1touch.io
Data Aware Security

1TOUCH.IO INVENTA & COMPLIANCE

FEBRUARY 2021

TABLE OF CONTENTS

GOOD BUSINESS SENSE IN PRIVACY REGULATIONS

The Internet provides fantastic business opportunities and is one of the driving forces behind unparalleled global economic growth. With more and more people transferring parts of their lives online, and the rise and pervasive nature of social media companies - privacy has become one of the most critical issues we face today. Customers and users increasingly want to know and control the personal information companies collect -and what they do with it.

Legislators have rescinded to these concerns: more than a hundred countries around the world have some version of privacy laws and privacy regulatory bodies. Because technology companies provide services and goods worldwide, they face unique challenges in adapting to privacy regulations across different markets and locations.

Private Data and Personal Data

Private data is data about people: it is either data that identifies an individual or data that we can use in conjunction with other data to identify someone. **Personal data** would be unique data that can identify a specific individual, such as an ID number. **Personally Identifiable Information**, or PII, is data that we can use to identify a specific individual when linked to other data pieces, such as a name and a physical address. Private data can include a name, physical address, email address, ID number, social security number, etc.

When we discuss private data, the discussion should include talk about the nature of the data, the medium of the data, and the technological and legal issues surrounding the acquisition, storage, use, and disposal of that data.

It is almost impossible for a technology company to avoid acquiring private data: many companies keep registration databases where users can register their names, email addresses, and sometimes physical addresses, credit card numbers. Unavoidable private data gathering is especially true for companies in industries such as healthcare, finance, and communications - which collect extraordinarily private and sensitive information about their customers.

Understandably, companies use the data they collect on their customers to drive business decisions. Companies base their pricing decisions, marketing decisions, future development plans, and more on their customers' behavior. Moreover - in many cases, customer data is the product, traded and used to increase business IP (e.g. YouTube, Facebook, etc.). It is therefore in the best interest of companies that this data would be accurate, accessible, and useful.

At the same time, customers might have conflicting ideas and interests regarding their private data: many people want to be able to know what private data companies collected about them. Others want the privilege to decide what happens to their private data, data that many people feel belongs to them somehow, even if they did not collect it and are not storing it themselves.

Companies need to develop strategies to protect customer information. Companies must also develop strategies on how to comply with privacy regulations. Regulators can impose fines that punish companies, but fines are not necessarily these companies' most significant concern. Customers may avoid companies that do not protect their privacy and do not handle their private information adequately. Private data management is not just a regulatory requirement: it's also a matter of trust. It is a business requirement in this current age: without private data management, businesses will not be able to attract and keep customers and grow.

Privacy regulation reconciles these competing interests by providing transparent guidelines to companies and consumers regarding what is allowed and prohibited. The regulations also specify what data customers can request from companies and even update and delete.

Complying with Global Privacy Regulations

There are many different laws and regulations governing data protection and privacy around the world. Some of the most impactful include the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). The GDPR governs data privacy for European companies and companies that collect information from European customers, regardless of where they operate or register. The EU is the largest economy globally, making the GDPR so important and influential, and many companies find it vital to comply with GDPR. The GDPR also influenced other later regulations, including the CCPA. However, even regulations influenced by or modeled on GDPR are not identical to the GDPR. For example, the GDPR and CCPA define personal information differently: CCPA regulation, which has more vague categories than the categories for private data in the GDPR, might define some pieces of information as private data.

When companies move into new markets, even when moving from the EU to the US or the US to the EU, localization and investment in implementing new regulations is necessary. Companies must justify the data they collect differently under different regulations, as well as change registration forms in response to changes in regulations. Sales and Marketing departments must adapt their techniques and approaches to how customers consent and what kind of prior notification is required.

Because data privacy status differs between countries, it might be prohibitively expensive to comply with all regulations over time. However, technology companies can't afford to ignore these regulations. Many regulations can impose very high fines, and reputational damage can be substantial.

PRIVACY & REGULATORY COMPLIANCE WITH 1TOUCH.IO

The purpose of privacy regulations is to provide transparency and control. Regulators try to describe to customers how companies collect private data, what type of private data they collect, and how it must be stored and protected. Privacy regulations also give customers tools to query companies regarding the private data they have collected and the ability to amend and even delete some of it.

In response to advances in data gathering technologies, some countries developed the "right to forget," where private individuals have the privilege to ask companies to delete, in essence, "forget," some of the private data they have collected.

Privacy Challenge	1touch.io Inventa Solution
Global Regulations	Up-to-date catalog with location of all personal data records & copies that can be controlled by customizable workflows
Customer Consent	Workflows for locating, editing, and/or deleting all instances and elements of customer data
Expanding Networks	Automatic scanning with up-to-date catalog that expands as network scope grows
Data Breaches	Pre-breach protection by identifying location of personal data and copies for enhanced security.
Post-breach Recovery	Support for full analysis of personal data movements and identification of all leak points

Designed for Privacy

1touch.io's Inventa allows companies to provide the best service they can to their customers by properly discovering, classifying and inventorying private data: using its proprietary scanning technology, Inventa delivers awareness of how and where private data enters the organizational network, how and where it is distributed, and where it is stored and copied. Sensitive data may be lost and/or privacy compliance violated without comprehensive knowledge of where sensitive information is across the enterprise.

Awareness of the locations of all copies of personal data records Is crucial to privacy regulation compliance: companies routinely copy and distribute data between repositories, operators, departments, and even partners and third-party contractors. Awareness of the location of all the copies of private data in the network is a prerequisite to any compliance with privacy regulations. Inventa provides real-time status of the location of all private records: all copies, all instances, all associated and partial data elements.

Because regulations allow customers to ask companies to amend or even delete their private data, companies must know where they store all the copies of this data. In some cases, an organization must provide customers with a full manifest of the private data the organization collected. Since companies can store private data in multiple locations and formats, maintaining an up to date catalog of private data in the network is vital.

Inventa allows companies to identify how and where private data flows into their network, as well as locating all private data element locations. This allows companies to fully control, change, and remove private data records per customer requests, fulfilling consent and control regulatory compliance. Inventa supports customizable consent workflows withing the system, which enable organizations to fully manage the process of customer control and consent of their private data records.

As companies grow, they introduce new products when they enter new markets, maintaining this catalog becomes more complicated. Many network mapping and data scanning solutions rely on manual or partially manual operations and do not scale up well.

Inventa offers unique automatic network mapping and data scanning features, which identify private data in the network and in organizational repositories. As organizational networks grow and new repositories and network elements are added, Inventa's scanners simply expand their scope, and Identify the personal Information entering and existing the new organizational components, maintaining an up-to-date catalog of all personal Information without resorting to manual discovery or additional installations.

Designed for Security

Data breaches are a severe threat to any organization managing sensitive data; they occur when malicious players access privileged information unlawfully. Even companies that invest heavily in cybersecurity are vulnerable to these attacks, as almost a third of data breaches involve phishing attacks.

A regulatory body examined not only the company's behavior before the breach, to check how it protected itself against such attacks, but also how it responded following the attack. Many companies respond to attacks by beefing up cybersecurity indiscriminately; however, without precise analysis tools like 1touch.io, companies are left in the dark regarding both the extent of the damage, and the appropriate response. Many companies will invest heavily in overzealous security on sensitive information, like financial records, while neglecting to shield personally identifiable information that malicious players can exploit. Companies do this because personal information is gathered in many different channels and points of contact, and stored over different systems, and in different ways – rendering it extremely difficult to both locate and protect.

Personal information Is vulnerable because companies do not protect the data in their organizational network in the same way they protected information shared outside the company. 1touch.io tools locate sensitive information in all instances, over the entire system – going so far as to analyze and monitor data exchanged over network nodes, providing total transparency and control over data dissemination.

Conclusion

Customers expose enormous droves of private data to commercial companies all over the world. Regulators responded to this by creating privacy regulations in over 100 countries. Companies find that they must invest time and resources complying with these regulations, which, although similar, still require localization and implementation.

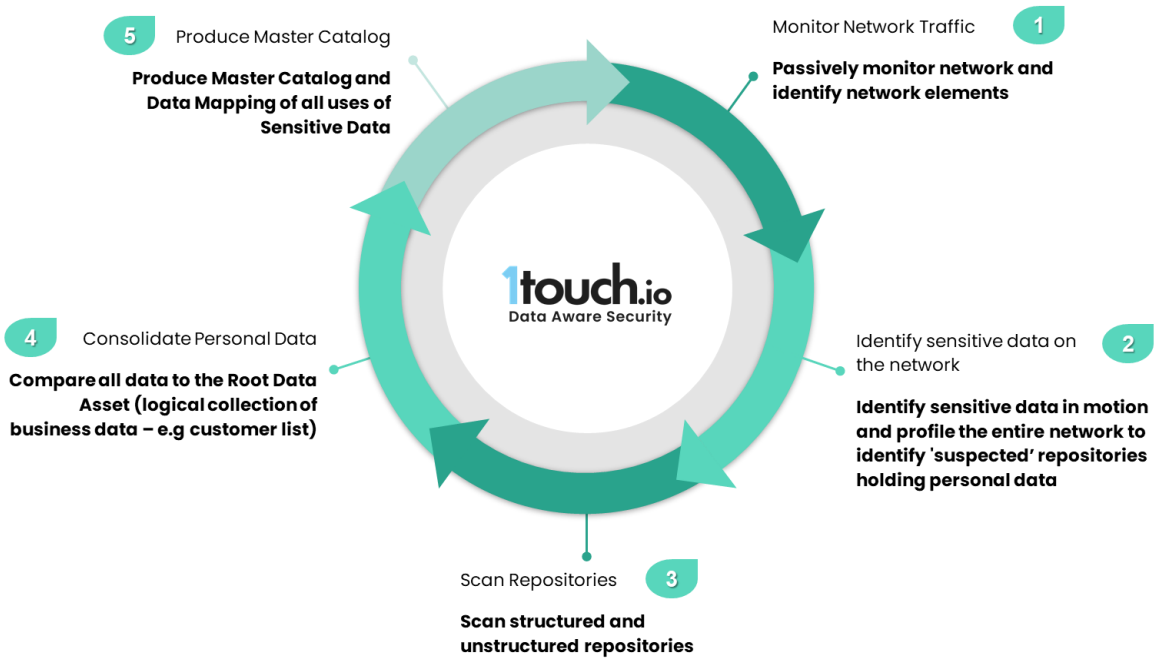
1touch.io Inventa offers companies a unique and flexible set of tools that scan and map private information across the organizational network and repositories, identifying the location of all private data records, copies, and partial elements.

Using Inventa, companies can easily adapt operational workflows to comply with existing, new, and updated regulations, as well as support all customer consent and control policies: ensuring compliance as well as customer confidence and satisfaction.

.

INVENTA 1TOUCH.IO

1touch.io Inventa™ uses a proprietary passive network packet capture process to discover personal sensitive Information stored and moving throughout the organizational network. This allows Inventa to identify repositories (databases, applications, file systems, log files, etc.) where sensitive data resides, and scan them to get full visibility into the depth and breadth of the data. Inventa™ then analyzes and consolidates the data identified by those scans into a structure that allows the user to access, view, and export this data to support a variety of business cases: responding to data access requests, identifying unauthorized data migration, implementing data minimization, alerting to exposure of sensitive data in unprotected locations, and more.



Inventa™ is the only network-based data privacy solution to implement data-in-motion and data-at-rest techniques to automatically discover information related to identities across a wide variety of structured and unstructured data sources.

Inventa™ creates a data subject-centric picture by correlating all discovered records back to the identity to which the information belongs.

This process allows Inventa™ to discover any sensitive data, whether it can be found on-premise or in the cloud, whether the data is structured or unstructured, and whether it is in motion or at rest, to create a master catalog

. Inventa™ leverages artificial intelligence and machine learning to consolidate and normalize identities to provide a unified view of sensitive personal data.

1touch.io uniquely uses network analytics to help your company discover both sensitive data and its use, even the data you didn't know existed.

1touch.io's Inventa is a data privacy platform with unprecedented data lineage techniques for data discovery and classification. Inventa gives companies complete visibility into their unknown usage of customer data by automating the discovery process and providing them with a comprehensive, accurate, and up-to-date master catalog. This visibility enables you to easily meet regulatory, compliance, and security requirements.