Consumer Privacy Expectations and the Impact on Buying Intentions

Edward L. Linde, II
Marist College

William S. Brown
Marist College

John C. Cary
Marist College

Pamela J. Harper
Marist College

Based on past research and attitudinal theories, this study intends to investigate the effect of attitudes about data privacy protection and disclosure and the perception of corporate data privacy performance on future purchase intention. Additionally, it seeks to understand the relationship between purchase behavior intensity, personal data privacy concerns and privacy expectations (attitude). A total of 271 usable surveys were gathered from United States consumers and analyzed by two multiple linear regression models and correlation analysis. The results show that attitude (data privacy protection and disclosure responsibility) and perceptions about corporate data privacy performance predict purchase intention. Furthermore, past purchase behavior intensity and personal data privacy concerns influence corporate data privacy responsibility attitudes. This study extends the current data privacy literature by understanding how data privacy expectations (attitude) and data privacy performance perceptions impact purchase intent and are influenced by personal data privacy concerns and purchase behavior.

Keywords: data privacy, privacy preferences, privacy expectations, buying intentions

INTRODUCTION

Many studies demonstrate the efficacy of consumer privacy expectations on buying intent. Okazaki et al. (2020) in a meta-analysis reviewing 1,103 effects in 304 papers, found that retail channels and data sensitivity wield significant influence on reducing or strengthening the impact of customer privacy concerns on key retail outcomes. More specifically, Cheah et al. (2022) found that consumer perception of trust significantly affects patronage intentions. A study by Van Slyke, Shim, and Johnson (2006) indicates that concern for information privacy affects risk perceptions, trust, and willingness to transact for a well-known merchant, but not for a less well-known merchant. Furthermore, Sharif et al. (2019) conclude that e-commerce operational performance and trust significantly impact consumer purchase intentions. The study

further demonstrates the need to understand the integrated impact of measures to protect against identity theft on consumer purchase intentions. Using a conceptual framework from gossip theory, Martin, Borah, and Palmatier (2017) link customer vulnerability to negative customer and firm performance.

Bloom et al. (1994) raised the issue of data privacy in marketing through a landmark paper in the Journal of Marketing. Essentially, the authors postulated that marketers needed to consider whether they can collect and share consumer information without the consumer's knowledge or consent.

Additionally, behavioral literature on data privacy demonstrates that certain factors may impact customers' decision-making surrounding their data (Acquisti, Taylor, and Wagman, 2016). More recent research supports the view that individuals are concerned about the collection of their data such that they are willing to change their behaviors to protect privacy (Marthews and Tucker, 2014; Tucker, 2018).

Literature Review

While much has been published on consumer data privacy, we have found that existing research needs to be synthesized into a collective understanding to reveal what is known and where gaps in knowledge exist. Pomret et al, (2020) found that existing research has focused on privacy concerns, not consumer privacy behavior. We concluded the same observation as we did our literature search. However, in our estimation, it is helpful to categorize the existing literature and organize existing findings to establish where additional research is needed. From our vantage point, the current literature can be categorized into data risk avoidance, Zero-Party Data Exchange, and Omni-Channel dynamics.

Data privacy risk avoidance studies look at organization or individual consumer attitudes about data breaches, implications and behaviors designed to mitigate their risk. Zero-Party data exchange research focuses on the personalization of marketing messages, pricing, and offers dependent on the consumer relinquishing personal information to facilitate this. Lastly, Omni-channel dynamics refers to data privacy concerns as inhibiting consumer adoption of eCommerce and/or enhanced physical shopping experiences that leverage private, personal information. These categories are not exhaustive as some research may not neatly fit into a grouping. Furthermore, overlaps can exist where a particular piece of literature could fit into multiple categories. Nonetheless, the authors feel that this approach is useful in navigating the extensive body of work that is out there.

Data Privacy Risk Avoidance

Having your identity compromised is a concern to both individuals and corporations. According to a 2022 study by the University of Warwick and the Thales Group, 33% of consumers worldwide experienced a data breach of their personal information, and 82% of these people saw a negative impact on their personal lives. Corporations fear the impact of a data breach for public relations embarrassment, brand equity, costs and regulatory penalties. The highly respected Ponemon Institute estimates that the average cost of a data breach in the United States was $9.48M.

From a consumer perspective, concerns about personal data being stolen or used improperly develop into attitudes that self-regulate personal behavior. These attitudes and publicized, visible data breaches create an environment of government regulations and corporate risk avoidance in their I/T operations and business processes. A good deal of past research has looked at this.

Quach, Thaichon Martin, Weaven and Palmatier (2022) discuss that four aspects of digital technology can create value for the marketer and consumer: 1) Data capturing 2) Data aggregation, processing, and storage, 3) data modeling and programming 4) Data visualization and interaction design. They propose that each category can enable data monetization and sharing, which create tensions with data privacy for consumers.

Woff and Lehr (2017) looked extensively at cybersecurity and the costs of data breaches in their research. The research evaluated the lack of empirical data, but as the rest of literature has focused on, it is all about cost and the derived risk mitigation.

Tanimura and Wehrly analyzed 152 data breaches from 117 publicly traded firms between 2000 and 2007. They found that the stock valuation declined on average by 23% from a data breach which was aligned to the estimated cost of dealing with the cleanup activities associated with it. They also determined

little reputation impact unless it involved employee data. Again, the focus was on costs and not on the impact on consumer behavior.

In contrast, Sinanaj and Zafar (2016) found data breaches do not impact shareholder value long-term but did have a significant cost to firm reputation on social media. Sharma, Oriaku and Oriaku (2020) also studied the costs associated with mitigating the effects of data breaches and found that the costs were higher and the risk greater when private personal data was involved. Martin, Borah and Palmatier (2017) found that the consumer's perceived vulnerability of data use and breaches was more likely the issue than data privacy concerns. This sense of vulnerability was a more accurate way to understand customer responses to the use of their data and could be mitigated by better transparency and control of the consumer data on the part of the marketer, according to Martin, et al.

Dongre, Mishra, Romanowski, and Buddhadev (2019) have established a plausible methodology for quantifying the cost of a data breach which feeds into the established narrative that the primary reason for data privacy is risk mitigation. A previous study from Loyton and Wotters (2014) looked at risk assessment and a data breach's tangible and intangible costs.

Chellappa and Pavlou (2002) showed that trust is linked to perceived data security which can be considered as surrogate for perceived consumer risk. In other words, consumer trust decreases when the belief that data security is lower. Finally, Choong, Hutton, Richardson, and Rinaldo (2017) observed that information security extends beyond the I/T function and into the marketing organization of a firm.

Zero-Party Data Exchange

Zero-party data is a term developed by Forrester Research to describe how some consumers will relinquish personal information in exchange for special pricing, promotional offers, and more personalized marketing. In other words, the consumer intentionally and proactively shares the data with the marketer as defined by Forrester. This data is often more accurate and reliable than third party acquired data. Palmatier and Martin (2019) found that loyalty programs were often used for this purpose. Other research suggests that this model works, because consumers feel that they are receiving something of value for providing sensitive information. The authors adopted a consumer journey model from Grewal and Roggeveen (2020) to map where data privacy threats might exist and where future research might take place. It is our observation that Zero-Party data probably requires extra attention around data privacy protection to prevent the loss of customer loyalty that has been directly entrusted via the relinquishing of personal data.

Zero-party data exchange is a relatively new concept compared to the longstanding practice of using purchased third party data for marketing purposes. Its use is projected to become pervasive, but there is not much current academic literature that exists.

Polloioli (2022) contends that Zero-party data is not a replacement but rather a complement to first party data (behavioral data) and that consumer concerns about data privacy still prevail. In fact, Karwatzki, Dyntynko, Trenz and Veit (2017) found in an experimental test that providing data transparency and control is insignificant in influencing the consumer's willingness to share personal data. We don't share this view, so our research seeks to explore this. Kraft, Kumar, Harmeling, Singh, Zhu, Chen, Duncan Fortin and Rosa (2020) identified four key criteria in the consumers view of the data exchange with a retailer (data ownership, data intimacy, data permanence and data value) as a theoretical framework for the process. While this model is logical, the authors did not conclusively prove it and instead proposed eleven questions requiring additional research. Based on our literature review, these questions require original quantitative data collection and analysis as today's existing body of knowledge cannot answer them.

Omni and Digital Channel Dynamics

The emergence of digital channels has changed the traditional retail landscape to one in which many consumers use physical in-person shopping and online web sites to shop and purchase transactions. Alexander and Chan (2019) maintain that synthesizing and using customer data across different sales channels is the key to delivering a good omnichannel experience. Yet, consumer privacy concerns often inhibit customers from relinquishing data, especially in digital transactions. Li et al (2019) found this to be the case in their research.

McCole, Ramsey, and Williams (2010) found that privacy and security considerations shape consumer attitudes about online shopping, which impact trust. Park et al. (2012), found that lack of trust was an inhibitor to certain consumers making online purchases. Zhang et al. (2019), theorize that delivering trustworthiness and credibility can overcome this and increase purchase intention. Cheah, Lim, Ting Liu, and Quach (2020) did find a significant relationship between trust and patronage intention in omnichannel retailing. These researchers also confirmed earlier studies that showed that privacy concerns negatively influence customer trust. The authors concluded that omnichannel retailers must build trust by addressing consumer data privacy concerns.

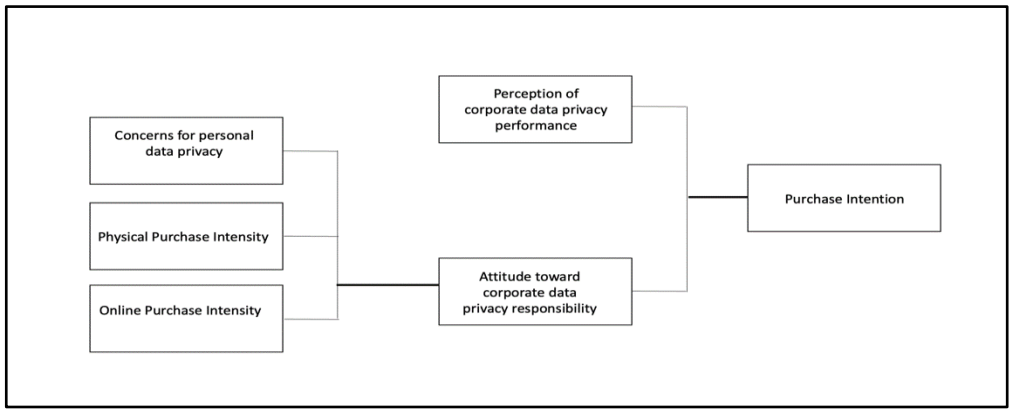
McCole, Ramsey and Williams (2008) built a regression model that found that trust in a vendor, trust on the internet and in third parties positively influence online purchase behavior. The authors also found that trust in the vendor becomes more important when the consumer has higher privacy and security concerns. Pramannik and Prabhu (2022) used factor analysis to identify eight determinants to perceived concerns and risks for e-commerce sites: customer confidence, trust, cyber security cognizance, accountability and policy issues, geopolitical and data sharing concerns, counterfeit products, e-transactional fraud, and protective attitude. This can be distilled into consumer confidence and trust in data privacy as important considerations for consumer adoption of digital commerce.

Chellappa and Pavlou (2002) found that perceived security and reputation were significant predictors of trust for eCommerce (digital) transactions, with financial liability being a weak influence. The researchers also found that data encryption data protection and authentication were significant antecedents to perceived security. These findings have important policy and operational practices implications for building consumer trust in omnichannel marketing.

Song and Cheng (2023) found that a product's privacy attributes dramatically influenced pricing in omnichannels. Choi and Nazarth (2014) determined the lack of security controls is an inhibitor to purchasing through digital sales channels and proposed a model for rebuilding trust once a data breach had occurred. Martin and Murphy (2017) have suggested that retailers might use privacy protection as a competitive differentiator. In its 2024 Data Privacy Benchmark Study, Cisco found that 97% of surveyed organizations felt obligated to use data ethically. We propose that ethics must be defined and perceived in the minds of the consumer and not by the organization's internal, myopic view.

Existing research has established a sound relationship between privacy concerns and trust and how trust is a tenet for purchase intentions. However, our literature search found that there is a dearth of academic research on how privacy expectations combined with privacy performance perceptions affect purchase intentions. In other words, would consumers who had high data privacy expectations and positive privacy performance perceptions be more inclined to purchase from a marketer who is perceived to responsibly manage data privacy? The literature review of Song and Cheng (2023) found little evidence that researchers studied data privacy and consumer behavior influencing the retailer's decisions. Furthermore, no research has established what factors drive consumer expectations about corporate data privacy responsibility. We believe that personal data privacy concerns and past purchase behavior are factors and would actually be antecedents to purchase intentions. We were intellectually curious and therefore postulated a theoretical model to advance our collective understanding in this area.

FIGURE 1
PROPOSED ROLE PRIVACY RESPONSIBILITY ATTITUDES AND PERCEIVED PRIVACY PERFORMANCE ON PURCHASE INTENTION MODEL



Researchers, 2023

Figure 1 defines the conceptual model of how we believe consumer privacy responsibility attitudes are shaped by past buying behavior and personal data privacy concerns. These expectations and the consumer's perception about corporate data privacy performance influence future purchase intentions.

Thus, our hypotheses follow:

H1: *The higher consumer data privacy expectations are, the higher purchase intent is to buy from a responsible marketer.*

H2: *The higher the perceived organizational data privacy performance is, the higher purchase intent is to buy from a responsible marketer.*

H3: *Attitude about corporate data privacy responsibility is shaped by the consumer's concerns for personal data privacy and the level of their physical and online purchase intensity.*

H3A, 3B, & 3C – See Tables 4 & 5 for these sub-hypotheses.

When we use the term "responsible marketer", we are referring to a marketer who is ethically practicing consumer data privacy protection and disclosing data retention, reuse and spillover practices and policies to its consumers that it is doing business with, as perceived by those consumers.

METHODOLOGY

Data Source

A market study collected 271 questionnaire data from U.S. respondents across all age groups, income levels, educational levels, and ethnicities. The researchers engaged American Pulse to collect the data, using an online panel. The raw survey data was weighted using industry standard statistical procedures to ensure the sample reflects the overall population that we were studying, *based on the Census Bureau's American Community Survey.* American Pulse's partner network of online panels includes more than 10 million potential respondents. Online panel surveys are non-probability surveys where respondents "opt-in" to participate. A random selection of respondents was invited to participate in the survey who meet various demographic criteria including age, gender, location, ethnicity, religion, income, and education. The large respondent universe allowed for a diverse and broad sampling pool, which helped to minimize sampling bias by increasing the likelihood of capturing a wide range of perspectives and characteristics representative of the United States population.

Sample weighting minimizes potential sampling biases by improving sample representativeness of the target population.

Table I shows that the sampling design and execution produced data representative of the United States population, including age, gender, ethnicity, education, and income to mitigate selection bias and ensure accuracy. The survey instrument was designed to collect demographics, purchase behavior, general data privacy concern, attitudes about corporate data privacy responsibility/performance, and purchase intent, respectively.

The respondents were asked to estimate both their online and physical purchase behavior intentions. Online shopping patronage was measured as the number of online purchases made during the past twelve months (Hansen and Jensen, 2009, Shim et al., 2001). The same measurement was used for the in-person purchase question. The data privacy concern section included questions about respondents' overall concerns about their personal data privacy, attitudes about corporate data privacy responsibility and performance and consumer sensitivity to corporate disclosure of data storage, reuse, and spillover practices. Finally, we examined the potential relationships between data privacy expectations, data privacy performance and the impact on purchase intent. Respondents were instructed to base their input based on doing business with a large organization as defined by having more than 500 employees and $50 million or more in revenue per year.

The sample was stratified across income categories to have equal representation for analysis purposes: 19.9% of the respondents earned $20,000 or less, 19.9% earned $20,001 to $50,000, 19.9% made $50,001 to $100,000, 19.9% earned $100,001 to $200, 000 and 20.4% had incomes over $200,000. The sampling design ensured that we had equal representation across income levels. Table 1 provides a brief overview of our participants' profiles.

Questionnaire Design

All the constructs were measured by multiple seven-point Likert-type scales ranging from 1 to 7, where 1 point to "strongly disagree" and 7 specifies "strongly agree." Specifically, respondents were asked about their level of agreement relative to whether corporations were responsible for protecting consumer data privacy and disclosing business practices relative to storage, reuse, and spillover of consumer data. The respondents were also asked their level of agreement on how well companies performed on these items. Concern about their own data privacy was assessed using the same 7-point Likert-type scale.

Purchasing behavior intensity was measured by asking respondents to state their annual purchase transaction volume for online and in-person categories in five distinct ranges from none to 50 or more. Table 2 contains this information.

Before administering the survey to a wide audience, the questionnaire was pretested using LinkedIn and Facebook social media and yielded complete and accurate responses.

TABLE 1
PARTICIPANTS' DEMOGRAPHIC STUDY

Gender	%	Age Cohort	%	Education	%	Ethnicity	%
Male	49.8% (135)	Post War	8.7% (24)	Elementary	1.5% (4)	African American	16.7% (45)
Female	49.3% (134)	Boomers	22.2% (60)	High school	44.4% (120)	Asian	6.8% (18)
Other	.9% (2)	Gen X	25.8 (70)	2-yr College	15.9% (43)	Caucasian	57.1% (155)
		Millennials	21.3% (58)	4-yr College	21.7% (59)	Hispanic	13.6% (37)
		Gen Z	21.9% (59)	Graduate	16.5% (45)	Multi-Racial	3.1% (8)
						Other	2.7% (7)

As noted in Table 1, the respondents were equally represented by females and males. No observed statistical differences were noted in measurements associated with our research hypotheses.

TABLE 2
BUYING BEHAVIOR INTENSITY

Online purchases	%	In Person Purchases	%
None	6.7% (18)	None	7.5% (20)
1-9	31.6 (86)	1-9	19.6% (53)
10-29	32.5% (88)	10-29	28.8% (78)
30-49	11.6% (32)	30-49	17.5 % (47)
50 or more	17.6% (48)	50 or more	26.6% (72)

Data Analysis

The survey data was analyzed using IBM SPSS V29 software for descriptive and inferential statistics. There were four 7-point Likert scale questions about consumer attitudes about a corporation's responsibility for maintaining data privacy (Overall data privacy maintenance, disclosure on data storage, disclosure on data reuse and disclosure on data spillover). The responses to these questions were consolidated into one variable using the transform function within SPSS. There were four similar questions relative to consumer perceptions about the corporate performance on maintaining data privacy, where those responses were also combined in the same manner. Previous academic research supports this approach to our analysis (Boone, H. N., and Boone, D. A., 2012). "The idea that Likert scales which combine the summated effects of multiple Likert-type items has become widely accepted, resulting in quantitative interval scale scores. Literature from Allen and Seaman (2007), Boone and Boone, (2012), Brown (2011), Carifio and Perla (2007), Clason and Dormody (1994), and Willits, Theodori and Luloff (2016) also support this.

A variety of descriptive statistics were run to examine the dynamics of consumer attitudes and perceptions about corporate data privacy practices. Overall, we found that consumers are concerned about data privacy and had a lower confidence in public corporations managing this well. Forty-five percent of the respondents agreed or strongly agreed that they were concerned with their own personal data privacy. Almost sixty-eight respondents agreed or strongly agreed that large corporations should be held responsible

for maintaining consumer data privacy, yet only 32.7% agreed or strongly agreed that these corporations were doing a good job maintaining this privacy. This represents a 35.20%-point gap in expectations versus perceived performance; showing that improvement is needed. We also found similar attitudes (expectations) about corporate responsibility for disclosing personal data storage, reuse and spillover practices to consumers and similar perceptions about corporate performance in these areas of data privacy.

The key question is, would consumers intend to purchase from a marketer who they deemed to be more responsible in maintaining data privacy? To explore this, we created an overall regression model and an underlying regression model to understand the drivers of attitudes toward corporate data privacy responsibility.

Regression Model # 1

As shown in Table 3, the regression model shows that the higher consumer data privacy expectations are, the higher the purchase intent is to buy from a responsible marketer and the higher the perceived organizational data privacy performance is, the higher purchase intent is to buy from a responsible marketer with an adjusted R^2 of .378 at a significance level of <.001. Therefore, hypothesis H1 and hypothesis H2 are proven.

Correlation Analysis

A correlation analysis was performed to examine the relationship between personal data privacy concerns, in-person buying intensity, and online buying intensity on consumers data privacy responsibility attitude. All three variables strongly correlate to the consumer's beliefs about an organization's responsibility for maintaining data privacy. As Table 4 illustrates, each of these variables are correlated to data privacy responsibility attitude at a significance level <.001. To analyze this further, a second regression analysis was performed.

Regression Model # 2

The researchers used the basis of the correlation analysis to run a regression model that demonstrates that the level of personal data privacy concern and the level of online and in-person buying activity (intensity) form the basis of a consumer's attitude about corporate data privacy responsibility. As shown in Table 5, the regression analysis shows that data privacy concerns and the intensity buying behavior drive consumer attitudes (expectations) about corporate data privacy responsibility. Therefore, H3 is proven in the regression model at the <.001 significance level. These are the underlying drivers of the attitude dimension of our theoretical consumer behavior model outlined in Figure #1. According to Cassell and Bickmore (2000), online trust is lower than face-to- face interactions in a physical store, which might explain why the online purchase intensity variable had a significantly lower P value than physical purchase intensity.

TABLE 3
REGRESSION MODEL #1

Hypothesis	Beta	t-statistics	r^2	Adj. r^2	F value	p-values	Decision
			.383	.378	83.101	<0.001	Supported
Constant	6.195	5.318				<0.001	
H1: Privacy Responsibility Attitude	0.551	11.111				<0.001	Supported
H2: Privacy Performance Perception	0.174	4.499				<0.001	Supported

TABLE 4
CORRELATION ANALYSIS

Hypothesis	Data Privacy Responsibility Attitude	p-values	Decision
H3: Personal Data Privacy Concern	.490	<0.001	Supported
H4: Online Purchase Intensity	.254	<0.001	Supported
H5: Physical Purchase Intensity	.407	<0.001	Supported

TABLE 5
REGRESSION MODEL #2

Hypothesis	Beta	t-statistics	r^2	Adj. r^2	F value	p-values	Decision
			.336	.329	45.090	<0.001	Supported
Constant	10.720	9.652				<0.001	
H3: Personal Data Privacy Concern	1.318	8.006				<0.001	Supported
H4: Online Purchase Intensity	0.473	1.824				.069	Supported
H5: Physical Purchase Intensity	1.202	4.886				<0.001	Supported

DISCUSSION

Overall, 45.40% of our respondents agreed or strongly agreed that they were concerned about their own personal data privacy and how their personal data might be used was a concern. Almost 68% of those surveyed felt that large enterprises should be held responsible for maintaining data privacy for consumers doing business with them. We found that consumers also strongly expected companies to disclose their data privacy practices around data storage, reuse, and spillover. Data storage or persistence pertains to how long data will be stored. Data reuse relates to data being repurposed, including the intentional sharing or sale of personal data to other firms. Spillover refers to data being used typically with a third party as part of business processes, such as transaction processing.

An example might be that a retailer using a third-party processor for credit card transactions. Almost 68% of the consumers surveyed felt that large companies had an obligation to disclose data storage practices and 66% felt that data repurposing practices should be disclosed. In addition, 63.7% of our respondents agreed or strongly agreed that disclosure of data spillover was a corporate responsibility.

So, we have established that this is important to consumers. But what is the perception among consumers relative to how well large companies are performing in this area? Perceptions are especially important when actual, empirical data about data privacy performance is unavailable to these consumers.

Overall, consumers do not feel that companies are doing a good job at protecting consumer data privacy or disclosing their practices. Only 32.7% of those surveyed agreed or highly agreed that companies were performing well in protecting consumer privacy, with 18% somewhat agreeing. Consumers rated the performance of large companies in disclosing data privacy practices even lower with only 27% agreeing or highly agreeing that companies were performing well on disclosing data storage practices. Only 26% and 25% of those surveyed agreed or strongly agreed that large companies are performing well on disclosing data reuse and data spillover practices, respectively.

Table 6 shows significant gaps between consumer privacy expectations and the perceived performance of large corporations in these areas. The gaps are large, ranging from 35.2% to 40.8%. The expectations,

performance and measured gaps are based on the percentage of respondents agreeing or strongly agreeing from the seven-point Likert scale.

The gap analysis shows that corporations have a great deal of work to do to improve their perceived performance on protecting consumer data privacy across the four dimensions of this. We view this as an opportunity for forward-thinking organizations to take a proactive and ethical stance in developing data privacy safeguards, building ethical data use policies, and clearly articulating their data privacy policy to their consumers. Based on our findings, building trust through ethical data privacy policy and disclosure will ultimately create a competitive advantage.

TABLE 6
GAP ANALYSIS-EXPECTATIONS VS. PERFORMANCE

	Expectation	Performance	Gap
Maintaining Data Privacy	67.9%	32.7%	35.2%
Disclosing Data Storage Practices	67.6%	27%	40.6%
Disclosing Data Repurposing Practices	66%	25.2%	40.8%
Disclosing Data Spillover Practices	63.7%	25.1%	38.6%

Data privacy policy and practices within organizations have been largely manifested by risk avoidance and regulatory compliance. Data breaches that compromise consumer privacy are a major business issue and the focus of increasing government intervention. These breaches can be very expensive.

Empirical data suggests that organizations are performing poorly in protecting consumer data privacy. A 2022 survey of 21,000 consumers across 11 countries and 5 continents, conducted by the University of Warwick and the Thales Group found that globally, 33% of all consumers experienced a data breach of their personal information of which 82% saw a negative impact on their personal lives. In the United States it was 48%. The same study found that 21% of consumers who experienced a data breach stopped doing business with the company and 42% of these individuals requested that their personal information be deleted. This is corroborated by the Ponemon Institute (2015) which found that 47% of Americans were personally affected by cybercrime. Interestingly, in another study, Mayer et. al., (2021) found that 74% of a sample of 413 consumers who had a data breach were unaware of the breach. These same consumers tended to blame their behavior for the breach and often felt it was inevitable. McNulty (2007) found that 78% of customers would unlikely continue shopping at a store once they learned about a data breach. Berezina, et. al., (2012), found that within the hospitality industry, a data breach hurt perceived service quality, customer satisfaction, and repurchase intentions.

Sinanaj and Zafur (2016), found that data breaches negatively impact social media sentiment and organizational reputation but do not necessarily impact the shareholder value of a corporation. However, Taniura and Wehrly (2009) found that organizations that experienced a data breach had a negative stock return of -23% and postulated that this is due to the direct costs of mitigating the breach's impact, rather than the reputational impact of the breach. Choong, et. al., (2017), findings reaffirm the negative impact on stock valuations from data breaches and argue that loss of customers, loss of trust, reputation, perceptions of risk, and brand equity are also negatively impacted.

According to the Ponemon Institute, in 2023, the average data breach cost was $4.48M globally, with the cost in the U.S. being much higher at $9.48M. According to Wolff and Lehr (2017), the Ponemon data breach survey is well-known and looks at the direct costs of detecting and responding to data breaches but does not reflect preventative measures. Numerous researchers have studied the effect of data breaches on stock prices with Spanos and Angelis (2016) finding 76% of 37 reviewed papers showing a significant negative impact of data privacy breaches on stock prices. Dongre, et. al., have developed cost function equations that express the quantitative impact of consumer data privacy breaches, including one from a consumer perspective. The Equifax and Target data breaches were used as case studies to develop these equations.

Casual observation suggests that companies do not disclose their data privacy guidelines or practices on public websites or other customer-facing communications. This is confirmed by LaRose and Rifon (2007) who found most privacy policy statements are obtuse and noncommittal. This is unfortunate as perceived security is viewed as a critical prerequisite of trust (Choi and Nazareth 2014) In those instances where marketing discloses data privacy, it is done within the context of granting permission to opt in for marketing communications or providing consent for some type of transaction. The language disseminated is certainly not transparent, understandable, or positive in terms of stating proactive procedures protecting the consumer's privacy. Rather, it is arcane, confusing, and obtuse legal language designed to protect the corporation and their interests. Even experienced attorneys have difficulty reading through the pages of disclaimers, indemnification clauses and other extensive terms and conditions of the agreement. It's no wonder that organizations don't foster trust around data privacy or are not perceived as doing a good job of protecting it and disclosing practices.

CONCLUSION

Previous academic research focused on the negative aspects of consumer data privacy practices, rather than exploring whether strong protection of consumer data might be positively aligned with purchase intentions to do business with firms perceived as doing a good job of protecting confidential personal information. This previous work tended to study past occurrences rather than taking a forward-looking perspective and focusing on purchase behavior intentions. Government oversight and regulation have caused firms to approach data privacy as a risk mitigation proposition rather than an opportunity to establish greater consumer trust and create some competitive differentiation around this important dimension of a brand.

Sarathy and Robertson (2003) proposed a model that could describe the influencing factors on a firm's privacy strategy. These "external and uncontrollable factors included national history and culture, global society trends in privacy protection, legislation and the sensitivity of the collected data. They contended that organizations needed to build an ethical perspective of data privacy that balanced self-interest with the needs of consumers and society or faced increased regulation. While we agree with this premise, the authors believe placing consumers privacy interests first will lead to a business advantage. This study has discovered that placing the consumer's needs for data privacy foremost in business practices increases the likelihood that consumers with higher personal privacy concerns and higher past purchase activity will purchase from them. Consumers who demonstrate high past buying intensity are a very attractive segment as they will likely be the strongest purchasing group in the future. In short, responsible corporate data privacy practice is rewarded in increased buyer purchase intention.

This study discovered that consumers who believe strongly that corporations are responsible for maintaining data privacy are more inclined to purchase from marketers who are perceived as doing a good job of maintaining data privacy and disclosing their data privacy practices around data storage, reuse, and spillover. The study also found that corporate data privacy responsibility attitudes are formed based on concerns about individual data privacy and the intensity of physical and online purchase behavior. This is new discovery that addresses gaps in existing research and improves our understanding of how consumer behavior is impacted by how data privacy and how organizations manage it.

Theoretical and Managerial Implications

This study offers several important theoretical contributions. First, this study has discovered two critical antecedents to future purchase intention: attitude toward corporate data privacy responsibility and perceptions of data privacy performance and disclosure transparency. Secondly, the study determined the drivers of attitude toward corporate data privacy responsibility are personal privacy concerns and the intensity of buying behavior. Based on our literature review, we believe these are new, noteworthy contributions to our understanding of consumer behavior relative to data privacy. Past research primarily looked at tradeoffs consumers would make regarding data privacy in exchange for receiving more relevant and targeted messages and offers. It also looked at the negative impact of data privacy breaches and

regulations as the reason to be concerned about data privacy rather than a positive force that could be a win-win for both consumers and the business.

To date, consumer data privacy in organizations has been managed as a compliance issue and a necessary expense to mitigate regulatory risk or an embarrassing data breach. Laws and punitive fines such as those imposed by the European General Data Protection Regulation (GDPR) have shaped corporate data privacy policy and practices. From a more positive perspective, marketers and consumers alike realize that personal data can be used powerfully to improve relevancy, targeting and customization to improve the buying experience. Are these two perspectives mutually exclusive? No, this study definitively illustrates that pursuing open, transparent, and clear set of data privacy practices that consumers can see and engage with can create a buying preference for the responsible marketer. Rather than viewing data privacy as a compliance and risk issue, organizations can create a competitive advantage by communicating and executing data privacy as part of their customer dialog. Marketers seek to build engagement and trust with customers. Earlier findings from Vail et al. (2008) determined that complex privacy policies that are hard to understand diminish confidence and trust in a firm. Grabner-Krauter and Kalusha (2003) established that demonstrating trust is essential in business-to-consumer electronic transactions. McCole, Ramsey, and Williams (2009) found that trust in the vendor increases when consumers have higher privacy and security concerns. Mayer, Davis and Schoorman (1995) defined trust as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control the other party." Delivering data privacy and communicating about it in a transparent manner that consumers can see and understand is a policy that all corporations need to embrace and adopt as a strategy and set of operational practices.

Historically, data privacy has been the responsibility of those managing compliance and the I/T functions in a corporation. We suggest that the marketing function needs to be included in this, as data privacy is about establishing and maintaining trust with the firm's customers. This needs to be managed by marketing. We further contend that a forward-looking, consumer centric, proactive data privacy strategy potentially offers a vehicle to deliver more customer value and to create a competitive advantage through differentiation in this area. No other academic research has looked at this before or made this case.

From an operational standpoint, this means clearly and transparently disclosing how consumer data will be used, reused, stored, and shared in easy-to-understand language that creates trust. Without compromising proprietary technological infrastructure information, corporations would serve themselves well in disclosing their practices for safeguarding consumer data that instills confidence and motivates buyers to prefer doing business with them over other firms. To succeed, marketers must adequately disclose how they are safeguarding their personal data, how long it will be retained, how data may be repurposed (reused) and where data may spillover. Organizations who prioritize customer data privacy needs over the need to sell consumer data to generate short-term monetary value will prosper in the long term. We contend that practicing data privacy ethics manifests a customer-centric organizational culture and, as this study shows, the foundation for a competitive marketing advantage.

Future scholars are invited to expand the study's coverage to understand how consumer behavior might be shaped by privacy concerns regarding artificial intelligence in the same light. Furthermore, this research can be expanded to examine whether consumers are willing to pay a price premium for products and services with a higher degree of consumer data protection and by how much. Brands that offer more value can charge a price premium over undifferentiated competitors. How might exceptional data privacy practices factor into a brand's perceived value? This study could also be expanded to look at smaller businesses and other geographies.

REFERENCES

Abdul-Muhmin, A.G. (2011). Repeat purchase intentions in online shopping: The role of satisfaction, attitude and online retailers' performance. *Journal of International Consumer Marketing*, *23*(1), 5–20.

Acquisti, A. (2014). The economics and behavioral economics of privacy. *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, *1*, 76–95.

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

Alexander, B., & Cano, M.B. (2019). Futurizing the physical store in the omnichannel retail environment. In W. Piotrowicz & R. Cuthbertson (Eds.), *Exploring Omnichannel Retailing* (pp. 1–20). Cham: Springer.

Allen, I.E., & Seaman, C.A. (2007). Likert scales and data analyses. *Quality Progress*, *40*(7), 64–65.

Berezina, K., Cobanoglu, C., Miller, B.L., & Kwansa, F.A. (2012). The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, *24*(7), 991–1010.

Bernard, E.K., & Makienko, I. (2011). The effects of information privacy and online shopping experience in e-commerce. *Academy of Marketing Studies Journal*, *15*, 97–110.

Bloom, P.N., Milne, G.R., & Adler, R. (1994). Avoiding misuse of new information technologies: Legal and societal considerations. *Journal of Marketing*, *58*(1), 98–110.

Boone, Jr., H.N., & Boone, D.A. (2012). Analyzing Likert data. *The Journal of Extension*, *50*(2), 48–56.

Brown, J.D. (2011). Likert items and scales of measurement. *Statistics*, *15*(1), 10–14.

Carifio, J., & Perla, R.J. (2007). Ten common misunderstandings, misconceptions, persistent myths and urban legends about Likert scales and Likert response formats and their antidotes. *Journal of Social Sciences*, *3*(3), 106–116.

Cassell, J., & Bickmore, T. (2000). External manifestations of trustworthiness in the interface. *Communications of the ACM*, *43*(12), 50–56.

Cheah, J.-H., Lim, X.-J., Ting, H., Liu, Y., & Quach, S. (2022). Are privacy concerns still relevant? Revisiting consumer behaviour in omnichannel retailing. *Journal of Retailing and Consumer Services*, *65*, 102242.

Chellappa, R.K., & Pavlou, P.A. (2002). Perceived information security, financial liability, and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358–368. https://doi.org/10.1108/09576050210447046

Choi, J., & Nazareth, D.L. (2014). Repairing trust in an e-commerce and security context: An agent-based modeling approach. *Information Management & Computer Security*, *22*(5), 490–512.

Choong, P., Hutton, E., Richardson, P.S., & Rinaldo, V. (2017). Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. *Journal of Marketing Development and Competitiveness*, *11*(1), 59–66.

Cisco. (2024). *Data Privacy Benchmark Study*.

Clason, D.L., & Dormody, T.J. (1994). Analyzing data measured by individual Likert-type items. *Journal of Agricultural Education*, *35*(4), 31–35.

Creyer, E.H. (1997). The influence of firm behavior on purchase intention: Do consumers really care about business ethics? *Journal of Consumer Marketing*, *14*(6), 421–432.

Dongre, S., Mishra, S., Romanowski, C., & Buddhadev, M. (2019). Quantifying the costs of data breaches. In *Critical Infrastructure Protection XIII: 13th IFIP WG 11.10 International Conference, ICCIP 2019, Arlington, VA, USA, March 11–12, 2019, Revised Selected Papers*, *13*, (pp. 3–16). Springer International Publishing.

Fogg, B.J., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., . . . Treinen, M. (2001, March). What makes web sites credible? A report on a large quantitative study. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 61–68).

Grabner-Kräuter, S., & Kaluscha, E.A. (2003). Empirical research in on-line trust: A review and critical assessment. *International Journal of Human-Computer Studies, 58*(6), 783–812.
Grewal, D., & Roggeveen, A.L. (2020). Understanding retail experiences and customer journey management. *Journal of Retailing*, *96*(1), 3–8.
Hansen, T., & Jensen, J.M. (2009). Shopping orientation and online clothing purchases: The role of gender and purchase situation. *European Journal of Marketing*, *43*(9/10), 1154–1170.
Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*(2), 263–291.
Karwatzki, S., Dytynko, O., Trenz, M., & Veit, D. (2017). Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems*, *34*(2), 369–400.
Krafft, M., Kumar, V., Harmeling, C., Singh, S., Zhu, T., Chen, J., . . . Rosa, E. (2021). Insight is power: Understanding the terms of the consumer-firm data exchange. *Journal of Retailing*, *97*(1), 133–149.
Kumar, D.V., & Dange, U. (2012). *A study of factors affecting online buying behavior: A conceptual model*. Available at SSRN 2285350.
LaRose, R., & Rifon, N.J. (2007). Promoting i-safety: Effects of privacy warnings and privacy seals on risk assessment and online privacy behavior. *Journal of Consumer Affairs*, *41*(1), 127–149.
Li, N., & Zhang, P. (2002). Consumer online shopping attitudes and behavior: An assessment of research. *AMCIS 2002 Proceedings*, *74*.
Lim, Y.J., Osman, A., Salahuddin, S.N., Romle, A.R., & Abdullah, S. (2016). Factors influencing online shopping behavior: The mediating role of purchase intention. *Procedia Economics and Finance*, *35*, 401–410.
Maples, C., & Thales Group. (2022). *Consumer Digital Trust Index*. Retrieved from https://www.thalesgroup.com/sites/default/files/prezly/documents/04102022_PR_Thales%20Trust%20index_EN.pdf
Marthews, A., & Tucker, C. (2023). What blockchain can and can't do: Applications to marketing and privacy. *International Journal of Research in Marketing*, *40*(1), 49–53.
Martin, K.D., & Murphy, P.E. (2017). The role of data privacy in marketing. *Journal of the Academy of Marketing Science*, *45*, 135–155.
Mayer, P., Zou, Y., Schaub, F., & Aviv, A.J. (2021). "Now I'm a bit {angry:}" Individuals' awareness, perception, and responses to data breaches that affected them. In *30th USENIX Security Symposium (USENIX Security 21)* (pp. 393–410).
McCole, P., Ramsey, E., & Williams, J. (2010). Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns. *Journal of Business Research*, *63*(9–10), 1018–1024.
McNulty, E. (2007). Boss, I think someone stole our customer data. *Harvard Business Review*, *85*(9), 37.
Nehf, J.P. (2007). Shopping for privacy on the internet. *Journal of Consumer Affairs*, *41*(2), 351–375.
Polonioli, A. (2022). Zero party data between hype and hope. *Frontiers in Big Data*, *5*, 943372. doi:10.3389/fdata.2022.943372
Pomfret, L., Previte, J., & Coote, L. (2020). Beyond concern: Socio-demographic and attitudinal influences on privacy and disclosure choices. *Journal of Marketing Management*, *36*(5–6), 519–549.
Pramanik, R., & Prabhu, S. (2022, March). Analyzing cyber security and data privacy models for decision making among Indian consumers in an e-commerce environment. In *2022 International Conference on Decision Aid Sciences and Applications (DASA)* (pp. 735–739). IEEE.
Priyadharshini, A.K., & Mathew, S.K. (2016, September). The impact of individual privacy and personalization on online buying behavior: An experimental study. In *2016 IEEE International Conference on Management of Innovation and Technology (ICMIT)* (pp. 150–155). IEEE.
Quach, S., Thaichon, P., Martin, K.D., Weaven, S., & Palmatier, R.W. (2022). Digital technologies: Tensions in privacy and data. *J. of the Acad. Mark. Sci.*, *50*, 1299–1323.

Regner, T., & Riener, G. (2017). Privacy Is Precious: On the Attempt of Lifting Anonymity on the Internet to Increase Revenue: Privacy Is Precious. *Journal of Economics & Management Strategy*.
Sánchez, M., & Urbano, A. (2019). Security in digital markets. *Journal of Business Research*, *101*, 485–491.
Sarathy, R., & Robertson, C.J. (2003). Strategic and ethical considerations in managing digital privacy. *Journal of Business Ethics*, *46*, 111–126.
Schoorman, F.D., Mayer, R.C., & Davis, J.H. (1996). Organizational trust: Philosophical perspectives and conceptual definitions. *Academy of Management Review*, *21*(2), 337–340.
Sharma, N., Oriaku, E.A., & Oriaku, N. (2020). Cost and effects of data breaches, precautions, and disclosure laws. *International Journal of Emerging Trends in Social Sciences*, *8*(1), 33–41.
Shewan, D. (2020, February 25). Ethical marketing: 5 examples of companies with a conscience. *Wordstream.*
Shim, S., Eastlick, M.A., Lotz, S.L., & Warrington, P. (2001). An online prepurchase intentions model: The role of intention to search. *Journal of Retailing*, *77*(3), 397–416.
Sinanaj, G., & Zafar, H. (2016). Who wins in a data breach? A comparative study on the intangible costs of data breach incidents. *Journal of Information Privacy and Security*, *12*(4), 216–229.
Song, Z., & Cheng, J. (2023). Omnichannel expansion for traditional retailers: Considering consumers' privacy concerns. *Managerial and Decision Economics*, *44*(7), 3997–4010. https://doi.org/10.1002/mde.3931
Spanos, G., & Angelis, L. (2016). The impact of information security events on the stock market: A systematic literature review. *Computers & Security*, *58*, 216–229.
Tanimura, J.K., & Wehrly, E.W. (2009, October). The market value and reputational effects from lost confidential information. *International Journal of Financial Management*, *5*, 18–35.
Theodori, G.L., & Luloff, A.E. (2000). Urbanization and community attachment in rural areas. *Society & Natural Resources*, *13*(5), 399–420.
Tucker, C.E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, *51*(5), 546–562.
Vail, M.W., Earp, J.B., & Anton, A.I. (2008). An empirical study of consumer perceptions and comprehension of web site privacy policies. *IEEE Transactions on Engineering Management*, *55*, 442–454.
Varian, H.R. (1996). *Economic issues facing the Internet*. Consortium for Research on Telecommunications Policy.
Willits, F.K., Theodori, G.L., & Luloff, A.E. (2016). Another look at Likert scales. *Journal of Rural Social Sciences*, *31*(3), 6.
Wolff, J., & Lehr, W. (2017, March 31). Degrees of ignorance about the costs of data breaches: What policymakers can and can't do about the lack of good empirical data. *SSRN*.