receive as a result of providing their personal information and, hence, risking their privacy. Common outcomes are customized offerings, personalization value, streamlined customer–firm interactions, access to free services, and even financial compensation. Consumer privacy literature has begun to show people value these outcomes and are increasingly willing to provide their information as quid pro quo (Schumann et al. 2014). In spite of findings in support of distributive justice, the literature also notes a parallel privacy paradox implying that consumers value these marketer provided outcomes while at the same time experiencing feelings of vulnerability in relinquishing personal information (Awad and Krishnan 2006).

Fair information policies, as typified by the procedural dimension of justice theory, have been shown to effectively alleviate consumer privacy concerns and provide companies maximum benefit. Consumer perceptions that a firm's privacy practices are fair promote trust and enhance willingness to provide information, while simultaneously reducing negative behaviors including falsifying information and negative word-of-mouth—key variables that form consumer privacy literature's foundations (Wirtz and Lwin 2009). Conversely, complex privacy policies that reduce consumer comprehension are viewed as being less fair and, accordingly, diminish confidence and trust in the firm (Vail et al. 2008). Procedural justice literature often involves firms' privacy policies and consumers' interpretation of them. Collectively, this work finds that privacy policies have been declining in readability and increasing in complexity over time (Milne et al. 2006), but that consumers view such policies as representations of firms' procedural fairness and hence, desire straightforward policies that help them understand how their information is captured, used, protected, and shared (Vail et al. 2008).

Additional ethical perspectives show potential to enhance understanding of privacy. For example, the power-responsibility equilibrium model derived from Murphy et al. (2005) advocates for a connection between social power and social responsibility, where a powerful partner is obligated to protect and promote felt equality of the less dominant partner. As applied to marketer–consumer privacy questions, research suggests consumers react negatively to power imbalances where firms fail to promote felt equality in information exchange (Lwin et al. 2007). In marketing, ethical theory development and analyses to further disentangle contemporary data privacy questions, in an effort to advise how marketers *should* manage those concerns, are needed. For example, the Ferrell and Gresham (1985) model of ethical decision making could aid understanding by bridging the societal concerns over information use with the roles of firm opportunity and individual behavior in treating consumer information responsibly.

Psychology of privacy

Unlike foundations that underpin the role of privacy in society, which have coalesced around a few frameworks, theories advanced to explain the psychology of consumer privacy are far more disparate. This difference in framework cohesiveness likely stems from the fact that the societal perspective is largely concerned with what marketers ought to do, whereas the psychological perspective must grapple with the vast number of highly nuanced ways that consumers can interpret privacy-laden questions. We overview a handful of the more commonly used (but not exhaustive) social psychological approaches and findings to explain data privacy as organized by privacy concerns, privacy outcomes, and enhancing forces that can influence the way in which consumer perceptions may shift in relation to determinants or consequences.

Consumer privacy concerns

Much literature has focused on understanding and measuring privacy concern as a consumer psychological construct. Privacy concern surfaced as a best proxy for understanding consumers' feelings about their information privacy. Multiple measurements of privacy concern have been advanced over the years, and it has been investigated together with a variety of drivers and outcomes. In the first, well-established measure of people's self-reported worry about privacy Smith et al. (1996) offer a multidimensional scale that includes concerns across (1) information collection, (2) unauthorized secondary use (internal and external), (3) improper access, and (4) error protection. Their scale was updated in 2004 to more purposefully consider dimensions of consumers' information privacy concerns in an online realm (Malhotra et al. 2004). This measurement-focused work, mainly published in information systems journals, has received more limited adoption and use in the marketing literature. Early privacy research in marketing favored direct questions to consumers in various contexts (e.g., Phelps et al. 2000). For example, Sheehan and Hoy (2000) developed measures inspired by the FTC's core privacy principles advanced in 1998, to study privacy concerns. Specifically, these authors use a set of instruments that span the dimensions of (1) awareness of information collection, (2) information use, (3) information sensitivity, (4) familiarity with entity, and (5) compensation.

Because it was widely considered the best approach to gauge consumer feelings, particular privacy concern measures are widely examined both as a focal outcome (e.g., Dinev and Hart 2004) and predictor variable (e.g., Milne et al. 2004) up to about 2010. As a predictor variable, consumers' heightened privacy concerns often are linked to a number of common information privacy outcomes including willingness to disclose information and purchase intention. However, findings that privacy concerns diminish disclosure and purchase intention are much more nuanced than intuitive, which on the surface may appear to deter consumer–organization interaction. Although early work found greater concern led to increased negative consumer response (Sheehan and Hoy 1999), other research has found that privacy concerns are highly contextual and bounded by a number of constraining factors that include fairness perceptions (Culnan and Armstrong 1999), privacy policy strength (Lwin et al. 2007), and firm trust (Mothersbaugh et al. 2012).

As an outcome measure, privacy concerns appear to be increasing over time among both older and younger consumers, although it is increasing more sharply for older consumers (Goldfarb and Tucker 2012). Privacy concerns have been shown to diminish with stronger individual and regulatory controls (Martin 2015; Sheehan and Hoy 2000). Consumer perceived control also is a mediating mechanism through which privacy protections prove effective (Xu et al. 2012). Earlier work found that perceived vulnerability, but not perceived control, influenced privacy concerns (Dinev and Hart 2004). More recently, privacy concern is measured as an individual difference variable, with emphasis on understanding the role of felt control reported across consumer samples. Privacy concern has been conceptualized as a mediating or moderating condition in more complex investigations of information privacy relationships. In the former example, research finds that privacy concern is one mechanism through which a website's personalization promotes click-through (Bleier and Eisenbeiss 2015a). In the latter, privacy concern moderates consumers' tendency to falsify information as a result of perceived control and the company's approach to eliciting information (Norberg and Horne 2014).

Consumer privacy outcomes

Data privacy research often explores the conditions and situations where consumers are willing (unwilling) to disclose information. Social exchange theory and behavioral decision theory have gained traction in this space, with increasingly nuanced findings. Unlike social contract theory's emphasis on norms governing marketer-stakeholder privacy questions, these theories stress rational cost-benefit consumer calculations about data privacy. Specifically, consumers weigh the consequences of their personal information disclosure against the value offered by the marketer. Social exchange theory argues that consumers will reveal personal information when perceived benefits outweigh perceived costs, whereas behavioral decision theory considers consumer evaluation of losses and gains in risky decisions (Gabisch and Milne 2014). As one clear example of cost-benefit tradeoffs surrounding information exchange, Hann et al. (2007) find that U.S. consumers are willing to pay $30–45 to protect their privacy in contexts of secondary use, unauthorized access, and error. Other segments of consumers were less pragmatic and were willing to exchange personal information for greater convenience.

Additional research explores varied outcomes of consumer information exchange. One early example finds sensitive consumer information can be obtained through the technological interface of the computer, making it appear to "behave" in accordance with social norms of interaction to induce reciprocity (Moon 2000). Related findings show consumers are more likely to share private information in deeper relationships, but they are less likely to reveal private, embarrassing information in these same interactions (White 2004). Company signals, such as privacy seals (e.g., BBBOnline or TRUSTe) also increase consumers' willingness to reveal information, and promote positive perceptions about the organization (Miyazaki and Krishnamurthy 2002). Interface appearance, question intrusiveness, and the cueing of a privacy policy also can influence the extent

to which consumers are willing to provide information (John et al. 2011). A notable finding involves priming, where being made aware of a privacy policy decreases consumers' disclosure. In a subsequent study, these authors find people are willing to disclose increasingly sensitive information when they believe others have done so signaling reduced risk in disclosure (Acquisti et al. 2012). Finally, consumer perceptions of their ability to control the information they disclose, as well as realized customization benefits, increase their willingness to disclose (Mothersbaugh et al. 2012).

Related to (un)willingness to disclose information, however, is consumers' propensity to provide false information, or engage in some other negative consumer response behavior, that undoubtedly troubles firms reliant on accurate consumer information. In the context of information privacy, reactance theory can explain some consumers' response to highly targeted and personalized marketing messages they believe violate their privacy (Tucker 2014). Consumer reactions to targeted and personal marketing communications, ultimately, can manifest as communication avoidance, information falsification, derogatory word-of-mouth, or other negative behaviors (White et al. 2008). Consistent with reactance theory, these consumer responses surface as unintended contrary reactions to marketing appeals that would otherwise be likely to invoke feelings of value and personalization benefit (Goldfarb and Tucker 2011a). Consumers are more likely to negatively react when they perceive a power imbalance related to the firm's privacy practices (Lwin et al. 2007). Finally, organizational information elicitation style, increased consumer control and data transparency show promise in reducing reactance and other forms of negative consumer response (Martin et al. 2016; Norberg and Horne 2014; Wirtz and Lwin 2009).

A parallel stream of research examines purchase intentions as the focal outcome of privacy concerns, rather than information disclosure. Given the extent to which marketers can now access vast amounts of consumer information whether or not that information is voluntarily provided (Nill and Aalberts 2014), willingness to disclose appears to be declining in research prominence. Website quality and design, as well as privacy, security, and other presentation features are among the strongest factors driving purchase intent as mediated by trust (Bart et al. 2005; Schlosser et al. 2006). Privacy policy statements increase the benevolence and integrity dimensions of trust, but do not increase willingness to buy independently. However, this research and related work finds that privacy, security, and other information evaluated as most relevant and beneficial to consumers for positive purchase intent can be category specific (e.g., Miyazaki and Fernandez 2000). Slightly different results, however, occur in large field experiments which show increased purchase behavior from sites with stronger privacy policies (Tsai et al. 2011). Using actual spending data, these authors suggest that consumers may be willing to pay a premium for privacy. Goldfarb and Tucker (2011a) also examine purchase intentions in an online advertising context and find both congruence and obtrusiveness increase ad recall and purchase intention separately, yet the effect does not hold when the ad is both congruent and obtrusive.

More recently, marketing researchers acknowledge that purchase, or purchase intent, is not always the relevant firm outcome of interest for data privacy questions. For many firms (e.g., Facebook and Instagram) that offer free digital services, data are their primary sources of value by which to derive advertising revenue and secure positive stock market performance. Thus, emerging research has investigated questions of advertising acceptance, and service usage given privacy concerns. For example, research evaluates the extent to which consumers will accept various forms of advertising in exchange for a free online service (Schumann et al. 2014). Importantly, this study is one of the first to find that consumers largely endure more targeted advertising, relinquishing some privacy, as the proverbial price they pay for customization and free services. As a related performance variable, click-through rates can capture advertising acceptance. Results show that click-through is enhanced with greater consumer control, especially when ads are targeted and personalized (Tucker 2014). Greater trust also enhances click-through, which can be further promoted by transparent data collection and use methods (Aguirre et al. 2015).

Consumer privacy enhancing factors

Trust In contexts where privacy is salient, trust promotes positive marketing outcomes that include consumer willingness to disclose, purchase intent, click-through, and advertising acceptance. In addition to being suggested as an antecedent to privacy concerns, trust also has been examined as a primary mediating mechanism in consumer willingness to engage with a firm in online and mobile platforms (Aiken and Boush 2006; Bart et al. 2005; Schlosser et al. 2006). This foundational work catapulted trust into a dominant role in privacy research. For example, organizations' covert use of privacy-compromising technologies such as cookies damages trust and reduces purchase intent (Miyazaki 2008). Firm efforts toward enhancing trust serve as promotive mechanisms, in contrast to efforts to reduce privacy concerns, which are reactive mechanisms (Wirtz and Lwin 2009). This research suggests trust can promote both consumer information disclosure and encourage consumer–firm relationship formation in privacy-relevant contexts. Most recently, trust plays a beneficial role in alleviating privacy concerns in contexts where retailers have personalized or targeted consumer content (Aguirre et al. 2015; Bleier and Eisenbeiss 2015a). Finally, although trust is reduced with greater consumer vulnerability created by corporate data practices, negative effects can be softened through

firm transparency and control (Martin et al. 2016). This recent study also shows trust is a key mediator to negative consumer behaviors that include negative word-of-mouth, falsifying information, and switching.

Personalization In spite of the value that personalization offers to consumers through novel communication messages, product and service recommendations, and individualization, it produces mixed effects on consumer outcomes in the privacy literature. Of course, the key tradeoff consumers relinquish for these values involves more extensive release of their personal information and hence, reduced privacy. Personalization concepts have taken on new meaning in today's highly digital marketing environment, explored in detail recently in Chung et al. (2016). Privacy literature, in particular, has evolved from studies that consider how email personalization leads to reactance (White et al. 2008), to examining of how advertising-website content matching promotes click-through and purchase intent (Bleier and Eisenbeiss 2015b; Goldfarb and Tucker 2011a). A key question about the personalized value–information tradeoff relates to whether information was provided willingly or not, given marketers' vast ability to obtain data overtly or covertly through a variety of means, as examined in Aguirre et al. (2015) and Miyazaki (2008), among others. Personalization can lead to enhanced engagement through click-through, but the information collection must be made known or consumers feel vulnerable. Similarly, personalization's effectiveness in promoting click-through when consumers are concerned about privacy is bounded by their feelings of trust (Bleier and Eisenbeiss 2015a).

Control In a large, natural experiment, Tucker (2014) found that people responded favorably to more personalized and targeted advertisements when they had greater ability to control their personal privacy settings. This result echoes similar ones that suggest people are more receptive to highly customized marketing communications, of which firms are now capable, when they have some control over the information disclosure process (Norberg and Horne 2014). Indeed, Xu et al. (2012) posit that consumers' perceived information control is the focal mechanism through which various methods such as self-protection, industry self-regulation, and government mandates diminish privacy concerns. Martin et al. (2016) discover that control can suppress a spectrum of data privacy vulnerabilities, and also can promote trust and reduce emotional violation in such contexts. However, Brandimarte et al. (2012) find consumers may disclose too much information, leaving them vulnerable, when they perceive greater controls. The ideal manner in which to provide consumer controls in information privacy contexts remains an open question, warranting future research. It is a delicate issue because a marketer's ability to create perceptions of control does not necessarily reflect actual control. Because consumer reactance to carefully tailored marketing messages is highly undesirable to firms that invest substantially in these approaches, theoretical and ethical frameworks that can help illuminate the privacy–reactance–control relationship represent important future research.

Economics of privacy

A limited body of research examines the economics of privacy, or rather, how firms manage consumer privacy. Studying sensitive and even potentially controversial privacy-salient firm behaviors pose data collection obstacles; however, understanding the ways companies treat consumer privacy is critically needed. In one investigation that does bridge consumer and marketer privacy preferences, Milne and Bahl (2010) identify both synergies and disconnects between those views. Not surprisingly, consumers are more likely to choose closed boundaries between themselves and the organization than are marketers. Groupings of reluctant consumers versus receptive consumers are identified, with the former segment far less accepting of privacy-relevant technologies. The receptive group, interestingly, was more accepting of new technologies than even marketing managers, who report a desire for more prevalent permission boundaries in consumer exchanges. These findings suggest that organizational privacy practices likely deviate, at least to some extent, from the wishes and desires of their customers, once again emphasizing the need for additional corporate privacy policy research.

Organizational privacy models

Given the complexities involved with simultaneously understanding consumer and organizational privacy questions, much work on the firm side employs economic modeling techniques to study data privacy outcomes. Rust et al. (2002) use theoretical models to map the consumer economics of internet privacy. The authors derive a free market system where privacy is not regulated, and find that consumer privacy erodes to the point that a market for privacy emerges. Consumers can pay for a certain amount of privacy, but as privacy continues to erode, the quality of firm value provided in exchange deteriorates. Similarly, Conitzer et al. (2012) model consumer repeat purchase specifically showing how firms can use an existing customer's information to price discriminate in future purchases. Propositions derived from this model indicate a firm is most profitable in exchanges when buyers can freely maintain anonymity, but also that consumers benefit most when anonymity is somewhat costly. Third party privacy gatekeepers also influenced consumer prices. Both sets of authors find these gatekeepers worked to the detriment of consumers as they negotiated with firms to

make anonymity free. Collectively, these studies show organizations depend on some baseline data privacy protection for smooth function of the overall market system.

In an additional example, Casadesus-Masanell and Hervas-Drane (2015) derive a mathematical model that examines some firm behaviors given consumer data privacy. This model advances propositions that analyze strategic interactions generated by consumer information provision and corporate disclosure of that information to advertisers, trying to identify the optimal situation for firms in divulging consumer information, prices, and other revenue sources relative to competitors. Results suggest that privacy can soften the intensity of competition when consumers are heterogeneous so that firms can effectively differentiate in their privacy practices (as communicated through their privacy policies). A key assumption, however, is that consumer willingness to pay for privacy is not particularly high so firms disclosing their information can operate profitably. This and related economic theoretical work points to a market for privacy and, hence, the potential for firm differentiation using privacy as strategy. We will elaborate on these points later in the paper.

Organizational privacy failures

A small body of research has examined firm outcomes given notable information security breaches, or alternatively, an extreme form of a privacy failure. Information security failures and data breaches are on the rise, affecting growing numbers of firms from various industries and around the world (Ponemon Institute 2015). Although the business press estimates firm losses to data breaches in the millions of dollars, academic research that studies corporate performance effects from large privacy failures remains underdeveloped. The research that does investigate privacy failures is primarily in the information systems literature, and often examines how technical enhancements to security may mitigate negative breach effects (e.g., Campbell et al. 2003; Hovav and D'Arcy 2003), or contextual factors that predispose firms to breaches such as geography and industry (Sen and Borle 2015). Complicating this body of knowledge is that there remains some question about the extent to which a privacy failure actually harms the company, leaving little justification for companies to enhance privacy protections (Kannan et al. 2007).

Literature that captures firm privacy failures largely omits consumer implications from the conceptual framing of the problem. A few exceptions featured in the marketing literature do consider consumer effects of privacy failures including one that casts information security breaches as a firm service failure (Malhotra and Malhotra 2011). Although this research is conducted using an event study methodology across breached firms over time with similar contextual characteristics (e.g., industry, firm size, past breach) to information security literature in other disciplines, service failure logic is extended through the findings. A second exception examines consumer defenses against privacy failures, studying how people behave both online and offline to guard against identity theft (Milne et al. 2004). In a third example, Martin et al. (2016) pair two consumer-focused investigations of company data management perceptions with a third, parallel study of firms' actual data management following a security breach. They find corporate provisions of transparency and control offset consumer reported vulnerabilities and soften negative firm performance effects of the breach. Although this project does bridge consumer and organizational domains, further research spanning both contexts is needed.

Organizational privacy self-regulation

In an analysis of whether U.S. firms should be held to more stringent consumer privacy protections, similar to that of the EU, Bowie and Jamal (2006) assert that such measures are not warranted. They advocate for a set of best practices or key features in the form of the firm's privacy policy, which remains the primary vehicle by which organizations describe their efforts around accessing consumer data and, ultimately, protecting consumer privacy. If privacy policies are well-constructed and coupled with opt-in provisions, these authors argue firm self-regulation represents a sufficient means for protecting consumer privacy. Additional research asks the self-regulation versus legislation question in a slightly different way by examining data breach litigation and settlement values incurred by firms (Romanosky et al. 2014). Their findings show that of companies suffering even a massive data breach, only about 4 % of those breaches are pursued by legal action. Yet, of those that were litigated in this research sample, the settlement rate was higher than expected (approximately 50 %). The low probability of litigation coupled with the context of a data breach (a potentially rare occurrence in some industries) suggests firms will continue to favor minimal consumer information privacy regulation, controlling the aspects of privacy management under their dominion (e.g., privacy policies; data security measures).

Corporate privacy policies are an important communication mechanism for customers, regulators, and the public at large about procedures for collection, use, and protection of valuable customer information. As such, privacy policies function as critical evidence of a company's efforts toward privacy self-regulation. Indeed, early research drawing from a sample of nearly 2500 consumers found that 84 % of people reported reading privacy policies, and that such a policy influenced their trust in that firm (Milne et al. 2004). Given this evidence of perceived importance surrounding such a policy, subsequent research investigates the mechanics behind consumer interpretation of privacy policies, as well as more objective assessments of the readability and intuitive appeal of these communications. Privacy policies have become less readable over time (average

reading ability level that measures in the college-age range), and significantly longer (Milne et al. 2006). Perhaps more troubling is their finding that customers have been shown to project their personal privacy expectations onto company policies, leading to an overreliance on the firm to protect their information when that may not at all be the case.

Longitudinal shifts in policy composition, coupled with consumers equating policy contents with actual firm behavior, augurs for needed future research that deconstructs privacy policies and their dimensions in more precise detail. Specifically, if privacy policies are valued and used by customers, how can companies reverse the trend toward greater complexity? Likewise, if privacy policies truly communicate a company's approach to the management of consumer information, can their specific dimensions be linked to firm performance outcomes to delineate best practices? Conversely, can corporate behaviors captured through dimensions of privacy policies portend firm privacy failure risk? Martin et al. (2016) find evidence that privacy policies can represent a good proxy for the extent to which firms provide customers greater transparency and control, linking those dimensions to firm performance and consumer behaviors. Moreover, their results show that a strong privacy policy can shelter a firm from potential spillover effects related to a close competitor's privacy failure. These findings, coupled with the general trend toward company self-regulation of consumer information privacy practices suggests that a clear, cogent privacy policy is of the utmost importance.

Data privacy: synthesizing diverse perspectives

Marketing scholarship increasingly has emphasized the critical role of engaging customers on cognitive, emotional, and behavioral levels (e.g., Brodie et al. 2011) and, ultimately, forming long-term relationships with them (Palmatier et al. 2006). Doing so requires heavy investments in *knowing* customers—understanding their preferences, likes, and dislikes, but also their thoughts, feelings, and actions. Given this weighty charge, consumer data collection initiatives have surfaced on a broad scale, using technologies ranging from simple loyalty cards to sophisticated video monitoring and GPS tracking systems. Ultimately, this focus on truly knowing one's customers gave rise to the use of big data and analytics in marketing.

Proponents argue that consumer information gathering initiatives are no different than a small shopkeeper from bygone times knowing her/his clientele by personally interacting with them regularly, over time. This proverbial shopkeeper would know where a customer lived in their small village or town. S/he would know her/his profession and how s/he spends her/his leisure time. The shopkeeper would know whether the customer had children, and if so, likely would know their ages, genders, and probably what they enjoyed studying in school. This individual would be privy to family births and deaths, and through the course of her/his interactions with the customer, would probably have an important influence on family consumption. The relationship between this shopkeeper and her/his clientele is an intimate, and deeply personal one. Given that consumers no longer buy goods from a single, general store, nor does modern infrastructure limit people to services within their geographic proximity, the types of relationships described also are a relic of the past. Yet, in spite of the vast changes in the marketer–consumer relationship, marketer desire to understand and connect with customers arguably is stronger than ever. Likewise, the benefits consumers receive from greater marketer access to their information are widely understood. Some include free online and in-store services, more relevant information and advertising content, promotions tailored to specific interests, personalized discounts, and overall, a superior experience (Lenard and Rubin 2010).

However, contemporary consumers often are one or more steps removed from the marketer, either because of the distant nature of the transaction from the brick-and-mortar location (i.e., e-commerce), or through frontline salespeople who themselves are not in contact with marketing decision makers, or even through automated and self-service formats. Consequently, marketers must use other means for gathering consumer information than were available to our shopkeeper. In the absence of this one-to-one personal relationship, marketers have a variety of technologically enabled methods for knowing customers. Of course, some of these are acquired directly from the consumer such as one's name and address for purchases through the mail or online. Consumers often willingly provide information such as an email address, thereby granting a marketer permission to communicate with her/him using this platform. However, the lines surrounding consumer willingness to provide information become blurry. Marketer use of cookies (online tracking mechanisms) was at one time a controversial debate, which effectively resolved to give marketers wide ability to track consumers' web movements on a large scale (Laczniak and Murphy 2006). While consumers can disable these trackers, they do so at the peril of diminished or entirely thwarted browsing functionality.

Other technologies and tools further advance the ability of marketers to know their customers. Online behavioral targeting, for example, uses consumer web tracking technologies to create a customer profile and, accordingly, aim advertising and other marketing communications at them using the parameters of that profile (Nill and Aalberts 2014). Online behavioral targeting, when detected through strong personalization and obtrusiveness, has been shown to heighten privacy concerns (Goldfarb and Tucker 2011a). But as we know, not all behavioral targeting can and is detected. Many marketers have become so skilled in understanding and predicting consumer behavior that they resort to using distracting features in

their marketing communications to make such highly personalized targeting less obvious. The retailer, Target, whose analytical prowess was made infamous when they accurately predicted a teenage girl's unrevealed pregnancy, now disguises the prominence of highly customized ads derived from profiling analytics among tangential, less salient ads (Duhigg 2012).

Behavioral profiling derived from online and in-store shopping behaviors clearly is one powerful approach to knowing customers. In the context of retail shopping or e-commerce, one might argue that being observed in some sense is not uncommon or surprising. Recall the opening example of supermarket shopping in Caudill and Murphy (2000) that nicely captures consumer expectations for in-store behaviors. Data aggregating tools have allowed marketers to push the boundaries of organic customer observation through new abilities to synthesize data from spaces in which consumers may not expect marketers to be. These observations may derive from social media, to unrelated searches on topics such as health concerns, to consumers' cars and televisions, to their mobile phones (Kshetri 2014). Mobile marketing through location-based services such as GPS continue to gain in sophistication and use. For example, geo-fencing allows marketers to target promotions to consumers as they enter a proximal radius of the marketer's brick-and-mortar location. However, research suggests this type of promotion may cannibalize predetermined customer sales. Companies now advocate for geo-conquesting, or targeting a promotion to a consumer as they enter the proximal radius of a close competitor's brick-and-mortar location (Fong et al. 2015). Clearly, a marketer must possess capabilities for monitoring consumers' precise locations to allow such an approach to be executed accurately.

Given these highly sophisticated and potentially intrusive marketing tactics, it is perhaps not surprising that consumer backlash to information use appears to be growing. Ultimately, consumers cite privacy violations, feelings of vulnerability, threat of fraudulent activities, and a general creepiness factor in their perceptions of marketers' data use (Kshetri 2014). They also have become savvier in understanding the significant value of their information to marketers. To illustrate, a recent Ernst & Young report found that half of the consumers they surveyed declared they would be less willing to share their personal information in the future, leading the analysts to conclude that the proverbial golden age of free data will likely grind to a halt in 2018. According to this research, companies already are preparing for reduced access to data provided willingly by consumers, making more subversive data capture methods attractive (Ernst & Young 2015). Whether the big data phenomenon truly culminates in consumers drawing the proverbial line in the sand remains to be seen. That marketer behaviors and approaches to managing consumer information has escalated to such extremes in the conversation brings us back to the powerful foreshadowing of Bloom et al. (1994), and others such as Jones (1991) and Laczniak and Murphy (2006) whose perspectives collectively implore marketers to be mindful of using new technologies responsibly. Clearly some companies misuse information or heighten consumer privacy risk through novel technologies, however, other firms increasingly are committing to the ethical use of new technologies and stronger protection of their customers' privacy. This class of marketers appear to be using data privacy as a strategic differentiator.

Privacy as strategy

Academic literature has hinted at themes of data privacy as firm strategy, but to date this thinking remains underdeveloped. For example, Culnan and Armstrong (1999) find that consumers are more willing to grant marketers permission to use their information when the company's procedures for information use are fair—a case for procedural justice. In return, they argue these firms will obtain greater access to rich user data, providing them a competitive advantage over peers with consumer information procedures that are perceived as less fair. By modeling the economics of consumer privacy, Rust et al. (2002) demonstrate that it is in marketers' best interest to offer at least some baseline protection to avoid complete erosion of privacy-based customer utility. Similarly, Casadesus-Masanell and Hervas-Drane (2015) study marketers' ability to compete with privacy both in their primary market as a source of superior targeting and marketing to consumers, and in the secondary market where consumer information is sold to third-parties as a separate revenue generating source. Their economic models show that firms can compete on privacy when consumer preferences for it are heterogeneous so that common privacy practices can be effectively differentiated. They also show that strategies where marketers attempt to exploit consumer information in both primary and secondary markets is high risk, and that to avoid privacy backlash corporations should emphasize one or the other. Ultimately, the authors conclude that competing on privacy is both feasible and likely to be successful under certain conditions.

In addition to academic research and scholarship that considers how marketers might differentiate on privacy, managerially-focused work suggests data privacy best practices. As one example, based on their collection of scholarly research, Goldfarb and Tucker (2013) use a managerial platform to advocate in favor of firms' stronger consumer privacy protections. They argue strong privacy management provides consumers a positive brand experience, leading to competitive advantage. As such, firms should not view stringent privacy measures as costs or constraints, but rather opportunities to improve the customer experience. Improved customer experience, in turn, should secure loyalty and strengthen relationships grounded in the perceived value of privacy protections. Others draw from consumer surveys to assess basic data privacy issues

and to evaluate aspects of these practices of greatest concern (Morey et al. 2015). These authors propose "Enlightened Data Principles" for managing consumer data that include teaching customers, providing aspects of control in managing data, and enhancing value in exchange. These articles represent just two practical prescriptions around managing consumer information and preserving privacy. In spite of the multiple calls for tempered use of consumer data and heighted concern for user well-being, few firms have yet to adopt these best-practice measures. Every time a new data breach compromising consumer privacy and security is announced, we are all too aware of marketers' existing deficiencies in this arena.

Protecting consumer privacy has featured centrally in social and business conversations with the recent refusal of Apple to grant U.S. law enforcement backdoor access to the iPhone of a known terrorist. Indeed, headlines about the debate spoke directly to the notion of using privacy as strategy by referring to government prosecutors' quotes that Apple's refusal "appears to be based on its concern for its business model and public brand marketing strategy" (Lichtblau and Apuzzo 2016). The company's refusal does, indeed, involve marketing to the extent that they are interested in protecting consumer information, property, and privacy—attributes they know their customers value. In their explanatory letter to their users about the case, Apple writes,

> We built strong security into the iPhone because people carry so much personal information on our phones today, and there are new data breaches every week affecting individuals, companies and governments. The passcode lock and requirement for manual entry of the passcode are at the heart of the safeguards we have built in to iOS. It would be wrong to intentionally weaken our products with a government-ordered backdoor. If we lose control of our data, we put both our privacy and our safety at risk. (http://www.apple.com/)

Beyond Apple, a limited number of firms is emerging that appears to be competing on strong consumer privacy protections. Interestingly, some of these examples evolve from industries that have been heavily criticized for deficiencies in consumer privacy protection. A widely publicized example involves Microsoft's Scroogled campaign (also overviewed in Casadesus-Masanell and Hervas-Drane 2015), where they clearly single out Google as violating consumer privacy through practices such as combing contents of Gmail messages to personalize advertising and behavioral targeting that is enabled through their Google search engine results. This approach to direct competitive positioning did not gain momentum, however, with some experts blaming the overly pointed references to Google, rather than a more nuanced approach to what Microsoft was doing right on the privacy front, as a key reason for the campaign's failure. When Microsoft's marketing and branding was recently overhauled, top-level decision makers determined that Scroogled had no place in their messaging (O'Reilly 2015).

As companies continue to grapple with consumer information privacy questions, and as long as they compete in markets where privacy protections can be differentiated and are valued by customers, using privacy as a strategy remains a viable option to marketers. Recently, wireless provider Verizon incurred significant fines for not informing and allowing opt-out of super-cookies, powerful consumer tracking devices that cannot be seen or erased by its customers and that provide detailed browsing history and other personal information about users. Interestingly, AT&T also has super-cookie technology, but the Federal Communications Commission (FCC) felt that the company had adequately notified and allowed opt-out for their customers (Peterson 2016). Although AT&T does not currently appear to be using this decision as competitive positioning, in an industry as competitive as the wireless carrier business, such an approach is feasible and increasingly likely to resonate with consumers.

So what can be learned from the vast body of privacy research and the intersections across consumer, organizational, and ethical intersections that helps inform a strategic approach to privacy as strategy? As we see from the preceding examples, using a privacy-centric approach to competitive differentiation can be risky as experienced by Microsoft with Scroogled. So too, AT&T would likely think carefully about positioning on privacy against the latest Verizon ruling given their low scores on privacy protection rankings as documented by the Electronic Frontier Foundation (EFF) in 2015.[2] EFF rankings show Google and Microsoft nearly tied with each other, perhaps suggesting another reason for Scroogled's failure. Conversely, Apple ranks in EFF's top five best privacy protecting companies. Together, these insights suggest that for privacy as strategy to be effective, firms must proverbially practice what they preach as consumer perceptions of privacy deficiencies are likely to be widely shared and well-known.

Yet, additional dimensions also are salient to consumers. Across many investigative categories and settings, consumer control represents a powerful privacy promoting mechanism. Given trends identified in the Ernst & Young report, marketers would be wise to preempt information refusal with a more nuanced stance toward providing consumers control of their personal data, how it is collected, used, and shared. Using data in shrouded ways also is likely to create greater information refusal. Our review shows marketers benefit from transparency

[2] The EFF index is comprised of five key protection areas including (1) following industry best practices, (2) telling users about government data demands, (3) disclosing data retention policies, (4) disclosing content removal requests, and (5) opposing government backdoor access to data (www.eff.org).

in consumer information practices. As Morey et al. (2015) identify, consumers are increasingly knowledgeable of their digital profile and ways their data are used. Acknowledging a savvy modern consumer and appealing to that knowledge through transparent and trust-enhancing practices also seem a prerequisite for anchoring on privacy as strategy.

Finally, marketers need to implement privacy protections in a way that is mindful of competitive actions. Not only do our examples suggest that juxtaposing one's privacy practices against a direct competitor can be risky, academic research also has identified spillover effects to firms when a close rival suffers a privacy failure (Martin et al. 2016). When consumers view firms in a given industry as being similar on important dimensions, a privacy failure by one can lead to perceptions that privacy deficiencies are endemic to all. As such, firms have an incentive to monitor competitor privacy practices as well as strive to visibly outperform those competitors on privacy. Just as companies attempt to lead in strategic product and service enhancements, so too there may be first mover advantages on consumer privacy protection. Collectively, we offer the following tenets as best practices for privacy as strategy derived from academic research and marketing practice.

- Firms that *prioritize data privacy in an authentic way* will experience positive performance, including favorable market response, customer loyalty, and engagement benefits. Given today's privacy-savvy consumer, firm efforts lacking authenticity will be easily identified.
- Firms that *involve their customers in the information privacy dialogue* will experience positive performance. For privacy as strategy to be successful in the long term, it must involve open and transparent communication with customers, as well as with the regulators who oversee information acquisition, use, and sharing practices.
- Firms that implement privacy promoting practices will experience positive performance under the condition that they *align data privacy practices across all aspects of the firm*. Again, cosmetic or partial privacy efforts will become apparent to consumers.
- Firms that *focus on what they do right* with respect to data privacy will experience positive performance. Highlighting one's own strengths rather than emphasizing others' potentially deficient practices appears to be better accepted by consumers.
- Firms that *commit to data privacy practices over the long-term* will experience positive performance, as well as benefit from relaxed regulatory oversight. Adopting a stance toward privacy as strategy cannot be a short-term approach designed for quick benefits.
- Finally, firms that embody these privacy as strategy tenets will experience heighted consumer trust. *Trust serves as a key mechanism* to positive performance and other firm relational benefits. Yet, companies must realize that while trust takes time to build, it can be eroded quickly with lapses on any of the previous tenets.

Future research avenues

We have attempted to highlight gaps in privacy knowledge and identify theoretical frameworks that demonstrate promise for enhancing understanding of contemporary data privacy questions. Drawing from what is known and what remains less studied, we offer ideas for future research that can provide especially useful insights across this dynamic and fast-moving conceptual and practical domain. As described, marketer practice using customer data and analytics has evolved beyond current understanding advanced through privacy scholarship. With this in mind, several future research questions offer substantial potential to extend our collective thinking about modern privacy challenges. This list is by no means exhaustive, but illustrates some of the most noticeable gaps given the current state of research.

- What theories and approaches offer the greatest potential to enhance understanding of *cutting edge technologies* such as geo-conquesting, RFID tracking, and super-cookie use with clear consumer, organizational, and ethical privacy intersections?
- In the absence of a strong legal framework for sanctioning privacy violations, how can normative ethical theory pave the way for *what organizations should be doing to exceed consumer privacy expectations*, as well as to over-comply with legal mandates in order to preserve their ability to self-regulate?
- How might we better understand *consumer preference and choice related to organizational use of their information*? Behavioral decision theories may help shed light on this question, and identify ethical quandaries that surface and suggest approaches for alleviating them.
- How can we more fully *recognize privacy/vulnerability tradeoffs* relevant to an individual and the various dimensions of her/his identity? For instance, which consumer groups perceive themselves as the most vulnerable to information privacy abuses?
- How might we understand *firm recovery strategies to re-engage customers after massive privacy failures*? How do these firms navigate consumer, ethical, and legal challenges following a privacy failure? Furthermore, how does the market evaluate recovery effectiveness in such situations?
- How might we capture *cross-cultural and cross-national variation of privacy concerns* across stakeholder groups? Do firms and regulators manage consumer information in unique ways when privacy concerns do not factor centrally? What unforeseen harms surface in cultures where privacy is not highly valued (for example, in societies such as China)?

Conclusion

This research captures the current state of data privacy scholarship in marketing and related disciplines. The concept of consumer information privacy is hard to define, as acknowledged by privacy scholars, practitioners, and regulators. Although a coherent subset of theoretical approaches provide robust understanding through deep insights, in some ways this focus has constrained our view of privacy to consumer, organizational, ethical, and legal silos. Empirical findings and relationships extracted from the vast privacy scholarship in marketing echo this observation, with significant progress occurring within narrow relationships in tightly defined spaces. In response, we take a necessary step toward expanding the privacy domain across these borders, emphasizing compelling synergies that span multiple interests. By synthesizing privacy across these areas, we advocate for a holistic way of thinking about organizational use of consumer data, and how this fits into a bigger societal picture. Discussion of privacy as strategy offers but one example. Future research directions also should embody a holistic approach, blending the many consumer, organizational, ethical, and legal concerns that feature in contemporary data privacy questions. Since stakeholders are affected in multiple and potentially unforeseen ways, additional work in this important domain remains critical and needed.

Acknowledgments The authors are grateful for the insightful feedback of the Editor-in-Chief and the anonymous reviewers.

References

Acquisti, A., John, L. K., & Loewenstein, G. (2012). The impact of relative standards on the propensity to disclose. *Journal of Marketing Research, 49*, 160–174.

Acquisti, A., John, L. K., & Loewenstein, G. (2013). What is privacy worth? *The Journal of Legal Studies, 42*, 249–274.

Aguirre, E., Mahr, D., Grewel, D., Ruyter, K. D., & Wetzels, M. (2015). Unraveling the personalization paradox: The effect of information collection and trust-building strategies on online advertisement effectiveness. *Journal of Retailing, 91*, 34–59.

Aiken, K. D., & Boush, D. M. (2006). Trustmarks, objective-source ratings, and implied investments in advertising: Investigating online trust and the context-specific nature of internet signals. *Journal of the Academy of Marketing Science, 34*, 308–323.

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

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics, 67*, 107–123.

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*, 13–28.

Bart, Y., Shankar, V., Sultan, F., & Urban, G. L. (2005). Are the drivers and role of online trust the same for all web sites and consumers? A large-scale exploratory empirical study. *Journal of Marketing, 69*, 133–152.

Bleier, A., & Eisenbeiss, M. (2015a). The importance of trust for personalized online advertising. *Journal of Retailing, 91*, 390–409.

Bleier, A., & Eisenbeiss, M. (2015b). Personalized online advertising effectiveness: The interplay of what, when, and where. *Marketing Science, 34*, 669–688.

Bloom, P. N., Milne, G. R., & Adler, R. (1994). Avoiding misuse of new information technologies: legal and societal considerations. *Journal of Marketing, 58*, 98–110.

Bowie, N. E., & Jamal, K. (2006). Privacy rights on the internet: Self-regulation or government regulation? *Business Ethics Quarterly, 16*, 323–342.

Brandimarte, L., Acquisti, A., & Lowenstein, G. (2012). Misplaced confidences: privacy and the control paradox. *Social Psychological and Personality Science, 4*, 341–347.

Brehm, J. W. (1966). *A theory of psychological reactance*. Oxford, England: Academic Press.

Brodie, R. J., Hollebeek, L. D., Juric, B., & Lilc, A. (2011). Customer engagement: Conceptual domain, fundamental propositions, and implications for research. *Journal of Service Research, 14*, 252–271.

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*, 431–448.

Casadesus-Masanell, R., & Hervas-Drane, A. (2015). Competing with privacy. *Management Science, 61*, 229–246.

Caudill, E. M., & Murphy, P. E. (2000). Consumer online privacy: legal and ethical issues. *Journal of Public Policy & Marketing, 19*(1), 7–19.

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus Privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management, 6*, 181–202.

Chung, T. S., Wedel, M., & Rust, R. T. (2016). Adaptive personalization using social networks. *Journal of the Academy of Marketing Science, 44*, 66–87.

Conitzer, V., Taylor, C. R., & Wagman, L. (2012). Hide and seek: Costly consumer privacy in a market with repeat purchases. *Marketing Science, 31*, 277–292.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science, 10*(1), 104–115.

Culnan, M. J., & Bies, R. J. (2003). Consumer privacy: Balancing economic and justice considerations. *Journal of Social Issues, 59*(2), 323–343.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organization privacy: Lessons from the Choice Point and TJX data breaches. *MIS Quarterly, 33*, 673–687.

Dinev, T., & Hart, P. (2004). Internet privacy concerns and their antecedents measurement validity and a regression model. *Behaviour & Information Technology, 23*, 413–422.

Dolnicar, S., & Jordaan, Y. (2007). A market-oriented approach to responsibly managing information privacy concerns in direct marketing. *Journal of Advertising, 36*, 123–149.

Duhigg, C. (2012). How companies learn your secrets. In *New York Times Magazine* .Retrieved April 4, 2016 from www.nytimes.com/2012/02/19/magazine

Dunfee, T. W., Smith, N. C., & Ross, W. T. (1999). Social contracts and marketing ethics. *Journal of Marketing, 3*, 14–32.

Emerson, R. M. (1976). Social exchange theory. *Annual Review of Sociology, 2*, 335–362.

Ernst & Young (2015), Megatrends 2015: Making sense of a world in motion. *EY Global Report*.

European Commission (2016). EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy

Shield. Retrieved April 4, 2016 from http://europa.eu/rapid/press-release_IP-16-216_en.htm.

Ferrell, O. C., & Gresham, L. G. (1985). A contingency framework for understanding ethical decision making in marketing. *Journal of Marketing, 49*, 87–96.

Fong, N. M., Fang, Z., & Luo, X. (2015). Geo-conquesting: Competitive locational targeting of mobile promotions. *Journal of Marketing Research, 52*, 726–735.

Foxman, E. R., & Kilcoyne, P. (1993). Marketing practice, and consumer privacy: Ethical issues. *Journal of Public Policy & Marketing, 12*, 106–119.

Gabisch, J. A., & Milne, G. R. (2014). The impact of compensation on information ownership and privacy control. *Journal of Consumer Marketing, 31*, 13–26.

Goldfarb, A., & Tucker, C. (2011a). Online display advertising: targeting and obtrusiveness. *Marketing Science, 30*, 389–404.

Goldfarb, A., & Tucker, C. E. (2011b). Privacy regulation and online advertising. *Management Science, 57*, 57–71.

Goldfarb, A., & Tucker, C. (2012). Shifts in privacy concerns. *American Economic Review, 102*, 349–353.

Goldfarb, A., & Tucker, C. (2013). Why managing customer privacy can be an opportunity. *MIT Sloan Management Review, 54*, 10–12.

Goodman, M. (2016). *Future crimes: Inside the digital underground and the battle for our connected world*. New York: Anchor Books.

Hann, I. H., Hui, K. L., Tom Lee, S. Y., & Png, I. P. L. (2007). Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems, 24*, 13–42.

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management & Insurance Review, 6*, 97–121.

John, L. K., Acquisti, A., & Loewenstein, G. (2011). Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research, 37*, 858–873.

Jones, M. G. (1991). Privacy: A significant marketing issue for the 1990s. *Journal of Public Policy & Marketing, 10*, 133–148.

Kahneman, D. (2003). A perspective on judgement and choice: mapping bounded rationality. *American Psychologist, 58*, 697–720.

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

Kshetri, N. (2014). Big data's impact on privacy, security and consumer welfare. *Telecommunications Policy, 38*, 1134–1145.

Laczniak, G. R., & Murphy, P. E. (2006). Marketing, consumers, and technology: Perspectives for enhancing ethical transactions. *Business Ethics Quarterly, 16*, 313–321.

Langenderfer, J., & Miyazaki, A. D. (2009). Privacy in the information economy. *The Journal of Consumer Affairs., 43*, 380–388.

Lanier Jr., C. D., & Saini, A. (2008). Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review, 12*, 1–45.

Lenard, T. M., & Rubin, P. H. (2010). In defense of data: Information and the costs of privacy. *Policy & Internet, 2*, 149–183.

Lichtblau, E., & Apuzzo, M. (2016). Justice department calls Apple's refusal to unlock iPhone a 'marketing strategy.' *New York Times*. Retrieved March 11, 2016, from www.nytimes/2016/02/20/business/.

Lwin, M., Wirtz, J., & Williams, J. D. (2007). Consumer online privacy concerns and responses: A power-responsibility equilibrium perspective. *Journal of the Academy of Marketing Science, 35*, 572–585.

Maignan, I., & Ferrell, O. C. (2004). Corporate social responsibility and marketing: An integrative framework. *Journal of the Academy of Marketing Science, 32*, 3–19.

Malhotra, A., & Malhotra, C. K. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research, 14*, 44–59.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns: The construct, the scale, and a causal model. *Information Systems Research, 15*, 336–355.

Manjoo, F. (2015). 'Right to be forgotten' online could spread. In *New York Times* .Retrieved April 4, 2016 from www.nytimes.com/2015/09/06/technology

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*, 210–227.

Martin, K. D., Borah, A., & Palmatier, R. W. (2016). Data privacy: Effects on customer and firm performance. *Journal of Marketing, In-Press*. doi:10.1509/jm.15.0497.

Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information privacy: Corporate management and national regulation. *Organization Science, 11*, 35–57.

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*, 138–149.

Milne, G. R., Rohm, A. J., & Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs, 38*, 217–232.

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

Miyazaki, A. D. (2008). Online privacy and the disclosure of cookie use: Effects on consumer trust and anticipated patronage. *Journal of Public Policy & Marketing., 27*, 19–33.

Miyazaki, A. D., & Fernandez, A. (2000). Internet privacy and security: An examination of online retailer disclosures. *Journal of Public Policy & Marketing, 19*, 54–61.

Miyazaki, A. D., & Krishnamurthy, S. (2002). Internet seals of approval: Effects on online privacy policies and consumer perceptions. *Journal of Consumer Affairs, 36*, 28–49.

Moon, Y. (2000). Intimate exchanges: using computers to elicit self-disclosure from consumers. *Journal of Consumer Research, 26*, 323–337.

Morey, T., Forbath, T., & Schoop, A. (2015). Customer data: Designing for transparency and trust. *Harvard Business Review, 93*, 96–105.

Mothersbaugh, D. L., Foxx II, W. K., Beatty, S. E., & Wang, S. (2012). Disclosure antecedents in an online service context: The role of sensitivity of information. *Journal of Service Research, 15*, 76–98.

Murphy, P. E., Laczniak, G. R., Bowie, N. E., & Klein, T. A. (2005). *Ethical marketing*. Upper Saddle River, NJ: Pearson.

Nill, A., & Aalberts, R. J. (2014). Legal and ethical challenges of online behavioral targeting in advertising. *Journal of Current Issues and Research in Advertising, 35*, 126–146.

Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Palo Alto, CA: Stanford University Press.

Norberg, P. A., & Horne, D. R. (2014). Coping with information requests in marketing exchanges: An examination of pre-post affective and behavioral coping. *Journal of the Academy of Marketing Science, 42*, 415–429.

O'Reilly, L. (2015). Microsoft has finally abandoned its Google-bashing 'Scroogled' ad campaign. In *Business Insider* .Retrieved March 11, 2016 from www.businessinsider.com

Ohlhausen, M. K. (2014). Privacy challenges and opportunities: The role of the Federal Trade Commission. *Journal of Public Policy & Marketing, 33*, 4–9.

Palmatier, R. W., Dant, R. P., Grewal, D., & Evans, K. R. (2006). Factors influencing the effectiveness of relationship marketing: A meta-analysis. *Journal of Marketing, 70*, 136–153.

Peterson, A. (2016). FCC cracks down on Verizon Wireless for using 'supercookies.' Washington Post. Retrieved March 11, 2016 from www.washingtonpost.com/news/.

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing, 19*, 27–41.

Ponemon Institute (2015). 2015 Cost of data breach study: Global analysis. *Ponemon Institute Research Report*, available at (www.ibm.com/services).

Rainie, L., & Duggan, M. (2016). Privacy and information sharing. In *Pew Reseach Center* .Retrieved April 4, 2016 from www.pewinternet.org

Rawls, J. (1971). *A theory of justice*. Cambridge, MA: Harvard University Press.

Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. *Journal of Empirical Legal Studies, 11*(1), 74–104.

Rust, T. R., Kannan, P. K., & Peng, N. (2002). The customer economics of internet privacy. *Journal of the Academy of Marketing Science, 30*, 455–464.

Schlosser, A. E., White, T. B., & Lloyd, S. M. (2006). Converting web site visitors: Investment increases consumer trusting beliefs and online purchase intentions. *Journal of Marketing, 70*, 133–148.

Schumann, J. H., Wangenheim, F. V., & Groene, N. (2014). Targeted online advertising reciprocity appeals to increase acceptance among users of free web services. *Journal of Marketing, 78*, 59–75.

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314–341.

Sheehan, K. B. (2005). In poor health: An assessment of privacy policies at direct-to-consumer websites. *Journal of Public Policy & Marketing, 24*(2), 273–283.

Sheehan, K. B., & Hoy, M. G. (1999). Flaming, complaining, abstaining: how online users respond to privacy concerns. *Journal of Advertising, 28*(3), 37–51.

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

Singer, N. (2012), Mapping, and sharing, the consumer genome. New York Times. Retrieved April 4, 2016 from www.nytimes/2012/06/17/technology.

Smith, J. H., Milberg, S. J., & Burke, J. B. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 167–196.

Solove, D. J. (2008). *Understanding privacy*. Cambridge, MA: Harvard University Press.

Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. New Haven, CT: Yale University Press.

Tirunillai, S., & Tellis, G. J. (2014). Mining marketing meaning from online chatter: strategic brand analysis of big data using latent Dirichlet allocation. *Journal of Marketing Research, 51*, 463–479.

Tsai, J. Y., Egelman, S., Cranor, L., & Acquisti, A. (2011). The effect of online privacy information behavior: An experimental study. *Information Systems Research, 22*, 254–268.

Tucker, C. E. (2014). Social networks, personalized advertising and privacy controls. *Journal of Marketing Research, 51*, 1547–7193.

Vail, M. W., Earp, J. B., & Antón, A. I. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management, 55*, 442–454.

Warren, S., & Brandeis. L. (1890). The Right to Privacy. In F. Schoeman (Ed.), *Philosophical Dimensions of Privacy* (pp. 75–103). Cambridge: Cambridge University Press (Originally published in Harvard Law Review, 4 p. 193).

Westin, A. (1967). *Privacy and freedom*. New York: Antheneum.

White, T. B. (2004). Consumer disclosure and disclosure avoidance: a motivational framework. *Journal of Consumer Psychology, 14*, 41–51.

White House (2012). *Consumer data privacy in a networked world: A framework for protecting privacy and promoting innovation in the global digital economy*. D.C.: Washington.

White House (2014). *Big data: Seizing opportunities, preserving values*. D.C.: Washington.

White, T. B., Zahay, D. L., Thorbjørnsen, H., & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters, 19*, 40–50.

Wirtz, J., & Lwin, M. O. (2009). Regulatory focus theory, trust, and privacy concern. *Journal of Service Research, 20*, 1–18.

Xu, H., Teo, H. H., Tan, B. C. Y., & Agarwal, R. (2012). Effects of individual self-protection industry self-regulation, and government regulation on privacy concerns: A study of location based services. *Information Systems Research, 23*, 1342–1363.