Deloitte.
Digital

From tracking to trust.

Stronger bonds of loyalty and trust begin by giving consumers more control over the data you collect and how it is used.

People want to do business with brands they trust. Eighty-three percent of surveyed consumers said that trustworthiness is the emotional value they most associate with their favorite brands.[1] Globally, trust is the top nonintrinsic factor that consumers consider when making a purchase.[2]

One of the primary keys to trust—in business as in life—is transparency. Unfortunately, many companies have often fallen short of full transparency about the way they collect, use, share, sell and transfer personal data, which can lead to widespread consumer mistrust and new regulations. The impending end of third-party browser cookies, coupled with new privacy regulations such as the European Union's General Data Privacy Regulation[3] (GDPR) and the California Consumer Privacy Act[4] (CCPA), are changing the playing field—making it clear that old ways of consumer data collection, usage, sharing and sale are no longer feasible.

There is a better way—one that can help address the concerns of the people you aim to reach while also lighting your path to growth.

By giving your audiences not only transparency but also full control of the data you collect about them, and by *doing so in ways that align with your brand's values and voice*, you can establish trust with new prospects who—more and more—value personalized brand experiences, while deepening the loyalty and growing the value of existing customers.

The future is first-party data.

It's no secret that the ability to foster better customer experiences (CX) has tangible business value. Already, the companies at the forefront of CX are driving five times better revenue growth compared to CX laggards.[5]

Improved CX isn't just better for brands; consumers themselves welcome personalization—when it's provided appropriately. We found that three out of four surveyed consumers expect brands to know their purchase history with the brand—and be able to call upon that information to provide personalized experiences.[6] Other research indicates that two out of five surveyed consumers are willing to pay up to 20 percent more for an impressive experience.[7]

Providing those personalized, human experiences depends on quality data—particularly first-party data such as email and physical addresses, size and color preferences, website activity and customer service histories, and more. By collecting the relevant data and connecting it across customer touch points you can make better decisions and orchestrate a more coherent omnichannel brand experience.

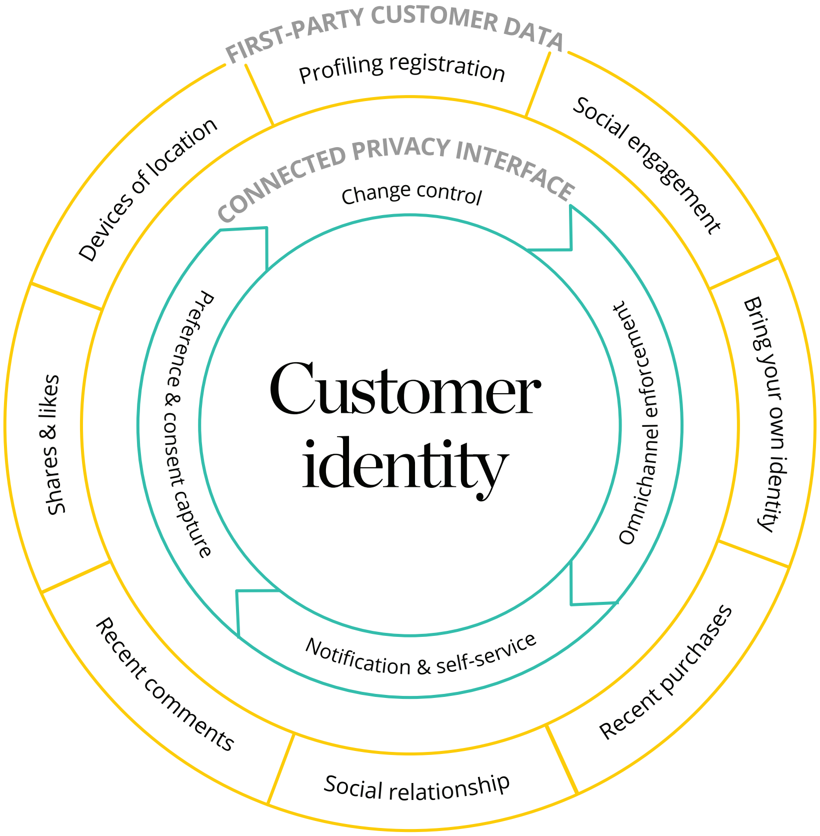
Over the past two decades many brands have also depended on third-party data, including personal information gleaned through the use of third-party browser cookies. These cookies are placed by sites other than the one that the internet user is directly interacting with, typically when an advertisement is displayed on the page but also through the use of invisible tracking pixels and other means. Third-party cookies can track user behavior across the sites where the third-party server places ads or tracking pixels—providing advertisers with information about the consumer's interests, location, browsing history and other activities.

But misuse and overuse of third-party cookies for profiling and tracking have led to backlash from consumers—who increasingly employ ad blocking technologies or clear their browsing histories on a regular basis. Unwanted tracking practices have also been part of the impetus for sweeping consumer privacy measures such as GDPR and CCPA. By 2022, no major web browser will support third-party cookies.[8]

The implicit message is loud and clear: unwelcome tracking, default opt-in, one-size-fits-all treatment, and opaque privacy and data policies and practices are no longer acceptable. That means that brands need to rethink how they go about collecting, storing, using, sharing, and selling first-party customer data if they want to be able to provide the personalized experiences that customers desire.

FACETS OF THE 360-DEGREE CUSTOMER VIEW.

First-party customer data (**outer circle**, below) is an increasingly valuable business asset. By providing your customers with a transparent and simpler notice as well as better preference, consent, and individual rights privacy controls for the data you collect through a connected privacy interface (**inner circle**), you can begin to piece together a full, dynamic picture of each individual customer—putting his or her needs and preferences at the center of everything you know and do.



AN EXAMPLE CONSENT MANAGEMENT CHECKLIST:

- Privacy policy is provided on every webpage that collects personal information.
- Privacy policy explains personal information collection, use, sharing, sale and transfer.
- Privacy policy is updated in the last 12 months and any time there is a change to data processing.
- Privacy policy states that personal information will or will not be shared with unaffiliated third parties.
- Privacy policy states how personal information is protected.
- Consent obtained for third-party information sharing (including sale).
- User provided the ability to revoke consent for information sharing (including sale).
- User allowed to revoke consent for data being sold to third parties.
- Privacy policy explains customers' rights (access, deletion, etc.).
- Preference center provided to manage preferences and consent.
- Consent obtained to save buying preferences.
- Consent obtained for sending marketing emails.
- Consent obtained for marketing alerts for methods other than email.
- Consent obtained to save logistics-related information.
- Preference center provides information regarding third parties that are receiving personal information.
- Privacy policy includes information on how to contact the privacy office.

The next-generation privacy interface.

Today, in response to the requirements of GDPR and CCPA, browser cookie disclosures and controls are a common feature across the web. That's a positive step—but hardly enough to build real trust with customers and prospects and help them feel comfortable sharing more information with you.

We recommend a new approach to data privacy, one that gives the customer fine-grained control and informed consent regarding data collection, usage, sharing, sale and transfer. Such an approach can provide customers control over a range of choices, from toggling preferences for marketing communications, to managing the apps that have access to their data, to connecting (or disconnecting) trusted devices and accounts.

In spirit, this approach is about creating a relationship of openness, collaboration and mutual benefit with each individual customer by revealing what you know (or want to know) about them; how you are using it, sharing it, selling it and moving it; what choices the customer has; and what benefits can be expected.

In practice, this means creating a next-generation privacy center that is easy to find and navigate, is secure, and is valuable to the customer. The particulars of your implementation will vary based on your business, but should generally provide six specific capabilities:

1 Strong and fine-grained preference and consent management

Your privacy interface should allow customers and prospects to digitally consent & manage their preferences and consent in a centralized, easy-to-find privacy hub. It should also break up consent requests so these customers know exactly what they're consenting to, and allow them to consent to certain processing and reject other processing.

2 Transparency of data practices

Throughout the interface you should explain, in plain and clear language, how the customer's data will be used (including sharing with and/or sale to third parties), what controls / security are in place, and what choices they have.

3 Explicit opt-in

Customers should be asked to proactively *choose* to opt in, rather than setting opt-in as the default when collecting consent.

4 Self-service data access

Provide an on-demand method for each customer to access their personal data, and allow each customer to scale their requests depending on what they seek.

5 Easy capabilities to revoke consent as well as to delete data

Consent and opt-in are not a one-time event. Customers should be allowed to revoke consent at multiple points in time. Upon request for data deletion, you should be able to identify and demonstrate the identity of the requestor and execute the deletion request within the legal response time required by local laws.

6 Up-to-date information

As new information is captured or as policies evolve, your interface should support a model for notification about what has changed—and what choices the customer has to block the use, sharing and sale of data related to those changes.

Ask respectfully for the right information at the right time.

When and how first-party personal information is collected can have a dramatic impact on whether customers trust you and choose to opt-in and continue to participate. That's part of the problem with blanket privacy policies: They typically require users to decide *too soon* about *too much*, before the user has even decided whether you're worth getting to know.

It's important to start with the basics—for example, collecting an email address or enabling social login. Then from there, deepen the relationship over time through additional data and consent requests such as personal preferences and email list signup—while you demonstrate that you're putting that data to good use through improvements to their customer experience along the way. Following this pattern you can build a stronger foundation of trust with your customers, while collecting more valuable information.

In order to achieve this goal, data collection and consent management should be viewed through the lens of user experience design and be incorporated into journey mapping in the same way that other content and features are addressed. Users shouldn't have to seek out a page buried in their profile or settings in order to find out what you're going to do with the email address they just gave you. That explanation should instead be provided when you ask for the email address, in a way that flows consistently with the rest of the user experience and echoes your brand voice. *(Please see sidebar, "Privacy as branding.")*

And when you use the customer's data to enhance their experience, you should show how you did so—for example, by explaining that your recommendation of a cool-blue comforter made of bamboo fibers was based on the customer's past purchase of blue drapes and products made of renewable materials, combined with your knowledge that cold weather is forecast in the customer's ZIP code. Doing so helps demonstrate and reinforce the value that you are providing in exchange for the customer's consent.

As part of embracing this new paradigm, it's important to consider the types and quantities of data you collect, given the work it will require to manage the data while remaining in compliance with privacy regulations. Even with clear consent, there is no sense in collecting data about individuals who are not your audience or collecting data that has no value; and now more than ever there is increased risk in doing so. For example, the cost of noncompliance with CCPA could reach as high at $7,500 per record, which adds up when organizations are storing millions of records.

This means that you should focus on data quality over quantity, audience quality over quantity, and experience quality over tracking:

- **Only collect what's meaningful**, knowing that you may be required to disclose that data on an individual basis.
- **Stop collecting data from people who are not your audience**, knowing that you can't provide meaningful experiences for them and they won't contribute to (and may in fact slow) your revenue growth.
- **Focus on providing better content and experiences**, knowing that is ultimately a better way of building engagement and trust than surreptitious tracking.

From customer consent to business value.

Your customers are not email addresses or devices. They are living individuals with different needs, preferences and circumstances. They're willing to share information with you—but only if they know it will provide them with valuable, personalized, more human experiences in return.

By earning their trust through transparent privacy policies and practices, you can begin to collect the data you need in order to provide those experiences. But earning consent is ultimately just the first step. In order to truly understand and serve your customers, you need to connect what you know about them at an individual level, and then feed that information into a predictive decisioning engine to help orchestrate consistent, contextually sensitive omnichannel experiences.

An artificial intelligence-powered customer data platform (CDP) can help set the foundation for success—while also furthering you on the road to a single-source, customer-controlled privacy interface. By allowing you to merge the data you have about your customers across touch points, a customer data platform can help facilitate a more nuanced understanding of each individual customer, while also providing each customer with easier, unified access to data records in the event that they wish to change preferences or consents and access or delete personal data.

With the CDP in place you can then apply business intelligence, analytics and machine learning to personalize and automate the messaging, medium, frequency and cadence that frames your engagement—at business scale, in human terms. As a result, you can provide experiences that reward and further expand customer trust, deepening your relationship along the way.

PRIVACY AS BRANDING.

Marketers have long recognized the importance of engaging leads and customers with a unified, reliable brand voice that reflects the values of the brand. By behaving in familiar and predictable ways, you establish expectations with your audiences; by delivering on those expectations, you can help build trust.

Collecting the right customer data in the right ways is an increasingly important aspect of embodying core brand values. Words like "trust," "customer focus" and "openness" are among the most oft-cited values of companies today.[9] Companies should work to determine that those values apply to their data privacy and consent practices.

Your privacy and consent practices can also provide an opportunity to demonstrate and strengthen consistency of voice across the customer experience. In a basic sense, a transparent approach to data practices allows you to set expectations for how the customer's data will be used—and then execute on those expectations without surprises.

By explaining your practices and policies in the same language and tone you use across other communications, you can make it clear that you view privacy and consent as core elements of the customer experience and relationship rather than as just "fine print."

And when you earn the consent of customers to gather and use their data, you become better able to understand the needs, context, expectations and emotional state of your audiences, and respond in ways that feel human, empathetic and helpful.

Allowing you to become, in a real sense, reliable.

Those companies that are successful in aligning their approach to privacy with their core brand can build meaningful competitive advantage in the emerging trust economy.

Entrust your customer to trust you.

Putting customers and prospects in control of privacy and data represents a significant paradigm shift for some companies.

It means moving from a mindset focused on short-term, quick-hit results toward one focused on the longer customer journey. It means shifting goals and metrics away from *volume* of leads and instead focusing on *quality* of connections.

It means trusting that **customers will trust you if you let them decide**. And if they don't show that trust, the solution still isn't to circumvent their consent ... it is to work harder for their trust.

Here are some questions to consider as you work toward a more sustainable privacy pact with customers.

- What change in culture and metrics will be needed in your marketing organization to make this shift?
- Do you actually know where all your data (structured, unstructured) is in real time?
- Have you catalogued data processing (e.g., use, sharing, sale, transfer, disposal, etc.)?
- Have you leveraged data processing metadata to put policies in place to preclear data for business use (e.g., analytics, marketing, advertising, etc.)?
- What are the layers of preference and consent management that will be needed in order for you to provide the level of individual self-service and control that your customers seek?
- Can your preference, consent and individual rights (access, deletion) controls scale to accommodate demand?
- Do you know which stakeholders within your organization are using what data to drive engagement?
- What are the data-related risks in your organization, given regulatory changes? Are you able to demonstrate that your existing controls account for data everywhere via business and risk reporting?
- How can you better express your brand's values and voice through your privacy and consent policies and tools?

The landscape has changed.
Consumer expectations coupled with new regulations mean it is more important than ever for businesses to develop new ways of building trust while collecting and acting on customer data.

By proactively taking steps to improve your privacy practices, you can comply with regulations, improve customer trust, and fuel the systems that elevate the human experience for customers. The brands that do this well can build stronger bonds of loyalty and trust—and can strengthen their potential to grow customer lifetime value as a result.

GET IN TOUCH

Naresh Persaud
Managing Director
Deloitte and Touche LLP
napersaud@deloitte.com

Dan Frank
Principal
Deloitte and Touche LLP
danfrank@deloitte.com

Linda Walsh
Managing Director
Deloitte and Touche LLP
lwalsh@deloitte.com

Angel Vaccaro
Hux Practice Leader
Principal
Deloitte Consulting LLP
avaccaro@deloitte.com

Sources

1. Deloitte Digital, Exploring the Value of Emotion-Driven Engagement, May 2019, https://www.deloittedigital.com/content/dam/deloittedigital/us/documents/offerings/offerings-20190521-exploring-the-value-of-emotion-driven-engagement-2.pdf.
2. Edelman Intellectual Property and Edelman Intelligence, 2019 Edelman Trust Barometer Special Report: In Brand We Trust?, 2019, p. 9, https://www.edelman.com/sites/g/files/aatuss191/files/2019-07/2019_edelman_trust_barometer_special_report_in_brands_we_trust.pdf.
3. General Data Protection Regulation, enacted May 25, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC.
4. California Consumer Privacy Act of 2018, enacted 2018, effective January 1, 2020, http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=.
5. Gartner, 2019 Customer Experience Management Study: Marketers Take More Control as CX Expectations and Budgets Rise, https://www.gartner.com/en/marketing/research/2019-customer-experience-management-study (registration and download required).
6. Forrester, Transform Customer Processes and Systems To Improve Experiences, April 15, 2019, p. 2,https://www.forrester.com/report/Transform+Customer+Processes+And+Systems+To+Improve+Experiences/-/E-RES72102#.
7. Deloitte Digital, Exploring the Value of Emotion-Driven Engagement, May 2019.
8. Oracle, One Size Doesn't Fit All, July 2019, https://www.oracle.com/corporate/pressrelease/jeanne-bliss-customer-experience-073019.html, p. 7-8.
9. James Archer, "20 Words You Can Drop From Your Core Values Right Now," Inc., January 22, 2014, https://www.inc.com/james-archer/20-words-you-can-drop-from-your-core-values-right-now.html.

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.

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