TREASURE DATA VentureBeat

VENTUREBEAT SPECIAL ISSUE

How Data Privacy is Transforming Marketing

Report

Introduction

How are advances in data privacy and technology changing the way marketers engage with consumers?

Treasure Data partnered with VentureBeat to explore what trends are shaping the future of marketing, and how organizations can use technology to transform their operations, keep their data safe, secure and compliant, and deliver experiences that meet consumer expectations.

Explore top articles from the issue:

- Marketing in the era of data growth and privacy
- What the end of third-party cookies means for personalization
- Data privacy is expensive — here's how to manage costs
- Putting data privacy first — a global approach to data governance

VentureBeat

Marketing in the era of data growth and privacy

By Sharon Goldman

This article is part of a VB special issue. Read the full series here: How Data Privacy Is Transforming Marketing.

For more than two decades, the holy grail of marketing has been focused on one-on-one connections between brands and shoppers. Companies that previously used television commercials to target the masses raced to take advantage of technologies like third-party cookies that tracked consumers across the internet — sweeping up vast swaths of easy-access data in order to serve precise ads to potential customers who might be interested in that very thing at that very moment.

Now, the marketing landscape is in the midst of another near-total transformation, thanks to a growing focus — by consumers, regulators and Big Tech companies — on data privacy.

By 2023, 65% of the world's population will have modern privacy regulations protecting personal data, according to Gartner, while only 10% had those protections in 2010. The EU's GDPR and California's CCPA have led the way. Meanwhile, in late

June, the Energy and Commerce Committee formally introduced the American Data Privacy and Protection Act (ADPPA) to the U.S. House, marking a major step forward for congressional data privacy negotiations.

It's getting real

"I think the wake-up call is here," Anthony Katsur, CEO of IAB Tech Lab, told VentureBeat.

IAB Tech Lab is a nonprofit consortium with a global member community, created to develop foundational digital media technology and standards. "The industry is starting to react to the fact that this is real, and it's going to become more real with real penalties, real fines, real ramifications for your business," he said.

Beauty retailer Sephora is one company that is already feeling the heat, with a $1.2 million settlement with the State of California announced last month.

Meanwhile, third-party cookies have been almost completely phased out. Chrome, the most popular browser, remains the last major holdout, as Google recently announced it won't get rid of third-party cookies in Chrome until the second half of 2024. But while this gives marketers a reprieve, advertisers see the writing on the wall about the deprecation of third-party cookies and most major brands have long been testing other options.

In addition, some Big Tech companies have changed their privacy policies. Tim Cook, Apple CEO, has called protecting privacy "the most essential battle of our time" and Apple released App Tracking Transparency in its April 2021 mobile software update. Meanwhile, Google announced a multiyear plan to update Android privacy policies in February 2022, in order to catch up to Apple in limiting third-party data sharing on its devices.

Marketers are second-guessing individual targeting

All of this has led to a dizzying sea change for marketers, experts say, who have to adjust to a new age of marketing in a world focused on data privacy.

"I think for the first time in 10 years, we see marketers second-guessing whether or not one-to-one communication and personalization is actually what they should strive for any longer," said Samrat Sharma, global marketing transformation leader at PwC. "The reality is it's not clear that will be possible or necessary."

Audience-based communication will still be the norm, he emphasized, "The question will be how to do that in a way that's still personalized because we do know people don't want to feel individually targeted."

The trick is, consumers want it all, which means marketers have to walk an increasingly treacherous tightrope to meet their expectations. According to Boston Consulting Group (BCG) research, two-thirds of consumers want ads that are personalized to their interests, yet nearly half are uncomfortable sharing data to create personalized ads.

"At the core of it, the consumer is getting more aware of their privacy and demanding more from the value exchange around providing more privileged access to the brands," said Sharma. "That's what's driving regulators to act, but then, in turn, manufacturers and publishers can respond to that," he explained.

A new marketing direction

In a shifting marketing universe where shoppers crave personalization but also want privacy protection, what is a marketer to do? The answer, experts say, is to market smarter, with different formats and even newer technologies that help maximize conversion while keeping data privacy at the forefront.

"It's not going to be as simple as just targeting people based on third-party data," said Andrew Frank, VP analyst at Gartner. "If you are a retailer or financial services company and you have a direct relationship with your customers, you have a lot more opportunities to solicit consent for personalized services."

Companies that have an indirect relationship with consumers, such as in consumer packaged goods, will have to start looking at more subtle efforts, like contextual targeting, an emphasis on tailored creative, and advanced artificial intelligence (AI) and analytics capabilities that can optimize based on non-personal signals, he explained.

That has led to many, many efforts to replace third-party cookies with privacy-focused alternatives. Frank says he's bullish on recent innovations such as IAB Tech Lab's seller-defined audiences, in which rather than publishers sharing person-specific identifiers with advertisers like a cookie-based ID or an email address — audiences are grouped into categories based on demographics, interests and purchase intents using IAB Tech Lab's Audience Taxonomy standard.

"This enables publishers and retailers to define audiences for brands in a constructive way that doesn't violate privacy," Frank said. "I think they're still working on modifications to the transparency and consent framework that would enable some kind of secure market for conceptual data in the advertising space."

Zero-party data, which goes beyond first-party data to focus on data that consumers voluntarily and deliberately share through website activity, messages, profiles and quizzes is becoming an essential trend, according to Vivek Sharma, CEO and cofounder of Movable Ink, which uses AI to personalize marketing content.

"If you fill out a wedding registry, that's an example of zero-party data — you're actively telling them what your preferences are and what you're interested in," said Vivek Sharma (no relation to PwC's Samrat Sharma). "But this whole world of third-party data — where your information is broadcast — is over and done. No credible company is betting on that in the future."

Still, Katsur says he doesn't think there will ever be a single solution to the future of addressability — the ability to target specific individuals — at scale for marketing purposes.

"It's going to be a portfolio solution, whether that be first-party identifiers or seller-defined audiences," he said, adding that IAB Tech Lab also recently formed a working group to advance privacy enhancing technologies (PETs). This working group brings together developers working on advanced cryptography, data science and privacy, as well as security systems engineers, to develop privacy-enhancing standards and software tools using encryption, de-identification and machine learning.

"That said, I think we're on the cusp, perhaps, of a third act in digital marketing where I think there's an opportunity for a renaissance in the ecosystem," Katsur said. "There will be pain and turbulence, but I will not count out this industry in their ability to innovate to solve for the needs of marketers, media companies and consumers."

Things marketers should do

1. Evaluate your investments

“I think there is a need to invest in new technologies and reevaluate the investments you may have made three or four years ago because the landscape has changed and it will probably continue to change,” said Gartner’s Frank.

This is a volatile period, he explained, with big shifts in regulatory constraints, technology and what marketers can expect to deliver in terms of data access.

“For some retailers and publishers, this looks like an opportunity because they have the capacity to capture data and use it as part of their relationship building, such as through a loyalty program,” he said.

Others will need to invest in emerging technologies such as data clean rooms, which enable the secure collaboration of organizations around consumer data without leaking personal data to counterparties.

“I think those technologies hold a lot of promise and clearly require some investment and experimentation to get right,” he added.

2. Work in partnership across the organization

If consumers value privacy, and that trend is growing, technology solutions have to be in service to customers, said PwC’s Samrat Sharma, adding that while it is easier said than done, it has to start with partnering across the organization.

“It’s about what you are trying to achieve,” he said. “If you don’t do it in partnership with IT or transformational teams, then you might stand up a DMP replacement, for example, but it won’t address broader business goals.”

That means areas including analytics, IT, marketing and transformation need to come together so that everyone knows what the ultimate goals are, then ask “How are the technology and solutions we’re deploying in service of those goals?”

3. Ask the right question

Frank added that one of the biggest questions he gets from marketers is, "How can we continue to target and measure our advertising in a way that keeps us accountable to the business under these increasingly restrictive constraints?" However, that may not be the right question, he explains.

"I think the question that they should be asking is, how can we design a future that both respects consumer privacy and interests in general, and still enables us to deliver the best possible experience to our customers in a way that enhances the value of our brand, as opposed to genericizing it?" he said. Of course, these questions don't have easy answers: "I think this is a problem that has a solution," he said. "I think the road to the solution is very complicated and thorny."

Marketers won't wait to take action

Today's consumers, of course, can easily vote with their feet — or with a website click.

"So, it's incumbent upon the marketing and advertising industries to figure out how to give consumers the privacy and data security they want, as well as the personalization they crave," said Katsur.

"If they're going to be served ads, they might as well be relevant," he added. "And let's be clear: advertising isn't going away. I think we all realize that."

As the holiday season approaches, complying with the new world of data privacy is becoming table stakes, added Movable Ink's Vivek Sharma.

"Marketers have to put on their thinking caps and go back to the drawing board about fundamentally creating value for their customers and earning their customers," he said.

Still, experts agree it is early days when it comes to solving issues related to marketing and data privacy.

"I think I'm somewhat optimistic in the long term, but I think it's one of those situations where you have to be careful not to confuse a clear view for a short distance," said Frank.

But marketers aren't just going to wait for the final nail in the third-party cookie coffin to take action, emphasized PwC's Samrat Sharma. "There's still uncertainty, but they know they need to do something," he said. "Everyone's sick of kicking the can down the road. They're moving forward with solutions."

VentureBeat

What the end of third-party cookies means for personalization

By Taryn Plumb

This article is part of a VB special issue. Read the full series here: How Data Privacy Is Transforming Marketing.

We've been shaking the crystal ball on the cookieless future, and it's still cloudy — we know it's coming, but we're not sure when, or how exactly it will play out.

Still, now is the time for organizations to prepare, lest their marketing methods become obsolete.

It is imperative, experts say, that enterprises be proactive in balancing the dual consumer demand for privacy and personalization. How can they achieve this? By harnessing lower-level types of data — including second-party, first-party and zero-party — and leveraging artificial intelligence (AI) in a way that is both ethical and accurate.

“Moving forward, brands have to think about how to collect data transparently and use it in a way that delivers value to the customer,” said Stephanie Liu, privacy and marketing analyst at Forrester. “That’s a relatively new mindset for marketers, and many are struggling today because for decades they’ve prioritized benefits to the business while neglecting the customer.”

Comparing first-party data and third-party data

Essentially, first-party data is “data that customers and companies share ownership of,” said Andrew Frank, VP analyst at Gartner. This lets a brand tailor experiences in the way of loyalty programs and incentives.

Putting it in human terms: First-party data is like being friends with someone and sharing information directly, said Liu.

“You know each other well and your friendship can deepen over time,” she said.

Third-party data, by contrast, is akin to having an acquaintance who you’ve mostly heard things about “through the grapevine” — and not all that is accurate.

“Personalization has turned into an amorphous catch-all, but when it comes to asking customers for data, brands need to think about what data they need, how they’ll use it to benefit the customer and how they’ll encourage customers to actually share that data,” Liu said.

With changes occurring and more afoot, “marketers are facing data deprecation,” she added.

Cross-site tracking is becoming more difficult, privacy regulations are adding new consent requirements, consumers are more protective of their data and walled gardens are limiting data access and use.

“It’s not just the death of third-party cookies,” said Liu. “There are multiple significant forces impacting marketers’ ability to collect and use customer data.”

The power of AI

Organizations are increasingly leveraging AI to fill in this gap. AI and machine learning (ML) models can categorize and segment third-party data to correlate, segment and make predictions.

Liu pointed to one common use case of lookalike modeling. When a customer hasn't shared "a plethora of information about themselves," a brand can take what it does know about them and try to match them with customers who look similar, she explained.

"It's a way of filling in the gaps for customers whose profiles are data scarce," said Liu.

Unsurprisingly, there are risks. If someone has chosen not to share much about themselves, it's probably because they don't know the brand well or don't see value in sharing data, she pointed out.

Brands can nail it pretty accurately and personalize based on data a customer hasn't explicitly shared, but this can be perceived as "creepy and invasive," she said. Case in point: The infamous example of Target recognizing a customer was pregnant before she'd even broken the news to her own father.

On the other hand, if a brand gets it wrong, it risks personalizing off faulty assumptions.

"So, marketers need to think about what benefit the customer will get from this type of modeling and if the benefits (to marketers) are worth the risks (to customers)," said Liu.

'Small data' trend

The conventional wisdom is that the most cutting-edge AI is dependent on large volumes of data. However, other approaches do not require massive labeled datasets — a few examples are transfer learning, data labeling, artificial data, reinforcement learning and Bayesian methods, according to the Center for Security and Emerging Technology.

This is what's known as "small data."

"Behaviors have changed so much in so many different ways in society around the world, that the data you collect is less indicative of the future than it used to be," said Erick Brethenoux, VP analyst at Gartner.

Organizations may have a lot in terms of volume, but not quality, he said. And, when there isn't enough quality data or data is fragmented, that's when model accuracy decreases.

This is prompting the use of additional AI techniques in the background to "enhance or complement" data, said Brethenoux. For example, in insurance, applying knowledge graphs to provide more context and better accuracy.

"The people who say they have too much data don't know what is in their data," said Brethenoux.

Other types of data collection

But, as third-party data from cookies to fuel AI models decreases, brands can increasingly rely on another tool: "Zero-party data."

This was termed by Forrester in 2017, and it refers to data that a customer proactively and intentionally volunteers. Such as, Liu said, product preferences, purchase intent, and content preferences.

For example, they can specify, "I have a cat." A brand can then use this information to show them cat products on their site or app — and stay away from hawking dog products.

"This is data customers are choosing to share with a brand because they like the brand and are getting some benefit or value in return," said Liu. It is much more transparent and straightforward than buying from a data broker, she said, and helps reduce the creepiness factor of "why do you know that about me?"

Right now, it's still just a concept, contended Frank. He does see it evolving into something "more substantial," and potentially used with distributed or decentralized ledgers.

Still, he pointed out that first and zero-party data, where there is "incentivized consent" is not always permitted — or even a possibility. More generic categories that don't sell directly — say, a tissue paper supplier — don't have that ability, and the cost of losing access to third-party data is higher.

Second-party data

Another emerging method for procuring data? Second-party data via data clean rooms. This is a collaboration between brands with direct relationships to consumers with brands that don't, explained Frank.

Data clean rooms allow companies to leverage intelligence extracted from personal data without exposing personal data to any parties, he explained.

A new Interactive Advertising Bureau standard is "seller defined audiences," which allows companies with large amounts of data to define an audience that an advertiser could buy without revealing specifics, he said.

Then there are concepts such as Unified ID 2.0, an unencrypted alphanumeric identifier created from emails or phone numbers. This method allows advertisers to target specific consumers without compromising their privacy.

Responsible AI — and marketing

The key to all this is getting the right kind of consent, and making sure that that is always honored and enforced in different contexts.

Then, of course, there's the imperative that AI models be responsible, ethical and trustworthy — undoubtedly one of the most pressing discussions occurring in tech right now. Respective to third-party data, organizations must be cautious and seek advice on how to use it, said Brethenoux.

"It is the responsibility of the organizations getting that data to do that work," he said.

The future of procuring data, said Frank, could either be a "walled garden" concept, where a few large companies have a great wealth of data and sell that data; a "consent economy" controlled by consumers; or a decentralized, self-sovereign identity where people would control their identity.

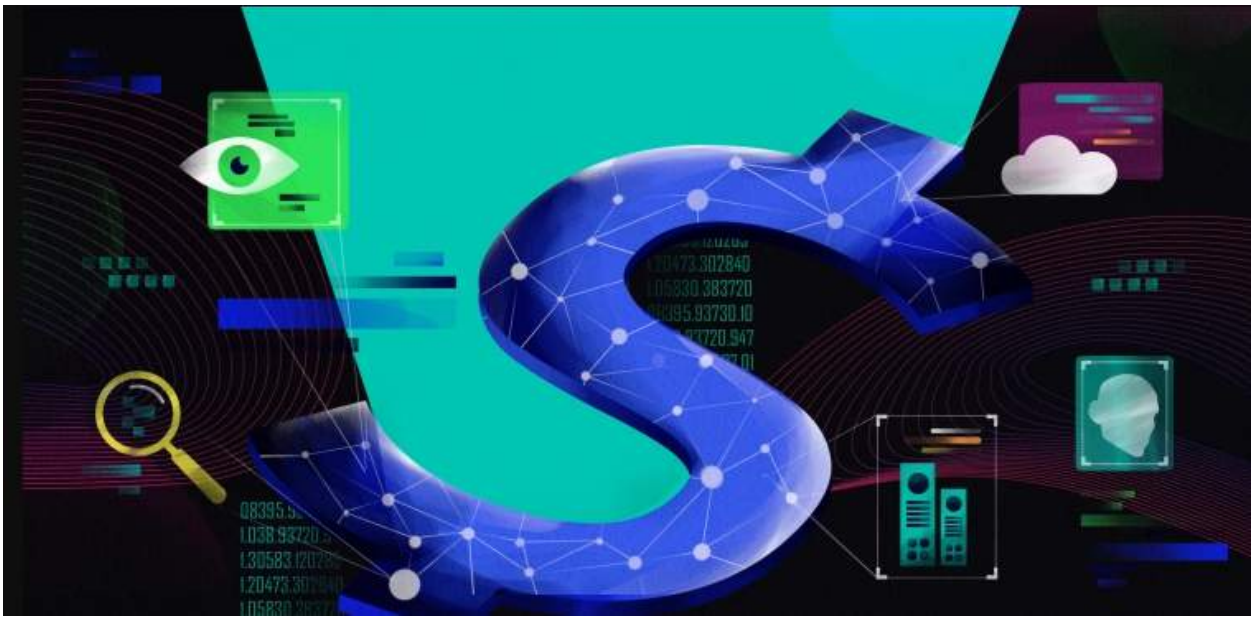
In any case, "we're heading for a world where people do have more control over their personal data and can make more intelligent decisions with how they share it with brands," said Frank.

Ultimately, third-party data isn't going to go away, said Frank. Brands just must get smarter about how they use all other types of available data — whether that's zero, first, second, or creative procurement of third-party data that respects privacy.

In the meantime, continue to keep an eye on that cookieless crystal ball.

VentureBeat

Data privacy is expensive — here's how to manage costs



By Sri Krishna

This article is part of a VB special issue. Read the full series here: How Data Privacy Is Transforming Marketing.

Data privacy has always been a top priority in both consumer and business circles. Individuals, including company employees, demand more control over how their personal data is used and greater transparency into how businesses manage customer information. If data is the currency of the future, then ensuring data privacy is the key to gaining user trust.

In light of high-profile breaches and data leakage incidents such as the Sunburst SolarWinds attack, the Estée Lauder customer database leak, the discovery of Facebook and MGM Resorts confidential data on the dark web, the resurgence of WannaCry, REvil and other ransomware attacks companies have realized the need for robust data privacy strategies and processes.

Solutions should focus on how personal data is collected, processed, stored, shared, retained and destroyed while ensuring data availability and integrity and safeguarding assets from unauthorized access. This should also cover agreeing, blocking and disabling online cookies.

In cases where organizations are sharing data with each other, including those of third-party vendors, the above practices also apply. Executives need to collaborate to balance risk, transparency, customer and stakeholder satisfaction, and compliance. Needless to say, privacy policies must strike a balance between risk, prioritization, the cost of failure or breach as well as management commitment and operational and reporting costs.

According to Gartner research, 75% of all organizations will restructure risk and security governance for digital transformation as a result of imploding cybersecurity threats, insider activity, and an increase in attack surfaces and vulnerabilities. Some companies have even appointed chief privacy officers, who are custodians and responsible for this important function. Enlisting services of privacy and compliance consultants vis-à-vis full or partial in sourcing are also active and ongoing considerations of management.

Non-compliance costs

Data privacy often comes at a huge price — one that can't be quantified in certain terms because the implications are vast.

"It's easy to see that data breaches can be costly for companies of all sizes. Companies should be investing in data protection at all levels like encryption, access control and incident response to prevent dangerous and expensive attacks," said Soumendra Mohanty, chief innovation officer and chief strategy officer of data analytics company, Tredence.

"The cost of non-compliance are massive from both a financial and reputational perspective. It can cost companies up to nearly $31 million to maintain compliance, depending on the industry, yet non-compliance can quickly double those numbers," Mohanty said.

Fines, legal fees, and the loss of business are all potential consequences of failing to meet regulatory requirements. In some cases, companies may even be forced to shut down if they cannot comply with regulations.

According to a HelpSystems report, the costs of non-compliance continue to grow annually, increasing by 45%over the past decade. These costs incorporate fines and penalties, the indirect costs of reputational harm, revenue and time lost, and business interruptions.

Data privacy losses go beyond dollar value

“The true cost of data privacy, broadly, is their trust with their customers,” said Akbar Mohammed, lead data scientist, Fractal AI. “In this era of customers increasingly becoming tech-savvy, as soon as they realize that their data isn’t secure, the company will risk loss of trust from consumers. This eventually results in a lot of business disruption.”

Almost all companies that need to collect data for their operations should have a data privacy infrastructure in place. Companies should also set up dedicated security and compliance teams surveying data and technology assets along with maintaining an aggressive threat detection policy. It’s imperative for companies today to have a data strategy and have policy and procedures governed by a data governance entity.

“For large organizations, it’s best to have regular audits or assessments and get privacy-related certifications,” Mohammad said. “Lastly, train your people and make the entire organization aware of your activities, your policies.”

Data Privacy compliance regulations that matter

To help project costs and financial implications, companies should be mindful of existing legislation and regulations like GDPR, the CCPA, HIPAA, the FTC Act and the GLB Act — alongside those on the horizon to address the pressing privacy and data challenges facing business operations everywhere.

Navigating data privacy management

As per Dan Garcia, CISO of EnterpriseDB, a provider of software and services based on the open-source database PostgreSQ, organizations should prioritize the security of their data, which first starts with discovery within the systems.

Having controls mapped to a data classification policy helps ensure appropriate protections from cyber threats such as cybercriminals. It’s a conscious effort within and across the business to support more secure practices. Organizations lacking internal resources, employee education, appropriate encryption and firewalls, and adopting poor password and privacy practices could experience a serious breach and resulting lawsuits that could cripple their business.

Its imperative organizations invest in a strong backup solution, as backing up important files and information is essential for data security. With reliable backups in place, an organization

can withstand common occurrences like system failures, hard disc failures, corruption, and ransomware scenarios.

“Cybercriminals have become skilled at identifying where backups are stored and purging them during ransomware attacks, so organizations should pay extra attention to how backups are protected, storing them in offsite locations, and ensuring they are securely managed,” he said.

Developers and business leaders alike seek data ownership and control and they simply don’t have time— or money — to waste. As enterprises adopt a cloud-first approach to their data management, they should invest wisely in technology providers that ensure robust privacy measures—without sacrificing ownership and access to their data.

Data privacy checklist

There is no one-size-fits-all checklist for data privacy management, as the specific requirements will vary depending on the type and size of the company, as well as the industry sector. Nonetheless, Evalueserve’s VP and Global Head of Data and Analytics Swapnil Srivastava shared some tips on managing data privacy within a company in order of importance and cost.

Cost Overhead	Why is it Important?
Data protection initiatives	Country-specific laws mandate strong governance and control of customer personal data
Investments in specialized technologies to protect data and IT infrastructure assets	Implementing compliance solutions require investments in specialized software
Compliance audits	Companies are mandated to report to regulatory authorities and demonstrate proof of staying compliant.
Compliance policy development	Clear policies with roles, responsibilities, and ownership must be implemented in organizations regarding compliance activities.

Incident response ecosystem	As part of responding to a situation of breach of compliance, companies must invest in incident response solution
Staff Certification	Mandated by regulatory authorities
Communications and training	To ensure organizations have trained officials to engage, roll out, and implement a compliance strategy
Redress activities	To enable companies, to have standard operating procedures to deal with and settle issues arising out of breach/fall out of a compliance violation

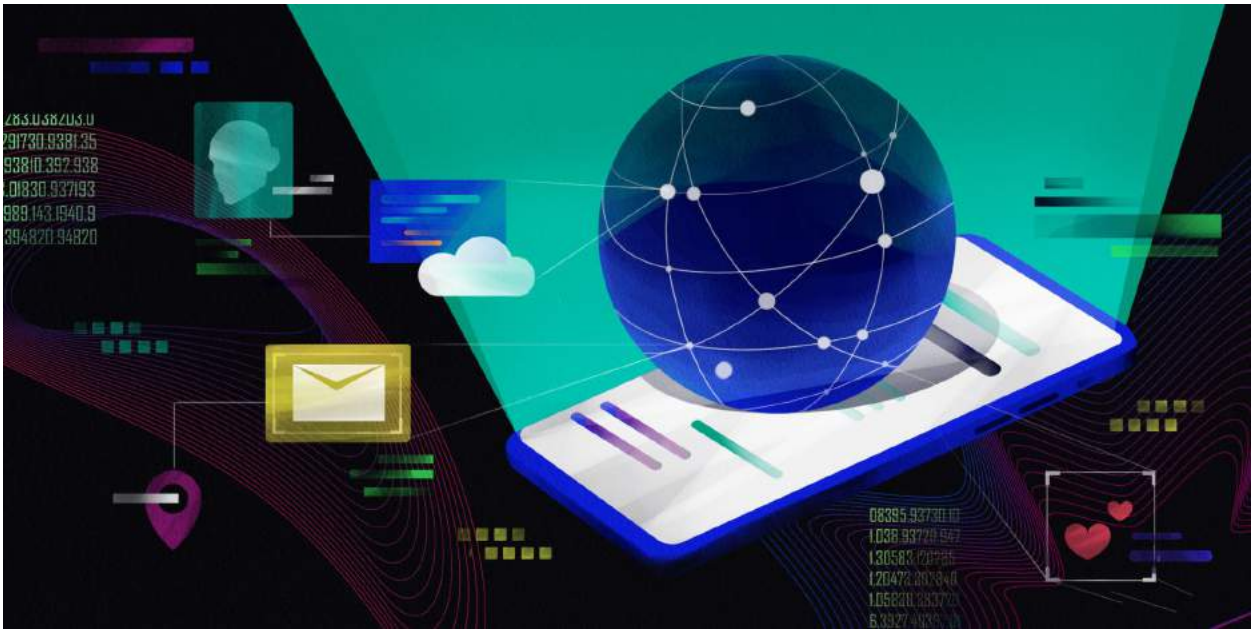
Sridhar Damala, CTO of Acuity Knowledge Partners, recommends companies to look at privacy by design rather than an afterthought if they wish to spend less than most companies.

"Privacy by design ensures that you have the foundation built for scalability," he said. "If you have the right set of tools, processes and automation in place from day 1, your spend on data privacy will be incremental rather than linear."

VentureBeat

Sponsored

Putting privacy first: A global approach to data governance



By Helen Huang, Treasure Data

Global organizations are often a complex web of brands, subsidiaries, entities and corporations, consisting of separate teams that interact with thousands of customers. During these interactions, there are millions, if not trillions, of data points collected, processed, analyzed and activated every day.

In an ecosystem that must now uphold consistently evolving regulations, navigate the deprecation of third-party cookies, and keep a promise of privacy to customers, how can companies ensure that their entire organization, along with their networks of external and agency partners, are up for the challenge of global compliance?

The privacy problem

For global enterprises, navigating this proverbial minefield can seem impossible. Different regions, or citizens of a certain region regardless of where they are in the world, may be

subject to different levels of legislation. And companies face ever-changing data management requirements to secure the right opt-ins and ensure compliance. People may also interact with multiple brands across the enterprise, which can result in duplicative or siloed records that all ultimately belong to the same customer. These are all challenges for companies that want to have visibility into the entire customer journey across a wide brand portfolio.

How personally identifiable information (PII) is shared between different teams also needs to be considered to ensure the right teams get access to only the data they need, and sensitive information is withheld at the right times. How is data being shared between second or third parties, or cross-functionally between sales, marketing, customer service and finance, for example? Lack of governance or controls can lead to risk of data breaches which can compromise the system, brand reputation and consumer trust, and result in costly fines.

Only about one-third of customers believe that companies are currently using their data responsibly. (McKinsey)

Then, there's the issue of scale. Companies grow, and customer data grows with it. But so does the need to continuously keep up with regulatory obligations. This requires a certain level of agility to quickly adapt. For example, slowdowns can leave marketing teams overly reliant on IT to execute campaigns, which creates roadblocks for innovation or growth as systems are updated. This results in a backlog — costing the company, but also the consumer, who can be left with a less-than-satisfactory customer experience.

Going global with governance

So, you have your data, your teams, your company and a need to integrate consent and governance into the mix. How does that look within the tech stack?

- First, start off by creating a smart 360-degree customer view. This means collecting data from across the organization into one unified customer data platform. This process exposes and consolidates duplicative content that may exist across silos, and paints a clearer picture of a customer's interactions across the entire customer journey. It also sets a foundation for all members of the organization to work off of the same unified customer profile.
- Integration with consent management platforms allows consumer privacy preferences to be seamlessly captured as part of your 360-degree customer view. By integrating

consent into the customer journey, companies can quickly create tailored experiences based on consumer opt-ins and specific privacy preferences.
- Permissioning, or data separation, within your data platform allows for greater control over who gets access to what types of PII, and when. This requires the organization to map where data is coming from, where it's going, and how access is handled without risk of security breaches.
- Identity resolution capabilities help decipher customer activity with decreased reliance on third-party cookies, helping to fill in the gaps that otherwise may exist.
- Data clean rooms provide a safe and secure environment for external partners to ensure only the right information is exchanged between parties in a way that meets compliance requirements.
- Low-code/no-code capabilities give non-technical teams (like marketing, sales and customer service) the ability to work with data quickly and with less reliance on IT, freeing up technical teams to focus on other projects while remaining agile to security updates.

92% of marketers consider a CDP important to their privacy and compliance efforts. (Treasure Data/Advertiser Perceptions)

Creating a connected data foundation

Outside of the tech stack, achieving global data privacy and governance practices requires collaboration across the enterprise. Leadership must come together to understand their privacy obligations, establish a framework for consent management and find a way to deliver a relevant value exchange with customers.

To start, leadership should ask themselves the following questions:

- *What does our data management process look like today? How mature are our current capabilities? What is our risk?*
- *What is missing from our tech stack to complete our privacy goals?*
- *How will data be governed centrally across the organization?*
- *How can we prioritize projects to achieve compliance quickly and effectively?*
- *What do we need to do to ensure our plan can scale to meet future needs?*

- *How can we empower our people to understand and uphold our governance policies as part of the customer journey?*

Putting data privacy first

Privacy and consent are now pillars for how companies connect with people — and that's not going to change anytime soon. Upholding personal preferences opens doors for contextualized experiences, meaningful interactions, and clarity around the customer journey. With the right tools and the right strategy, global organizations can get secure value from their data, integrate their teams and establish a framework for success.

Helen Huang is a Principal Product Manager at Treasure Data, focused on privacy, security and governance safeguards within the CDP. With over 10 years in the data privacy B2B space, she loves monitoring the regulatory landscape, learning about cutting edge ad technologies, and exchanging views on their combined impact on consumer trust.

TREASURE DATA

Treasure Data Customer Data Cloud helps enterprises use all of their customer data to improve campaign performance, achieve operational efficiency, and drive business value with connected customer experiences. Our suite of customer data platform solutions integrates customer data, connects identities in unified customer profiles, applies privacy, and makes insights and predictions available for Marketing, Service, Sales, and Operations to drive personalized engagement and improve customer acquisition, sales, and retention.

Treasure Data is trusted by hundreds of Fortune 500 and Global 2000 companies,has won numerous awards, and has been named a strong performer and leader by top analyst firms. Headquartered in Mountain View, CA, Treasure Data has offices in Japan, South Korea, England and France to help leading brands around the world make the connection. To learn more, visit www.treasuredata.com.

Request a demo today

treasuredata.com | +1 (866) 899-5386