SYNTASA

DATA COMPLIANCE

The world's data is growing at a rapid rate. Experts estimate that there will be a 4,300 percent increase in annual data generation by 2020. Consumer-facing brands in particular have seen, and will continue to see, huge increases in customer data as shopping behavior continues to move online. Customer interactions with websites, mobile apps, advertisements, emails, and more generate troves of data every day.

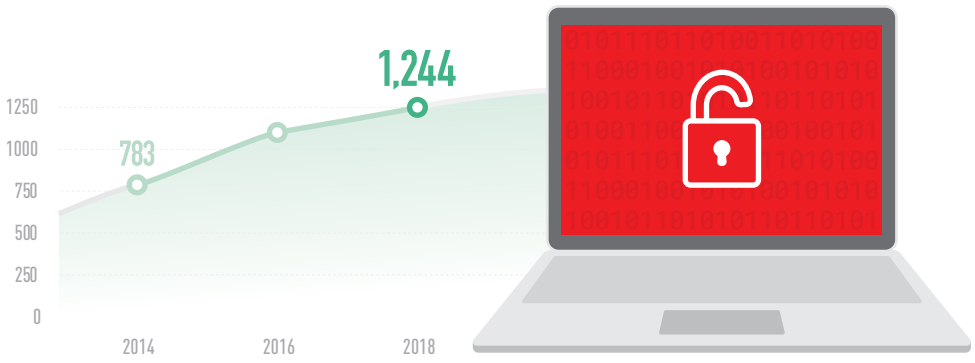
The volume of this behavioral data is precisely what makes this information so powerful for businesses, who can leverage it to create a 360-degree view of each customer, improve product recommendations, hone attribution models, and more. However, this data explosion also introduces potential privacy and security concerns that today's companies must anticipate and address.

Securing customers' personal identifiable information (PII) is particularly crucial. PII is "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means," according to the U.S. Department of Labor. Information that directly identifies a person includes one's name, birth date, home address, or phone number; indirect identifying information includes one's age, race, and gender.

Companies who do not properly secure PII can face significant negative consequences. First, and perhaps most obviously, they risk violating customer trust. They may also be subject to heavy regulatory fines under legislation like the California Consumer Privacy Act (CCPA) and the European Union's General Data Protection Regulation (GDPR), both of which aim to increase and protect individuals' data privacy and security. (It's important to note that these regulations apply to any company that does business in California or the EU, respectively.)

In addition, businesses without proper guardrails in place are increasingly vulnerable to cyber-attacks from criminals looking to steal PII. Such cyber-attacks are on the rise, with a reported 1,244 data breaches in 2018 vs. 783 in 2014, according to Statista. The average cost of a data breach in 2019 was $3.92 million, while mega breaches (>1 million compromised records) could cost businesses more than 10 times that ($42 million), and a breach of 50 million records could cost $388 million to resolve, according to IBM. Even a small business with few records could see losses in the tens of thousands.

Data breaches from cyber attacks



Average cost of a data breach in 2019: ***$3.92 Million***

Potential starting cost of a mega breach in 2019: ***$42 Million***

Costs of Non-Compliance

Business disruption

Data breach vulnerabilities

Productivity loss

Revenue loss

Fines/settlements

Data subject complaints

Erosion of public trust

SYNTASA

How Syntasa Can Help

Syntasa recently worked with a large bank based in the U.K. to prevent personally identifiable information (PII) from appearing in their Adobe Analytics fields. This was a persistent problem that the bank encountered as it processed Adobe Analytics data from 51 national markets.

Even with a rigorous data governance program, PII will inevitably end up in places where it's not meant to be. This can result from problems with a company's systems, but also user error. Customers may put a credit card number in a field intended for something else. Third-party affiliates might embed PII in URL parameters which then show up downstream in your company's analytics reporting. Given the range of potential missteps, it's important to have backup procedures in place.

In order to address this particular bank's concerns, Syntasa utilized a sophisticated pattern matching function that includes repetition and alternation in order to scan all data as it is ingested into Adobe fields. Syntasa screens for any PII — e.g., account numbers, phone numbers, and email addresses — that may have inadvertently made its way downstream. The system flags any information that is found, then overwrites and redacts it in production systems. In addition, Syntasa alerts analysts of the discovery, and makes the unredacted data available for the bank's data IT team in a quarantined environment. This system is now in place across all 51 of the bank's markets in order to ensure customers' PII is safe and secure.

Data is ingested using Hive function

Scanned for Personally Identifiable Information

Any PIIs that are found in tables get flagged

PIIs are overwritten and redacted

The Syntasa Platform

Data Compliance is just one of many uses of the Syntasa Customer Intelligence Platform. While many other compliance vendors are point solutions that will only solve that one specific problem, the Syntasa platform can handle multiple additional simultaneous use cases (like Journey Analytics, Personalized Recommendations, Algorithmic Ad Targeting, Churn Reduction, Algorithmic Attribution, and Fraud Detection) on the same up-to-date data.

Syntasa developed our Customer Intelligence Platform to deliver all of the capabilities you need to deliver intelligent customer experiences. It provides an integrated data + AI/ML + activation pipeline, along with a suite of products that ingests raw data, stitches activity for each individual, creates features, trains models, deploys algorithms to production, and activates them. It uses the concept of Apps (and the sequencing of these apps) to improve reliability and efficiency and accelerate time to value to provide a significant return on investment over home-grown solutions.

Importantly, the Syntasa Platform runs natively in your enterprise virtual private cloud, enabling you to keep your sensitive customer data inside your firewall.