



Consumer privacy in retail:

The next regulatory and competitive frontier

You have likely received a distinctive and personalized retail offer based on your preferences and past buying behaviors. While many may like the individualized attention, consumers are becoming increasingly aware of how their data is used and more sensitive to privacy matters. In an ever-more-complex data environment, retailers face a growing list of global and state privacy regulations aimed at protecting consumers. The penalties, which can quickly surpass the billion-dollar mark, are too steep to ignore.

Mishandling data can mean placing future revenues at risk. Advanced privacy policies protect consumer data, but they do so much more. They create the ability to leverage more accurate information to create a more intimate and trusting relationship with the consumers. Privacy policies should be in line with, if not central to, the retailers' business strategy to build and maintain this consumer trust. As a result, retailers should become more trust-focused and consumer-centric in their policies regarding data privacy.



Consumers are more privacy-aware

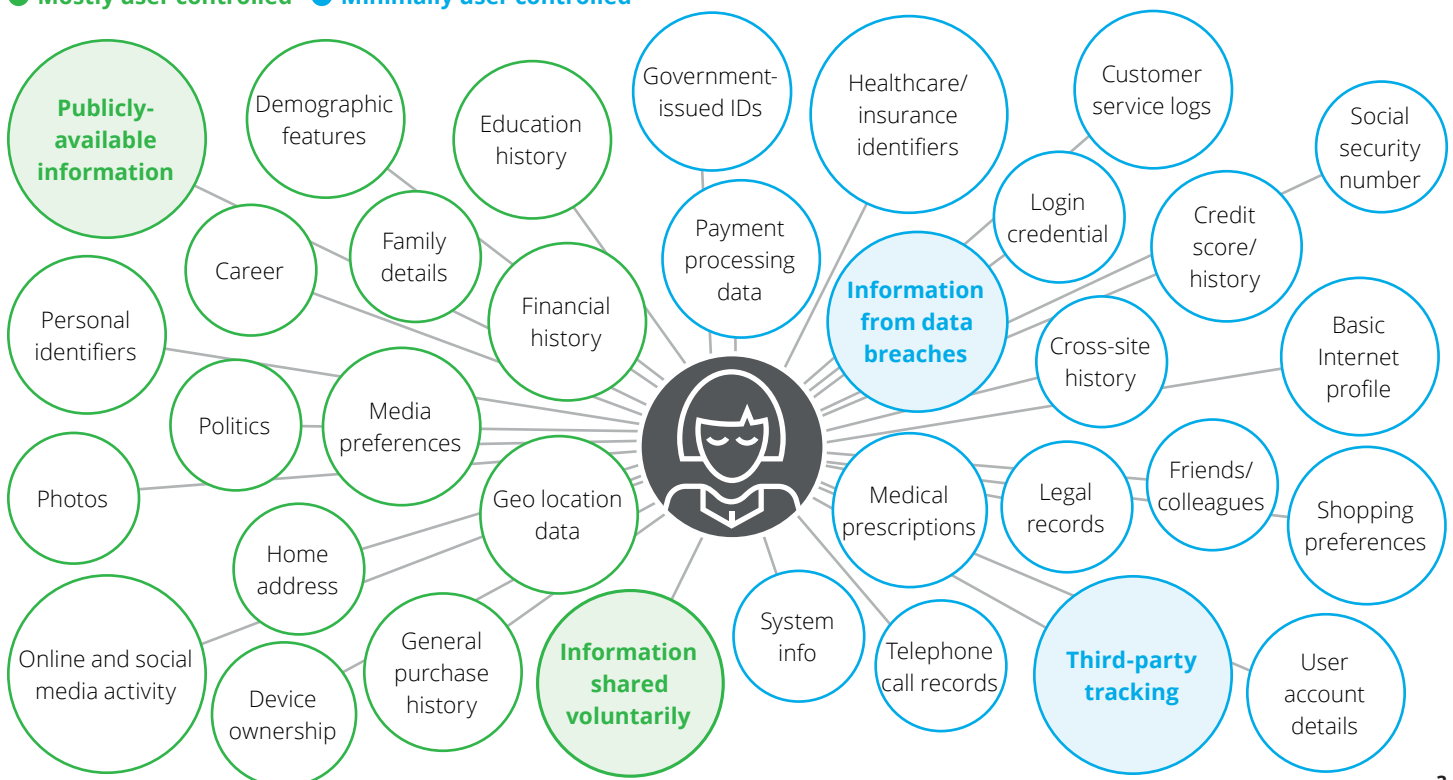
High-profile data breaches and privacy infractions have made consumers more aware that their data is at risk. Deloitte's US Consumer Data Privacy Survey shows that one in every three Americans has been exposed to data compromise. From 2016 to 2018, the volume of breached records in the United States grew twelve-fold.¹ Nearly half of consumers feel that they have little to no control over their personal data.² The vast majority believe that they should be able to opt out of the sale of their personal data.³ Figure 1 shows the various types of consumer information that is exposed; many consumers do not even realize that some of this is accessible. Not being able to see or control how their personal data is used can leave consumers feeling helpless.

But all is not lost. Nearly three in four consumers are willing to share personal data if they receive things like better pricing, special discounts, or exclusive offers.⁵ Also, when consumers trust a retailer and are satisfied with their privacy policies, consumers are more likely to be open or neutral about sharing personal data (73 percent) compared to those who are dissatisfied or unaware (57 percent).⁶

Gaining consumer trust may be hard for some retailers. Only 5 percent of consumers place the retail industry at the top in ensuring data privacy, compared to 63 percent for banking.⁷ Nearly two-thirds of consumers say retailers, not the government or tech vendors, are responsible for data security. Lacking consumer trust but still being held accountable places retailers in a difficult position.⁸ The introduction of new regulations might serve as a catalyst.

Figure 1. Consumers are unaware of the abundance of personal data they reveal daily⁴

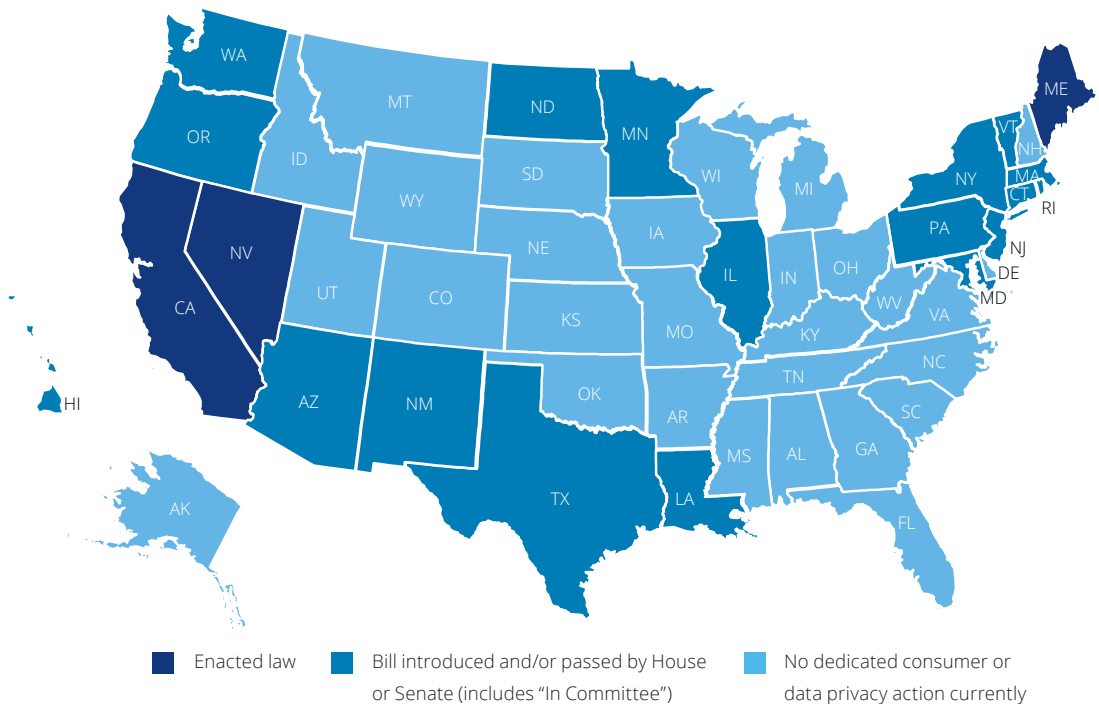
● **Mostly user controlled** ● **Minimally user controlled**



Privacy regulations accelerating

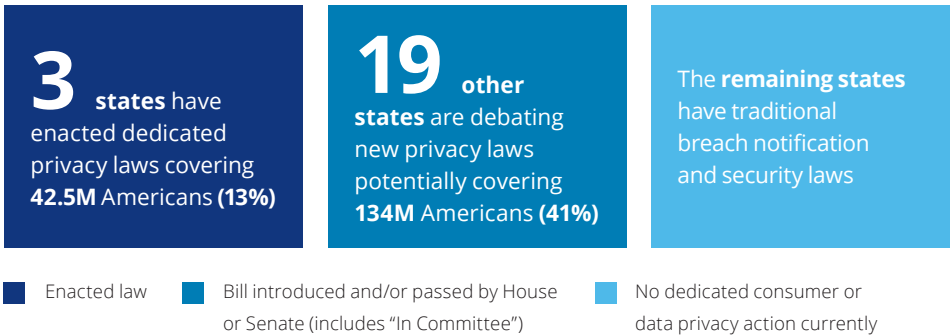
The European Union’s General Data Protection Regulation (GDPR), launched in May 2018, was an early warning to many US retailers. Now similar privacy initiatives, incremental to traditional cybersecurity laws, are coming to our shores. The lack of a single, federal mandate has placed the onus on states to craft their own privacy laws. This has the potential to create a patchwork of legislation that could be confusing and complex to manage (see figure 2).

Figure 2. State of privacy legislation in the United States



Source: Deloitte analysis of legislations related to privacy passed or enacted in 50 US states as of September 2019.

Figure 3. Reach of state-driven privacy legislation in the United States
New privacy regulation coverage by US population (327 million)



Source: Deloitte analysis of legislations related to privacy passed or enacted in 50 US states as of September 2019.






As of this writing, nearly half of all US states are developing data privacy legislation. Three states (CA, ME, NV) have already enacted laws. Figure 3 demonstrates the reach of new privacy regulations in the US.⁹ By far the largest initiative is the California Consumer Privacy Act (CCPA). Set to go into effect January 1, 2020, the CCPA includes a strict set of regulations regarding consumer privacy similar in scope to the GDPR.

The CCPA's noncompliance penalties are significant. A relatively small privacy incident involving only 5 percent of California consumers could cost a retailer as much as \$5–\$10 billion in civil penalties and statutory damages, or 50 percent to 150 percent of revenue for a retailer with \$10 billion in annual revenue. That translates to ~5 to 15 times earnings before interest, tax, depreciation, and amortization (EBITDA) based on retail industry benchmarks.¹⁰ Current privacy programs cost a fraction of that, roughly 0.35 percent of revenue on average.¹¹ For more information on CCPA, please see Deloitte's ["A quick reference guide for CCPA compliance."](#)

Retailers should be data-wise and privacy-conscious

For the past several years, retailers have focused on using data to:

-  Learn more about consumers;
-  Create deeper relationships with frequent buyers; and
-  Communicate in more personal ways with individual customers.

Retailers have gathered huge amounts of consumer data using advanced technologies such as location tracking and facial recognition, while digital-focused or more advanced retailers are even capturing voice.

In a typical large retail chain store, data is gathered from a myriad of touchpoints. Figure 4 depicts a shopper journey in a store from a data and analytics perspective. Data collected from in-store sensors or geo-tracking[†] can provide a valuable input for better shopper personalization. For example, artificial intelligence (AI) assistants can provide product recommendations based on specific shopper data. While the data collected can provide a faster, more relevant engagement for the shopper, it also comes with some risk to the retailer. That data should be protected from unauthorized access or unintentional sharing with third parties and adhere to advancing cybersecurity and privacy standards.

Data collected from customer touchpoints will grow from a total of 33 zettabytes (ZB)[‡] in 2018 to 175 ZB by 2025, a growth of 142 ZB in the next seven years.¹² Dealing with that much data places a strain on retailers in several ways, including making it harder to introduce strong consumer data privacy programs.

Retailers who don't have clear policies about privacy or don't have a good way to address privacy concerns can create confusion in the market. This can be exacerbated as retailers experiment with new technologies that provide access to brand new sources of data. It can also introduce the "creep factor" if new tracking technologies, such as facial recognition or emotional tracking, are not communicated to consumers in a way that explains the rationale and value.

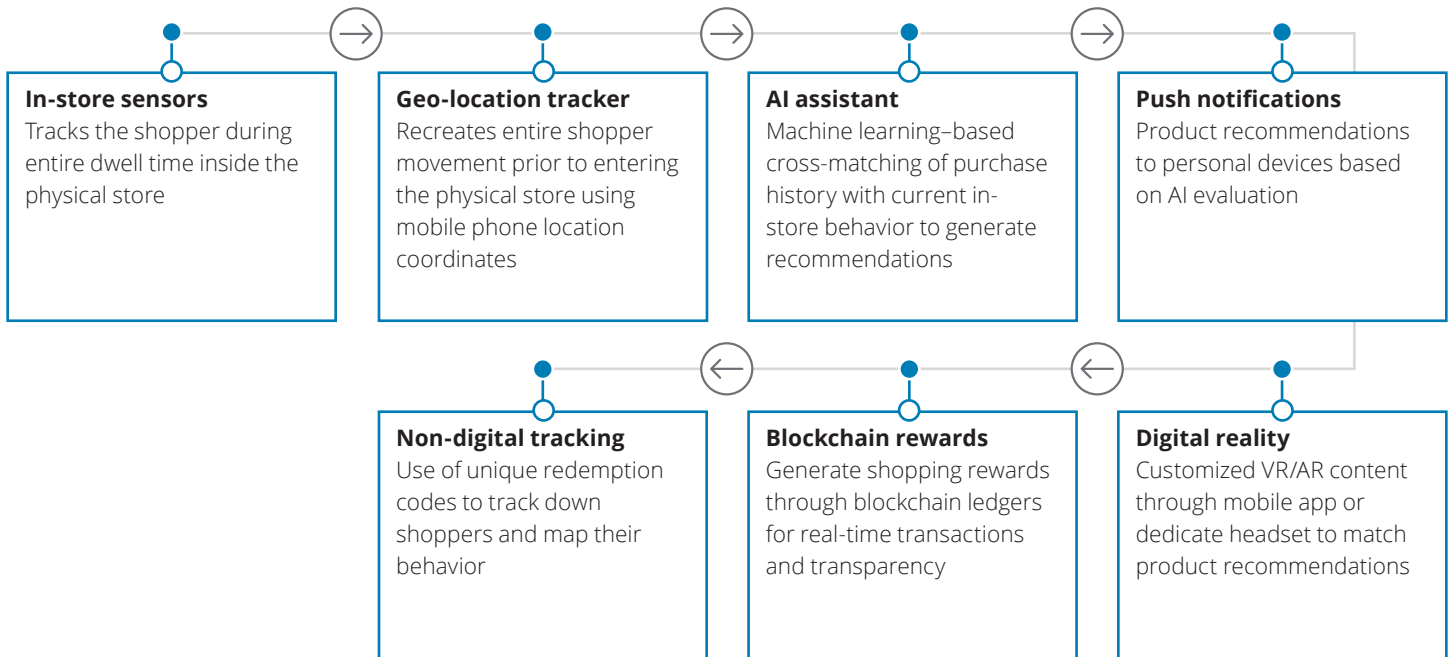
Consumers struggle to understand what information retailers collect or how they use it. Over two-thirds of consumers believe that retailers use their data for target marketing.¹³ What's more, 55 percent of consumers believe retailers share data with third parties or sell it to outside buyers.¹⁴ Retailers have an opportunity to engage consumers on how data is being used to build trust. For instance, retail executives in our survey indicated the top three uses of consumer data is for increasing efficiencies in operations (53 percent), improving product selection (52 percent), and enhancing in-store services or experiences (49 percent).¹⁵

[†] Identifying a person's current, physical location by obtaining GPS data from their smartphones or other GPS-enabled devices.

[‡] Zettabyte (ZB) = 1 trillion gigabytes (GB).

Figure 4. Example of a data-driven consumer journey that can drive experience or exposure

The approach



The impact

Experience: What can go right



Speed



Relevance



Engagement

Exposure: What can go wrong



Intrusive activations



Unknown uses of
personal info



Third-party access
to data



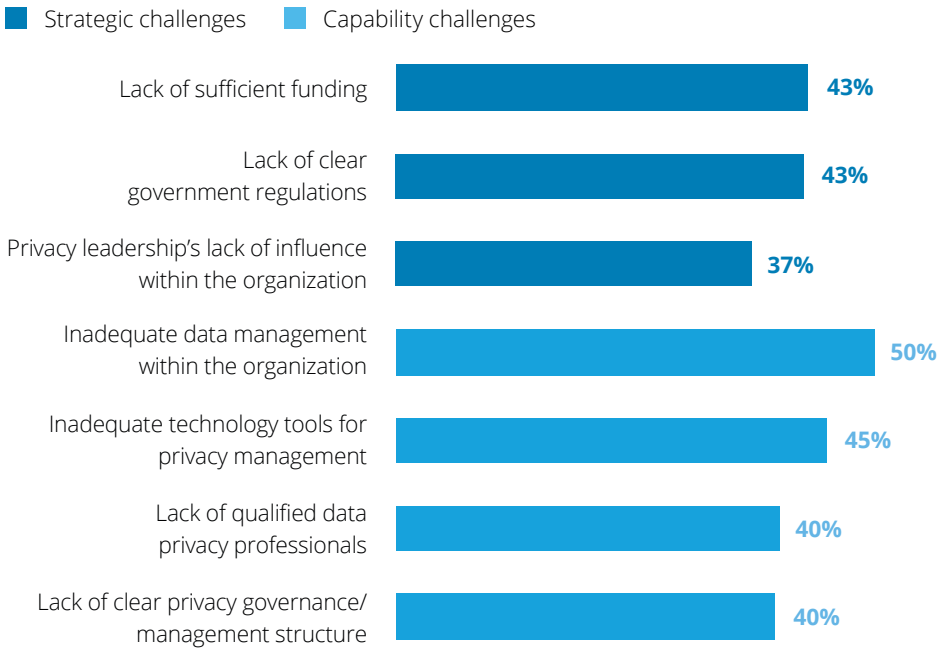
Many retailers are outwardly showing more concern about consumer privacy as they continue to face challenges internally. Over half of retail executives believe regulations around consumer privacy will have a major or significant impact on their business.¹⁶ At a strategic level, only 1 in 5 retail executives surveyed believes that they have done an adequate job of integrating their data privacy strategy with their overall corporate or business unit strategy.¹⁷ Addressing this misalignment could be a significant opportunity.

As retailers collect more and more data, they must overcome a fairly complex internal environment. Nearly two-thirds say their organization has more than 50 information systems (spreadsheets,

customer relationship management [CRM], data warehouses, data lakes, mainframe applications, point-of-sale, cloud applications, email servers, etc.) that hold consumer data.¹⁸ Consumer data residing in multiple systems without a way to bring it all together can make it harder to introduce programs designed to protect consumer privacy. Fully half say inadequate data management is a challenge to implementing consumer privacy programs, the top response of all executives.¹⁹

At the same time, many retailers are struggling to find ways to pay for needed privacy programs. Almost half of retail executives say that lack of funding for privacy policies is a primary strategic challenge.²⁰

Figure 5. Challenges in designing and implementing a consumer privacy strategy

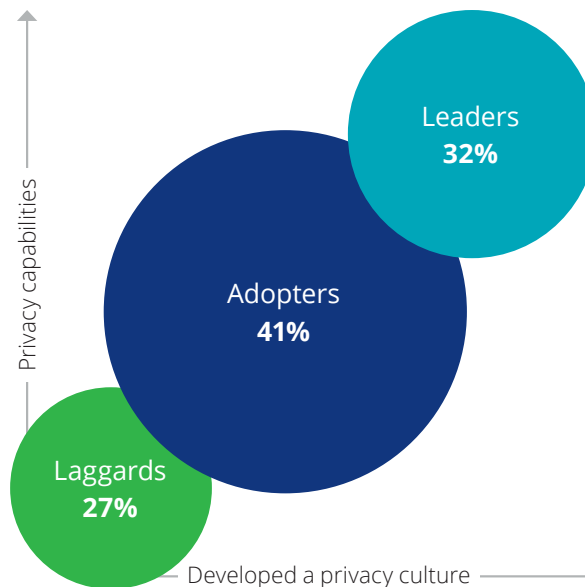


Three different ways today's retailers approach privacy

A closer look at the results of Deloitte's retail executive survey helped us classify the way retailers approach privacy. Three major categories emerged that were significantly different in their approach to privacy (figure 6):²¹

- Leaders are trust-focused, consumer-centric:** These retailers have a privacy policy that is a prominent part of the corporate strategy; they focus on the consumer and make it a priority to protect consumer privacy with an intentional focus on building and maintaining trust. About one-third of surveyed executives fall into this group (32 percent).
- Adopters are testers and aspirers:** These retailers are working to increase their focus on privacy, but the level of focus still varies within the organization. This accounts for most executives (41 percent).
- Laggards are process-focused, tactical:** These retailers may have privacy policies on paper, but their capability to maintain effective privacy controls is immature and highly tactical. These organizations have not made consumer privacy a business priority, thinking of privacy as largely a legal and compliance issue, and this is reflected in the way they operate. This accounts for about a quarter of those surveyed (27 percent).

Figure 6. Differing approaches to consumer privacy



Trust-focused, consumer- centric retailers move the bar on data privacy

Trust-focused, consumer-centric retailers are much more likely to have made privacy an essential part of their business strategy, corporate culture, and internal operations. Gaining consumer trust is a key attribute. As a result, their privacy focus is consumer-centric, which ties into its business strategy. Leaders in this space align their business and privacy strategies across the company, driving a culture of engagement. Leading retailers manage their data in a way to create a holistic view of the consumer, give consumers greater access to information, and invest in cybersecurity technology and processes. Based on our analysis, the organization-wide emphasis on privacy can be examined through four key areas: consumer centricity, strategic alignment, data management, and security and infrastructure, as shown in figure 7.

Figure 7. Focus areas in developing a privacy strategy



Trust-focused, consumer-centric retailers (Leaders) and process-focused, tactical retailers (Laggards) have very different approaches to privacy. Leaders think of privacy as an important part of their corporate makeup. They regularly have discussions about privacy, so they can keep improving their policies and practices. Leaders embed privacy focus within every level of the organization, starting at the C-suite, and put the consumer at the center of the conversation. When defining and reviewing policies, they think about the customer's point of view—the services they













receive and the experiences they have—and keep the consumer in mind when deciding how and when to use data. Leaders also demonstrate high levels of transparency with their customers, communicating regularly with customers to inform them what their rights are when it comes to their personal data and the type of information collected.

Laggards, on the other hand, tend to approach privacy as a legal necessity. They use contracts and notices to introduce policies and publish a minimum of support

documentation. They are more focused on their internal operations and make their decisions about privacy based largely on how policies will impact their own security and business operations to reduce legal or regulatory risk.

While Leaders far outpace Laggards, there is still an opportunity for improvement. Even Leaders face challenges across all four areas and may be more mature in some areas but lacking in others (see figure 8)²²

Figure 8. Comparison of leaders and laggards across our key areas

	Laggards Process-focused and tactical	Adopters Testers and aspirers	Leaders Trust-focused and consumer-centric	Leaders vs. laggards
 Consumer centricity				
Purpose of consumer data collection optimally defined	<div><div></div></div> 5%	<div><div></div></div> 18%	<div><div></div></div> 38%	7.6x 
Usage of consumer data collected optimally defined	<div><div></div></div> 0%	<div><div></div></div> 15%	<div><div></div></div> 39%	39.0x 
 Strategic alignment				
Optimized privacy governance structure	<div><div></div></div> 7%	<div><div></div></div> 18%	<div><div></div></div> 39%	5.6x 
Optimal integration of privacy with corporate or business unit strategy planning	<div><div></div></div> 4%	<div><div></div></div> 20%	<div><div></div></div> 42%	10.5x 
 Data management				
Data retrieval made easy to get a holistic view of our customer	<div><div></div></div> 5%	<div><div></div></div> 30%	<div><div></div></div> 56%	11.2x 
Data structured to limit access on a "need-only" basis	<div><div></div></div> 22%	<div><div></div></div> 38%	<div><div></div></div> 77%	3.5x 
 Security and infrastructure				
Optimized data collection based on "data minimization"	<div><div></div></div> 2%	<div><div></div></div> 18%	<div><div></div></div> 38%	19.0x 
Optimized information security program to prevent violations	<div><div></div></div> 4%	<div><div></div></div> 21%	<div><div></div></div> 45%	11.3x 

Source: Deloitte Retail executive survey on US Consumer Data Privacy Survey (n=201).

A pathway to a new consumer privacy standard

While some retailers have moved the bar on data privacy, there remains a lot of work to do. In examining the differences in approaches, it is time for the retail industry to advocate for a consumer privacy standard that has trust at its core and consumer centricity as its guide.

Future leaders in data privacy should adopt a set of guiding principles that align across the entire organization. No longer can privacy strategies be siloed in one function or one business unit but should be shared and cultivated through a privacy culture promoted from the top to the bottom of the organization.

Consumer centricity: Begin by putting the consumer first and gain their trust. Make it easy for consumers to express and manage their privacy and data preferences, so they feel more engaged in the process. Create a central location for setting all consumer preferences (opt-in/out, permissions, access, etc.). Be transparent about what data your organization is collecting and avoid introducing the “creep factor” with new technologies.

Leading companies outside of retail are beginning this process by creating a single, consumer-accessible location for all their relevant personal data. Individuals can view settings, make changes, download data collected, and even ask to be forgotten. Consumers want to know what is collected, how it’s used and why, and opt out if desired. While increasing consumer control may decrease the amount of consumer data collected, it may likely improve the quality and applicability of the data to the business.

Strategic alignment: Embed privacy as a key element in your organization’s business strategy. This can drive smarter use of consumer data in all parts of the business from digital to marketing to stores and the supply chain. It allows parameters to be set for each area to justify the business case for their use of the data.

Elevate the privacy function to the C-suite, such as chief data officer or chief privacy officer, empowering it as the source of policy and truth for consumer data collection, data ownership, and data usage. Then promulgate privacy policies to all functions to advance privacy alignment and empowerment to all areas of the business.

Data management: Treat consumer data like the valuable asset it is by creating a single source of truth for consumer data. Much as companies employ enterprise resource planning (ERP) systems to integrate and automate back-office functions, building a central consumer data repository can allow retailers to command better control of their data. Not only could this help with meeting new privacy regulations, it would provide a real 360-degree view of the consumer. Patchwork integrations and abstracted layers between customer data sources are challenged in providing a holistic view of the consumer. Many times, the data lineage or provenance is not even known, complicating matters more.

Security and infrastructure: To achieve this end, data classification should be embedded into the business at every point, from entry and collection to transfer and usage. By implementing tools to track the flow of data, retailers gain a deeper understanding of the data collected on each consumer and provide policy enforcement mechanisms to automate compliance activities. These capabilities can enhance the ability to build and maintain trust with the consumer.

Finally, secure consumer data through a robust cybersecurity strategy, program, and infrastructure. Remove barriers so data can be protected everywhere—in the cloud, in the organization, or anywhere else it might be used. But be careful not to address cybersecurity purely from a technology perspective. Yet another cybersecurity tool is not the only answer, and many organizations are suffering tool fatigue given the rapid increase of cybersecurity concerns and challenges over recent years. Automation is great, but security starts and stops with each employee. The retailer's employees are its first line of defense—the

human firewall—and the most effective retailers are ones that regularly train their employees on how to handle and protect consumer data. Make privacy a central part of every design element, including cybersecurity practices, wherever data is used in the business (aka privacy by design).

First and foremost, building a strong privacy strategy can help gain the trust of the consumer. But how does your organization move forward? We have outlined a few starting points to assist on the pathway to achieving better privacy capabilities and outcomes for your organization.

Internally, always focus on the consumer experience, but with data privacy in mind. Act now and formulate or promote a data champion function to the forefront, elevating data to the valuable asset it is and embrace privacy-by-design principles.

From an external perspective, be at the head of impending privacy legislation by working with leading retail trade associations to lead standards development. And always be transparent with both consumers and regulators about the sources and uses of the data collected.

Today's retailers are performing a delicate balancing act with data. While preparing for upcoming privacy regulations, they're also having to address the fact that consumers want more control over their data. This forces retailers to be both data-smart and privacy-aware. To do this successfully, retailers are making privacy a strategic imperative and they're actively working to build trust with consumers.

The retailers who lead in this area are changing how they view data. They're seeing it as a way to drive growth, and they're conducting business in a way that makes privacy a central part of consumer interactions. They're creating more meaningful data, enhancing consumer engagement, and reducing exposure to risk—all while staying ahead of concerns about how data is used and protected. Many retailers will be able to achieve a positive privacy return-on-investment (ROI) with better, more relevant, and more actionable data. Moving to a new privacy industry standard is just the start; transparency with consumers about what you collect and how you use it can go a long way in developing trust.

Figure 9. Actions to support a new industry standard



2019 Deloitte United States retail executive survey on consumer privacy

To obtain a view of how retail organizations are addressing privacy-related issues, Deloitte surveyed 201 retail industry C-level executives, senior management, and senior directors in various retail organizations from US-based companies during the months of April and May 2019. All respondents were required to have direct relationship (such as decision-making, policy implementation or roles being directly affected by the policy) with their company's privacy initiatives. The respondents represent more than 10 retail sub-sectors to ensure diversity of business and types of consumer relationships.

2019 Deloitte United States consumer survey on personal data and privacy

To better understand the prevailing trends and opinions related to personal data and consumer privacy, Deloitte surveyed 2,000 individuals in a nationally representative sample, reflective of the United States population. This survey was conducted online using an independent research panel between April and May 2019. The survey has a margin of error for the entire sample of plus or minus three percentage points.



For additional results from Deloitte's retail privacy surveys and more recommendations on how to become a leader in consumer privacy, visit www.deloitte.com/us/consumer-privacy.

Endnotes

1. Identity Theft Resource Center (via Statista.com - Cybercrime: number of breaches and records exposed 2005–2018)
2. 2019 Deloitte US Consumer Survey on personal data and privacy (n=2,000)
3. Ibid.
4. Deloitte analysis of privacy breaches, news coverage, consent forms and 2019 Deloitte US Consumer Survey on personal data and privacy (n=2,000)
5. Ibid.
6. Ibid.
7. Ibid.
8. Ibid.
9. Deloitte analysis of legislations related to consumer privacy passed or enacted in 50 U.S. states as of July 2019
10. Deloitte analysis of violation fines under the California Consumer Privacy Act (CCPA) assuming a retailer with 5% population share in California. Likely impact costs as percentage of revenue and EBITDA are calculated for a US retailer with annual sales of \$10 billion.
11. APQC Benchmarking study - Total cost to perform the process group - Develop and implement security, privacy, and data protection controls. (2017)
12. IDC - 'The Digitization of the World – From Edge to Core' (November 2018) – Global Datasphere size and estimated growth
13. 2019 Deloitte US Consumer Survey on personal data and privacy (n=2,000)
14. Ibid.
15. 2019 Deloitte US Retail Executive Survey on consumer privacy (n=201) among industry C-level and senior business executives during April-May 2019. All respondents were required to have direct relationship (such as decision-making, policy implementation or roles being directly affected by the policy) with their company's privacy initiatives.
16. Ibid.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid.
21. Using 2019 Deloitte US Retail Executive Survey on consumer privacy, cluster analysis was done to identify the attributes differentiating retailers and identified three distinct segments: 'Leaders', 'Adopters', 'Laggards'. These groups exhibit statistically significant differences in their approach and performance around privacy-related activities.
22. 2019 Deloitte US Retail Executive Survey on consumer privacy (n=201) among industry C-level and senior business executives during April-May 2019. All respondents were required to have direct relationship (such as decision-making, policy implementation or roles being directly affected by the policy) with their company's privacy initiatives.

Authors

Rod Sides

Principal
Deloitte LLP
rsides@deloitte.com
+1.704.887.1505

Matt Marsh

Partner
Deloitte & Touche LLP
mamarsh@deloitte.com
+1.612.397.4575

Contributors

The authors would like to thank **Steve Rogers**, **Bryan Furman**, and **Lupine Skelly** of Deloitte Services LP and **Rama Krishna V. Sangadi** and **Arun Tom** of Deloitte SVCS India Pvt L for their contributions to this article.

Rob Goldberg

Principal
Deloitte & Touche LLP
robgoldberg@deloitte.com
+1.813.619.4680

Michael Mangold

Senior Manager
Deloitte & Touche LLP
mmangold@deloitte.com
+1.612.659.2795



Deloitte Insights Consumer Industry Center (the "Center") provides a forum for innovation, thought leadership, groundbreaking research, and industry collaboration to help companies solve the most complex industry challenges.

About the Center

Technology is changing at a rapid pace, and so are consumers. How will these changes impact the way our clients do business in the future? Deloitte Insights Consumer Industry Center (the Center) provides premier insights based on primary research on the most prevalent issues facing the Consumer industry to help our clients run effectively and achieve superior business results.

The Center is your trusted source for information on leading trends and research that connect insights, issues, and solutions for Deloitte's four Consumer sectors: Automotive, Consumer Products, Retail, Wholesale & Distribution and Transportation, Hospitality and Services.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States, and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.