White paper:

Automate Data Access Rights Fulfillment

Data rights are the heart of modern privacy regulations: learn how to automate fulfillment and manage data access with advanced data intelligence and data-centric privacy.

Table of contents

Introduction

At the heart of modern privacy regulations is the need for organizations to be able to account for how they collect and process personal data, not just in the aggregate, but on an individualized basis for potentially millions of customers.

First enshrined under the EU General Data Protection regulation (GDPR), and now replicated to a lesser or greater extent by the California Consumer Privacy Act (CCPA) as well as regulations across the globe, these data access rights have quickly emerged as a set of critical compliance, privacy protection and security concerns.

> **Non-compliant companies face fines, civil liability, and loss of brand equity**

Far-reaching Impacts to Enterprises

For enterprises, this creates a new level of responsibility and need for transparency to account for all the data they collect and process on an individual. These data access rights based on new standards of not just what data an enterprise holds but whose data it is now present fundamentally new operational challenges for enterprises' data-driven business strategies.

Firstly, these rights require enterprises to establish a foundation for accountability by mapping the data estate, identifying all personal information based on context as compared with the current standard of directly identifiable attributes (PII) and accurately inventory the data by person and state of residence. The CCPA - just like the GDPR and other regulations - also introduces the need to able to respond to data access and deletion requests with a comprehensive and accurate report within specific timelines.

Secondly, as organizations wrestle with a growing volume of requests and the ensuing complexity of manually assembling accurate data access reports, both the costs of privacy compliance and the risks of non-compliance escalate. Moreover, for data deletion requests, enterprises must be able to ensure not only that have satisfied individual deletion requests, but that no new data is collected.

Further compounding the challenge are GDPR requirements to manage user consent to collecting and processing data, and similar CCPA requirements to provide and honor Opt Out rights for selling data (also known as “Do Not Sell” requests). These requirements introduce the need to report on whether consent or a “Do Not Sell” request was recorded, but more importantly to correlate the individual’s decision to their specific attributes and be able to demonstrate their consent parameters are operationalized.

This whitepaper examines how corporations can automate the mapping of their customer or employee data to drive data protection and compliance programs, efficiently manage their internal data access rights processes as well classify and correlate data at scale when dealing with complex, diverse environments.

> At the heart of modern privacy regulations is the need for organizations to be able to account for how they collect and process personal data.

Discovery, Mapping and Correlation

Find PI and PII

Unlike PCI DSS, or similar mandates which focus on Personally Identifiable Information (PII) only (such as Social Security Numbers or credit card details), both the EU GDPR and the CCPA define personal data or personal information as data related or associated to an individual. The CCPA defines "personal Information" much more broadly than earlier regulations covering sensitive information, and extends beyond direct identifiers. Personal information under CCPA, for example, includes information that identifies, relates to, describes, or is capable of being associated with a particular consumer or household, both direct and inferred attributes.

The CCPA definition includes IP addresses, geolocation data, biometric information, and "unique identifiers" such as device and cookie IDs, Internet activity information like browsing history, commercial information such as products or services purchased or consuming histories or tendencies, and characteristics concerning an individual's race, color, sex (including pregnancy, childbirth, and related medical conditions), age (40 or older), religion, genetic information, sexual orientation, political affiliation, national origin, disability or citizenship status.

Inferences that have been drawn from personal information "to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes" are also considered "personal information."

These requirements stand in stark contrast to existing capabilities built for the PCI era, aimed at simply finding and enumerating a specific set of identifiers. These technologies, typically using regular expressions for pattern matching or relying on inconsistent metadata like column or table names, fail at determining whose data it is in order to address privacy regulations, or establish based on context what should be considered personal data or information.

BigID uses innovative correlation and identity intelligence to establish how identifiable data relates to a consumer identity, helping to uncover “dark data” and infer via correlation which attributes are associated with either GDPR data subjects or California consumers for inventorying and potential de-identification.

> **At the heart of data access rights ins the need to account for an individuals data.**

Mapping Across Data Stores

Most large organizations face the daunting challenge of mapping and understanding their data across large volumes and growing diversity of data sources. Data privacy regulations in turn do not make the distinction between data source types for compliance requirements. As many enterprises have discovered, lack of visibility into personal data stored in an AWS S3 bucket does not insulate the company from a data breach, or potential privacy violation.

Regulations like CCPA and the EU GDPR require covered organizations to find a person’s data across all their data stores. Traditional data discovery tools provide limited data source coverage - forcing companies to settle on either unstructured files or relational databases, and then collate findings to assemble a report.

BigID is the first discovery technology that can find, classify and correlate data across unstructured, structured, Big Data, SaaS, IaaS, data warehouses, messaging platforms, critical business applications like SAP and Salesforce.

Offering the largest data source coverage of any commercial data discovery or intelligence platform, BigID gives enterprises the ability to automate data rights across the entirety of their data sources.

Correlate By Identity

At the heart of the data access rights is the need to account for an individual's data. Without the ability to automatically index whose data is where, automating data rights fulfillment is practically close to impossible. After all, each of the data access rights relies on the ability to determine where all the data that relates to an individual and their profiles are stored and processed across the enterprise's infrastructure.

BigID's correlation and machine learning technology uniquely finds personal information across the enterprise that is reasonably associated or linkable to an individual California consumer and automatically assigns state residency without having to move any data. This identity-aware approach is purpose-designed for modern privacy requirements.

Advanced Data Access Rights Management

Customization for External and Internal Reporting

While enterprises are required to comply with data access rights, how they respond and operationalize reporting is driven by specific business concerns. Using BigiD, operators can customize reporting templates and define settings based on business rules for specific user types and data reporting categories – as well as redact how the attribute and purpose of processing is represented externally. Proof of consent can be directly integrated into reports with the ability to compare it to actual purposes of use and assess validity.

> **How enterprises respond and operationalize data access reporting is driven by specific business concerns.**

Also, enterprises can maintain different forms of data access reports (or DSARs) for internal use that shows all associated data stored everywhere for a data subject, and a summary report for external consumption. For data deletion requests, BigID provides enriched task delegation workflows for data owners based on where the individual's data is stored. Through integration with ticketing systems, enterprises can easily track and manage tasks associated with individual data elements that must be masked, encrypted, redacted or deleted.

With BigID, analysts can search the inventory by multiple attributes to directly identify a user's personal information.

> “A cornerstone of emerging privacy mandates, especially those built on EU GDPR principles, is the requirement for sustainable compliance.”

Data Rights Validation and Assurance

A cornerstone of emerging privacy mandates, especially those built on EU GDPR principles, is the requirement for sustainable compliance. Rather than assessing compliance on a quarterly basis, enterprises are now expected to proactively identify and respond to risks to personal and private information on an ongoing basis.

For the Right to Be Forgotten and consent withdrawals, BigID can enable a deletion workflow process with specific details and physical location of all applicable consumer information eligible to be purged or staged for deletion. Enterprises can further validate and provide ongoing assurance that data has been removed from processing flows and erasure has taken place with a search against the inventory, validating the deletion process was comprehensive and is being respected on a continuous basis.

Flexible Integration Architecture

Of necessity, data rights fulfillment and report management cannot be seen in isolation. For enterprises to be able to scale and automate, privacy operations should be able to be programmatically integrated with other enabling tools like data governance technologies and data access rights lifecycle management tools. This requires the ability for organizations to easily consume privacy insights and findings via APIs into their processes and workflows, and to be able to propagate business terms and categories to the personal information inventory. By connecting business context with personal data intelligence, enterprises can better achieve the outcomes of accuracy and accountability.

Integrate with Lifecycle Management

Most organizations have mature processes for dealing with compliance workflows and lifecycle management. Privacy regulations both add incrementally to the compliance, but also introduce a new set of workflows that must be operationalized across stakeholders and assessed in the context of a lifecycle.

For instance, enterprises should provide a portal for data access requests that can be automatically directed to the relevant IT teams, and then track the status of responses and report production against the timelines stipulated by regulations.

To ease automation across the data rights lifecycle, BigID provides companies a diversity of options as to where they can capture and manage data rights requests including leading workflow management tools and home-grown portals. Once a request is captured, BigID provides workflows to verify a request based on specific attributes and process a targeted scan by individual on demand. This can be done one by one or as a bulk process programmatically. The found data can then be used to report back to the consumer or employee with comprehensive customization features available for each business department to tailor their data rights reporting back to the individual or regulator. The individual data fields can also be selectively masked, so the process of fulfillment doesn't involve exposing personal data to the analysts completing the fulfillment tasks.

Data Governance and Business Glossary Integration

In many instances, it falls to the CDO's offices to operationalize privacy compliance. CDOs are also often responsible for helping organizations catalog their data and ensuring that business terms are consistently understood and relevant to stakeholders. Many organizations face the challenge of deciding what data categories qualify as personal information, and data catalogs can be a useful tool for enabling information stewards and business users to determine which data elements should be treated as personal information. In turn, these categories defined by business users can be applied via business glossary integration into found data elements in the personal data inventory.

Improving the accuracy of reporting and enhancing automation through bidirectional metadata exchange of data findings and data catalog business terms, categorization or data descriptions can help enterprises align their data governance and privacy operations. By mapping the business terms to physical and logical data elements represented in the inventory and then updating the data catalog when new data elements are discovered, enterprises can leverage the benefits of accurate data insights and business context to streamline data access rights processes.

Through programmatic integration with leading data catalogs, data governance and data lineage tools, BigID enables consistent workflow for data governance and privacy as well as drives higher accuracy and automation for data subject rights - including deletion requests.

Conclusions

For large enterprises with complex infrastructure and substantial data and application estates, it is essential to leverage technology that enables a clear understanding as to where data lives across the enterprise; maps data flows to illustrate how that data is moving between applications and systems, and with whom that data are shared; easily contextualizes all personal information across the company based on an individual consumer's identity; as well as facilitates quick organizational responses to consumer access and deletion requests; and provides privacy assurance for auditing purposes and defending against lawsuits and regulatory actions.

Without the assistance of purpose designed discovery, classification and correlation technology, large enterprises will find incredibly difficult to automate the process of understanding whose data they have and provide the accurate information at the scale required to respond to an influx of consumer requests. Without this foundation in place, enterprises will be in continual catch up mode, and cannot forge ahead with repeatable processes as new privacy requirements inevitably emerge.

Equally, enterprises require the flexibility to be able to translate how privacy requirements relate to their business, and their specific data estate. When data discovery and mapping is supported and supplemented by advanced data right managements, and can easily integrate with lifecycle management and data governance tools, enterprises can effectively operationalize and scale their data access rights initiatives and maintain privacy first business initiatives built on data insights. Without these elements, however, enterprises will not only contend with operational inefficiencies, but also face the risk of penalties and customer discontent.