PRIVITAR

Data Privacy is Essential to Using Consumer Data to Power Business Growth

www.privitar.com

The Need to Leverage Customer Data is Rising

From banking and insurance to telecommunications and technology, enterprises across industry lines increasingly realize how crucial customer data is when creating a personalized experience and achieving growth targets. Consumers are shifting their brand loyalties, online destinations and buying habits to those organizations that provide the most tailored and efficient trusted experience.[1] Behavioral data is compelling:

- 86% of consumers state that personalization is an important factor in their buying decisions.[2]
- 73% of consumers prefer brands that will take into account their personal details.[3]
- 44% on average across industries have expressed frustration when their experience isn't personalized.[4]

Increases in Breaches, Privacy Regulations and Customer Expectations Create Urgency for Data Privacy

In the midst of increased demand for a personalized consumer experience comes regulations and trends that seem in direct conflict with these goals. While consumers want an experience tailored to their needs and interests, they are also sensitive to their personal data being collected, and how it may be used. From 2016-2018, the volume of data breaches reported increased twelve-fold.[5] Customer concerns about when and how their data is being collected, stored and protected has risen as a result.

Regulatory bodies have responded decisively. Over 100 countries now have data protection laws in place,[6] focusing on safeguarding personal information. Personal information can include data ranging from address and bank account number to lesser known regulated data, such as demographic data you collect or buy, or browsing or sales history that can be used to positively or reasonably infer demographic information about an individual.

Regulatory bodies have greater power to investigate potential violations and issue fines as well as other enforcement actions. Newer legislation, such as CCPA, include protections called the Private Right of Action. Individuals are granted the right to pursue damages against a company when they feel legally aggrieved. These damages can be significant. In the case of CCPA, individuals can claim damages of $100-$750 per person for distress alone. Damages for actual harm are uncapped.

With this increasing risk and regulation, sensitive customer data must be protected to ensure your organization is minimizing exposure and maintaining hard-won customer trust and brand integrity. Enterprises must adapt and standardize on a centralized data privacy solution that consistently mitigates risks and optimizes data utility to safely enhance the customer experience and underpin growth initiatives.

Data Privacy is an Essential Element of Data Management

Organizations must protect customer data to minimize the impact of data leaks, ensure regulatory compliance, and preserve brand integrity. Yet they must maintain their ability to use that personal information to create a differentiated customer experience that increases sales, customer satisfaction, and customer lifetime value. Failing to ensure privacy while extracting insights creates serious risk. Conversely, unnecessarily limiting data use in the name of privacy significantly limits the type of tailored customer experience that allows organizations to differentiate compete effectively.

Data-driven enterprises typically have many different data stakeholders with many distinct and simultaneous goals: increasing conversion rates, evaluating the customer journey to enhance upselling and cross-selling opportunities, maximizing services utilization, predicting and

1. McKinsey & Co. "Customer Experience: New Capabilities, New Audiences, New Opportunities." Online. 2017. **2.** Reavie, Vance. "Three Ways Artificial Intelligence Can Enhance Your Personalization Strategy." Online. 2018. **3.** Ibid. **4.** Accenture. "US Consumers Turn Off Personal Data Tap as Companies Struggle to Deliver the Experiences They Crave." Online. 2017. **5.** Deloitte. "Consumer Privacy in Retail: the next regulatory and competitive frontier." 2019. **6.** Consumers International. "The State of Data Protection Rules Around the World." **7.** The Economist. "Smartphones are Driving Americans to Distraction." Online. 2019.

avoiding customer churn, and personalizing every part of the customer experience. The sheer volume and scope of data analyzed using Machine Learning and Artificial Intelligence can yield critical insights for enterprises that make full use of the data in an increasingly competitive environment. Customers linked to email addresses, home addresses or phone numbers may not even need to be registered members with an organization in order to have their behavior analyzed. Every page view, email open, search, purchase and abandoned item can provide more context and insight, allowing organizations to infer relationships between consumers, or determine information like gender, income, age, profession, and political positions:

- Behavioral discounts offered via Machine Learning models can lend insight into consumer activity. For example, mobile driving apps meant to offer discounts to safe drivers can also evaluate how and when smartphones are being used for other purposes while the driver is behind the wheel.[7]
- Focused demographic trends leveraging anonymized data can allow the best strategic marketing approach for each. For example, evaluating usage data for a smartphone user can indicate URLs visited, which in turn can reveal approximate ages, current location, or political preferences.
- Advanced analytics using millions of interaction touchpoints ranging from direct customer transactions through social media activity. For example, banks looking at economic, social and attitudinal activity across multiple channels can aggregate this data to pinpoint a strategy that sends ads for specific milestones. Customers about to have a baby can receive an ad to open a college savings account, and are more likely to click and open it. Banks can leverage this to forge deeper ties with their customer base.

As these insights sharpen, enterprises can more accurately target life milestones, current events or issues that better engage customers and drive purchasing decisions. With this huge increase in data, however, comes more urgency to protect this data from breach or misuse. Simply protecting insights with security measures like Access Control does not sufficiently allow sharing the information across channels and keeps data siloed. Data Privacy is crucial in ensuring enterprises are maximizing data utility while minimizing the threat of data leakage and regulatory non-compliance, and its resulting restrictions and fines.

A Customizable Approach to Protecting Data is the Only Way to Ensure the Widest Range of Use Cases can be Met

- Protect all personal information. All sensitive customer data you collect and store must be de-identified for analysis. Only unless strictly necessary in catering to a personalized campaign intended to craft the customer experience should data be re-identified to minimize risk and exposure. A wide range of de-identification techniques allows for the most comprehensive privacy coverage while permitting the best use of customer data.
- Controlled Reversibility. Data should only be re-identified by approved individuals, and not in every case. Ensuring control over when and how de-identified data can be re-identified and acted upon is critical in protecting customer privacy while leveraging the information to increase customer lifetime value.
- Controlled Linkability. De-identified data must still allow for the discovery of trends and insights. As more data becomes available, it should be consistent to enrich existing de-identified data models and provide additional customer insights. In parallel, data must be tightly controlled to ensure that any unintended enrichment or linkability is prevented.

- Scalability. As Machine Learning and Artificial Intelligence process ever-growing volumes of valuable data, it is critical that the ability to de-identify and leverage that data is able to keep up with the demands of an organization's systems.
- Compatibility with modern data architectures. Ensuring data privacy should not negatively impact an organization by requiring a shift to a new technology stack. Nor should it require a significant shift in process to become effective.
- Traceability. Make sure that the reason for data collection and transmission is tracked, as well as who has access to it and when.

The Privitar Data Privacy Platform™: Safely Use Sensitive Data to Maximize Customer Engagement and Lifetime Value

Using consumer data gives organizations a competitive advantage and helps foster and solidify relationships with their customers. Maximizing data utility while adhering to consumer privacy laws, the Privitar Platform offers functionality that assists in automating, centralizing and precisely managing the different requirements that allow the best use of sensitive information.

- De-identification. Privitar provides the full range of techniques to anonymize data while maximizing utility and insights. You can control the degree of anonymization according to what level of information is appropriate and when.
- Controlled Linkability. Privitar's Protected Data DomainsTM allow a centralized method to control what data can be linked. Within each one, referential integrity of the data is protected, but between them linkage is prevented, allowing each organization to control which sets of data are linked and how.
- Controlled Reversibility. Privitar also enables you to control reversibility so that you can re-identify anonymized data after analysis, if required.
- Scalability & Automation. Privitar includes a comprehensive set of RESTful APIs that enable organizations to automate and orchestrate their data de-identification and provisioning processes. Programmatically configure policies that ensure personalized campaigns and online retargeting are adhering to the appropriate privacy policies at scale.
- Architecture Compatibility. The Privitar Platform supports on-premise, hybrid and cloud environments. It accommodates a wide range of technology platforms and data processing models, allowing it to fit seamlessly into existing technology stacks.
- Traceability. Privitar Watermarks™ are unique technology that enable end-to-end traceability of sensitive data. Watermarks allow tracking and management of when a dataset was generated, who it was generated for, when it should be deleted and where it can be used.

Contact us:

e: info@privitar.com
t: UK +44 203 282 7136 / US +1 857 347 4456
w: www.privitar.com

PRIVITAR

@PrivitarGlobal

www.privitar.com