Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

ELSEVIER

Journal of Retailing 96 (4, 2020) 474–489

Journal of Retailing

Data Privacy in Retail

Kelly D. Martin [a,*], Jisu J. Kim [b], Robert W. Palmatier [b], Lena Steinhoff [c], David W. Stewart [d], Beth A. Walker [a], Yonggui Wang [e], Scott K. Weaven [f]

[a] College of Business, Colorado State University, Fort Collins, CO 80523-1278, USA
[b] Michael G. Foster School of Business, University of Washington, 254 Mackenzie Hall, Box 353200, Seattle, WA 98195-3200, USA
[c] Institute for Marketing and Service Research, Faculty of Business and Social Sciences, University of Rostock, USA
[d] 319 Conrad Hilton Business Center, Loyola Marymount University, 1 LMU Drive, Los Angeles, CA 90045, USA
[e] Capital University of Economics and Business (CUEB), Beijing, China
[f] Department of Marketing, Griffith Business School, Department of Marketing, Griffith University, Queensland 4222, Australia

Available online 21 September 2020

Abstract

Unprecedented, exponential growth in the amount of consumer data collected by retailers across various customer touchpoints has made safeguarding data privacy a key priority. Data privacy in retail contexts requires convergence among three key stakeholders—consumer, retailer, and regulatory—each of which has unique roles and viewpoints. With a global perspective and a multimethod data collection approach, combining in-depth expert interviews, a large-scale consumer survey across four countries, and global case studies, this research identifies three emergent themes for understanding the convergence of these three stakeholders' interests: (1) big data as a driver of customer relationship performance, (2) profound impacts of regulation, and (3) privacy protection as a proactive retail strategy. These themes underscore the complex interrelations among consumers, retailers, and regulatory forces. The delineated research opportunities in turn may foster deeper understanding of these stakeholders, their perspectives, and their convergence.

Keywords: Data privacy; Big data; Privacy concerns; Personalization; Privacy regulation

Understanding data privacy in retail settings demands consideration of the convergence of consumer, retailer, and regulator interests. For all three types of actors, dramatic transformations affect their shared and unique roles with regard to ensuring data privacy in the current big data and advanced data analytics era. As retailers gather vastly increasing amounts of data—expected to increase in size from 33 zettabytes (1 zettabyte = 1 trillion gigabytes) in 2018 to 175 zettabytes by 2025 (Sides et al. 2019)—*consumers* express discomfort about the risk of data breaches and retailers' use of "uber-personalized" contacts that feel invasive and creepy (PwC 2018). Yet nearly 74% of *retailers* report their plans to increase their technology spending (TotalRetail 2019) and customer personalization through tools such as location tracking, facial recognition, emotion tracking, and voice encoding and interpretation, all of which might aggravate consumers' sense of vulnerability (Martin, Borah, and Palmatier 2017). This sense of vulnerability is particularly heightened during turbulent times, such as the COVID-19 pandemic, in which context increasingly sensitive consumer data (body temperature, contact identities, travel history) may be accessed and used by various actors (Brough and Martin 2020). In response to such tensions, *regulators* are enacting and revising their policies, such as Europe's General Data Protection Regulation (GDPR), California's Consumer Privacy Act (CCPA), and dozens of other regulations adopted at state and local government levels (Palmer 2019).

The convergence of these three main stakeholder groups' interests in data privacy may represent a tipping point for big data and privacy, producing both salient risks and privacy threats, but also great potential for retailers. Increasing

* Corresponding author.
E-mail addresses: kelly.martin@colostate.edu (K.D. Martin), jisukim2@uw.edu (J.J. Kim), palmatrw@uw.edu (R.W. Palmatier), lena.steinhoff@uni-rostock.de (L. Steinhoff), david.Stewart@lmu.edu (D.W. Stewart), beth.walker@colostate.edu (B.A. Walker), wangyonggui@cueb.edu.cn (Y. Wang), s.weaven@griffith.edu.au (S.K. Weaven).

https://doi.org/10.1016/j.jretai.2020.08.003
0022-4359/

evidence signals that stakeholders are seeking new ways to protect and expand consumer privacy, using collaborative rather than confrontational approaches. Such developments are not well reflected in current retailing research, which continues to focus primarily on confrontational, risky, and threatening themes (Martin and Murphy 2017). Inspired by the positive, collaborative developments at the consumer–retailer–regulatory interface, we seek explicitly to consider the bright side, by *examining manifestations of data privacy from a global perspective; integrating the roles of consumer, retailer, and regulatory stakeholders; and delineating research opportunities that are germane to gaining a better understanding of each stakeholder group*.

In particular, by leveraging extant research and a multimethod approach to collect original, empirical data, we identify three emergent themes that catalyze collaboration and increasing consumer–retailer–regulatory convergence in relation to the collection and uses of consumer data in retail. First, we substantiate the role of *big data as a driver of customer relationship performance*, because it enhances customer value perceptions. Second, we underscore the *profound impact of regulation* in shaping consumer–retailer interactions. Third, we shed light on the potential of *privacy protection as a proactive retail strategy*, which can provide an innovative source of competitive advantages for retailers.

In our multimethod approach, we corroborate each theme by integrating insights from qualitative and quantitative data sources. First, we conducted depth interviews with eight senior-level executives from different industries, to gain their expert perspectives on retailers' data privacy practices. Second, we conducted a large-scale, global survey of 1,007 consumers across four countries (Australia, China, Germany, United States), which captures their general and industry-specific (retail, IT, financial services) data privacy experiences. Third, our global research team used select survey findings to develop brief, in-depth case studies pertaining to relevant issues in global data privacy business practices. Jointly, these data collection and analysis efforts provide a unique perspective on consumer–retailer–regulatory convergence and inform our three emergent themes.

Accordingly, this study advances extant knowledge in three main ways. First, we establish emergent themes to illustrate current issues related to the collection and use of consumer data in retail settings. Each theme arose from and is substantiated by three data sources, such that the combination of qualitative (depth interviews, case studies) and quantitative (survey) methodologies underscore the validity of findings. Together, the three themes provide a more balanced view of the potentials and pitfalls of data privacy in retail, emphasizing bright-side evidence that tends to be ignored by current perspectives on related topics. Although each theme focuses on one of the three key stakeholder groups—consumer (Theme 1), regulation (Theme 2), or retailer (Theme 3)—they also reflect the convergence and interrelations among those stakeholders. For example, regulation shapes the consumer–retailer interaction, in that retailers must adhere to privacy regulations in their dealings with consumers. These three themes coherently emphasize the complex interactions and diverse perspectives that must be taken into account in data privacy research in retailing.

Second, we provide a global perspective on data privacy. Most extant research focuses on a single country, or even a specific firm in a single country, depending on the availability of empirical data. The United States is overrepresented. Yet privacy perspectives are driven by a country's culture, so consumers', regulators', and retailers' views on data privacy are inevitably (whether consciously or subconsciously) influenced by their cultural environment. Our survey consolidates perspectives of consumers across four countries on four continents, thus offering rich insights gathered from a culturally diverse sample of consumers. The case studies in turn showcase country-specific examples of differential retailer or regulatory approaches to data privacy and consumers' reactions, which establishes an outline of key tensions in global privacy perspectives, to inform retailers seeking to expand to other countries and cultures.

Third, we delineate rich research opportunities that can systematically enhance understanding of the three key stakeholders in retail data privacy contexts. Knowledge pertaining to their convergence has remained relatively limited. To advance data privacy research, we need a solid foundation, reflecting shared and unique perspectives, motivations, and influence mechanisms, across consumers, retailers, and regulatory groups. In support of this effort, we propose specific research avenues and questions that researchers may pursue to gain deeper knowledge about each actor, move the field toward a big picture of the retail privacy triad, and facilitate identification of interrelations, tensions, and bright spots across these stakeholders.

Data Privacy in Retail: Emergent Themes from a Global Perspective

In reviewing research in multiple disciplines, we find that privacy notions largely have been applied in contexts specific to consumers, regulation, or retail. These ongoing conversations in separate research streams provide preliminary evidence of the three emergent themes involving consumers, regulation, and retailers as three key stakeholders when it comes to data privacy in retail settings (Fig. 1). For *consumers*, big data support increasing personalization, as offered and investigated by practitioners and researchers. Bleier and Eisenbeiss (2015) observe that online personalized ads improve click-through rates, especially in early purchase decision stages, but that over-personalization is possible if customers' preferences are unstable and change over time. Other studies explore how to leverage big data, with methods such as adaptive personalization using social networks (Chung, Wedel, and Rust 2016) or latent Dirichlet allocations to mine online chatter and understand brand positioning (Tirunillai and Tellis 2014).

Privacy protection instead might be used as a competitive strategy by *retailers* (Martin and Murphy 2017). According to theoretical models, firms can profit by differentiating consumers by their preferred level of information disclosure, though doing so might diminish disclosure-related revenues (Casadesus-Masanell and Hervas-Drane 2015). In an exploration of the emerging idea of allowing customers to pay for

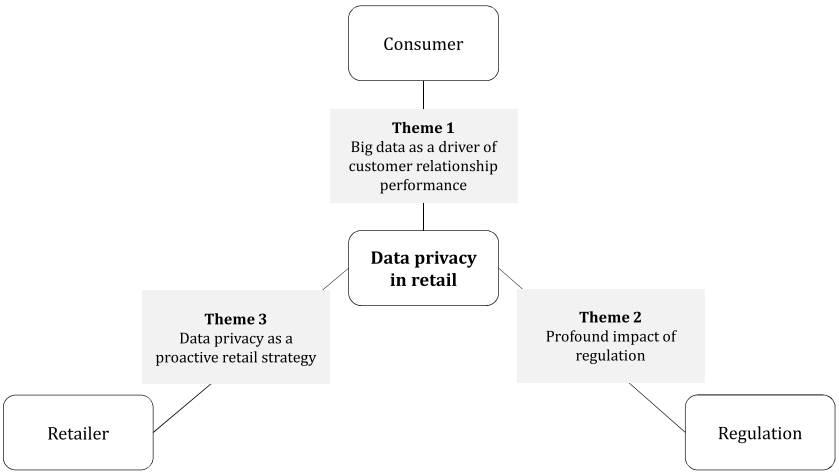


Fig. 1. Three emergent themes on data privacy in retail.

privacy, the findings indicate that in a duopolistic setting, firms do not necessarily benefit from charging more for privacy, whereas privacy costs always increase profits in monopolistic settings (Montes, Sand-Zantman, and Valletti 2019).

The interactions of consumers and retailers also depend on privacy *regulations*. Such privacy policies can be a good proxy for the degree of transparency and control that firms provide their customers, which then inform both customer and firm performance (Martin, Borah, and Palmatier 2017). Moreover, stronger privacy policies can mitigate the potentially negative spillover effects triggered by a data breach suffered by a close competitor (Martin, Palmatier, and Borah 2018). Although empowering customers with data privacy can help mitigate the negative impacts of breaches, in certain conditions, regulations that require full privacy can be detrimental to consumer welfare (Taylor and Wagman 2014). Contrary to a general sense that privacy regulations are costly to firms, a recent study shows that policies that require firms to ask for consent to obtain customers' personal information can benefit both consumers and firms, assuming conditions of asymmetric competition and price discrimination (Hoffmann, Inderst, and Ottaviani 2020).

Investigative Approach

We draw from these three research streams to examine consumer–retailer–regulatory convergence and study their interconnections, rather than their separate or unique implications. To establish novel insights about the role of big data and privacy for retail, as well as substantiate consumer-, retailer-, and regulation-specific insights from extant research, we collect data using three approaches. In our attempt to understand firms' experiences with managing data and protecting privacy, we started by conducting in-depth interviews with eight senior-level executives who determine or manage their firms' data privacy practices (Table 1). We identified these informants from leads gathered from an advisory board on which one of the authors is a member; colleagues from this board provided additional relevant contacts. The interviews were conducted by two authors via conference call, which were recorded and transcribed. The interview protocol includes eleven questions, pertaining to opportunities and challenges associated with data privacy and the role of data privacy in retail, regardless of their own industry orientation. We also encouraged these expert informants to take the conversation in topical directions of their choosing. Their industry profiles and experience involve market research, privacy solutions, consulting, financial services, and health care.

Then a second data collection effort involved a large-scale, global survey conducted in four countries on four continents: Australia, China, Germany, and the United States. The author team created and pretested the research instrument, which consisted of questions about consumers' experiences with data privacy. The respondents indicated their general sense of vulnerability if they grant companies access to their personal information, their degree of worry about data disclosures, their privacy concerns, and their perceptions of regulations and protections, among other topics. Members of the author team, local to each country in which the survey was administered, translated and back-translated the instrument, then administered it to a minimum of 200 respondents in each country, recruited using local online data collection platforms. Table 2 provides details about the data collection procedures. Survey measures are detailed in Appendix, and Table3 contains the descriptive statistics and correlations aggregated over the four country samples.

In addition to general data privacy perceptions, the 1,007 respondents across the four countries provided insights specific to a company they chose, from the retail, IT, or financial services sector. That is, for each randomly assigned sector, respondents selected the company they purchased from most frequently, from a drop-down list of five consumer-facing firms. These firms were the top five companies in terms of sales revenue within each sector, according to the *Fortune* ranking in the United States and equivalent, country-specific rankings available in Australia, China, and Germany. The participants indicated the perceived data-enabled value they received from this firm as customers, as well as their share of wallet, loyalty intentions, switching intentions, and willingness to opt-in to data sharing with this focal firm. Fig. 2 presents the outcome variables by country and industry. If a respondent did not purchase from any of the listed

Table 1
Depth interviews: informants' executive profiles.

Informant	Role	Company business scope	Years data privacy experience	Connection to retail environment
1	Business Unit President	Global Privacy Solutions	19	Retail Company Clients
2	Chief Security Officer, Chief Privacy Officer, Chief Compliance Officer	B2B Software Security	23	Retail Company Clients
3	Chief Executive Officer	Human Resources Solutions	25	Retail Company Clients
4	Chief Privacy Officer	Retail and Financial Services	17	Retail End Consumers
5	Chief Executive Officer	Health Rating and IT	21	Retail End Consumers
6	Chief Confidentiality Officer	Global Consulting	28	Retail Company Clients
7	Director	IT Consulting	5	Retail Company Clients
8	Chief Executive Officer and Founder	Privacy Solutions	10	Retail Company Clients

firms, she or he was reassigned to another sector and drop-down list. If they could not identify any company across any of the three sectors, respondents were thanked and redirected to the end of the survey.

Finally, after analyzing the survey findings, the research team worked together to derive short case studies about a particular question or finding of interest that emerged from the data. Thus, the three themes we present are informed by insights from our interviews, survey findings, and short case studies in a global context.

Theme 1: Big Data as a Driver of Customer Relationship Performance

As a fundamental premise, big data drive superior retail performance. This ability to enhance firm performance outcomes underpins retailers' quest for new technologies and new ways of interacting with customers. Because their multiple, varied, data-based applications have proven so beneficial, retailers appear unlikely to scale back their big data efforts (TotalRetail 2019). Consumers also reap rewards. Thus, the mutual benefits drive firm performance generally and customer relationship performance specifically. Elements of this emergent theme arose from all three of our investigative approaches.

Interview insights

We asked the executive informants to describe their experiences and impressions working with retailers that use customer data. A director of IT consulting for a large, international company described customer data and their management as foundational to retailer success, echoing academic insights and evidence (Bradlow et al. 2017; Grewal, Roggeveen, and Nordfält 2017). This informant's firsthand knowledge, gained from advising retail clients, informs his perspective, which pertains directly to the first emergent theme:

> Retailing is a bit ahead of the curve, yet still subject to data breaches. They have put themselves out there to create personal experiences, so they have learned to protect customer data. While they are not perfect, they know they need to do this to be competitive. Everyone wants the Amazon effect. Market forces are pushing in this direction.

That is, even if some retail practices or approaches increase worry, consumers value personalized experiences (Aguirre et al. 2015), and capabilities and technologies that provide personalized experiences are well-positioned to fulfill this value proposition, which constitutes an important source of competitive advantage (Inman and Nikolova 2017). An IT consulting director affirms the effectiveness of big data for retail clients, such that

> Data provide a huge competitive advantage. Personalization works as a marketing strategy. Customers like it but it requires data.

This quote provides an excellent summary of the mutual consumer–retailer benefits of big data: They facilitate rich customer connections and retailer advantages, and the value often is enough that customers willingly relinquish information to obtain it.

Survey insights

The global survey responses reveal customer-level perceptions of the data-enabled value they receive from the companies they select, in relation to four behavioral outcomes: reported share of wallet, loyalty intentions, switching intentions, and willingness to opt-in to the company's data collection efforts. With a two-level hierarchical multivariate analysis (customers nested within companies) using HLM 8.0, we regress the four outcomes on two forms of data-enabled customer value, which reflect customers' perceptions of firms' ability to tailor the purchase experience or prices to their individual tastes (Chellappa and Sin 2005). These two measures of data-enabled customer value capture the extent to which customers believe the company provides (1) a better experience by using customers' personal information (customer experience value) and (2) lower prices or even free services, due to its use of customer data (customer economic value).

Table 2
Global survey: data collection details.

Sample characteristic	Country Australia	China	Germany	United States	Overall
Collaborating consumer panel provider	Qualtrics Australia	Wenjuanxing	Consumerfieldwork	Qualtrics U.S.	—
Survey language	English	Chinese	German	English	—
Sample size	235	300	225	247	1007
Respondent gender					
Female	125 (53.2%)	144 (48.0%)	115 (51.1%)	173 (70.0%)	557 (55.3%)
Male	110 (46.8%)	148 (49.3%)	110 (48.9%)	72 (29.1%)	440 (43.7%)
Prefer not to say	0 (.0%)	8 (2.7%)	0 (.0%)	2 (.8%)	10 (1.0%)
Respondent age group					
18-24 years	37 (15..7%)	70 (23.3%)	21 (9.3%)	40 (16.2%)	168 (16.7%)
25-34 years	42 (17.9%)	107 (35.7%)	35 (15.6%)	77 (31.2%)	261 (25.9%)
35-44 years	39 (16.6%)	75 (25.0%)	33 (14.7%)	58 (23.5%)	205 (20.4%)
45-54 years	35 (14.9%)	26 (8.7%)	44 (19.6%)	24 (9.7%)	129 (12.8%)
55-64 years	35 (14.9%)	16 (5.3%)	37 (16.4%)	17 (6.9%)	105 (10.4%)
65+ years	47 (20.0%)	6 (2.0%)	55 (24.4%)	2 (.8%)	110 (10.9%)
Prefer not to say	0 (.0%)	0 (.0%)	0 (.0%)	29 (11.7%)	29 (2.9%)
Respondents per sector					
Retail	75 (32.0%)	104 (34.7%)	72 (32.0%)	76 (30.8%)	327 (32.5%)
IT	80 (34.0%)	102 (34.0%)	79 (35.1%)	83 (33.6%)	344 (34.1%)
Financial services	80 (34.0%)	94 (31.3%)	74 (32.9%)	88 (35.6%)	336 (33.4%)
Retail company selected					
Top 1	Harvey Norman (30; 40.0%)	Tmall (74; 71.2%)	Amazon.de (60; 83.4%)	Walmart (43; 56.6%)	—
Top 2	Myer (21; 28.0%)	JD (26; 25.0%)	Otto (5; 6.9%)	Amazon (21; 27.6%)	—
Top 3	Kogan (12; 16.0%)	Suning (2; 1.9%)	Müller (5; 6.9%)	Target (9; 11.8%)	—
Top 4	David Jones (8; 10.7%)	Gome (2; 1.9%)	Galeria Kaufhof (1; 1.4%)	Costco (2; 2.6%)	—
Top 5	Costco (4; 5.3%)	Dashang (0; .0%)	Karstadt (1; 1.4%)	Macy's (1; 1.3%)	—
IT company selected					
Top 1	Apple (35; 43.8%)	Huawei (47; 46.1%)	Google (33; 41.8%)	Google (39; 47.0%)	—
Top 2	Samsung (19; 23.8%)	ZTE (26; 25.5%)	Microsoft (22; 27.8%)	Apple (31; 37.3%)	—
Top 3	Microsoft (18; 22.5%)	Inspur (17; 16.7%)	Samsung (13; 16.5%)	Microsoft (10; 12.0%)	—
Top 4	Telstra (8; 10.0%)	China UnionPay (8; 7.8%)	Huawei (6; 7.6%)	Dell (3; 3.6%)	—
Top 5	Fujitsu (0; 0.0%)	Haier group (4; 3.9%)	Apple (5; 6.3%)	IBM (0; .0%)	—
Financial services company selected					
Top 1	Commonwealth Bank (31; 38.8%)	ICBC (29; 30.9%)	Sparkasse (49; 66.2%)	Chase Bank (27; 30.7%)	—
Top 2	ANZ (15; 18.8%)	CCB (27; 28.7%)	Volksbank Raiffeisenbank (11; 14.9%)	Wells Fargo (26; 29.5%)	—
Top 3	Westpac (15; 18.8%)	ABC (19; 20.2%)	Commerzbank (9; 12.2%)	Bank of America (25; 28.4%)	—
Top 4	National Australia Bank (NAB) (11; 13.8%)	Life Insurance (13; 13.8%)	Deutsche Bank (4; 5.4%)	Citibank (8; 9.1%)	—
Top 5	Bendigo Bank (8; 10.0%)	Ping An (6; 6.4%)	HypoVereinsbank (1; 1.3%)	Morgan Stanley (2; 2.3%)	—

In the results in Table 4, customer experience value emerges as a strong, significant predictor of each behavioral outcome at the customer level. When companies use customers' personal information to devise a better experience, customers allocate more of their share of wallet to that company ($\gamma = 2.91, p < .001$), report greater loyalty intentions ($\gamma = .41, p < .001$), are less likely to switch to a close competitor ($\gamma = -4.18$, $p < .001$), and are more willing to opt-in to further data gathering efforts ($\gamma = .38$, $p < .001$). Perceptions of greater economic value instead significantly influence only their willingness to opt-in to further data gathering efforts ($\gamma = .15$, $p < .001$). At the company level, an indicator variable signifies if the firm is a retail company, which we include as a focal independent variable in the level-two model. When we do so, we determine that customers report allocating a greater share of wallet to retail companies ($\gamma = 2.91$, $p < .01$) and lower intentions to shift business away from a chosen retailer ($\gamma = -5.77, p < .05$). Therefore, favorable behavioral responses by customers regarding firms' uses of their personal information are driven less by financial savings or reduced costs and more by a desire to receive a better, more customized experience. Considering the informants' reported commitment to retailers in this sample, these effects should be particularly noteworthy to such firms.

Table 3
Global survey: descriptive statistics and correlations.

Variables	Mean	Std. deviation	1	2	3	4	5	6	7	8	9	10	11
1. Customer Experience Value	4.49	1.33	1.000										
2. Customer Economic Value	3.91	1.50	.527**	1.000									
3. Customer Share of Wallet	59.10	24.81	.166**	.110**	1.000								
4. Customer Loyalty Intention	5.45	1.35	.361**	.123**	.252**	1.000							
5. Customer Switching Intention	47.30	29.35	−.172**	−.098**	.111**	−.163**	1.000						
6. Customer Opt-In Willingness	4.62	1.35	.458**	.354**	.181**	.308**	−.153**	1.000					
7. Consumer Regulatory Protection	3.93	1.39	.276**	.233**	.153**	.054	−.060	.240**	1.000				
8. Country Internet Privacy Index	60.13	31.52	−.060	−.186**	−.052	.224**	−.129**	−.116**	−.126**	1.000			
9. Consumer Vulnerability	3.54	1.45	−.083**	.013	−.021	.024	.161**	−.049	−.106**	−.004	1.000		
10. Consumer Data Disclosure Worries	4.01	1.52	−.016	.072*	.058	−.116**	.152**	.065*	.037	−.292**	.463**	1.000	
11. Consumer Privacy Concerns	4.83	1.35	−.075*	−.063*	.045	.066*	.196**	−.015	−.130**	−.055	.605**	.413**	1.000

** Correlation is significant at the .01 level (2-tailed).
* Correlation is significant at the .05 level (2-tailed).

Table 4
Global survey: effects of data-enabled customer value.

	Customer share of wallet		Customer loyalty intention		Customer switching intention		Customer opt-in willingness	
Variables	γ (s.e.)		γ (s.e.)		γ (s.e.)		γ (s.e.)	
Intercept	56.27 (1.56)	***	5.52 (.08)	***	47.60 (1.71)	***	4.61 (.06)	***
Individual Level								
Customer Experience Value	2.91 (.73)	***	.41 (.06)	***	−4.18 (.90)	***	.38 (.04)	***
Customer Economic Value	.90 (.77)		−.04 (.04)		−.75 (.86)		.15 (.04)	***
Company Level								
Retailer Identifier	6.80 (2.55)	**	−.09 (.12)		−5.77 (2.72)	*	.07 (.10)	
Adjusted R^2	.05		.14		.03		.23	

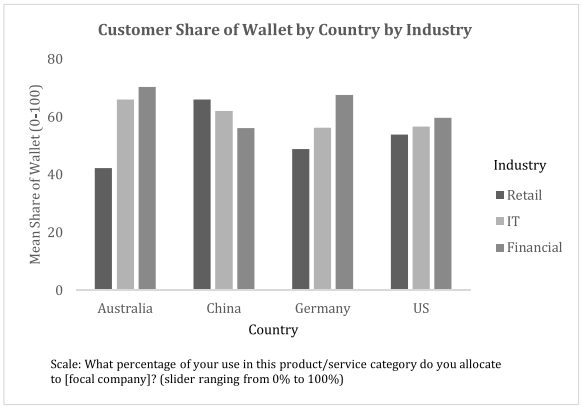
Note: *$p < .05$; **$p < .01$; ***$p < .001$.

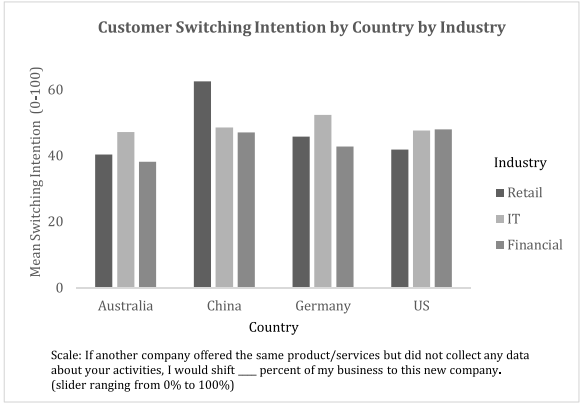
Collectively, these findings reinforce extant evidence that big data drive retail performance. In a global sample with consumers from four countries, across 60 different companies, the value resulting from personalized, improved customer experiences, established on the basis of big data, leads to critical behavioral rewards. Customers report greater shares of wallet and enhanced future loyalty toward companies that provide value through personalized experiences, beyond mere price discounts. This customer experience value also reduces intentions to switch, while increasing opt-in willingness for data-driven company applications. If retailers can demonstrate to customers how providing personal information leads to better experiences, they likely can unlock a host of behavioral benefits. These findings are consistent across all four countries in our sample, implying the universal nature of the beneficial customer outcomes that result from data-enabled customer value.

Case in brief: Australia

We consider a specific example from Australia that speaks to these data-enabled value benefits. This case also introduces trade-offs between enhanced personalization value and privacy, which sets the stage for our subsequent emergent themes. Woolworths is Australia's largest grocery retailer, with 995 stores and 115,000 employees, and it operates with diversified business interests (woolworthsgroup.com.au, 2019). In 2013, it acquired 50% of Quantium, a data brokering firm, for $20 million to enhance its customer information strategy and data analytics. The goal was to design customized promotions to build market share and maximize sales (Mitchell 2016). Quantium partners with Facebook to collect and analyze customer profile data (Digital Rights Watch 2016), including lifestyle characteristics and other sensitive information—often beyond what might be considered possible by the average consumer. Woolworths uses this information to design tailor-made, direct marketing promotions; its efforts have enabled the retailer to generate a 24% increase in customers' reported satisfaction with the marketing communications they receive (Pascoe 2017).

Yet data privacy remains a critical issue in Australia. Retail giants such as Coles and Woolworths enjoy vast access to consumer data from in-house and third-party loyalty programs such





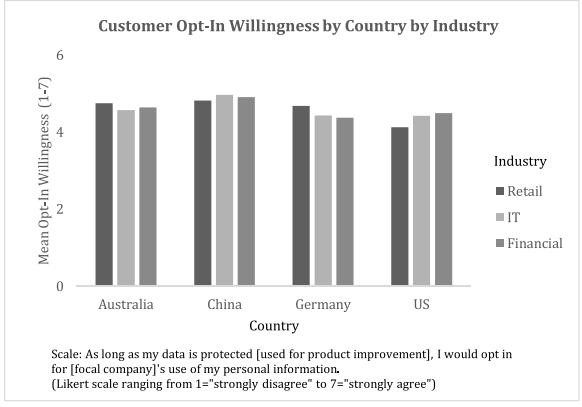


Fig. 2. Global survey: cross-country differences in customer share of wallet, loyalty intention, switching intention and opt-in willingness.

as FlyBuys or Woolworths Rewards loyalty programs (14.5 million users) (Rubinsztein-Dunlop 2014). Furthermore, the complicated Australian Privacy Act, with its unclear guiding principles and ambiguous terminology, has created increased confusion about information disclosure risks (Kemp and Vaile 2018). Yet innovations that enable greater data procurement and limit privacy continue to emerge, prompting ethical questions. For example, Australian retailers rely extensively on data brokers to develop their direct marketing strategies. The present state of privacy legislation, which imposes few regulatory limits on the data brokering industry, represents a threat to Australian consumers' privacy (Digital Rights Watch 2016).

Summary

In our interviews, the executive informants note how big data analytics facilitate rich customer connections and retailer advantages. The resulting value often is sufficient, such that customers willingly disclose information to obtain it. Our global survey suggests that across all four countries, the value resulting from personalized, improved customer experiences, supported by big data, leads to critical behavioral rewards, such as increased share of wallet, loyalty, and opt-in willingness and reduced switching intentions. The case in brief pertaining to Australia's leading retailer Woolworths illustrates how investments in big data analytics can pay off, in the form of substantially increased customer satisfaction, even if the country's complicated regulations pose a risk to consumers' data privacy. Despite growing concerns about consumer data privacy though, big data analytics deliver added value to both customers and retailers, which enhances customer relationship outcomes.

Theme 2: Profound Impact of Regulation

Regulations determine retailers' collection, use, storage, and overall management of customer data. But they often remain somewhat in flux, as evidenced by regulatory responses to consumer privacy protections required by the COVID-19 pandemic (Brough and Martin 2020). Their influence on consumers and retailers exemplifies the convergence of interests that motivates our research: Strong regulatory influences on retailers' big data uses and applications, as well as on consumer responses, emerge as dominant features in our executive interviews and empirical survey investigation. They also have prompted the creation of a new market, offering comprehensive data privacy compliance and strategy-focused services—some of which were developed by our interview informants.

Interview insights

The executive informants refer to business-as-usual in the post-GDPR era, signaling a collective realization that managing customer data in compliance with GDPR did not require many changes even after the law took effect in May 2018. Rather, the shifts that occurred reflected their ongoing need to monitor data privacy practices. Even within the EU, firm responses to GDPR have been mixed. For example, a survey of German executives revealed that 63% of respondents believe the law creates undue business process complexity, and 43% predict it

will decelerate business digitalization (Statista 2018a). Yet 56% of respondents from the same pool praise GDPR's effectiveness in setting global personal data standards and 46% consider the GDPR as a competitive advantage for EU firms (Statista 2018b). An IT consulting director echoed these sentiments in an optimistic prediction about GDPR's transformative role:

> Companies use [GDPR] as an excuse not to get data. If you architect it correctly through privacy-by-design and automate processes around the regulation, you can be compliant but still get data and use it competitively. Data is a currency. This is an opportunity for meaningful exchange. GDPR should not stop that but just change the parameters. Think for example about HIPPA [U.S. federal privacy regulations for health data] and how companies managed that when it went into effect. Now these companies have credibility around it.

At the time of our interviews, most informants also noted the challenge of the California data privacy law (CCPA), which was scheduled to take effect in January 2020. An informant who serves as the chief security, privacy, and compliance officer at a security software company summarizes some firms' reactions to the varied legal and regulatory frameworks governing consumer data use across different U.S. states:

> Right now, every state has a different data privacy law with which companies need to be compliant. We need a federal mandate on data privacy. Companies want some consistency. GDPR solved this for the EU, China has one policy. A federal mandate is needed.

This view is reflected in a formal letter to the U.S. Congress from the Main Street Privacy Coalition (2019), with the National Retail Federation and Retail Industry Leaders Association as members and cosigners, calling for uniform federal regulations. The coalition has expressed its concern about retailers' ability to comply with the current patchwork of state laws and requested a uniform federal law that would put customer interests in the center.

Survey insights

Whether federal regulation ultimately will pass in the United States and create uniformity remains an open question. Yet we observe some interesting consumer reactions to regulations at the national level, regarding their sense of being protected by the national regulatory environment. With regard to individual-level beliefs about a country's regulatory protection of consumers, or the extent to which consumers feel safeguarded by their country's national regulatory environment, we apply a one-way analysis of variance (ANOVA) to examine group differences in consumer regulatory protection beliefs and find significant differences across countries ($F_{3, 980} = 10.93$, $p < .001$). Pairwise comparisons reveal that consumers in countries with the strongest privacy protections (i.e., Australia [M = 3.98] and Germany [M = 3.80]) report no significant differences ($p > .40$). Yet consumer respondents from the Chinese sample report feeling significantly more protected (M = 4.26; $p < .05$) than consumer respondents from other countries in our sample. This result seems paradoxical, given China's relatively weaker privacy protections. Finally, the U.S. sample differed significantly from China and Australia (M = 3.61; $p < .05$) but not from Germany ($p > .40$) in these beliefs. The lack of pairwise differences may reflect the extent to which the effects of the EU-based GDPR have spilled over to U.S. customers by default, as a result of the regulation's scope and reach.

We also use a two-level hierarchical multivariate model in HLM 8.0 to examine how both consumer-level regulatory protection and country-level privacy protection indices might influence different consumer outcomes (consumers nested within countries; Table 5). In these analyses, we examine consumers' perceived vulnerability, data disclosure worries, and privacy concerns as outcomes of interest. To address the influence of their individual-level perceptions of the extent to which their country's privacy regulations protect their personal information and data security, we use the consumer regulatory protection measure from our ANOVA. Then to capture the influence of country-level privacy protection measures, we employ an established Country Internet Privacy Index (Best VPN.org 2020). The analysis shows that individual-level perceptions of consumer regulatory protections reduce consumer vulnerability ($\gamma = -.13$, $p < .10$) and privacy concerns ($\gamma = -.15$, $p < .10$). The country-level Country Internet Privacy Index negatively relates to both consumer-perceived data disclosure worry ($\gamma = -.02$, $p < .05$) and privacy concerns ($\gamma = -.004$, $p < .10$).

Although we do not intend to advocate for or against data privacy regulations, these global survey results reveal that regulatory protections can have suppressing effects on different measures of consumer vulnerability, worry, and concern about personal information and data privacy. These suppressing effects ultimately can benefit retailers. Yet consumers across the four country samples cite significant differences in the extent to which they feel protected by their governments' privacy regulations. Their sense of regulatory protection influences vulnerability, data disclosure worries, and privacy concerns. Finally, this effect manifests both at the individual level and when we examine the influence of privacy protections at the country level (i.e., Country Internet Privacy Index). No view of regulatory scope and influence exists without its internal contrasts though, as highlighted by the evidence from Germany. We consider the unique privacy regulatory landscape in China by unpacking some nuances in the following brief case.

Case in brief: China

China's new privacy standard, the Personal Information Security Specification, was formally implemented in May 2018. It establishes detailed provisions for the collection, use, sharing, disclosure, and storage of personal information (Han and Munir 2018). For consumers, its measures provide for personal information security, similar to GDPR. For example, retailers are required to clarify the purposes for which they gather information and their processing methods, as well as seek consumer consent. The standard also advocates for collecting only the minimum information needed to provide a particular product or service (Palmatier and Martin 2019). Finally, it suggests that retailers should grant consumers the ability to access, correct, and delete any personal information (Greenleaf and Livingston

Table 5
Global survey: effects of country- and individual-level regulation perceptions.

Variables	Consumer vulnerability γ (s.e.)		Consumer data disclosure worries γ (s.e.)		Consumer privacy concerns γ (s.e.)	
Intercept	4.97 (.32)	***	4.63 (.45)	***	5.67 (.34)	***
Individual Level						
Consumer Regulatory Protection	−.13 (.07)	*	.08 (.00)		−.15 (.08)	*
Country Level						
Country Internet Privacy Index	−.004 (.003)		−.02 (.01)	**	−.004 (.002)	*
Adjusted R^2	.01		.07		.02	

Note: *$p < .10$; **$p < .05$; ***$p < .01$.

2017). In response, Alipay cancelled its use of a default consumer review of a service agreement and instead offers identity verification and one-click hiding of billing data, to better protect data privacy (Sohu 2019). Other retail giants such as JD and Taobao have updated their privacy policies too.

Our data suggest that Chinese consumers express confidence in the national regulatory system and believe its relevant policies protect their personal information. Yet paradoxically, when asked, "What types of organizations are you most concerned about for keeping your information secure?" respondents ranked the government as their top worry. This inconsistency may reflect three factors. First, the Chinese government collects and processes personal information to realize social management functions; e-government services increasingly facilitate citizen communications (Janowski 2015) but also can create information leakage (Liu and Carter 2018) and cyber-attack risks (Ynlibs 2019). Second, government regulators both protect consumer privacy and oversee privacy security regulations (Reddick and Zheng 2018; Xu et al. 2012). Chinese consumers prefer stricter regulations and therefore rely on the government to manage their privacy, rather than turning to what they perceive as weaker forms of industry self-discipline (Yang and Liu 2014). Although the Chinese government has issued guidance related to privacy protection, some believe the existing laws do not go far enough for China's transitional economy (Miltgen and Smith 2015). Moreover, the centrality of government to information security protection efforts means that Chinese consumers tend to attribute any failure to the government. Third, people may have higher privacy concerns if they lack control over the personal information collected and used by specific institutions (Phelps, Nowak, and Ferrell 2000; Xu et al. 2012). When interacting with their government, consumers tend to express greater privacy concerns, because they perceive less control over that exchange.

Summary

Firm responses to GDPR have been mixed: Some perceive it as an undue burden, whereas others recognize its aid in setting effective global standards. In reference to CCPA, respondents note the challenges it highlights, due to inconsistent state laws, leading to calls for a unified U.S. federal law that prioritizes customer interests. Our surveys further show that consumers in four countries express different perceptions of the protection afforded by their country's privacy regulations. A sense of regulatory protection can suppress consumers' perceptions of their vulnerability, data disclosure worries, and privacy concerns; collectively, diminished vulnerability and worry work to the advantage of retailers. These effects emerge at both individual and country levels. For Chinese consumers specifically, their high confidence in national regulations to protect their data combine with their paradoxical assertion that the government represents their greatest worry when it comes to keeping their information secure. This inconsistency may reflect the various benefits and risks posed by universal control and management of consumer data. Privacy regulations have varying impacts, depending on a country's unique internal contexts, but a general consensus exists. Effective regulatory protection that prioritizes customer interests can suppress various privacy-related concerns and negative effects that might otherwise hinder consumer engagement with retailers.

Theme 3: Data Privacy as a Proactive Retail Strategy

A third key theme pertains to the opportunities for competitive advantages resulting from data privacy, when proactively integrated into a retailer's broader strategy. This notion goes beyond the findings that data privacy regulations can reduce consumer worries and enable retailer interactions. Rather, in this theme, data privacy functions as a positive differentiator for retailers. Insights from both the interviews and the global survey suggest that consumers value protection of their personal information and reward retailers that provide it. Another recent, large-scale investigation of data privacy in retail notes that it would be a "missed opportunity" if retailers fail to integrate their data privacy strategy with their overall corporate strategy, and yet, such integration appears to exist among only about 20% of all firms (Sides et al. 2019).

Interview insights

Examples of successful integration provide notable insights. One informant, currently the CEO for a human resources firm, spoke to her past experience with a large market research provider, which she considers "best" at using data privacy as a strategy:

> We lobbied heavily and worked with government to ensure competitive advantage and importantly, never collected [personally identifying information]. Our product design and measurement had data privacy built into it, and [many] years of measuring consumer behavior embedded a culture in [the

firm] that always made them super careful with customer data. Newer companies have not been raised that way, as they grew up among newer technologies and hence, put less emphasis on privacy. [My firm] would walk away from analytical techniques if they were not comfortable with the privacy aspects, such as web scraping.

Privacy as a retail strategy can manifest in a continuum of consumer benefits. On the one end, consumers' personal information can be protected using data minimization, privacy-by-design architecture, and strong data security systems. Retailers thus would aim to attain advantages by highlighting their novel protections as superior to rivals'. On the other end of the continuum, retailers may secure advantages by compensating consumers for their personal information, paying fair market prices for access to and the right to use these data. The idea of paying consumers for their information is gaining traction, and evidence continues to emerge about the value of such data, implying that consumers have increasing access to such insights (Palmatier and Martin 2019). Momentum for this idea also increased with advocacy efforts by former U.S. presidential candidate Andrew Yang and California Governor Gavin Newsom (Anderson 2019).

Survey insights

In our consumer survey, we asked four questions about the monetary value (open entry; adapted to the local currency and converted later to U.S. dollars) and level of compensation consumers would consider fair in exchange for the use of their personal information (financial or demographic) or for firms to sell their personal information. The amounts listed varied considerably. Yet we do not find any clear cross-industry differences in the amount of compensation customers perceive as appropriate in exchange for using or selling their personal information ($p > .30$), nor can we identify any cross-national differences in what compensation appears fair across countries ($p > .40$). The lack of significant differences at the industry (retail, IT, financial services) and country levels suggests that the notion of compensating customers for access to their personal information may be universally popular. This compensation option is just one example of how to use privacy strategically, yet the findings reinforce growing evidence of the effectiveness of such a strategy for ensuring a firm's competitive advantage. To understand privacy as a strategy, through the lens of a groundbreaking company in this domain, we examine compensation responses to Amazon, using German and U.S. samples.

Case in brief: Germany and U.S

Amazon is one of the most frequented retailers in both our German (Amazon.de) and U.S. (Amazon.com) consumer samples. Although we do not identify significant mean differences by country, if we specifically compare German and U.S. customers' compensation demands, in response to a hypothetical request from Amazon to use their personal data, we find that German consumers require more compensation (Table 6). Yet this finding cannot be attributed to German customers' attitudes toward Amazon.de, which repeatedly wins customer-centered awards, denoting it the most fascinating brand (ServiceValue 2019) or the most trusted retailer (ServiceValue 2018).

Rather, German and U.S. consumers' general understanding of the value of personal information may differ as a result of the distinct legal conceptions of data privacy that have evolved in each country. In Germany, the protection of personal data is a basic right. In a verdict related to the population census, Germany's Federal Constitutional Court in 1983 first determined people's basic right of informational self-determination, anchoring data privacy in the German Constitution. In contrast, U.S. legislation does not comprehensively situate data privacy within economic life; rather, it appears within broader consumer protection regulations but does not constitute a formal, codified right for U.S. citizens (Stewart 2017). Considering the relatively higher importance that German legislation and jurisdictions historically have assigned to the protection of people's privacy and personal data, it may not be surprising that German consumers assign more (financial) value to their personal data than U.S. consumers and request more compensation from the same retailer (i.e., Amazon). That is, a deeper analysis suggests that the discrepancy in responses stems not from negative customer perceptions of Amazon.de but rather from the greater value that German consumers grant to their personal data, compared with U.S. consumers, when it comes to Amazon and perhaps other retailers too. This brief case thus highlights one of the many unique intersections of retailer privacy strategies with varying consumer perceptions, influenced by the overarching regulatory framework. The intersection of all three forces is likely to shape many conversations about the global role of data privacy in retail, in the near and perhaps distant future.

Summary

Consumer data privacy can underlie a proactive retail strategy, implemented to establish a continuum of consumer benefits. The successful integration of data privacy into a firm's strategy might involve novel techniques that efficiently protect privacy, or it could extend to offering consumers compensation for their data. According to our survey results, across all industries and countries, no significant differences exist in the amount of compensation that customers perceive as appropriate; customer data compensation seemingly represents a universally popular idea. However, German consumers may require higher compensation than do U.S. consumers, because they consider personal data protection a basic right, as anchored in their constitution. This effect does not stem from a negative consumer perception of Amazon but rather from a higher value assigned to their data. Thus we argue that if firms decide to embrace the increasingly popular concept of compensating consumers for disclosing their personal data, they should consider how country-specific contexts inform consumers' perceptions of the value of their personal data.

Data Privacy in Retail: Research Opportunities Involving Three Key Stakeholders

The three themes emerging from our multisource data collection provide rich insights into the dyadic and triadic

Table 6
Compensation for Data Use and Sharing: Amazon Germany versus Amazon U.S.[a]

I would think it is fair if Amazon compensates. . .	Amazon Location	N	Mean	Std. Deviation	
$_____ for using my financial data (e.g., payment methods, purchase history, preferences)	Germany	60	$ 1,114.28	$ 6,463.94	
	U.S.	20	$ 398.75	$ 1,121.99	
$_____ for selling my financial data (e.g., payment methods, purchase history, preferences)	Germany	59	$ 22,618.51	$ 131,304.56	*
	U.S.	20	$ 1,106.45	$ 2,581.96	
$_____ for using my demographic data (e.g., age, ethnicity, zip code, etc.)	Germany	60	$ 2,125.40	$ 12,937.54	*
	U.S.	21	$ 68.00	$ 120.23	
_ for selling my demographic data (e.g., age, ethnicity, zip code, etc.)	Germany	59	$ 27,896.36	$ 144,697.74	*
	U.S.	21	$ 132.43	$ 237.32	

Note: *Denotes difference significant at $p < .10$ level.

[a] Note that we identify some large values reported by German consumers in Table 7. Many German respondents reported high compensation values (especially for *selling* customer data), even after reporting positive privacy beliefs about Amazon.de overall. We carefully examined the data and found that these values are not attributable to one or two outliers; many responses indicate high values. After discussing this finding, both among the author team and in consultation with a German legal expert, we believe two factors are at play. First, such compensation strategies are not widely used in Germany, so consumers may be unfamiliar with the idea of monetary compensation for personal data and thus unsure of how to respond. Second, German consumers may believe their personal data are not tradable in a financial deal, because they consider privacy a basic, non-negotiable right. In the United States, privacy is part of commercial law, so exchanging money for data makes more sense as a fair exchange. We expect that some German respondents reason that their privacy is "priceless" (explicitly indicated by one respondent) and thus report large values. Nonetheless, our small sample size and inability to verify the reasoning behind these values with respondents directly requires these explanations and findings to be interpreted with caution.

interrelations among the key stakeholders involved in data privacy issues, as synthesized in Table 7. Knowledge germane to each key player—consumer, retailer, and regulation—remains surprisingly limited though. Understanding the influence mechanisms and conditions that affect consumers, retailers, and regulation can lead to a more solid foundation for data privacy research; we accordingly suggest specific research avenues related to each stakeholder, informed by our emergent themes, but also in light of stakeholder convergence.

Consumer Intersections

For consumers, data privacy topics trigger specific emotions and cognitions, involving vulnerability, trust, and emotional violations (Martin, Borah, and Palmatier 2017). A key consideration is how privacy-associated emotions evolve throughout customer journeys. For example, what motivates consumers to overestimate the risks of data disclosure or underestimate its benefits? A related extension might investigate how consumers perceive the value of disclosing their data to retailers and the relative weight they assign to retailers' privacy standards, relative to other relational benefits (e.g., rewards, preferential treatment), that inform their perceptions of relationship quality. Data disclosure decisions may reflect consumers' distinct preferences about various data usages (e.g., product improvement, personalized ads, third-party sales). In some cases, consumers might seek ways to circumvent (e.g., using VPN) retailer data collection efforts. Understanding such behaviors can help firms proactively manage their methods, especially in relation to new technologies (e.g., artificial intelligence, Internet of Things, geo-location). Even remote work cultures warrant investigation, to determine how new working environments might affect consumers' perceptions of online privacy. Arguably, new work paradigms might desensitize consumers to information disclosures, or they could make them even more discerning. Questions also remain regarding cultural differences and how they inform consumers' expectations of regulatory protection. Do consumers in various cultures value strong consumer protection, or do they feel patronized and prefer freedom of choice and self-determination with regard to data privacy?

Retailer Intersections

The options for using a data privacy strategy to gain a competitive advantage remain almost completely open for investigation. Retailers need research insights into how to determine their consumers' privacy calculus (i.e., perceived costs and benefits of data disclosure) and expectations. With such insights, retailers can better frame data consent queries, whether as the gains achieved from consent or losses suffered without consent. In some industries or for specific products/services, personalization benefits might outweigh privacy losses more or less. To leverage privacy protection as a competitive advantage, retailers need to be able to anticipate whether their decisions to protect privacy, beyond legal requirements, will enhance consumer trust and favorable firm-directed behaviors sufficiently. Third-party certifications of good data privacy standards also might reinforce a competitive advantage. In the event of a data breach, retailers require guidance for mitigating the damage and repairing their relationship with consumers. Ultimately, any effort to leverage privacy strategies will demand reliable, specific performance indicators (e.g., impact of consumer consent versus non-consent for customer lifetime value). Finally, another important question involves how retailers might bridge a communication gap, between regulatory and legal data privacy terminology versus consumer-focused and layperson terminology.

Table 7
Summary of findings on three emergent themes on data privacy in retail.

Theme	Interviews	Survey	Case in brief	Implications
Theme 1: Big Data as a Driver of Customer Relationship Performance	Executive informants note that big data analytics facilitate rich customer connections and retailer advantages. And the value often is sufficient that customers willingly disclose information to obtain it.	Across all four countries, the value resulting from personalized, improved customer experiences, allowed by big data, leads to critical behavioral rewards such as increased share of wallets, opt-in willingness and future loyalty, and reduced switching intention.	**Australia:** Woolworths, Australia's largest supermarket chain acquired 50% of Quantium, a data brokering firm to enhance its customer data analytics. This contributed to a 24% increase in reported customer satisfaction with the marketing communications. However, the current complicated state of Australian privacy laws poses a threat to Australian consumers' privacy.	Despite the growing concerns on consumer data privacy, big data analytics can deliver customers and retailers the added value that leads to a host of enhanced relationship outcomes.
Theme 2: Profound Impact of Regulation	Firm responses to GDPR has been mixed—some perceive it as undue business complexity, while others perceive as effective global standards. Most informants note that CCPA posed many challenges due to inconsistent state laws and thus call for a unified federal law that makes customer interests central.	Consumers in four countries express different levels of feeling protected by the country's privacy regulations. Feelings of regulatory protection can suppress consumer vulnerability, data disclosure worries, and privacy concerns. This effect is observed in both individual and country-level.	**China:** Chinese consumers express high confidence in the national regulations and believe them to protect their personal information. However, they also rank the government as the highest worry about keeping their information secure. This inconsistency may be due to (1) the government collecting and processing data, (2) consumers relying on the government to manage their privacy but also attributing any failure to the government, (3) higher privacy conerns may be due to the lack of perceived control.	Privacy regulations have differential impact on consumers depending on the country's unique internal contexts. However, a general consensus is that an efficient regulatory protection that prioritizes customer interests can suppress various privacy-related concerns.
Theme 3: Data Privacy as a Proactive Retail Strategy	Successful integration of data privacy into firm strategy can vary on a continuum of consumer benefits—one end with novel techniques that efficiently protect privacy, and the other end with consumer compensation of their data.	Across all industries and countries, there was no significant difference in the amount of compensation that customers perceive as appropriate. This suggests that customer data compensation may be a universally popular idea.	**Germany and U.S.**: For Amazon, German consumers require higher compensation than do US consumers. This may be because German consumers consider personal data protection a basic right, as anchored in the constitution. Results suggest this effect does not stem from a negative consumer perception of the firm, but from higher value assigned to their data.	Consumer data privacy is emerging as a proactive retail strategy as it can be implemented based on a continuum of consumer benefits. Compensating consumers for disclosing their personal data is becoming a popular concept. However, firms must consider the country-specific contexts that inform consumers' perceived value of their data.

Regulatory Intersections

Interesting questions emerge regarding the effectiveness and features of different data privacy regulations around the world. Cultural norms (e.g., individualism, power distance) arguably affect the design and implementation of data privacy regulations across countries; levels of economic development also may inform a region's data privacy regulations. Once regulations go

into effect, regulators need to ensure compliance, but as privacy regulations shift and evolve, they may require a dynamic perspective, especially for global, online retailing practices that span national boundaries. Researchers might explore potential "new norms" for data disclosure and their impact on the design of privacy regulations. Certain regions are known for their high level of data privacy regulations (e.g., GDPR), which seemingly could limit their ability to foster an innovation culture (e.g., promote start-ups with technology-based products or services). But public welfare considerations also are pertinent, so regulators and governments must balance their efforts to ensure consumer trust in data collection efforts, consumers' own management of their personal privacy, and the accountability of retailers.

Conclusion

This article identifies three emergent themes surrounding big data and privacy at the intersection of consumer, retail, and regulatory interests. We share insights from top-level executives and draw from empirical evidence gathered through a large, global consumer survey; these combined sources confirm that big data have transformed the retail landscape, often in ways that benefit both consumers and retailers. Case studies inspired by our survey findings offer illustrative examples. Collectively, this evidence informs our research framework, which suggests fruitful research opportunities.

What might retail scholars and practitioners understand differently by considering implications derived from the three emergent themes? The insights gathered from these themes should inform and encourage research that, thus far, has not kept pace with rapid technological advances. For example, in the quest for data-enabled performance advantages, retailers might use novel technologies that extract consumer information without their knowledge or permission. What happens when consumers become aware of an unwanted disclosure of their personal information? Sometimes the extracted information involves video monitoring, facial recognition, or tracking of personal devices—each of which provide highly sensitive consumer data. Not only do we need to determine how consumers are likely to respond to such platforms, but the field also should establish predictions about likely evolutions in the retail technological landscape and their implications for a diverse range of consumer outcomes, whether positive (e.g., purchases, loyalty, engagement) or negative (e.g., defection, switching, punishing behaviors). As retailers become more sophisticated in their uses of advanced analytical techniques, new implications also emerge for customer acquisition, retention, and migration strategies. The retailing discipline should establish a better, broader understanding of how firms engage with existing and potential customers, in the face of both advancing technologies and shifting regulations. Doing so ultimately may help retail firms secure competitive advantages, through privacy as strategy.

As retailers continue to attempt to adjust to "business-as-usual" under GDPR, the CCPA, and other laws, our research advises them to expect to continue grappling with the profound impact of these regulations for some time. The ramifications of regulations for retailers continue to emerge, but we provide important preliminary evidence that they can be a pathway toward smoother, more confident consumer–data interactions. Global companies need consistent, coherent approaches to data privacy, despite cross-national regulatory differences, especially for achieving data minimization and collecting only the information needed to execute basic transactions. Each data point requires justification (Palmatier and Martin 2019). In this context, what effects does data minimization have on retailers, whose performance hinges on their ability to process consumer data? Furthermore, how do retailers undertake data minimization practices that require consumer data to be expunged from their systems over time? Do they address consumers' right to be forgotten, even after consumer data already are deeply embedded in their various systems and processes? Retailers further must decide whether they will comply with data privacy regulations or go beyond them to embrace a data privacy strategy. This decision has a range of performance implications. Retailers also might elect not to comply with regulations, and just hope to avoid detection, which creates other performance advantages and disadvantages; what are the ramifications, should they be caught?

Consumers appear to behave differently toward retailers if they know that strong regulatory protections at the country level safeguard their data. However, more research and evidence is required to understand whether and how regulation may put consumers at ease. For example, do stronger country-level regulatory protections encourage deeper, more meaningful consumer–retailer relationships? Or might data privacy regulations actually stifle consumer options and choice? If retailers experience undue constraints on their ability to serve customers, such that they simply cannot provide personalized experiences and still comply with regulations, how will consumers respond? Although much research attention has been devoted to the consumer–retailer disclosure setting, we know less about consumer–government disclosure contexts. Governments worldwide already practice tracking, monitoring, and surveillance of citizens, and people might react differently to unwilling disclosures to government agencies, compared with those to a retailer with which they voluntarily transact. Among U.S. consumers at least, some commercial businesses tend to be trusted more than the government (Rainie, Keeter and Perrin 2019). Important government versus retailer distinctions may emerge from such research, as might cross-national differences and cultural variations in privacy norms. The question also raises the issue of the appropriate relative balance between market mechanisms and government regulations when it comes to privacy protections.

The symbiotic relationship between consumers and retailers—the former appreciate personalized experiences and reward the latter with patronage—is unlikely to disappear, but it might be irrevocably influenced by regulatory forces, because consumers who are aware of data privacy mandates that protect their personal information and guard their data-driven transactions report greater comfort with relinquishing information. Considering the consistent calls from high-profile retail associations and U.S. firms for federal, uniform regulations, lawmakers may wish to examine growing evidence (e.g., from Europe,

Australia) about how data privacy regulations can facilitate consumer interactions with retailers, as well as level the playing field with regard to retailer compliance.

Whether regulation eventually becomes the law of the land in all countries remains an open question. In the meantime, we find evidence that retailers have room to improve their data privacy capabilities, which can secure their customers' interests and promote greater engagement. Data privacy is good for business. Beyond the clear performance advantages that we highlight in this research, retailers benefit from taking data privacy seriously, as described by the CEO and founder of a privacy solutions company:

> Technology is now advancing so fast that we cannot keep up. Privacy as control of information, such as notice and choice, will shift to questions of what kind of world we want to live in. Robotic automation and legal frameworks cannot handle it. Things are advancing so rapidly that there is no time to have the ethical debate. There is a monumental shift in the ways we are being monitored and surveilled and there is a worry that we don't have enough time to carefully create the world we want to live in. None of the frameworks we have, on any front, are designed to accommodate this.

Even as we acknowledge this expression of the urgent need for data privacy conversations, we are encouraged by the striking convergence of consumer, regulatory, and retailer imperatives. The time seems ripe for a breakthrough agreement regarding how to manage big data in the retail environment, responsibly and in a way that promotes all parties' interests. We hope the insights from our research help advance such objectives.

Author note

The authors thank the Coeditors, Anne Roggeveen and Raj Sethuraman, as well as Aaron Brough, Dhruv Grewal, and participants in the 2019 Thought Leaders' Conference on Data Privacy in Retail (University of Florence) for their helpful feedback that has improved this contribution. After the first author, the authors appear in alphabetical order.

Appendix.

Table A1

Table A1
Global survey: measures.

Theme 1: big data as a driver of customer relationship performance	
Data-Enabled Customer Value: *Customer perception of firms' ability to proactively tailor products' or services' purchasing experiences or prices to their individual tastes based upon their personal and preference information (*Chellappa and Sin 2005*).*	
Customer Experience Value	[Focal company] is able to provide customers a better experience by using their personal information.
Customer Economic Value	[Focal company]'s prices are lower, or its services are free, because of its customer data use.
Customer Share of Wallet*: Degree of engagement with company's products or services within category (*De Wulf, Odekerken-Schröder, and Iacobucci 2001*).*	
What percentage of your use in this product/service category do you allocate to [focal company]? (slider ranging from 0% to 100%)	
Customer Loyalty Intention: *Customer stated intention of continued use/interaction with the company (*Wagner, Hennig-Thurau, and Rudolph 2009*).*	
I am likely to continue to use the products and services of [focal company].	
Customer Switching Intention: *Customer likelihood of discontinuing relationship with the focal company in favor of a similar alternative (*Martin, Borah, and Palmatier 2017*).*	
If another company offered the same product/services but did not collect any data about your activities, I would shift ____ percent of my business to this new company. (slider ranging from 0% to 100%)	
Customer Opt-In Willingness: *Extent to which customer perceptions of company privacy protection encourage them to opt-in to data sharing (*Hann et al. 2007*).*	
Average of:	
As long as my data is protected (e.g., breach insurance up to $1 M), I would opt in for [focal company]'s use of my personal information.	
As long as my data is being used for product improvement, I would opt in for [focal company]'s use of my personal information.	
Theme 2: Profound Impact of Regulation	
Consumer Regulatory Protection: *Extent to which consumers feel protected by their country's national regulatory environment (new scale).*	
Average of:	
How protected to you feel by your country's regulatory environment? (seven-point scale ranging from 1 = "not at all" to 7 = "extremely")	
How likely do you believe government policies protect your data privacy? (seven-point scale ranging from 1 = "not at all" to 7 = "extremely")	
In general, how much does your country's government care about your privacy? (seven-point scale ranging from 1="not at all" to 7="extremely")	
Country Internet Privacy Index: *Extent to which a country takes steps to protect information shared online (Best* VPN.org 2020*)*	

Table A1 (*Continued*)

Theme 1: big data as a driver of customer relationship performance
Country-level composite score between 0 and 100 comprised of the following information:
Press freedom
Data privacy laws
Democracy statistics
Freedom of opinion and expression
Cybercrime legislation worldwide
Consumer Vulnerability: *Consumer perceptions of susceptibility to harm owing to companies' data privacy practices (*Martin, Borah, and Palmatier 2017*).*
Average of:
In general, the personal information companies have about me makes me feel:
Exposed
Insecure
Threatened
Vulnerable
Consumer Data Disclosure Worries: *Extent to which the sensitivity of one's personal data profile creates feelings of nervousness (new scale, adapted from work on Gossip Theory).*
Average of:
If others were to obtain the information about me that is online, it could cause me: (seven-point scale ranging from 1="no harm" to 7="great harm")
In general, how much do you worry about being the victim of a data breach? (seven-point scale ranging from 1="not at all" to 7="extremely")
Consumer Privacy Concerns: *Individual difference on attentiveness and familiarity with privacy threats (Malhotra, Kim, and Agarwal 2004).*
Average of:
I am sensitive to the way companies handle my personal information.
I am concerned about threats to my personal privacy.
Theme 3: Data Privacy as a Proactive Retail Strategy
Customer Compensation Request: *Customer perception of an adequate monetary payment by companies in exchange for personal information (*Palmatier and Martin 2019*).*
Please indicate the [country currency] amount you think is appropriate for below situation. (amount of money)
I would think it is fair if the company compensated me with [country currency] ____ for *using* my financial data (e.g., payment methods, purchase history, preferences).
I would think it is fair if the company compensated me with [country currency] ____ for *selling* my financial data (e.g., payment methods, purchase history, preferences).
I would think it is fair if the company compensated me with [country currency] ____ for *using* my demographic data (e.g., age, gender, ethnicity, zip code).
I would think it is fair if the company compensated me with [country currency] ____ for *selling* my demographic data (e.g., age, gender, ethnicity, zip code).

All items were measured on a seven-point Likert-type scale ranging from 1 = "strongly disagree" to 7 = "strongly agree," unless otherwise noted.
Overall, my strategy was to always talk about c̈onsumerïf we use the general section of the survey and talk about c̈ustomerẅhen we use the company-specific section of the survey. But I am also open to use c̈onsumeräcross the board, just let me know what your preference is.

References

Aguirre, Elizabeth, Dominik Mahr, Dhruv Grewal, Ko de Ruyter 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.

Anderson, George (2019), *Should Companies Have to Pay You to Use Your Personal Data?,* Retail Wire. October 4, (accessed May 5, 2020), [https://retailwire.com/discussion/should-companies-have-to-pay-you-to-use-your-personal-data/]

Best VPN.org (2020), *Internet Privacy by Country,* (accessed March 14, 2020), [https://bestvpn.org/privacy-index/].

Bleier, Alexander and Maik Eisenbeiss (2015), "Personalized Online Advertising Effectiveness: The Interplay of What, When, and Where," *Marketing Science,* 34 (5), 669–88.

Bradlow, Eric T., Manish Gangwar, Praveen Kopalle and Sudhir Voleti (2017), "The Role of Big Data and Predictive Analytics in Retailing," *Journal of Retailing,* 93 (1), 79–95.

Brough, Aaron R. and Kelly D. Martin (2020), "Consumer Privacy During (and After) the COVID-19 Pandemic," *Journal of Public Policy & Marketing,*, http://dx.doi.org/10.1177/0743915620929999

Casadesus-Masanell, Ramon and Andres Hervas-Drane (2015), "Competing with Privacy," *Management Science,* 61 (1), 229–46.

Chellappa, Ramnath K. and Raymond G. Sin (2005), "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management,* 6 (2–3), 181–202.

Chung, Tuck Siong, Michel Wedel and Roland T. Rust (2016), "Adaptive Personalization Using Social Networks," *Journal of the Academy of Marketing Science,* 44 (1), 66–87.

De Wulf, Kristof, Gaby Odekerken-Schröder and Dawn Iacobucci (2001), "Investments in Consumer Relationships: A Cross-Country and Cross-Industry Exploration," *Journal of Marketing,* 65 (4), 33–50.

Digital Rights Watch (2016), *Watchlist: Data Brokers,* (accessed March 14, 2020), [https://digitalrightswatch.org.au/2016/10/18/watchlist-data-brokers/].

Greenleaf, Graham and Scott Livingston (2017), "China's Personal Information Standard: The Long March to a Privacy Law (December 1, 2017)," *150 Privacy Laws & Business International Report,*, 25–8 (accessed August 20, 2019), [https://ssrn.com/abstract=3128593]

Grewal, Dhruv, Anne L. Roggeveen and Jens Nordfält (2017), "The Future of Retailing," *Journal of Retailing,* 93 (1), 1–6.

Han, Sarah Wang and Abu Bakar Munir (2018), "Practitioner's Corner Information Security Technology-Personal Information Security Specification: China's Version of the GDPR?," *European Data Protection Law Review,* 4 (4), 535–41.

Hann, Il-Horn, Kai-Lung Hui, Sang-Yong T. Lee and Ivan P.L. Png (2007), "Analyzing Online Information Privacy Concerns: An Information Processing Theory Approach," *Journal of Management Information Systems,* 24 (2), 13–42.

Hoffmann, Florian, Roman Inderst and Marco Ottaviani (2020), "Persuasion Through Selective Disclosure: Implications for Marketing,

Campaigning, and Privacy Regulation," *Management Science,*, http://dx.doi.org/10.1287/mnsc.2019.3455

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.

Janowski, Tomasz (2015), "Digital Government Evolution: From Transformation to Contextualization," *Government Information Quarterly,* 32 (3), 221–36.

Kemp, Katherine and David Vaile (2018), *Soft Terms Like 'Open' and 'Sharing' Don't Tell the True Story of Your Data,* UNSW Sydney Newsroom (accessed March 14, 2020), [https://newsroom.0unsw.edu.au/news/business-law/soft-terms-%E2%80%98open%E2%80%99-and-%E2%80%98sharing%E2%80%99-don%E2%80%99t-tell-true-story-your-data]

Liu, Dapeng and Lemuria Carter (2018), "Impact of Citizens' Privacy Concerns on E-government Adoption," *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age,*, 1–6.

Main Street Privacy Coalition (2019), *Principles for Federal Privacy Legislation, A Letter to the U.S. Congress,* (accessed March 19, 2020), [http://d22f3d5c92fe72fd8ca1-d54e62f2f7fc3e2ff1881e7f0cef284e.r22.cf1.rackcdn.com/Hill%20Letters%202019/Main%20Street%20Privacy%20Coalition%20Letter%20to%20Senate%20Cmtes%20(Nov%2021%202019).pdf].

Martin, Kelly D., Abhishek Borah and Robert W. Palmatier (2017), "Data Privacy: Effects on Customer and Firm Performance," *Journal of Marketing,* 81 (1), 36–58.

Martin, Kelly D. and Patrick E. Murphy (2017), "The Role of Data Privacy in Marketing," *Journal of the Academy of Marketing Science,* 45 (2), 135–55.

Martin, Kelly D., Robert W. Palmatier and Abhishek Borah (2018), "A Strong Privacy Policy Can Save Your Company Millions," *Harvard Business Review,*. February.

Miltgen, Caroline Lancelot and H.Jeff Smith (2015), "Exploring Information Privacy Regulation, Risks, Trust, and Behavior," *Information & Management,* 52 (6), 741–59.

Mitchell, Sue (2016), "Woolworths Sitting on Big Data Goldmine," *Financial Review,*, (accessed March 14, 2020), [https://www.afr.com/companies/retail/woolworths-sitting-on-big-data-goldmine-20161013-gs1cgw]

Montes, Rodrigo, Wilfried Sand-Zantman and Tommaso Valletti (2019), "The Value of Personal Information in Online Markets with Endogenous Privacy," *Management Science,* 65 (3), 1342–62.

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

Palmer, Danny (2019), *What Is GDPR? Everything You Need to Know about the New General Data Protection Regulations,* ZDNet.com (accessed March 19, 2020), [www.zdnet.com/article/gdpr-an-executive-guide-to-what-you-need-to-know]

Pascoe, Michael (2017), *Woolies Is Playing Smart. Coles Is Not, and It Shows,* Sydney Morning Herald (accessed March 14, 2020), [https://www.smh.com.au/business/companies/why-coles-is-in-the-dog-house-it-thinks-i-have-a-cat-20171102-gzd8w3.html]

Phelps, Joseph, Glen Nowak and Elizabeth Ferrell (2000), "Privacy Concerns and Consumer Willingness to Provide Personal Information," *Journal of Public Policy & Marketing,* 19 (1), 27–41.

PwC (2018), *Prepare for the Voice Revolution,* Consumer Intelligence Series (accessed August 21, 2020), [www.pwc.com/cisvoiceassistants]

Rainie, Lee, Scott Keeter and Andrew Perrin (2019), *Trust and Distrust in America,* Pew Research Center. July 22, (accessed April 6, 2020), [https://www.people-press.org/2019/07/22/trust-and-distrust-in-america/]

Reddick, Christopher G. and Yueping Zheng (2018), "Online Privacy Protection in Chinese City Governments: An Analysis of Privacy Statements," in *International E-Government Development* Cham: Palgrave Macmillan.99–120.

Rubinsztein-Dunlop, Sean (2014), *Coles, Woolworths Accumulating Consumer Data as they Prepare to Compete with Banks on Home Loans,* ABC News (accessed April 6, 2020), [https://www.abc.net.au/news/2014-08-06/coles-woolworths-preparing-to-enter-home-loans-market/5653288]

ServiceValue (2019), *Marken-Champions [English Translation: Brand Champions],* (accessed August 27, 2019), [https://www.servicevalue.de/wettbewerbe/branchenuebergreifend/marken-champions-deutschland/ranking/ranking-der-2388-marken/].

——— (2018), *Deutschlands größtes Vertrauensranking – Ranking: Versandhändler [English Translation: Germany's Biggest Trust Ranking – Ranking: Mail Order Companies],* (accessed August 27, 2019), [http://www.servicevalue.de/wettbewerbe/branchenuebergreifend/vertrauen-sranking/ranking/ranking-versandhaendler/].

Sides, Rod, Matt Marsh, Rob Goldberg and Michael Mangold (2019), *Consumer Privacy in Retail: The Next Regulatory and Competitive Frontier,* Deloitte Development, LLC (accessed August 21, 2020), [https://www2.deloitte.com/content/dam/Deloitte/us/Documents/consumer-business/us-retail-privacy-survey-2019.pdf]

Statista (2018), *Welchen der im Folgenden genannten Nachteilen der DSGVO stimmen Sie voll und ganz bzw. eher zu? Die Datenschutz-Grundverordnung . . . [English Translation: Which of the Following Disadvantages of the GDPR Do You Fully Agree to or Agree to? The GDPR . . .],* (accessed August 27, 2019), [https://de.statista.com/statistik/daten/studie/862497/umfrage/nachteile-der-dsgvo-aus-unternehmenssicht-in-deutschland/].

——— (2018), *Welchen der im Folgenden genannten Vorteilen der DSGVO stimmen Sie voll und ganz bzw. eher zu? Die Datenschutz-Grundverordnung . . . [English Translation: Which of the Following Advantages of the GDPR Do You Fully Agree to or Agree to? The GDPR . . .],* (accessed August 27, 2019), [https://de.statista.com/statistik/daten/studie/862487/umfrage/vorteile-der-dsgvo-aus-unternehmenssicht-in-deutschland/].

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

Sohu (2019), *Alipay Is Among the First to Reach the Highest Standards of National Privacy Protection,* (accessed August 20, 2019), [http://www.sohu.com/a/293141657_104421].

Taylor, Curtis and Liad Wagman (2014), "Consumer Privacy in Oligopolistic Markets: Winners, Losers, and Welfare," *International Journal of Industrial Organization,* 34, 80–4.

Tirunillai, Seshadri and Gerard J. Tellis (2014), "Mining Marketing Meaning from Online Chatter: Strategic Brand Analysis of Big Data Using Latent Dirichlet Allocation," *Journal of Marketing Research,* 51 (4), 463–79.

TotalRetail (2019), *Retail Technology Report: An Analysis of Trends, Buying Behaviors, and Future Opportunities,* Total Retail, Arm Treasure Data, NAPCO Research (accessed August 21, 2020), [https://www.mytotalretail.com/promo/2019-retail-technology-report/].

Wagner, Tillmann, Thorsten Hennig-Thurau and Thomas Rudolph (2009), "Does Customer Demotion Jeopardize Loyalty?," *Journal of Marketing,* 73 (3), 69–85.

Xu, Heng, Hock-Hai Teo, Bernard C.Y. Tan and Ritu Agarwal (2012), "Research Note: Effects of Individual Self-Protection, Industry Self-Regulation, and Government Regulation on Privacy Concerns: A Study of Location-Based Services," *Information Systems Research,* 23 (4), 1342–63.

Yang, Hongwei(Chris) and Hui Liu (2014), "Prior Negative Experience of Online Disclosure, Privacy Concerns, and Regulatory Support in Chinese Social Media," *Chinese Journal of Communication,* 7 (1), 40–59.

Ynlibs (2019), *360 Internet Security Center: Analysis Report on Data Leakage Situation of Government and Enterprise Institutions in 2018,* (accessed August 20, 2019), [http://www.ynlibs.com/doc-details?reportId=56394].