Customer experience marketing in the age of data privacy

Business Impact

Your customers are more aware of their data privacy rights than ever before. Organizations that don't take privacy seriously do so at the expense of their brand reputation and customer loyalty. To make it worse, noncompliance with regulations can be costly. For example, noncompliance with the California Consumer Privacy Act can result in consumers suing for up to $750 for each violation. And the state attorney general can sue for intentional violations of privacy at up to $7,500 each.

The Issue

With more data flowing into organizations from more sources than ever before, organizations have a unique opportunity to predict and enhance customer experiences. But there is a catch. The age of data privacy has arrived, and there is a huge risk for organizations not having a plan in place to secure their customers' personal data. In addition to financial losses, exposing sensitive data may damage business reputation and increase customer attrition. Consumers more than ever want to do business with organizations that make privacy and personal data protection a top priority.

The Experience 2030 global survey[1] says:

- 73% of consumers are concerned with how brands are using their personal data.
- 76% of consumers are concerned with the amount of data brands gather when they search for or purchase a product.
- 73% of consumers are concerned with how brands are using their personal data to the point where they feel it is out of control.
- 71% believe that companies and brands should not be allowed to share their data with other companies or brands.

Challenges

- **Maintaining a world class marketing organization.** Organizations must continue using data and customer experience platforms to predict and enhance customer engagements, but at the same time maintain the privacy of customers.
- **Inability to locate or identify PII.** Organizations may not know where all of their personally identifiable information (PII) is located, have a way to identify it as sensitive, or have an accurate depiction of companywide sources.
- **Poor protection**. Without well-defined processes, many organizations fall short when it comes to protecting and reporting on personal data.
- **Cost of complying with new data protection regulations.** Whether it's the GDPR in the European Union or similar regulations like the CCPA, penalties for noncompliance will be high.

[1] *Experience 2030: The Future of Customer Experience* by Futurum Research and sponsored by SAS.

The SAS® Difference

Best practices and proven technology for protecting PII

SAS offers trusted data access, identification, governance and protection along with best practices that tie together all the essential areas of PII monitoring. With SAS, you get:

- **Embedded data governance.** We provide a business glossary, lineage repository and data quality monitoring to keep everyone at your organization on the same page. Store business terms and owners, as well as their relationships to technical data assets like reports, data sets or files.
- **Superior detection capabilities.** Search your data assets to locate PII in varying file formats and in traditional relational databases, as well as emerging data sources.
- **Centralized and flexible reporting, visualization and monitoring capabilities.** Identify relevant issues quickly and send appropriate contacts notification of noncompliance.
- **Dynamic data masking.** Help ensure security by masking data at the point of entry from any data source – including SAS data sets, flat files, relational databases and big data technologies.

Case Study

A North American online retailer

Situation

To avoid fines, the company needed to identify, govern and minimize the risk of exposure for all the personally identifiable information it had collected and was using for marketing purposes. But there were inconsistent views of data, with no governance around queries – and there was no master view of revenue drivers across disparate systems.

Solution

SAS® for Personal Data Protection.

Expected Results

- A cleansed, single view of the customer to drive increased revenue through targeted marketing efforts.
- A common, secure entry point for data access and auditing.
- Role-based data masking and monitoring to meet compliance and regulatory requirements.
- Improved identification and governance of PII to avoid regulatory fines.

What if you could ...

Identify your data assets

What if you could identify PII that resides in various files and sources throughout your organization, then track the lineage and business concepts that are related to those technical data assets?

Give the right people access to the right data

What if you could set role-based permissions to anonymize, encrypt or hash data so that it won't fall into the wrong hands?

Trust your data

What if you could use built-in rules to monitor your level of data quality, engage the right users to remediate issues and actively enforce governance policies?

Generate visualizations to speed reporting and avoid penalties

What if you could generate interactive reports to help you achieve compliance and reduce penalties and fines?

SAS Facts

- SAS is a recognized leader in customer experience, data integration, data quality and analytics.
- 92 of the top 100 companies on the 2018 Fortune Global 1000® are SAS customers.
- SAS has customers in 147 countries, and our software is installed at more than 83,000 business, government and university sites.

Learn more about personal data protection from SAS: sas.com/personal-data.

To contact your local SAS office, please visit: sas.com/offices