McKinsey & Company

Marketing & Sales

Consumer-data privacy and personalization at scale: How leading retailers and consumer brands can strategize for both

Customer concerns about the security and privacy of their online data can impede personalized marketing at scale. Best-practice companies are building protections into their digital properties.

by Julien Boudet, Jess Huang, Kathryn Rathje, and Marc Sorel

November 2019

Personalization at scale is where retailers and consumer brands are competing to win. But in focusing on "playing offense" to capture value, executives are often overlooking their "defense": preserving, protecting, enabling, and accelerating the hard-won gains of their digital efforts by ensuring that personalization at scale keeps personal data secure and private.

As the enterprise risk of collecting, holding, and using consumer data to personalize offerings grows, so do the business-impairing consequences for those who fail to get it right. Despite these challenges and opportunities, most marketing leaders remain surprisingly unconcerned with how to manage data security and privacy.

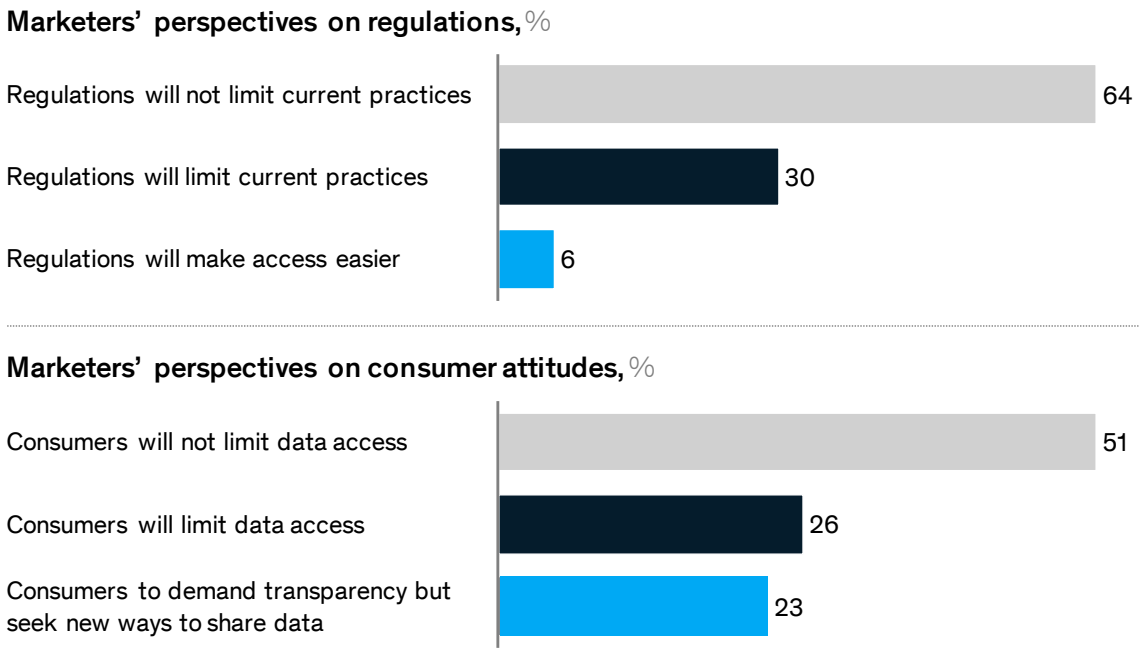
In a recent McKinsey survey of senior marketing leaders, 64 percent said they don't think regulations will limit current practices, and 51 percent said they don't think consumers will limit access to their data (Exhibit 1)—this despite other recent surveys showing that more than 90 percent of consumers are concerned about their online privacy, and nearly 50 percent have limited their online activity because of privacy concerns.[1]

Getting the security and privacy of personalization wrong can slow time to market for new applications, constrain remarketing and consumer-data collection, result in significant fines, or—worse—cause material harm to brand reputation through negative consumer experience. Getting it right reduces time to market, puts security and privacy at the heart of the company's value proposition, boosts customer-satisfaction scores, and materially reduces the likelihood of regulatory fines.

[1] Brian Byer, "Internet users worry about online privacy but feel powerless to do much about it," *Entrepreneur*, June 20, 2018, entrepreneur.com; and Rafi Goldberg, "Lack of trust in internet privacy and security may deter economic and other online activities," National Telecommunications

Exhibit 1

Many marketers feel confident that neither regulations nor consumer sentiment will limit data collection in the future.



Source: 2018 senior management personalization survey: Based on question 27: How do you expect regulations to affect personalization practices in your industry? And question 28: How do you expect customer behavior regarding data collection to evolve over the next six years?

Where to start

For most companies, getting security and privacy right begins with remediating and transforming the digital-marketing applications and systems that generate, transmit, consume, store, or dispose of consumer data (Exhibit 2). Leading brands make this part of a broader baseline assessment of data security and privacy across people, processes, and technology and tie it to business use cases.

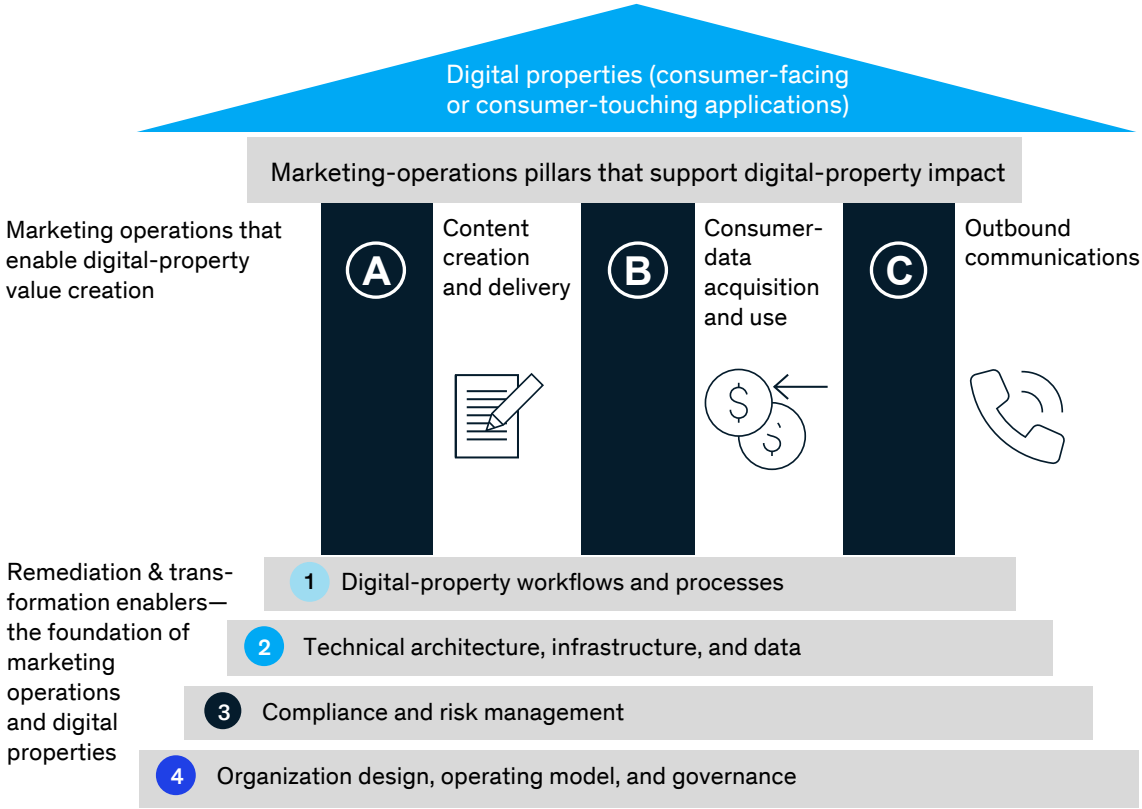
They also put marketing at the center of the effort, educating teams on the value at stake through, for example:

— establishing and enforcing standards on security and privacy for creative agencies

— using best practices for data protection in their day-to day-work

Exhibit 2

The marketing structure should enable digital-property remediation and transformation.



Descriptions (not exhaustive):

Ⓐ
a) **Content development** for consumer-facing brand websites
b) **Content delivery through e-commerce and merchandising** portraying products and brands in a way that allows the enterprise to "do business" with its customers

Ⓑ
a) **Cookie management** to granularly track and collect consumer-behavior data across properties as customers engage with them
b) **Remarketing** by using data to drive portrayal and placement of products and brands with which the consumer engages

Ⓒ
a) **Using consumer data from digital properties and other sources to drive outbound marketing** (such as pay-per-click, advertising, digital display)

1 Where and how digital assets/properties should be created and maintained

2 Technical capabilities, such as data lake or discovery scan tools, to facilitate collection, storage, management, and testing of consumer data

3 The global vs local policies, processes, and tools to adopt, follow, and validate to meet security-and-privacy obligations in a variety of regulatory environments

4 Agile organization and operating model that clarifies roles and responsibilities across functions and rationalizes external partners/agencies

— tokenizing consumer data

— ensuring consent compliance

— sanitizing data before using them in outbound communications and remarketing

— being accountable for incidents when they occur

The dialogue with marketing and other stakeholders in this context should be ongoing, to match the enterprise's evolving needs for data and technical capabilities and to capture the value from use cases.

An imperative on security and privacy can help with many things—from eliminating tech debt to breaking down silos—by opening iterative dialogue on data needs and new operational requirements between the business and the security and privacy functions. Aligning on core beliefs and a framework to approach the effort (Exhibit 3) can help the team quickly get the needed conviction and buy-in.

How to move quickly at scale

As the transformation of data management is piloted and scaled, prioritizing a few key actions to improve security and privacy will ensure outcomes that enable rather than disable the business.

Build a risk register for digital properties

Taking a risk-back approach can help the executive team defend its decisions on where and how to allocate spend on security and privacy. Understanding how properties such as information systems and assets map to each other, to the threat landscape, and to the business value chain also clarifies where eliminating risks can enhance enterprise value.

Exhibit 3

Company alignment on the core principles for transforming digital properties will enable personalization at scale.

Manage digital property the way you manage your people. Knowing the identity, performance, and safety of your applications is as important as knowing the identity, performance, and reliability of your people.

Anchor the approach in use cases. For a successful transformation, understand which business use cases the transformed digital properties will support, and clarify the architectural gaps you need to fill to support both properties and use cases.

Create and maintain a risk-based asset inventory. This will help to clarify your enterprise digital-property landscape, as well as compliance issues and business risk, and is an essential tool for prioritizing transformation initiatives.

Align risk with enterprise appetite. A risk-back, minimum viable approach to building security-and-privacy protections into the transformation of digital properties is a commercial imperative for personalization at scale.

Clarify roles, responsibilities, decision rights, and talent requirements across the organization. This is the key to ensuring you can quickly embed the cross-functional capabilities needed to bring new properties to market.

Implement the transformation by deploying cross-functional teams in agile sprints. This will not only mitigate execution risk—a requirement, not an option—but also enable you to capture value at scale and demonstrate that the process is iterative.

Clarify data strategy, governance, and policies, and build in the roles and requirements to make them work

The details of programs for data security and privacy may vary by company, industry, or the local regulatory climate. Consumer and retail enterprises, for example, often hold consumer data for no more than 13 months, in order to track consumer patterns through seasons and holidays. Auto retailers, on the other hand, often hold data longer, to reflect the longer time between automotive purchases, which tend to be multiyear, not annual. Other companies may tailor their global privacy policy to meet local regulatory requirements, such as General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA).

But some best practices are emerging as enterprises focus on data privacy and security. One leading privacy policy is the tokenization and sanitization of data before using them in remarketing. Further, leading institutions will align on the "minimum viable data and controls" required to preserve a long-term view of consumers and empathetically engage them at scale.

To embed awareness of security and privacy across an enterprise, some companies find it useful to create roles for business-information security and privacy officers (BISPOs) or "security and privacy ambassadors." Such programs can not only empower employee teams to become knowledgeable about organization practices on security and privacy but also ensure that the integrity of digital properties continues long after they are transformed and remediated.

In the event of a breach of data security or privacy, it is helpful to have in place incident-response plans that are "living documents" formed through the test-and-learn iterative process of simulation. These can help executive teams make better decisions faster about managing their digital properties—and their relationships with regulators.

Build security and privacy into enterprise analytics and application development

Consider the example of an enterprise seeking to transform itself into a platform company using consumer and customer data to cocreate application programming interfaces (APIs) to transform how consumers engaged with the brand. Before the enterprise built security requirements into its application development, it had missed at least one major market opportunity because of regulators' security concerns, frequently experienced application launch delays because of security-related rework requirements, and lacked capacity to verify whether around 80 percent of the business-support applications it developed annually complied with its requirements on security and privacy.

By building those requirements into its software-development policies, the enterprise made the software-developer team responsible for meeting them right from the start, in the design phase. The security-and-privacy team would only involve itself "by exception," if a development team declined to meet a specified requirement. This approach ensured that standards on security and privacy were met in more than 90 percent of applications developed, which reduced downstream rework, accelerated time to market, and put data protection at the center of the enterprise's value proposition to consumers.

Create and deliver role-based training on security and privacy

Given that more than 80 percent of enterprise cybersecurity incidents begin with a human clicking on malware, regular training tailored to key roles is essential to reduce the risks of personalization. Marketing teams, for example, might need to learn best practices for remarketing, such as parsing data to eliminate personal identifiability while preserving business value.

There are about 15 core employee behaviors that can be addressed and transformed through a focused campaign of annual training supported by unpredictable reminders, such as occasional emails and text messages or antiphishing test campaigns. Similarly, building security and privacy standards into performance reviews—for example, setting a

threshold for the number of security or privacy incidents in a line of business over a period of time—can ensure that the entire business, not just the experts on security and privacy, owns the problem and the solution.

Personalize security and privacy for the consumer

Leading financial institutions have already unlocked the value of increasing net promoter scores (NPS) by taking the hassle out of consumer validation processes. By reducing hold times, simplifying and tailoring multifactor authentication to meet consumer preferences, and placing data-protection controls for consumer-facing applications in the hands of the consumer, they are improving customer experience without compromising underlying security and privacy.

Leading retailers and consumer brands can adopt a product-management mind-set and delight consumers by building data-protection options into consumer-facing applications and support functions. By partnering with cutting-edge technology innovators, they can tailor processes to what is most convenient for the consumer. Good places to start are multifactor authentication by text, call, or randomly generated code, or built-in strong-password-generating tools to simplify password recall for consumers accessing a retailer's direct-to-consumer application. Measuring performance over time through commonly available customer-experience dashboards such as NPS can ensure that attempts to build security and privacy into consumer-facing applications are refined quickly and iteratively.

The opportunity around personalization at scale for consumer brands and retailers has never been more critical to capture. At the same time, the need to create a net positive consumer experience while avoiding the downsides of reputational, operational, legal, and financial risks is a hard balance to strike. Several core questions can help clarify where your enterprise stands—and what to do about it:

1. How does your personalization technology measure your customer's security and privacy experience?
2. What is your enterprise's critical-asset or -system risk register for data security and privacy?
3. How complete is your security-and-privacy technology stack, and how do you determine this?
4. How are you managing your data to derive value-creating analytic insight from personalization without causing value-destroying financial or operational loss due to privacy or security incidents?
5. What is the state of your secure software-development life cycle program?
6. How are you ensuring the secure operation of your cloud environment?
7. How are you ensuring that security and privacy are every employee's responsibility?
8. What is your capability aspiration for customer-data security and privacy, how are you measuring progress toward that aspiration, and how are you reporting progress to the board?

By answering these questions, companies can help ensure that personalization at scale is only a benefit, not a bane, to any consumer and brand.

Julien Boudet is a partner in McKinsey's Southern California office, **Jess Huang** is a partner in the Silicon Valley office, **Kathryn Rathje** is an associate partner in the San Francisco office, and **Marc Sorel** is a consultant in the Washington, DC, office.