Grant Thornton

Increasing trust through consumer-centric privacy practices

Meaningful privacy practices can help organizations engage consumers by enabling consumer-centric practices across the front and back offices. This article examines the varying stages of privacy program maturity and introduces a consumer-centric privacy model. In today's increasingly regulated digital world, organizations can empower consumers to manage their preferences with the organization. This article is designed to help organizational leadership, chief privacy officers, chief marketing officers and strategists take the first steps to enhancing their services in a privacy-first way.

In today's world, data is paramount in driving business growth. Analytics are leveraged heavily across industry to generate insights on consumers' behavior and spending in order to conduct targeted marketing to drive profit and growth. Handling and processing personal data has inherent privacy risks, and individuals are increasingly concerned with how organizations use and/or share their data. This, in turn, is causing organizations to reassess their data practices and ensure they are acting as good stewards of consumer data.

In addition to increased consumer attention, organizations have to contend with heightened privacy regulations. Increasingly, consumers' rights around how their personal information is used and shared have been granted as part of national and regional privacy laws — expanding consumers' power around consent to share or sell data to third parties, consent to marketing activities, or consent to certain types of processing. When the intake and management of consumers' consent choices lack central coordination, automation, and proactive thinking, the result can be frustrating for both consumers and organizations.

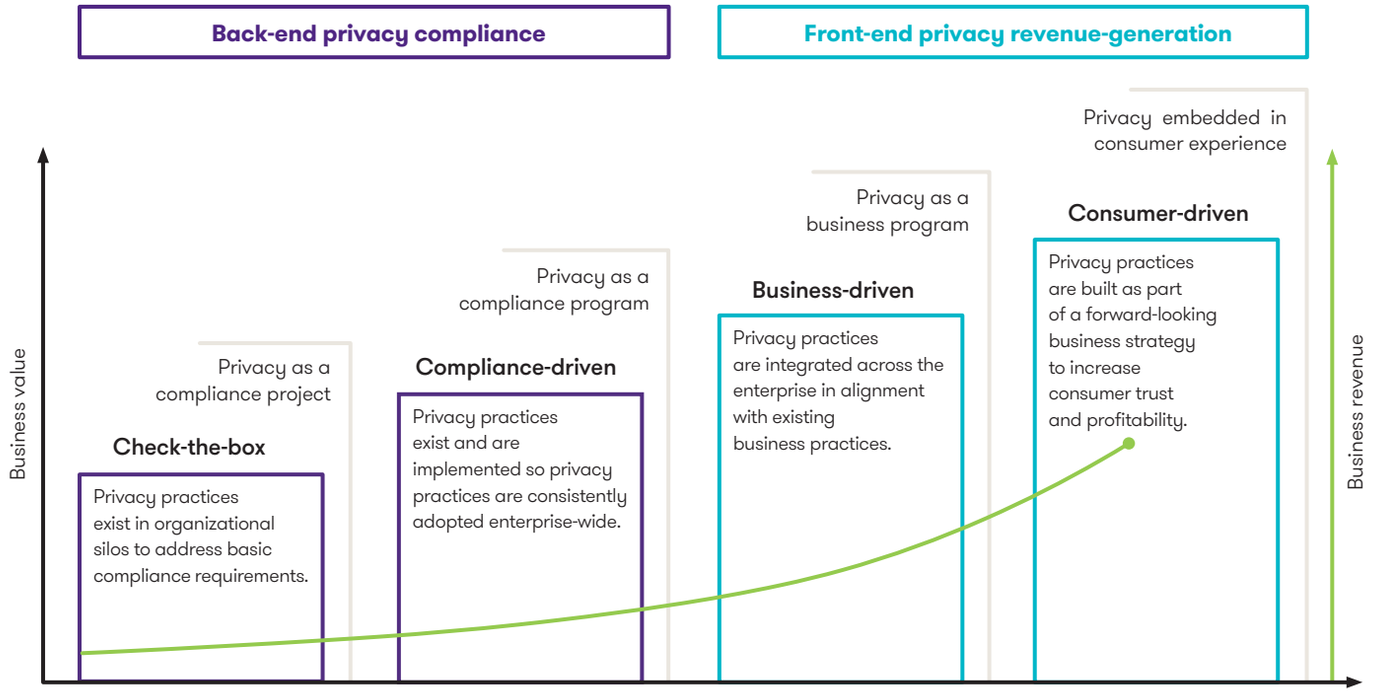
Businesses need to engage with consumers on a more personal level. Harnessing insights on consumer behavior and targeted outreach to deliver personalized content and advertising based upon traceable consumer signals are common practices in today's world. In the face of such regulation, organizations that rely on such data are challenged to find a way to connect with consumers while balancing privacy interests.

How do organizations bridge the gap? By embracing privacy and creating a positive consumer experience. This means giving consumers more control over their data in a balanced way. Enhancing consumer-managed communication preferences, including their consent, is a key to unlocking a streamlined consumer experience with embedded transparency and choice.

Privacy-enabled consumer-centric maturity model

The **privacy-enabled consumer-centric maturity model** demonstrates the evolution from a check-the-box, project-based compliance approach to managing privacy through a transformational, consumer-driven program where privacy is part of the brand strategy to increase consumer trust and profitability. The intent is to move privacy from a back-office compliance function to a front office consumer experience.

Grant Thornton's consumer-centric maturity model



Privacy is still a novel function for many organizations, and adapting to a complex regulatory environment can be challenging — especially for organizations that do not operate in regulated industries. The consumer-centric privacy maturity model helps organizations shift their mindset from merely addressing compliance to focusing on the consumer. Within this model, the consumer is the driver behind a maturing privacy program, allowing organizations to demonstrate that consumers' interests and consideration of their privacy rights are core parts of the business strategy.

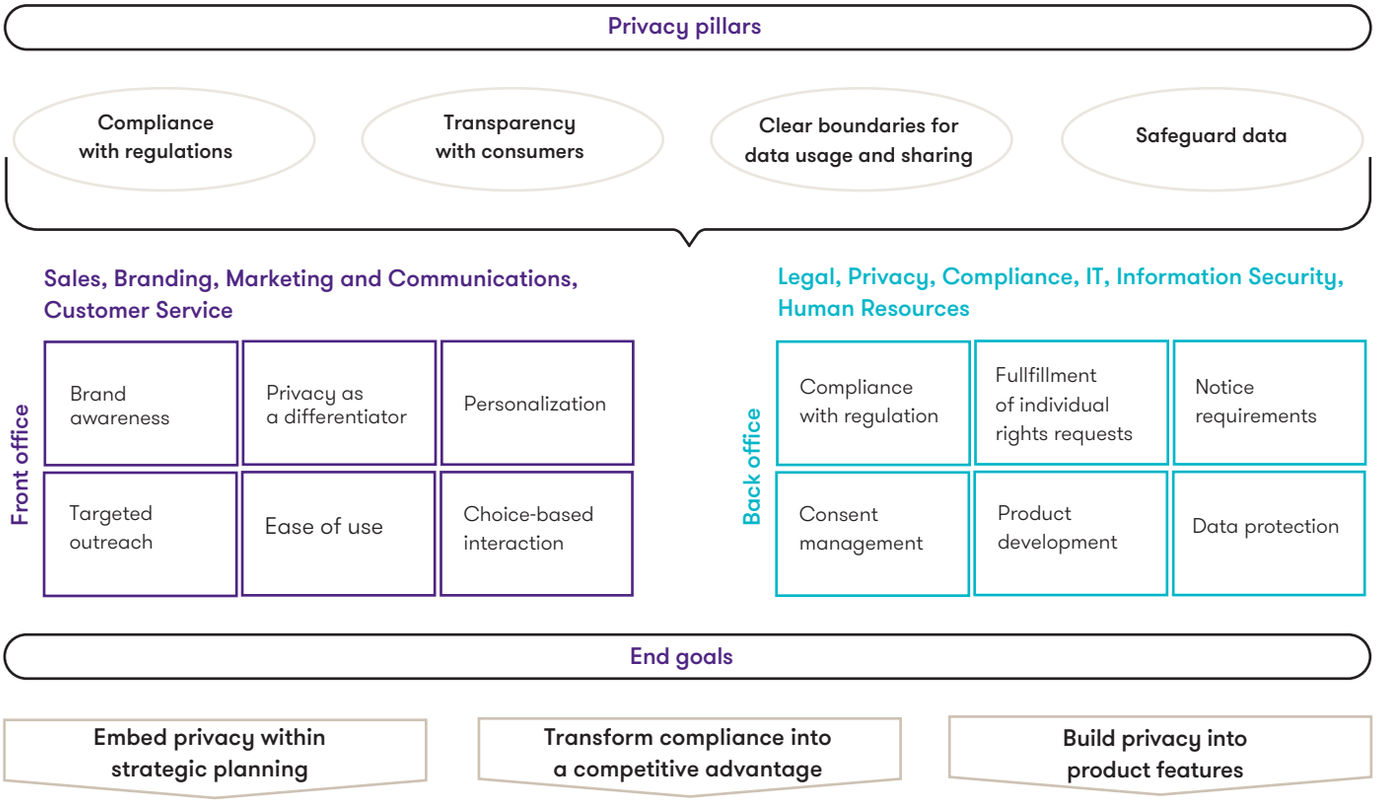
This is no easy task, but there are discrete steps that can be taken in order to meet this objective. Programmatic and enterprise activities — alongside leadership engagement and support — guide organizations to embed privacy into the consumer experience in order to create consumer-centric outcomes.

Moving toward a consumer-centric approach

Moving toward a consumer-centric approach requires cross-functional collaboration to successfully focus a privacy program on the consumer. This includes regulatory considerations as well as strategic considerations related to brand and organizational goals.

The **consumer-centric privacy framework** illustrates the foundational components of any privacy program: compliance with regulations, transparency with consumers, clear boundaries for data usage and data sharing, and safeguarding data. The shift from a compliance-based program to a consumer-based program is depicted through embedding privacy within the front office function. The end goal is to help organizations increase their privacy program maturity by embedding privacy within strategic planning, transforming privacy compliance into a competitive advantage and building privacy into product features.

Consumer-centric privacy framework



For organizations shifting to a consumer-driven approach, integrating privacy into the consumer experience starts with evaluating the consumer life cycle and identifying opportunities. Typically, privacy is seen as a back-office function, supported largely by legal and compliance departments in collaboration with IT and information security. To consider the consumer experience, this collaboration must expand to sales and marketing teams, product owners, and senior leaders who are focused on strategy and brand. As organizations address each of the four pillars of the framework, this cross-functional collaboration becomes paramount.

Most organizations begin their privacy compliance journey by addressing top priority privacy risks to support regulatory compliance. This requires organizations to undertake a number of activities to better understand how they are handling personal data: data discovery and inventorying, providing notice to consumers, establishing methods to appropriately track consent, and reviewing legal controls in place for sharing and transferring of personal data. Even as organizations shift from a check-the-box approach to a consumer-driven approach, these activities continue to serve as the foundation for privacy throughout the organization.

As organizations engage their consumers and take their compliance efforts a step further, they need to integrate privacy into their product, service and technology roadmap designs to set clear boundaries for data use and data protection. By establishing privacy as a key priority in the early stages of product development, organizations can demonstrate their respect for consumer privacy at the functional level, with features such as mobile application push notifications requesting permissions to collect personal data, toggle features to easily manage consent preferences and privacy FAQs made available as part of a sign-up process.

In order to move away from the reactive and rule-set approach, organizations also need to evaluate where, within the consumer experience life cycle, privacy can become a driver, and, subsequently, where choice and preference can be feasibly implemented. The privacy-centric culture organizationally embeds the importance of consumer privacy, including implications for organizational structure and incentives design.

From the back office:

- Privacy stakeholders must collaborate with sales, marketing and leadership to embed privacy into the brand and consider other cultural drivers to enable trust with the consumer. They should continue their conventional collaborations with compliance, IT and information security to ensure the commitments being made to consumers hold true.
- Legal or privacy teams must provide guidance to support the stakeholders who are most directly dealing with personal information. Product and services development must embed choice and preference into their programs and deliver products that allow for consumer choice, requiring back-end configurations of marketing platforms, re-engineering of the marketing campaign processes, or consent management solution implementation.

From the front office:

- Marketing and communications teams must integrate core privacy principles into their activities to ensure that outreach from the web and through social channels are clearly stated, and ultimately available for consumers to scale up or down depending on their choices.
- Sales channels must tailor interactions and initiatives based on the preferences communicated with increased insight into appetite for outreach and personalization. By doing so, organizations can build trust in the relationship by serving relevant content and creating opportunities for consumers to influence how they prefer to engage.
- Customer service teams, who ultimately have the most direct contact with the consumer base, must support consumers in managing their own preferences and triage complaints or issues that may arise.

Create value through increased transparency with consumers

As organizations pivot to a consumer-focused approach, increased weight on the second pillar of providing transparency to consumers is critical. Meaningful communication, action and choice are improvements over merely giving notice, which is often lengthy and difficult to follow due to heavy legal content. Both front office and back-office support is needed to enable consumers to become more empowered and can ultimately increase trust in the organization.

Transparency and data usage shift into a consumer-managed function, to streamline the user experience and provide ongoing choice. Safeguarding the data is the backbone of any program, and should be embedded throughout the life cycle of all product, service and process development.

Within a consumer-driven maturity model, the brand itself ties in privacy as a differentiator within the market. This includes factors such as establishing consumer-facing portals that enable consumers to manage and control privacy settings, and developing self-service engagement in a scalable fashion. Additionally, promoting the consumer's awareness of privacy has a direct impact on the brand itself. Internally prioritizing consumer privacy allows organizations to promote brand trustworthiness externally through the offering of controls that embody transparency and consumer control.

Enabling consumer control

The future of communication preference management is the enablement of consumer control of how personal data should be used or shared, centered on transparency with the consumer. While consumers are interested in a level of personalized targeting, they also want their privacy to be respected. Enabling consumer control allows organizations to embed basic principles of privacy into the business that strengthens the consumer relationship with the organization and enhances the organization brand.

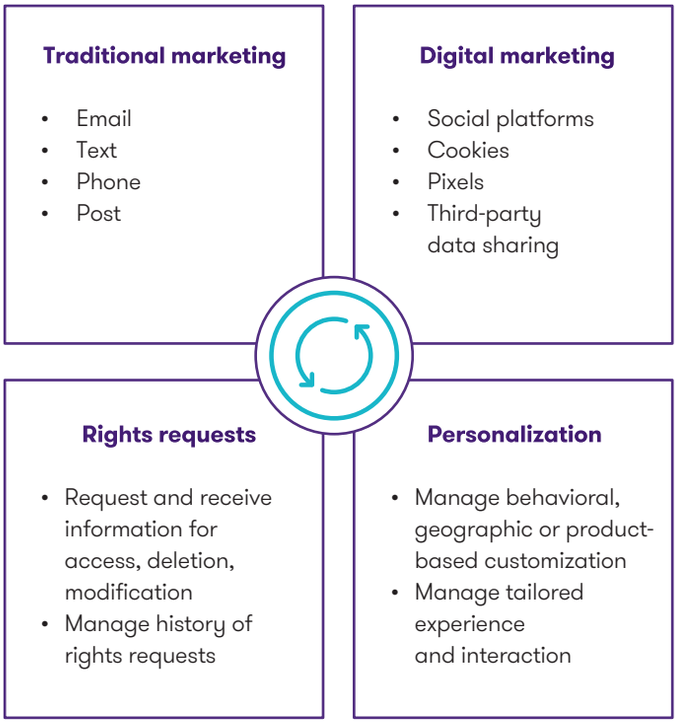
Privacy regulations set the rules behind the collection and processes of personal information. In Europe, the General Data Protection Regulation defines five attributes of legal consent: unambiguous, explicit, informed, freely given and recorded. In the Americas, laws such as the Telephone Consumer Protection Act, the California Consumer Privacy Act, and the Personal Information Protection and Electronic Documents Act, state that individuals should be given clear information on what an organization is doing with their information prior to providing consent. Similarly, the Australian Privacy Principles, which amends the Australian Privacy Act, establishes that consent must be informed, voluntarily given, current and specific, and individuals must have the capacity to provide consent. Consent in all circumstances must be revocable.

Certain organizations are already beginning to weave privacy requirements into their marketing strategies. In direct response to heightened privacy awareness and consumer interests, organizations such as Google, Apple, and Mozilla have already or are planning on phasing out the use of third-party cookies. A Google blog post announcing the phaseout explains, "Users are demanding greater privacy — including transparency, choice and control over how their data is used — and it's clear the web ecosystem needs to evolve to meet these increasing demands." These organizations are being proactive in phasing out ambiguous practices in light of regulations.

There is benefit in balancing privacy interests with the desires of consumers to receive targeted messaging on products or content that is of interest to them. Organizations that wish to strengthen relationships with consumers should drive transparency and enable consumers to exercise choice in a meaningful way to better engage with the organization. This provides the organization with meaningful insight into the consumer base and allows for further personalization of services, targeted campaigns and content strategies.

Personalization, defined as the practice of using data to deliver brand messages targeted to an individual prospect, is often viewed as counter to a privacy-enabled program; however, this does not need to be the case. There can be a balance between personalization and privacy where adhering to privacy regulations simultaneously creates opportunities to drive profitability by integrating consumer privacy preferences into personalized experiences. Embedded privacy through opt-in and opt-out choices for consumers allows a transparent and consumer-led engagement with an organization, helping the organization understand how consumers think and feel, and how this affects behavior. Additionally, this fuels creation of tailored experiences that align with consumer interaction points. Maturation of organizational capabilities enables personalized experiences and evolves as consumer expectations change over time.

One-stop shop for managing preferences



Going further, provide consumers with a self-service, one-stop shop for all their preferences that supports a representative range of preference management, from communication and personalization preferences to individual rights requests. Consumers gain immediate insight and control over their own information and the way the organization will engage; organizations can integrate with existing systems to centralize consumer communication preferences and reduce blanket opt-ins.

A consumer-managed preference center or portal allows consumers to have and endorse meaningful interactions with organizations by increasing transparency, streamlining ease of use, and enabling consumers to have a choice when it comes to the types of personalization and use of their information. Enabling a self-service model allows consumers easy access to their privacy settings and increased ability to customize how they interact with an organization. Identifying opportunities to provide and revoke consent can be made available through simplified and user-friendly mechanisms. In appropriately managing the collection of a user's preferences, organizations are better suited to sustain compliance with existing and emerging privacy regulations. This not only improves privacy posture, but allows for more thoughtful engagement with the consumer base.

In practice: A case study on consent management in retail

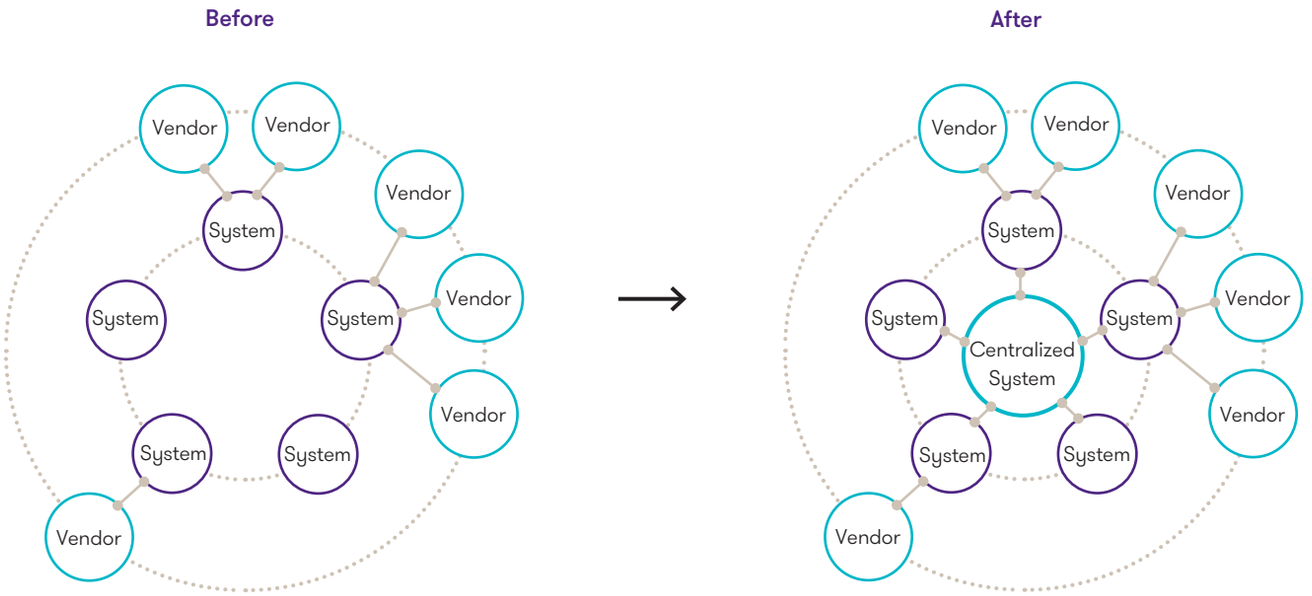
A United States retail organization engaged with consumers through multiple channels to provide marketing and personalization, and fulfill privacy rights requests under data privacy laws. The organization's goal was to take its disjointed consumer engagement and compliance approach and turn it into a consumer-driven enterprise initiative — meaning, they sought to simplify the user experience to empower consumers to manage their preferences and consent in a centralized self-service model.

This goal required both front office and back-office collaboration to create a consumer-centric privacy model. The organization developed a user portal with an intuitive and easy-to-manage preference center, inclusive of communication preference, individual rights and tailored personalization.

A new landing page to manage preferences was created for consumers with an account. For consumers who did not have an account, they could either set up an account or allow the account to be managed on their behalf by the organization. Upon request, consumers could either be provided one-time access to the portal or have customer service support them in modifying any and all preferences associated to their profile and account.

On the back end, the organization developed a unified approach to communication preference management. Regardless of method of communication, the organization sought to centrally manage communication preference management across its brands. They designed a centralized system to pull and push communication preferences across systems, where the preferences can be shared and applied consistently across the organization.

Back-office support model for streamlined consumer preferences



Through the establishment of a consumer-facing intake model and a back-end centralization of personal data, the organization was able to enhance its consumer experience and offer consumers control, while demonstrating privacy as a core value of its brand. This paid dividends on the back end as well, as fewer resources were required in the management of inquiries.

A note on privacy automation solutions

The privacy tech industry is booming. There are hundreds of solutions taking shape intending to solve privacy compliance challenges. This includes the privacy management workflow solutions, back-end data discovery technology that crawls systems for personal information, and consent management platforms.

Centralized consent management solutions are emerging, yet are still primitive. Many are largely designed to help manage cookie preferences, with some beginning to identify opportunities to integrate with existing systems to create a centralized consent and preference management function. There is a value in acquiring and configuring a solution to support tailoring consent to reduce blanket opt-ins. Ultimately, a solution like this, as it matures, would allow organizations to offer consumers a means by which to discretely manage their preferences — affording consumers control of their information while also continuing to allow organizations to generate insights based on interests.

These types of technologies typically require a significant level of back-end IT configuration and customization support to integrate with systems and vendor processes to be centralized. Organizations must still design and define the requirements for how the infrastructure would support the integration and coordination to design a centralized back end. Ultimately, such a solution can play a critical role in supporting both front-end user experience and back-end management of communication preferences as time goes on.

In conclusion: Helping your business grow

In the race to compliance, businesses are seeking to establish a quick means to meet the requirements of privacy regulations. As such, businesses often request blanket opt-in and opt-out of communications at the cost of allowing marketers to be able to contact consumers with targeted campaigns. With ambiguity in how to acquire consent, particularly on increasingly complex digital platforms, explicit consent may be a poor-fit solution for enhancing privacy protections for individuals.

There is a need to balance privacy interests with the desires of consumers to receive targeted messaging and content that is of interest to them. This involves elements of choice and transparency, and organizations should drive increased engagement by enabling consumers to exercise choice in a meaningful way. By considering privacy as less of a back-office function and more of a front office feature to be factored into strategic planning, branding, and product development, organizations can respond to increased privacy scrutiny with enhanced consumer transparency and empowerment of consumers to control and manage their own data.

Jump-start the consumer-centric privacy journey

Embed privacy within strategic planning

- Establish global **privacy principles** that go beyond check-the-box compliance
- Review organization values to **embed privacy into culture of organization**
- Embed privacy as part of **digital transformation** initiatives
- Evaluate **end-user expectations** throughout product design

Transform compliance into a competitive advantage

- **Review processing activities** in which there is direct engagement with consumer
- Identify areas where **consent or preferences are collected** to generate insights
- **Centralize management of preferences** to allow for compliant yet efficient consumer engagement
- **Develop self-serve portal** to empower consumers to manage their communications

Build privacy into product features

- **Design privacy-ready product features** to preempt regulatory concerns & exceed customer expectations
- **Integrate & operationalize privacy controls** to drive efficient scale of adherence to privacy requirements
- Drive increased engagement with consumers through **self-managed preference center**

As organizations begin on this transformation, they should consider the maturity of their privacy program, and where they are in their privacy journey. By bringing privacy into the forefront of their business activities, and establishing a repository of identified touchpoints with consumers, organizations have a strong foundation for creating a consumer-centric privacy foundation. This helps elevate transparency with consumers and promote end-user trust. From there, organizations can begin to take steps to refine their data collection ecosystem to be more consumer-centric.

This benefits the organization by increasing reputational trust and providing meaningful insight on consumer preferences in order to further unlock personalization of services and content. As organizations establish themselves as trusted users of personal information, they should consider embedding privacy and trust into their brand as a key tenet and differentiator. Privacy, to this end, becomes a revenue driver rather than inhibitor.

Contacts

Derek Han
Principal,
Cyber Risk Leader
E derek.han@us.gt.com

Chris Smith
Principal,
Strategy and Transformation
E chris.smith@us.gt.com

Ariana Davis
Senior Manager,
Cyber Risk
E ariana.davis@us.gt.com

David Koppy
Senior Manager,
Strategy and Transformation
E david.koppy@us.gt.com

GT.COM