ELSEVIER

Journal of Retailing 96 (4, 2020) 449–457

Journal of Retailing

Data Privacy in Retail: Navigating Tensions and Directing Future Research☆

Kelly D. Martin[a,*], Robert W. Palmatier[b]

[a] College of Business, Colorado State University, Fort Collins, Colorado 80523-1278, United States
[b] University of Washington, Michael G. Foster School of Business, Seattle, Washington 98195, United States

Available online 7 November 2020

Abstract

To understand data privacy in retailing, one must consider a myriad of consumer, retailer, and regulatory tensions, trade-offs, and compromises. Scholarly research on consumer data privacy in retailing remains a fruitful area of inquiry precisely because it confronts these critical tensions. As a scholarly domain, data privacy research investigates questions and contexts that are fraught with persistent conflicts and paradoxes. Despite some important advances, many pressing questions remain, leaving various tensions unresolved too. In this editorial, we review the role of data privacy in retailing, attending to focal consumer and retailer tensions. We also provide an overview of the unique contributions offered by the articles in this issue, stressing the novel insights they provide for retail theory and practice. This overview exposes three promising research directions that offer particular promise for informing the critical data privacy tensions that we identify and for expanding the relevance of data privacy research to encompass a broader set of retail implications. These research directions in turn may motivate future scholarly inquiry in retailing, inform retail management, and suggest public policy options.

Keywords: Data privacy; personalization; privacy paradox; information disclosure; retail channels

A clear sense of data privacy in retailing requires in-depth understanding of a myriad of consumer–retailer tensions, trade-offs, and compromises. Retail managers must balance demands to personalize customer experiences with worries about violating their privacy and inducing backlash. Notably, more than 70% of consumers report frustration when their retail experiences fail to provide personalization (Petro 2019), but more than 70% of consumers also express concerns about how companies use the data they collect (Auxier et al. 2019). This tension, which implies a "state of latent hostility or opposition between individuals or groups" (Merriam-Webster 2020), puts retailers in a seemingly impossible situation. Yet research also has begun to reveal some relevant exceptions, boundary conditions, and mechanisms through which retailers can partner with consumers to achieve mutually beneficial, data-based applications, personalization agreements, exchanges of data value, and collaborative interactions.

Understanding data privacy in retailing remains a fruitful area of research precisely because it seeks to confront these critical tensions. As a scholarly domain, data privacy research investigates questions and contexts filled with unresolved conflicts and paradoxes. For example, it reveals that retail consumers value personalization efforts and outcomes but are reluctant to share the information retailers need to execute such efforts (Aguirre et al. 2015). Retailers have access to sophisticated technologies that help them leverage their knowledge about customers, but they also risk appearing creepy should it seem they know those customers "too well" (Bleier and Eisenbeiss 2015). Navigating these tensions has produced robust literature already and continues to motivate scholars working in this space.

Journal of Retailing has been at the forefront of conversations related to novel uses of consumer information in retail applications. Its publications also have long warned of the threats to consumer privacy that can accompany such applications (e.g., Esmark et al., 2017; Inman and Nikolova 2017). Therefore, it is particularly fitting to use this special section to take stock of novel retail applications and their reliance on consumer data, as well as highlight the critical tensions related to data privacy in

☆ The special section guest editors are grateful to *Journal of Retailing* coeditors-in-chief, Anne Roggeveen and Raj Sethuraman, for their support throughout the editorial process. They also thank the special section authors and reviewers for their contributions.

* Corresponding author.
E-mail addresses: kelly.martin@colostate.edu (K.D. Martin), palmatrw@uw.edu (R.W. Palmatier).

https://doi.org/10.1016/j.jretai.2020.10.002
0022-4359/

academic retailing literature and in retail practice. By addressing these interfaces, the scholarly contributions that constitute this special section provide critical advances and new research directions. Yet even with these meaningful contributions, pressing questions remain unanswered, and crucial tensions remain unresolved. Therefore, we review the role of data privacy in retailing by attending to central consumer and retailer tensions. We explain how the articles in this special section offer novel insights for retail theory and practice, which in turn suggests three promising research directions. Efforts in these directions might inform critical data privacy tensions, as well as expand data privacy research to encompass broader, relevant retail implications that can inform retailing management and public policy makers.

Consumer Data Privacy in Retail: Focal Tensions

Protecting consumer data privacy is an important shared goal among retailers, regulators, advocacy groups, and consumers. Considering this unitary view, ensuring that consumers' personal information remains safe, secure, and used only for benign and beneficial purposes should be easily attainable. Yet in contrast with other marketing and retailing goals, for which improvements can create linearly increasing consumer benefits (e.g., customer value creation), protecting consumers' data privacy actually can impede the benefits that consumers receive, despite their expectation and valuation of them in other marketer and retailer interactions.

This unique situation arises from the varied consumer data privacy tensions that can occur in any combination of consumers, retailers, and regulators or within each entity alone. For example, consumers seek personalization but express equally forceful desires to limit their personal data sharing. Meaningful personalization by a retailer requires consumers to share rich information about themselves, their location, and their preferences freely (Aguirre et al. 2015), because through this information, retailers "get to know" their consumers. The tension between consumers' appreciation for unique, customized offerings and their reluctance to divulge sensitive details that make such customization possible hinders the value creation process for both parties. Tensions also involve regulators, such that retailers attempting to navigate recent data privacy regulations (e.g., EU's General Data Protection Regulation [GDPR], the California Consumer Privacy Act [CCPA]) must devote considerable time and resources to such efforts, which may mean they have to shift resources away from other customer value-creating initiatives. If they overcompensate in their protective efforts, retailers also might self-limit their personalization capacities, which would again stymie customization benefits. Although consumer data privacy research has investigated many of these paradoxes (Martin and Murphy 2017), substantial work remains to unpack the varied, dynamic, and complex tensions and challenges that continue to emerge with technological advancements.

Within academic research too, tensions arise regarding the best way to approach this research space. One perspective suggests a consumer privacy paradox, such that consumers are aware of data privacy threats but share information freely anyway (e.g., Barth and de Jong 2017). A wider stream of research instead cites considerable evidence that consumers do not understand the extent to which their data get used and are not equipped to protect themselves from harm (e.g., Kim et al., 2019; Palmatier and Martin 2019; Walker 2016). The extent to which customers are actually knowledgeable about the implications of their interactions with retailers is an open question, suggesting the need for researchers and practitioners to establish a clearer understanding of consumers' actual knowledge, to reveal the associated data privacy implications (Brough and Martin 2020). By incorporating consumer privacy knowledge, we can move beyond a paradoxical view that suggests people behave contrary to their stated privacy preferences. We believe doing so is critical. Consumers who self-identify as "privacy active" take explicit steps to guard their privacy, which ultimately may help resolve data privacy tensions, in ways that promote mutual benefits for consumers and retailers. In particular, many benefits require consumers to know and care about what firms do with their personal information, then realize that the exchange of personal information supports personalization efforts that they value. Even if consumers do not fully understand the complexities associated with data provision and protection, they believe a firm's data management practices reflect how they will be treated more generally as a customer (90%), so they refuse to purchase from retailers that they believe cannot be trusted with their data (91%) (Cisco 2019). These insights suggest that data privacy practices might offer a proxy for the nature and quality of the overall customer–retailer relationship, informed by consumer privacy knowledge. Navigating critical consumer–retailer tensions thus requires researchers to describe consumer data privacy knowledge and agency fully, especially in the context of increasingly complex retailer interactions and consumption activities.

Another important perspective for understanding persistent tensions presents the retailer as concerned about consumers and invested in protecting their privacy. Retailers' access to personalization tools hinges on their ability to infuse analytical applications with rich consumer data. A failure to protect consumers and their data would nullify this valuable arrangement. Contemporary discussions tend to center on retailers' compliance with complex regulations, such as the EU's GDPR or the CCPA, without acknowledging that many retailers sought to do the right thing by consumers even before the regulatory enforcement (Martin and Murphy 2017; Palmatier and Martin 2019). Of course, some retailers deserve their bad reputations, which suggests that understanding retailer orientations and motivations could clarify yet another tension that arises in both academic research and retail practice.

These identified tensions, which crop up in consumer data privacy studies in marketing and retailing, have notable implications for consumers, retailers, as well as regulators and their interactions. This recognition motivates this special section devoted to consumer data privacy in retailing. The articles it features represent important advancements, contributing insights about existing consumer data privacy tensions in retailing, as well as suggestions for beginning to resolve them. We draw from their collective insights to suggest additional research directions.

Overview of the Special Section

The articles in this special section advance data privacy research in retail contexts in important ways. To start, Bidler et al. (2020) reveal that consumers appear more willing to engage with a retailer, including entering information disclosure processes, if the process is more interactive, media-rich, and fun. Such evidence implies that retailers may benefit from gamifying consumer data disclosures, because anticipating gamification can evoke hedonic responses that increase disclosure likelihood. Providing entertaining, hedonic benefits is not enough though; textual justifications for the need for the data collection also are critical. That is, a fun setting is helpful but not sufficient, and consumers still need to know why they are being asked to provide certain information and how doing so will benefit their further exchanges with the retailer. This finding resonates with Martin et al.'s (2020) finding, based on a global survey, that consumers report more positive firm outcomes when they sense that they receive some value from the exchange. Their results also indicate that firms benefit more from providing their customers with experience value, beyond the mere provision of economic value (e.g., lower prices), in exchange for their valuable personal information. Together, these contributions establish that consumers consider the value they can receive from exchanges, then respond to retailers accordingly.

With regard to personal information disclosures, Grosso et al. (2020) also determine that trust in the retailer functions as a global consideration. It can lessen the negative effect of privacy concerns on consumers' willingness to disclose personal information, a mitigating influence that emerges in multiple countries and for various retailers. Rather than trust, Aiello et al. (2020) demonstrate the influential role of retailer warmth perceptions for increasing consumers' willingness to disclose personal information. Warmth thus increases disclosure willingness, though perceptions of warmth communicated in disclosure requests vary, depending on the stage of the consumer journey. Their study helps clarify some stage-contingent factors in a consumer–retailer disclosure setting, with important implications for retailer privacy efforts, sensitive information requests, and other interactions between consumers and retailers.

This special section also features two big picture views. In their meta-analysis, Okazaki et al. (2020) establish a comprehensive synthesis of research into consumer privacy concerns. Their thoughtful analyses, reflecting input from more than 300 investigations of consumer privacy concerns, can inform continued privacy research at the consumer–retailer interface. Their findings also echo the key results offered by Martin et al. (2020). These inputs establish the need for more purposeful examinations of cross-cultural differences in privacy concerns, especially in parts of the world that have been less researched. Okazaki et al. also call for investigations of the confluence of regulatory, global, and consumer factors in the retail landscape.

In combination, the special section articles and their contributions suggests critical areas for further investigation. Their collective insights identify research opportunities that can advance understanding of data privacy in retailing in meaningful ways. In particular, unique aspects of both retail theory and retail management illuminate three notable gaps in our understanding of data privacy, as we elaborate next: the need to push beyond the boundaries of consumer information disclosure to zero-party data exchanges, data privacy as it unfolds during the consumer retail journey, and channel-specific perspectives on consumer data privacy.

Research Directions

Beyond Consumer Information Disclosure to Zero-Party Data Exchanges

Investigations of data privacy in retailing often address the nature of the information disclosure. In this special section, we find insightful explorations of how data privacy concerns might inhibit or encourage consumer information disclosures; they push existing boundaries to advance retail thinking and help clarify the implications of data privacy and information disclosure for both retailing theory and practice. But as novel technologies emerge, it is important to continue asking: What do we mean by information disclosure? Not all disclosure is created equal. How do the many and varied nuances surrounding information disclosure evoke other privacy concepts, pertaining to transparency, control, or trust? Are current theories in extant literature sufficient to facilitate a clear understanding of information disclosure? We posit that data privacy may be an important determinant of not just information disclosure but also of other consumer–retailer interactions. The insights derived from the articles in this special section also suggest that future investigations of information disclosure willingness and intentions need to shift in some concrete ways. We highlight three such ways.

First, many consumers willingly provide retailers with some limited, personal data (e.g., contact details, basic demographics). This form of information disclosure could be enhanced with practices and ideas suggested by the articles in this special section (Aiello et al. 2020; Bidler et al. 2020; Grosso et al. 2020), but as the nature of consumer information disclosure changes, its investigation also may need to be reimagined. For example, advanced retail technologies are not limited to traditional, online data entry fields that consumers populate manually to complete a purchase. Through novel touchpoint technologies such as location tracking, facial recognition, and emotion tracking, retailers can gather data invisibly and without explicit permission from consumers. Rather than making a conscious choice to disclose, consumers may lack an option to refuse. These changes raise new, highly sensitive privacy challenges and call into question existing theoretical views of consumer privacy and disclosure willingness (Okazaki et al. 2020). For example, consumers tend to define privacy according to whether they maintain control over their personal information (Martin and Murphy 2017; Stewart 2017). If technology-enabled touchpoints gather data without consumers' consent, or even their awareness, they inherently threaten this perceived privacy.

Second, beyond initial disclosures, consumers worry about retailers' use and protection of their data, and very few of them (5% in a recent survey) believe that retailers perform sufficiently

well (Sides et al. 2019). New technologies and opportunities to access consumer data continue to proliferate, but then so do potential threats and consumer concerns—especially among older consumers (55+ years) (Cisco 2019), a majority (73%) of whom acknowledge that they do not know and cannot manage how companies use their personal information. Around half (49%) believe they have no choice but to relinquish their data to receive services, and a similar percentage (46%) believe data protections are futile, because their information already is exposed. Younger consumers express concerns about retailers' use of their personal data too, including a sense that novel technologies may follow, spy, or eavesdrop on them, which prevents them from fully adopting certain retailer innovations. For example, nearly 70% of this consumer group report a reluctance to use voice technologies to engage with retailers, worried about intrusiveness or data security. As such, privacy issues can hinder technological adoption and retailer engagement (PwC 2018).

Third, retailers already have begun to reimagine consumer information exchanges using zero-party data disclosures. A term coined by Forrester Research, zero-party data refer to information that consumers knowingly, willingly provide to retailers in exchange for more meaningful personalization (Rowan 2020). The process for extracting zero-party data occurs in a conversation-like format between the retailer and consumer. Consumers receive incentives to engage in such conversations to gain better personalization, more appropriate product recommendations, and service suggestions. But the format still enables consumers to disclose only the information they want, in a format to which they agree. In other words, the data disclosure happens on consumers' terms. Retailers may encourage zero-party data disclosure with financial incentives and rewards, often under the auspices of effective loyalty programs (Palmatier and Martin 2019), and thus might offer worthwhile value for retailers too. In contrast, first-party data disclosures require retailers to make broad inferences about consumers' motivations from relatively basic, less personal consumer information. But with zero-party data, retailers might better understand why consumers behave in certain ways and in which contexts. Finally, because zero-party data disclosure is based on an existing consumer–retailer agreement, various transparency and control benefits should arise, which can engender trust and reduce both feelings of violation and the negative effects of unexpected data breaches (Martin et al., 2017). Consumers know what information they are sharing and why, so ultimately they can decide how much to reveal—which constitute ideal conditions to empower and foster trust. If the value received is sufficient, the consumer is more likely to share additional data over time, in cooperative rather than adversarial exchanges. Academic research has yet to investigate this new frontier of data disclosure; doing so may be highly fruitful.

Data Privacy and the Consumer Retail Journey

Aiello et al. (2020) capture consumer disclosure willingness at various phases of the consumer journey. Their insightful investigation demonstrates the relevance of consumer journey concepts for understanding data privacy and thereby highlights an important route for retailing theory and practice (Grewal and Roggeveen 2020). We recommend research into how data privacy unfolds throughout the retail experience and across the consumer journey too. Beyond intentional disclosures at the time of purchase, how should we understand how data privacy manifests, shifts, and changes during various phases in the consumer retail journey? In the discussion that follows and in Fig. 1, we map a series of data privacy concerns and questions across the consumer journey framework advanced by Grewal and Roggeveen (2020), consistent with Lemon and Verhoef (2016), suggesting research opportunities across phases and reflecting external influences.

Prepurchase. To date, data privacy in retail research mostly examines privacy concerns or events during the actual purchase stage. Yet the prepurchase phase of the consumer decision journey theoretically includes all consumer experiences that inform and lead up to an actual purchase. This phase encompasses the time from need recognition to purchase (Lemon and Verhoef 2016). In its most benign form, prepurchase uses of consumer data can produce product suggestions or cross-promotions. Potentially more serious, subversive, and influential violations also might occur in the prepurchase phase, designed to trigger consumer need recognition, define search parameters, or encourage a specific purchase. By definition, data privacy concerns can involve need recognition, suggesting an ability by retailers to use consumer information extracted in subversive ways to "suggest" or make salient specific consumption needs. In particular, a retailer might use consumer tracking or search history data, voice and text analyses, contents of email communications, social media posts, or even physical movement tracking to determine which product solutions to recommend during the customer's search. Academic research should seek to identify mutually beneficial ways for retailers to influence consumers during the prepurchase phase without violating their privacy or basic fairness considerations (e.g., charging a higher price to some consumers, on the basis of data gained from a prepurchase search). Can mutual benefit and value be created in the prepurchase phase, by using consumer data in ways that are transparent and provide consumers with more control?

Purchase. As Lemon and Verhoef (2016) note, the purchase phase of the consumer journey is the most widely investigated one in marketing research; the same trend holds for data privacy research in marketing and retailing. The substantial research that investigates consumers' willingness to disclose personal information to a retailer shows that this choice typically takes place at the moment of purchase. Thus it is pertinent for researchers to simulate a purchase transaction and ask participants if they would provide personal data in that situation. In practice, purchase interactions also are where retailers typically solicit consumer information, through personal information forms issued in digital channels or salesperson requests in brick-and-mortar settings. The former has received more research attention, likely reflecting the extensive use of online personal data requests during purchases. Even though such personal information is actively sought at this phase, it still represents first-party data, generally limited to basic demograph-

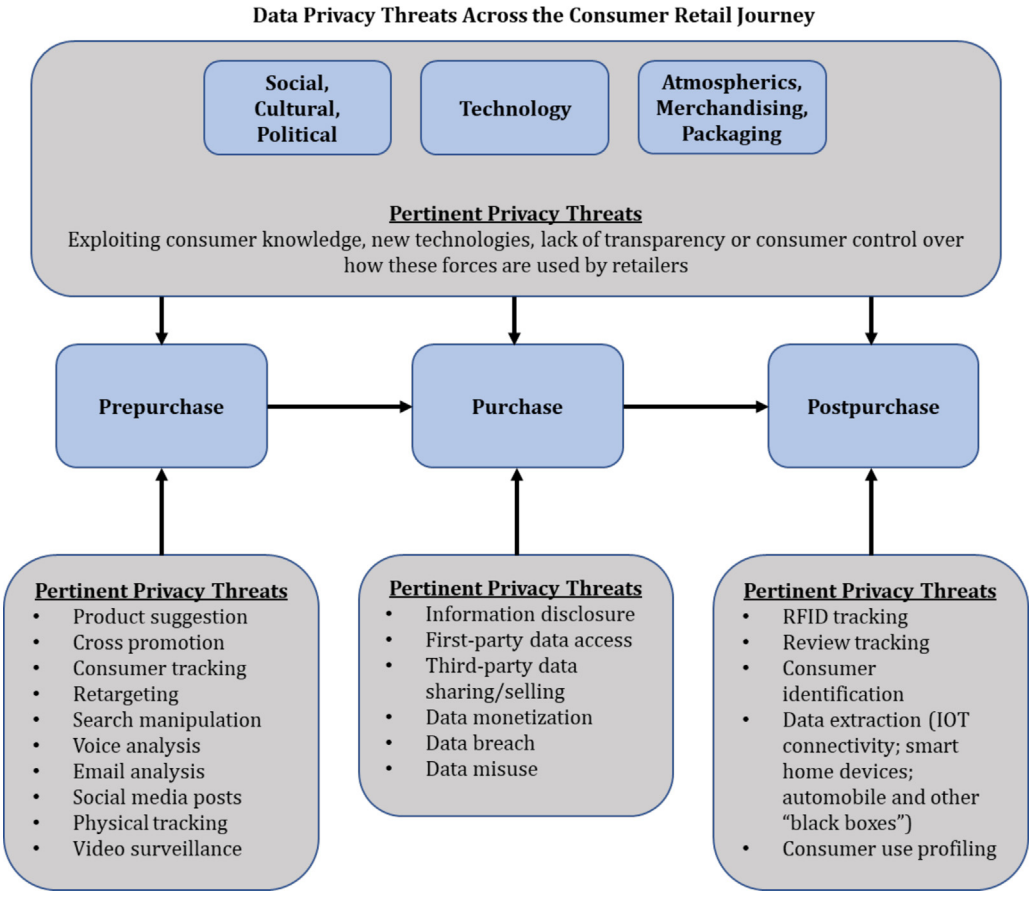

Fig. 1. Data Privacy Threats Across the Consumer Retail Journey.

ics or contact information from which retailers can only make indirect inferences. If researchers address the potential benefits of zero-party data exchanges at the time of purchase (or other phases of the customer journey), they might encourage a shift away from first-party tracking and inference making, as well as expand the use of zero-party data to reduce data monetization practices (i.e., consumer data extracted at the time of purchase are sold to various entities without consumer consent and contrary to their intentions). The purchase phase also is where consumer data tend to be breached, misused, or subject to identity theft. Researchers should seek solutions to prevent these catastrophic consumer privacy failures, as well as determine whether a firm can build a reputation for data and privacy protection that influences consumers' purchase decisions.

Postpurchase. Similar to prepurchase, the postpurchase phase of the consumer journey has received less attention associated with data privacy, despite its promise as a fruitful area of inquiry. This phase of the journey also appears particularly ripe for data privacy violations. Because it is lucrative for retailers to create a looping process (Grewal and Roggeveen 2020), in which a postpurchase phase reinforces the desire for future purchases and perhaps even engenders loyalty, retailers have considerable motivation to understand the consumer experience in this phase. Obtuse means for extracting postpurchase data include monitoring customer reviews, tracking social media activity, or requesting insights; in addition, RFID capabilities represent a potentially rich source of consumer data, because marketers can monitor how tagged products are consumed, shared, and disposed. In this sense, these technologies and their ability to garner highly personal, potentially sensitive information expose consumers to considerable privacy risks (Albrecht and McIntyre 2005). The proliferation of the Internet of Things (IoT) and smart home technologies also create postpurchase data privacy threats, because by design these smart devices monitor consumer behaviors and usage, relying on constant siphoning of consumer data. By many accounts, consumers do not realize the extent to which IoT and smart home devices extract their personal information (Molla 2019). Retailing scholarship thus might help create transparency and inform retail practice regarding appropriate, open, and honest uses of consumer data gathered through such technologies. Can meaningful dialogue occur between consumers and retailers on postpurchase topics, in ways that improve product performance and consumer experiences? For example, are there ways to make consumer reviews more dynamic and interactive so that the consumer and retailer exchange information willingly, rather than surreptitiously or in ways that promulgate conflict? How might open avenues for consumer–retailer cocreation ensure that meaningful consumer input on products and services is ongoing and gathered programmatically? Academic

research and practical insights about consumer data privacy at postpurchase phases thus are especially critical.

External forces. Beyond the three purchase phases, a variety of external forces shape the customer journey. Grewal and Roggeveen (2020) identify technological influences, sociocultural and political influences, and retail atmospherics; we assert that data privacy considerations inform or are informed by each of these forces too. Continued research should investigate data privacy as a critical outcome or driver of the way these forces influence the consumer journey. For example, how does private knowledge of a consumer's political affiliation shape a retailer's communication with that consumer in the prepurchase phase? Political affiliation affects postpurchase phase behaviors, such as dissatisfaction and complaining (Jung et al. 2017). If retailers are aware of this information, it might shape their postpurchase interactions, potentially leading to (un)favorable service interactions informed by political partisanship or complaint likelihood. Technology forces also create significant data privacy concerns because of their reliance on embedded uses of consumer data. Might novel technologies offer the intended benefits while still protecting consumer privacy? For example, consumers' prepurchase, in-store experience traditionally has been difficult to monitor and track. If technologies help retailers achieve this goal though, through technological systems and touchpoints, is there a way to avoid leading consumers to regard it as creepy? For example, perhaps interactive retail atmospheric tools might provide greater transparency, offer consumers some elements of control, and alleviate concerns. Similar protocols in a mobile environment also might make consumers more comfortable, such that they may perceive greater value from location tracking.

Channel-Specific Understanding

In their meta-analysis, Okazaki et al. (2020) find that privacy concerns differ by retail channel. Web channels decrease the effects of privacy concerns on usage behaviors and risk perceptions; social media channels increase disclosure and usage behaviors among those with high privacy concerns, but they also increase their risk perceptions. Such evidence of privacy concern variations across research contexts and retail platforms establishes that not all channels are created equally when it comes to consumer concerns and disclosures. Thus, in addition to moving beyond disclosure and accounting for the phases of the consumer retail journey, continued research needs to leverage multichannel investigations and analyses of data privacy questions. We examine some differences and suggest data privacy research devoted to web, mobile, social, and brick-and-mortar channels (Fig. 2). By mapping such variation, academic research can grant insights that inform retail practitioners about the best ways to mitigate data privacy concerns.

Web channels. Academic research has noted the need to investigate online privacy concerns since the early 2000s; Malhotra et al. (2004) adapt a privacy concerns scale to accommodate an online environment. Because the risks to data privacy in this channel are readily apparent, a flurry of research has followed, often focused on consumers' disclosure willingness toward online retailers. Beyond disclosure, notable topics include consumers' awareness of online tracking by cookies (Miyazaki 2008) and targeted advertising by retailers on web platforms (Kim et al., 2019). Less studied yet equally worthy of investigation is the question of how multiple consumer tasks performed across the web might interact to threaten consumer privacy. Are email and social platforms being integrated with mobile interfaces to surreptitiously profile consumers? To what extent are consumers aware of this integration, and do they employ persuasion knowledge to interpret personalization or targeted advertising suspiciously? Especially as millions of workers, students, and others have relied on online channels to work, attend school, and so forth during the COVID-19 pandemic, data repositories and third-party data aggregators have gained access to vastly increased personal information. With so many household members conducting their daily lives online, what are the implications for online retailers attempting to delineate who is doing what, and which purchases are made for whom? Do consumers welcome the convenience of online retail transactions, replacing in-person interactions, so much that they willingly relinquish their data? Or do increased daily online interactions make them more skeptical and jaded about providing even more information?

Social media channels. Social spaces by definition should allow consumers to share freely and disclose even highly sensitive information, in different formats (e.g., text, pictures, videos). Social media build community and are premised on ideas of sharing and open, transparent communication. Yet popular social media spaces such as Facebook have endured significant reputational damage due to their lack of data privacy protections, monetization of personal data, and massive data breaches. Such tensions should inform retailers seeking to establish a social media presence. Facebook, Twitter, and Pinterest feature "buy buttons" that allow consumers to complete purchases directly on the platforms (Meola 2019), so protecting data privacy is an increasingly complex task, and consumers must worry about data protections by both the retailer and the social media site. The retailer's presence manifests differently on social media versus e-commerce websites; do consumers relate to it differently, depending on the channel they use? For example, might consumers interact with retailers in social spaces more freely, willingly disclosing more information than if they visited a web store? If so, are consumers at greater risk? Retailers also should determine if they can foster stronger consumer relationships in social spaces by using messaging about privacy, as they use offline or on the web, or if different privacy interactions are required in social and community-like spaces.

Mobile. Mobile retailing has experienced dramatic growth, in the purchase stage and the prepurchase stage, particularly in relation to search efforts (statista.com). Mobile devices offer retailers a wealth of information about consumers' search habits, activities, and geographic movements. When paired with brick-and-mortar retail locations, mobile data allow retailers to triangulate movement and infer patterns. Such uses of consumer data are fraught with privacy concerns and subject to ethical debates. By using geoconquesting for example, a retailer can identify a consumer's geographic proximity to a competing

Data Privacy Research Directions: Selected Questions by Retail Channel Type

Web Channels	Mobile Channels
• Do consumers understand the extent and threat of data integration across multiple web/ecommerce channels with which they do business? Across face-to-face, mobile, and social interactions? • To what extent do consumers exhibit sufficient skepticism of retargeted ads or more surreptitious uses of their data across web channels? • How do consumers maintain the integrity of their (and their families') unique data profiles when so many people now work and school from home on connected devices? • How do consumers and retailers navigate fatigue and reluctance to share information when previously face-to-face transactions have moved online?	• How can retailers employ real-time, geographic targeting without appearing to stalk consumers? Can better consumer opt-in preferences be embedded into technologies? • What are long-term effects of geolocation monitoring and targeting on consumer trust and feelings of violation or harm? Should consumer vulnerability be accounted for? • For what types of mobile communications must explicit permission be sought to protect consumer privacy? Can retailers employ sufficient transparency with mobile ads? • How can researchers and retailers identify consumer preferences in this emerging channel to safeguard privacy while still enabling innovation?
Social Channels	**Brick-and-Mortar Channels**
• How do past privacy violations (e.g., Facebook and Cambridge Analytica) influence consumers' willingness to engage with retailers on these sites? • Given differences in consumer interfaces on web versus social platforms, do consumers understand and/or manage their data privacy preferences differently? How can retailers help in this process? • Does the community-based premise of social media lead to greater information disclosure to retailers on these platforms? Does it pose a consumer risk? • How do consumers manage relationships with retailers in these spaces while still guarding their privacy? How might the consumer journey unfold here?	• In what ways can academic research help understand technology integration/data triangulation within physical retail locations to protect consumer privacy? • Can retail theory and practice shed light on vast repositories of in-store video and surveillance and the measures in place to prevent wrongful identification? • Can facial recognition and consumer monitoring in physical retail locations offer consumer decision journey insights? If so, how should we glean them and still protect consumer privacy? • How do atmospherics, merchandising, and other elements of the retail environment interact to promote/prohibit consumer information disclosure?

Fig. 2. Data Privacy Research Directions: Selected Questions by Retail Channel Type.

retailer and send targeted messages or promotions, in an effort to thwart a sale. Accordingly, geolocation marketing can appear creepy and heighten consumer worries about being stalked. These technologies may shift consumer behavior in real-time though, so research is needed to understand the effects on consumer trust or violations of it. For example, if benign promotions do not hinge on location tracking, privacy concerns may be severe if retailers communicate through mobile channels, without explicit permission to do so. These messages appear more personal and intrusive than an email or targeted web ad, putting retailers at risk of backlash. In short, more research is needed to avoid unintended implications that stymie what appears to offer a sustainable retail growth option, ripe for innovation, without risking consumers' safety or challenging their communication channel preferences.

Brick-and-mortar. Even physical retail spaces leave consumers open to data privacy threats, especially those that contain novel technologies for consumer location tracking, movement monitoring, and mobile device recognition. To understand pre-purchase phases of the retail journey, retailers might track consumers' movements, using smartphone connections to the retailer's wifi, tracking kiosks and displays, or RFID integration between physical in-store markers and consumer loyalty cards. Traditional technologies have their own privacy risks though. In a study of *Fortune* 500 firms' privacy policies, Martin, Borah, and Palmatier (2018) find that many retailers disclose their practice of actively recording in-store video, but their tactics for doing so safeguard their interests in capturing and retaining consumer data and even selling those data to undisclosed third parties. Often such practices are framed as loss prevention efforts, but when coupled with facial recognition technology for example, they leave consumers prone to privacy threats. Although recent research has advanced our understanding of privacy threats in physical retail spaces (Esmark and Noble 2018; Esmark et al., 2017; Esmark et al. 2020), continued studies should investigate data privacy threats and consumer responses to them.

Conclusion

Firms can benefit from strengthening privacy practices and implementing customer-protecting privacy policies (for an overview, see Palmatier and Martin 2019). Customer-centric retailers thus have moved past arbitrary or haphazard exploitation of big data and data analytics (Business Wire 2019) and instead seek payoffs from mutually valuable consumer relationships and stronger company privacy practices. Business evidence affirms that firms with stronger data privacy practices enjoy tangible benefits (Cisco 2020), including shorter sales delays; diminished harm from data breaches; and enhanced agility, innovation, operational efficiency, investor appeal, customer loyalty, and customer trust. Returns on investments in

data privacy are estimated to reach 270%; larger firms report returns greater than 400% (Cisco 2020). The result may be a more authentic consumer experience, in which people can choose which retailers may target them, with which products and services, rather than accepting random contacts from brands in which they have no interest.

Data privacy research in retailing thus has flourished in recent years, as the pages of past issues of the *Journal of Retailing* show. With this particular special section, we also seek to highlight the ways that nuances of the retail environment and a vibrant retailing academic community make consumer data privacy research an especially ripe context for continued investigation. We hope this special section inspires ongoing work in this domain, by scholars and practitioners who focus their energies and talents on customer data privacy tensions. Such work can offer a source of realized mutual benefits and actionable solutions for consumers and retailers alike.

References

Aguirre, Elizabeth, Dominik Mahr, Dhruv Grewal, Ruyter Ko de and Martin Wetzels (2015), "Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness," *Journal of Retailing,* 91 (1), 34–49.

Aiello, Gaetano, Raffaele Donvito, Valentina Mazzoli, Laura Grazzini, Diletta Acuti and Virginia Vannucci (2020), "Privacy Roller-Coaster: Consumers' Willingness to Disclose Personal Information Throughout the Customer Journey in the Retail Context," *Journal of Retailing,* 96 (December), 490–506.

Albrecht, Katherine and Liz McIntyre (2005), *Spychips: How Major Corporations and Government Plan to Track your Every Purchase and Watch Your Every Move,* Nashville: Nelson Current.

Auxier, Brooke, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar and Erica Turner (2019), "How Americans Think About Privacy and the Vulnerability of Their Personal Data," *Pew Research Center,*. November 15, https://www.pewresearch.org/internet/2019/11/15/how-americans-think-about-privacy-and-the-vulnerability-of-their-personal-data/, downloaded April 6, 2020

Barth, Susanne and Menno D.T. de Jong (2017), "The Privacy Paradox: Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior: A Systematic Literature Review," *Telematics and Informatics,* 34 (November), 1038–58.

Bidler, Margarita, Johanna Zimmerman, Jan H. Schumann and Thomas Widjaja (2020), "Previewing a Meaningfully Gamified Data Disclosure Process to Increase Consumers' Willingness to Engage in Data Disclosure Processes," *Journal of Retailing,* 96 (December), 507–532.

Bleier, Alexander and Maik Eisenbeiss (2015), "The Importance of Trust for Personalized Online Advertising," *Journal of Retailing,* 91 (September), 390–409.

Brough, Aaron R. and Kelly D. Martin (2020), "Critical Roles of Knowledge and Motivation in Privacy Research," *Current Opinion in Psychology,* 31, 11–5.

Business Wire (2019), *Big Data Analytics in Retail Market Growth, Trends and Forecast 2019-2024: Growth of e-Commerce, Online Shopping, and High Competition for Customer Loyalty,* (accessed March 29, 2020), [available at: https://www.businesswire.com/news/home/20190626005385/en/Big-Data-Analytics-Retail-Market-Growth-Trends].

Cisco (2020), "From Privacy to Profit: Achieving Positive Returns on Privacy Investments," *Cisco Cybersecurity Series: Data Privacy Benchmark Study,*. January,. www.cisco.com/go/securityreports

——— (2019), "Consumer Privacy Survey: The Growing Imperative of Getting Data Privacy Right," *Cisco Cybersecurity Series,*. November,. www.cisco.com/go/securityreports

Esmark, Carol L. and Stephanie M. Noble (2018), "Retail Space Invaders: When Employees' Invasion of Customer Space Increases Purchase Intentions," *Journal of the Academy of Marketing Science,* 46 (May), 477–96.

Esmark, Carol L., Stephanie M. Noble and Michael J. Brazeale (2017), "I'll Be Watching You: Shoppers' Reactions to Perceptions of Being Watched by Employees," *Journal of Retailing,* 93 (September), 336–49.

Esmark, Carol L., Jennifer L. Stevens, Stephanie M. Noble and Michael J. Brazeale (2020), "Panic Attack: How Illegitimate Invasions of Privacy Cause Consumer Anxiety and Dissatisfaction," *Journal of Public Policy & Marketing,* 39 (July), 334–52.

Grewal, Dhruv and Anne L. Roggeveen (2020), "Understanding Retail Experiences and Customer Journey Management," *Journal of Retailing,* 96 (March), 3–8.

Grosso, Monica, Sandro Castaldo, Li Hua (Ariel) and Bart Lariviere (2020), "Contextualizing the Privacy Paradox in Retail: A Multi-level, Multi-country, Multi-industry Analysis of the Roles of Trust and Information Sensitivity," *Journal of Retailing,* 96 (December), 533–556.

Inman, J. Jeffrey and Hristina Nikolova (2017), "Shopper-Facing Retail Technology: A Retailer Adoption Decision Framework Incorporating Shopper Attitudes and Privacy Concerns," *Journal of Retailing,* 93 (1), 7–28.

Jung, Kiju, Ellen Garbarino, Donnel A. Briley and Jesse Wynhausen (2017), "Blue and Red Voices: Effects of Political Ideology on Consumers' Complaining and Disputing Behavior," *Journal of Consumer Research,* 44 (October), 477–99.

Kim, Tami, Kate Barasz and Leslie K. John (2019), "Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness," *Journal of Consumer Research,* 45 (February), 906–32.

Lemon, Katherine N. and Peter C. Verhoef (2016), "Understanding Customer Experience Throughout the Customer Journey," *Journal of Marketing,* 80 (November), 69–96.

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

Martin, Kelly D., Abhishek Borah and Robert W. Palmatier (2018), "A Strong Privacy Policy Can Save Your Company Millions," *Harvard Business Review,*. February 15 [available at: https://hbr.org/2018/02/research-a-strong-privacy-policy-can-save-your-company-millions]

———, ——— and ——— (2017), "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing,* 81 (January), 36–58.

Martin, Kelly D., Jisu J. Kim, Robert W. Palmatier, Lena Steinhoff, David W. Stewart, Beth A. Walker, Yonggui Wang and Scott Weaven (2020), "Data Privacy in Retail," *Journal of Retailing,* 96 (December), 474–489.

Martin, Kelly D. and Patrick E. Murphy (2017), "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science,* 45 (March), 135–55.

Meola, Andrew (2019), "Rise of M-Commerce: Mobile Ecommerce Shopping Stats and Trends in 2020," *Business Insider,*. December 17, (accessed September 10, 2020), [available at: https://www.businessinsider.com/mobile-commerce-shopping-trends-stats]

Merriam-Webster (2020), *Online Dictionary*, https://www.merriam-webster.com/dictionary/tension.

Miyazaki, Anthony D. (2008), "Online Privacy and the Disclosure of Cookie Use: Effects on Consumer Trust and Anticipated Patronage," *Journal of Public Policy & Marketing,* 27 (Spring), 19–33.

Molla, Rani (2019), "People Say They Care About Privacy but They Continue to Buy Devices That Can Spy on Them," *Vox,*. May 13, (accessed September 10, 2020), [available at: https://www.vox.com/recode/2019/5/13/18547235/trust-smart-devices-privacy-security]

Okazaki, Shintaro, Martin Eisend, Kirk Plangger, Ruyter Ko de and Dhruv Grewal (2020), "Understanding the Strategic Consequences of Customer Privacy Concerns: A Meta-Analytic Review," *Journal of Retailing,* 96 (December), 458–473.

Palmatier, Robert W. and Kelly D. Martin (2019), *The Intelligent Marketer's Guide to Data Privacy,* New York: Palgrave.

Petro, Greg (2019), "Retailers Walking a Tightrope Between Data Privacy and Personalization," *Forbes,*. May 17, (accessed September 13, 2020), [available at: https://www.forbes.com/sites/

gregpetro/2019/05/17/retailers-walking-a-tightrope-between-data-privacy-and-personalization/#2eba356e2fca]

PwC (2018), "Prepare for the Voice Revolution," *Consumer Intelligence Series,*, www.pwc.com/cisvoiceassistants

Rowan, Mike (2020), "Is Zero-Party Data the Way Forward for Personalized Marketing?," *Forbes,*,. March 23, (accessed September 13, 2020), [available at https://www.forbes.com/sites/forbesagencycouncil/2020/03/23/is-zero-party-data-the-way-forward-for-personalized-marketing/#6b0e735bb324]

Sides, Rod, Matt Marsh, Rob Goldberg and Michael Mangold (2019), "Consumer Privacy in Retail: The Next Regulatory and Competitive Frontier," *Deloitte Development,, LLC*. www.deloitte.com

Stewart, David W. (2017), "A Comment on Privacy," *Journal of the Academy of Marketing Science,* 45 (2), 156–9.

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