The Privacy Paradox

Balancing the expectation for hyper-personalized customer experiences in a hyper-regulated digital age

cheetahdigital.com

The Marketer's Conundrum

Any good marketer knows that excelling in the age of the consumer is all about creating tailored brand experiences that speak directly to customers' needs. But while they enjoy the convenience and relevance that these personalized engagements bring, consumers are also quick to withhold their personal data and demand increased privacy online.

This problem becomes even more muddied in the wake of major trust scandals and data breaches that give rise to increasingly strict data protection laws and regulations.

But personal data and targeted marketing go hand-in-hand. So what's a marketer to do?

This is the privacy paradox. Consumers simultaneously expect privacy and tailored brand experiences. Is it possible to deliver on both?

The Privacy Paradox
Marketers are being asked to create hyper-personalized experiences, while following privacy and security rules that are stricter than ever.

The short answer is "yes." With a fresh approach to consumer data, a commitment to security at every level of the organization, and a vigilant, proactive attitude toward risk management, brands can meet their customers' evolving expectations of transparency and control, while still delighting them with personalized experiences powered by data.

In this ebook, we'll explore:

- How consumers and marketers view the “privacy paradox”
- How marketers can enhance personalization by moving beyond third party data
- How privacy regulations are affecting marketing practices, both now and in the future
- How brands can take a proactive approach to privacy and security in an increasingly data-sensitive world

Exploring the **Privacy Paradox**

There's no doubt that consumers are more responsive to marketing that feels personal — targeted content, custom offers, and unique experiences that align with their preferences. But today's marketing runs on data. In order to create these personalized campaigns, marketers need to optimize their collection, storage, and use of consumer data.

At the same time, abuse and mishandling of data are a reality of modern life. Brands, consumers, and government entities all agree that privacy laws and regulations are needed to keep consumer data safe. For marketers, the challenge of meeting consumer expectations while keeping up with changing policies creates more gray area than ever.

The Consumer's Perspective

"I want it all."

Consumers want their personal data protected and used responsibly — or sometimes, not at all. When they volunteer information, they want to know how it's being used, why, and by whom. Understandably, they become concerned when they learn data is being collected and shared without their consent.

Concerns over shadowy data exchanges lead to fears about identity theft and anxieties over backroom decisions that limit social freedom and economic opportunity. Understandably, many consumers react by becoming more protective of their data, and less willing to share it with brands.

Yet today's consumers also expect boutique treatment. They want brands to tailor interactions and services to their needs and preferences. They want to be reminded of what time their flight is or what products they previously purchased. And they want consistent experiences across devices, whether online or in-store.

Consumers want to trust their favorite brands and services — and completely avoid those that don't respect their privacy.

The Marketer's Perspective

"Caught in the middle."

Delivering the quality content and services consumers expect requires getting to know the customer and their habits — the types of activities they enjoy and what behaviors they demonstrate while interacting with the brand (i.e., browsing before buying, response to email campaigns/ads, what days and times they're most likely to purchase, etc.). Creating these uniquely personalized experiences requires the collection (or creation) of ever more specific data points.

So marketers must lean on increasingly sophisticated data collection, management, tracking, profiling, and analytics tools. Their technology options are vast, which can also mean increased data being shared across the marketing value chain. But if done carelessly or unscrupulously, these practices can compromise long-standing industry rules, as well as the new breed of privacy laws and regulations, leading to large fines and loss of brand reputation in the market.

Questions Every Data-Driven Business Should Ask:

- How can I build trust with my customers?
- How can I meet the need for rich data while reducing security and privacy risks?
- How can I ensure genuine and inherent concern for security at every level of the organization?

A New Approach to **Consumer Data**

Marketers traditionally rely on two basic types of data to power their marketing efforts: first-party data and third-party data. The distinction lies in where the data comes from.

First-Party Data

This is data that's collected directly from the customer, typically during interactions like site browsing and sales transactions. It includes things like name, email address, mailing address, browsing habits, product preferences, etc. First-party data is often collected using tracking pixels, cookies, and transactions.

Since it comes directly from the source, first-party data provides valuable insights about how a customer interacts with your brand and how their behaviors change over time. So it's extremely useful for creating unique, personalized experiences. But as we've discussed, consumers are increasingly wary of sharing their data with brands — so first-party data isn't always easy to come by.

Third-Party Data

Third-party data is collected and compiled by outside vendors, and typically purchased or licensed by a brand. It can include any number of personal or anonymized data points, including information on demographics and online activity that can provide inferences about a consumer's interests and preferences.

Third-party data holds some degree of value for marketers, but it carries significant risk. Because it's amassed from a variety of sources, it's impossible to know the origin of a given data point. Information is often outdated or even contradictory — so campaign personalization based on third-party data can lead to a disjointed or even unpleasant customer experience. And since anyone can buy access to third-party data, it doesn't provide any competitive advantage for a brand.

Zero-Party Data

Many marketers may not be familiar with zero-party data — but they should be! Rather than being collected by one means or another, zero-party data is information a consumer voluntarily and intentionally shares with a brand. Unlike first- and third-party data, this means zero-party data can go beyond past behaviors and preferences to offer insights into people's motivations, intentions, and interests. Used in combination with first-party data, zero-party data provides a robust view of both the historical activity and the likely actions of a given consumer.

Zero-party data allows brands to build direct relationships with consumers, and, in turn, better personalize their marketing efforts, offers, and product recommendations. Essentially, zero-party data requires brands to strategically ask consumers for information, rather than relying on observations and inferences.

Zero-party data is a new approach to data strategy, but it provides a unique opportunity to build deeper and more meaningful connections with consumers.

Creating a Value Exchange

Even in today's environment of stricter privacy regulations and consumer mistrust, people are still willing to share their data. But they want control over how their data will be used, and they want to know there's a good reason for giving information to a brand.

In short, they want something of value in exchange for the data they share. This concept of a "value exchange" is the foundation of zero-party data collection.

Interactive experiences that conduct research, accrue opt-ins, and offer benefits for the consumer are the perfect vehicle for collecting zero-party data. Using strategically designed questionnaires, polls, surveys, quizzes, social stories, contests, and sweepstakes, marketers can quickly and easily collect data about consumers' motivations, intentions, interests, and preferences. In exchange for their participation, consumers should receive something of value, like:

- Discounts or coupons
- Personalized offers and recommendations
- Exclusive and/or targeted content
- Free trials
- Early access to new products/features
- Sweepstakes entries

Interactive experiences that conduct research, accrue opt-ins, and offer benefits for the consumer are the perfect vehicle for collecting zero-party data.

Of course, this short-term value exchange is only part of the equation. Zero-party data collected through these interactive experiences can be used to build deeper relationships over time, as well as more personalized future campaigns.

Privacy and personalization can coexist if consumers are entertained, engaged, and receive something in return for their attention and preference data. By leveraging the right mechanics, and offering a value exchange, marketers can receive unique, self-reported insights about what products their customers desire, what they look for in a service, and what motivates them to purchase.

The Basics of **Privacy and Security**

Regardless of how consumer data is collected, marketers have significant — and stringent — responsibilities with regard to privacy and security. Creating a value exchange makes it easier to collect self-reported data — leading to more accurate, useful insights about your customers — but this data is still subject to laws and regulations related to transparency, accuracy, minimization, and privacy control. In order to understand the implications of these laws, it's important to first understand the basics of both privacy and security.

Data Privacy vs. Data Security

Privacy and security are separate but complementary aspects of data protection. A company can have the most secure data systems and procedures in the world. But if the way they use data is questionable, they won't meet the privacy standards that consumers and lawmakers demand.

Conversely, privacy cannot exist without security. Marketers must build their privacy strategy on a strong security program to be successful. Aligning privacy strategies with security ensures a stronger program that can leverage security tools, technologies, and policies in implementing privacy principles.

Data privacy focuses on lawfulness, transparency, proportionality, choice, and control within a data environment. It is often organic and contextual, requiring a thorough understanding of user expectations vs. business needs. This includes:

- **Data inventory:** knowing where all of the personal data resides in the organization
- **Data processing:** knowing why, how, and by whom personal data is used
- **Data mapping:** knowing how all personal data enters and flows through the organization (or third parties)
- **Data security:** knowing how the data is protected in transit and at rest through technical and organizational measures (i.e., through tech, activities, and people)

Data security focuses on confidentiality, integrity, availability, and resilience of data environments. It is often technical and prescriptive, requiring a thorough understanding of system interactions and configurations. This includes:

- **Data encryption:** a security method where information is encoded and appears scrambled or unreadable until a user decrypts it with the correct encryption key
- **Data anonymization, de-identification, and pseudonymization:** the process of removing PII from data sets or reducing the real world identifiability of a user or their device
- **Data tokenization and hashing:** the process of substituting sensitive or plain text data with a non-sensitive or non-reversible equivalent when data should have no extrinsic or exploitable value (tokenization) or when it should have intrinsic value while still having no extrinsic or exploitable value (hashing)
- **Data minimization:** the belief that data processing should only use as much data as is required to successfully accomplish a given task

Understanding Personally Identifiable Information (PII)

Personally identifiable information (PII) is any data that could potentially identify a specific individual. Any data point that can be used to distinguish one person from another or could be used to de-anonymize anonymous data can be considered PII.

In addition to things like demographics, Social Security numbers, and contact information, the definition of PII has been expanded to include unique online identifiers that may be reasonably used to single out an individual across their various devices and engagement contexts.

Depending on how they are used, cookies, hashed email addresses, device and canvas fingerprints, and even statistically derived identifiers can be 'personal' and 'identifiable.' These identifiers can be linked together in complex graphs and associated with a variety of descriptive attributes informing audience segmentation and targeting decisions.

Sensitive data now includes (among others):

- Precise location data
- Browsing history
- Lifestyle choices
- Group affiliations
- Health and ailment data
- Biometric data
- Psychographics

It's Not Just Common Courtesy. **It's the Law.**

In 2018, marketers and data protection professionals alike were abuzz with the news of the enforcement of the General Data Protection Regulation (GDPR). Signed into being in 2016, the GDPR was seen as the advent of wide-ranging global privacy reforms. Respecting individuals' privacy rights and freedoms is central to the GDPR and GDPR-style laws like the California Consumer Privacy Act (CCPA), which will be enacted at the start of 2020.

In the wake of a shifting paradigm and increasing scrutiny, aligning business practices and technologies to higher standards of care is a brand imperative.

Under these regulations, individuals are granted strengthened rights to know how their data is being processed, to gain access to that data, and (under certain circumstances) to request that data to be "forgotten." In turn, regulators are granted additional powers to enforce compliance with individuals' rights requests. Effective rights compliance means that brands must (by law) coordinate requests with any vendor or business partner processing the individual's personal data.

As a result, we are in the midst of a paradigm shift. This new breed of privacy laws are principle-based and technology agnostic — and as evident from recent enforcement actions, size-indifferent. As regulators continue to respond to what they believe are tangible and existential modern threats to privacy, the debate around ethical data practices will only intensify.

GDPR's goal in Year One has been clear: focus on big tech, big data, and big ads to seek out the abuses of the past and correct them for the future. GDPR and similar legislative reforms have undoubtedly raised the bar for security and privacy around the globe, giving more control to individuals and requiring more accountability from businesses. In this way, aligning business practices with GDPR principles paves the way for responsible data management in any modern organization.

Taking Action on Privacy

Not only is prioritizing privacy the right thing to do for ethical businesses, it is also a major differentiator in the competitive marketplace. Amidst regular scandals highlighted in the news, proactively taking action is a way to distinguish oneself in the marketplace — whereas failing to act (or taking the wrong measures) is condemned as archaic and untrustworthy.

Staying vigilant requires regular privacy evaluations and principles like:

Privacy Impact Assessments (PIA)

It's impossible to secure something if no one knows it exists. Thus, regular and opportunistic risk assessments are a necessary part of any privacy toolkit, as new data (or new ways of using it) can carry unexpected risks to both individuals and brands. Organizations that handle large amounts of personal data or sensitive data conduct PIAs to audit their own processes and determine how they might affect or compromise the privacy of the individuals whose data they possess. As new projects or policies arise, a PIA helps:

- Ensure compliance with legal regulations
- Determine the program's risks and effects
- Evaluate ways to mitigate potential privacy risks

GDPR is the first global legislation to explicitly introduce the long-standing best practice of PIAs into a legal framework.

Privacy by Design (or Default)

Privacy by design means infusing concern for privacy at every level of the organization. In addition to conducting regular PIAs as part of sound product development, privacy by design ensures privacy considerations are baked into all product innovation, business, and partnership decisions. When done well, privacy by design is accomplished when privacy mindfulness is part of the organizational culture instead of a mandate that should be reactively adhered to. This requires regular training, awareness, and active participation by security and privacy personnel in data management, as well as every member of the company treating customers' PII as their own.

GDPR is the first global legislation to explicitly introduce privacy by design principles into a legal framework.

No One is Exempt from Ensuring Privacy and Security

The idea that consumers should have to give up their right to privacy just to enjoy certain products or services is both out-dated and unethical. Consumers do want marketing — but not if it means putting their most sensitive personal data at risk.

As governments around the world follow suit with GDPR to ensure the protection of their citizens and consumers, marketers and security professionals are scrambling to keep up and comply. But to actually be enforceable, privacy and security regulations must be a joint effort by both the government sector and the tech industry to ensure that consumers enjoy helpful, personalized experiences that don't compromise their identity.

Unfortunately, keeping up with individual state-by-state mandates will eventually prove too cumbersome for all but the largest and most privacy-savvy organizations. That's why brands must employ a foundational approach to privacy that starts at the top. Businesses of all sizes and industries must take precautions that not only ensure they're in the clear from legal repercussions, but keep their customers safe and happy.

Marketers Must Seek Out the Most Trustworthy Partners

Privacy and security are the new market differentiators. Partners who can help brands meet their business goals and privacy compliance objectives will succeed. Those who cannot will be forced out of the market. Marketers who want to take advantage of powerful data tools and campaign capabilities will choose partners who can keep personal data secure and privacy promises honored — without sacrificing mission-critical functionality or performance.

As a new generation of privacy laws and regulations seeks to hold all parties accountable for poor practices and harms, brands have even more incentive to work with only the most trustworthy vendors.

Cheetah Digital

A Partner You Can Trust

You can tell a lot about a company by how they treat customer data. And at Cheetah Digital, privacy and security are a top priority.

We take a global view of privacy and employ a multi-layered approach to secure our platform and protect your valuable data — as evidenced by our SOC 2 certification and pending HITRUST certification. Our team of privacy and security experts is constantly monitoring evolving data threats and eliminating potential issues before they ever impact our platform.

We use a number of strategies to protect client data, including:

- Best-practice application security protocols
- Compliance with data governance principles
- TLS-encrypted connections
- Ongoing security monitoring and reinforcement

Our global privacy and security team works to combat threats to valuable data in our care and to ensure that the privacy rights and freedoms of individuals can be met wherever we operate — today and into the future. That's why leading brands choose to partner with Cheetah Digital for responsible data management that keeps them compliant and trusted by consumers.

Learn more about our commitment to security and privacy at ***cheetahdigital.com.***

Meet our CSO, **Jill Knesek**

Cheetah Digital CSO Jill Knesek has more than 20 years of experience in cybersecurity. She is responsible for providing enterprise-wide leadership in all aspects of information security for the organization.

Prior to joining Cheetah Digital, Jill served as a special agent for the FBI, assigned to the Cyber Crimes Squad in the Los Angeles field office. During that time, she was the case agent for several high-profile investigations. She has also served in various high level security roles for other major corporations.

A frequent industry speaker, Jill was recently featured in the book, "Women Know Cyber: 100 Fascinating Females Fighting Cybercrime."

Cheetah Digital

Seamlessly deliver personalized interactions that drive lasting emotional loyalty

Track relevant interactions

Our deep POS and e-commerce integrations ensure member profiles are updated with purchase and redemption activities as they happen.

Reward your best customers

Go beyond points to offer special treatment to your best customers with a flexible tier structure that provides customers with unique earning opportunities based on their loyalty status.

Personalize offers and communications

Define, manage, and target highly personalized offers online, at the register, or even in-store with coupons, recommendations, and exclusive offers — whether digital or physical.

Take your program mobile

Give customers the gift of convenience with mobile capabilities that let you manage card balances and collect real-time insights. Don't have a mobile app? Create and launch a fully-branded one with Cheetah Loyalty.

Foster the customer voice

Enable loyal customers to be vocal advocates of the brand by conducting polls, inviting feedback, and rewarding them for the referrals they give across social media.

Protect your program

Protect the program you've worked so hard to build. With data encryption, security safeguards, and the highest compliance standards, we are constantly monitoring to detect anomalous patterns and automatically stop questionable activities.

It's time to look beyond transactional data to build thriving customer relationships that deepen at every touchpoint. With Cheetah Digital's marketing and loyalty solutions, you have an entire platform at your fingertips to build the most relevant, integrated, and profitable campaigns.

Start building lasting customer relationships at **cheetahdigital.com.**