Jordan Lawrence®

California Consumer Privacy Act

What's Your Exposure?

You can't avoid risks if you don't know they exist.

Private Right of Action for Any Violation

The recent CCPA amendment bill introduced by Senator Hannah Beth-Jackson and Attorney General Xavier Becerra would expand the private right of action rights available to residents under the CCPA. If approved, the amendment would allow consumers whose rights are violated to bring a private right of action against a business for a mere technical violation of the law or any slip up in fulfilling or responding to a data access request.

In addition, the proposed amendment would remove the 30-day grace period for enforcement actions for violations even if the business has "cured" alleged violations.

The Tipping Point for Plaintiffs' Attorneys

Savvy plaintiffs' attorneys are exploiting the rapidly changing data privacy and cybersecurity landscape. Private rights of action, statutory fines, and new theories of liability are supercharging litigation against companies of all types and sizes – and they never saw it coming.

Illinois' Biometric Information Privacy Act (BIPA) is a foreshadowing of what companies can expect to face under CCPA. A recent Illinois Supreme Court decision that damages do not need to be proven for an individual to file a private right of action has opened the floodgates to nearly 200 other class action suits that have been filed, primarily against employers. Unlike BIPA, which focuses on biometric data, CCPA has a broad definition of personal data, opening businesses up to even greater risk.

"To state a claim under BIPA, an individual is not required to show actual damages, but George says she nevertheless suffered an injury because the hotel violated her legal rights when it intentionally interfered with her ability to control her own sensitive biometric data and invaded her privacy." - Law360

California "Consumers" Includes Your Employees

If you have employees in California, they are part of your risk profile. The current scope of CCPA is not limited to only customers. It grants current employees, past employees, and job candidates that you didn't hire that are California residents the same rights as customers.

"While use of the term 'consumer' may suggest a particular type of relationship, the term is defined broadly to include any California resident – and as a result, in its current form the CCPA also will apply to information collected by covered businesses about their California employees." - Hunton Andrews Kurth

The Financial Risks Are Significant

Fines & Penalties Under the CCPA

Penalties for violations of the California Consumer Privacy Act remain unchanged under the proposed amendment:

- $100 to $750 per resident per incident or actual damages (whichever is greater).
- Injunctive or declaratory relief;
- Any other relief the court deems appropriate.

In addition, the California Attorney General can bring penalties of up to $2,500 for each violation or $7,500 for each intentional violation.

Calculate Your Potential Financial Exposure

When considering your potential exposure under CCPA, it's important to consider all of the "consumers" whose data you maintain – California residents who are customers, employees, employees' dependents, job applicants, volunteers, independent contractors, etc.

We developed a simple tool to calculate what your potential exposure might be under CCPA.

Example CCPA Exposure: Manufacturer

Current Employees:	4,200
Current Dependents:	16,800
Former Employees & Dependents:	15,000
Estimated Total:	36,000
12.5% California Residents: *Based on U.S. Census Data*	4,500
CCPA Statutory Damages:	$750 /violation

$3,375,000

Example CCPA Exposure: Retailer

Current Employees & Dependents:	2,100
Former Employees & Dependents:	3,000
Current & Former Customers:	100,000
Estimated Total:	105,100
12.5% California Residents: *Based on U.S. Census Data*	13,125
CCPA Statutory Damages:	$750 /violation

$9,843,750

Data Access Demands Trigger Litigation

Your Data Is A Discovery Minefield

The California Consumer Privacy Act removes the bar on discovery by granting California residents unprecedented access to their data held by companies along with a private right of action for any violation under the law.

Perhaps the greatest threat companies face under the CCPA are data access requests from residents exercising their rights and litigation that will be driven by the plaintiffs' bar.

- The right to request what personal information is being collected about them.
- The right to request the third parties with whom the business shares personal information.
- The right to know the business purpose for collecting or selling personal information.
- The right to request deletion of personal information.

Data Inventory Essentials

Companies that do not have a comprehensive and sustainable data inventory face a costly discovery nightmare and potential oversights when responding to data access requests that could spark unprecedented litigation. Companies that have taken a limited approach and only identified personal data in applications or databases fall short of their compliance obligations. You must know where your data is to protect it, delete it, report on it, or produce it.

Elements of an Effective and Defensible Data Inventory

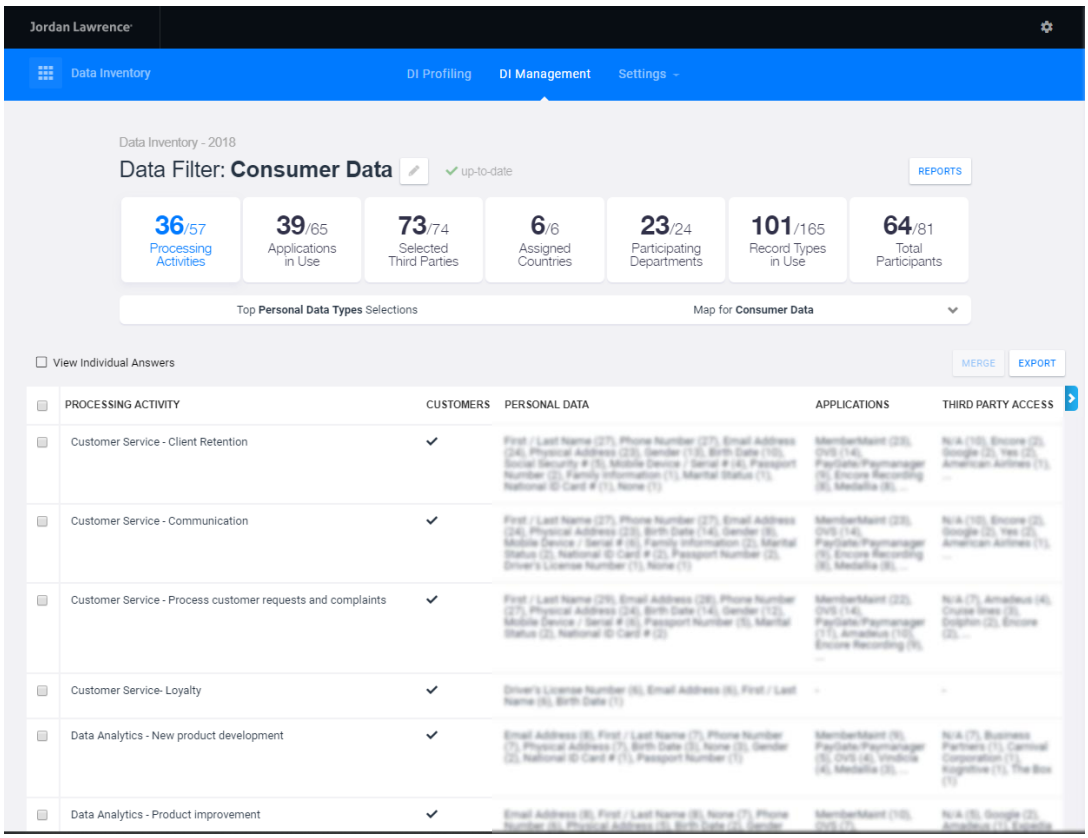
Your Data Inventory Informs Data Access Requests

In order to comply with the CCPA and be prepared to respond to data access requests in a compliant and timely manner, your data inventory should enable you to filter on specific data subjects and identify the following data points across the organization:

- What information is collected on specific data subjects.
- The specific types of personal data collected on data subjects.
- Where that information potentially resides across all locations and sources.
- The business purpose for collecting that information
- Third parties that access process or store that information.

How you develop and maintain your data inventory directly impacts your ability to comply and mitigate your risks. Data inventories managed using complex spreadsheets, Visio diagrams or empty-shell software are insufficient, unsustainable and don't provide a reasonable level diligence and compliance.

Example Data Inventory Filter: Consumer Data



A Defensible Path To Compliance

The January 1, 2020 deadline is fast approaching, and defensibility in your compliance processes is key. Enforcement for the CCPA is set to begin as early as July 1, 2020. However, there is a look-back period of one year – meaning a consumer can submit a data access request for their data held up to one year prior to the implementation date.

There are three foundational requirements the regulators and industry leaders agree companies must address effectively to demonstrate reasonable compliance and protect their companies:

1. KNOW YOUR DATA

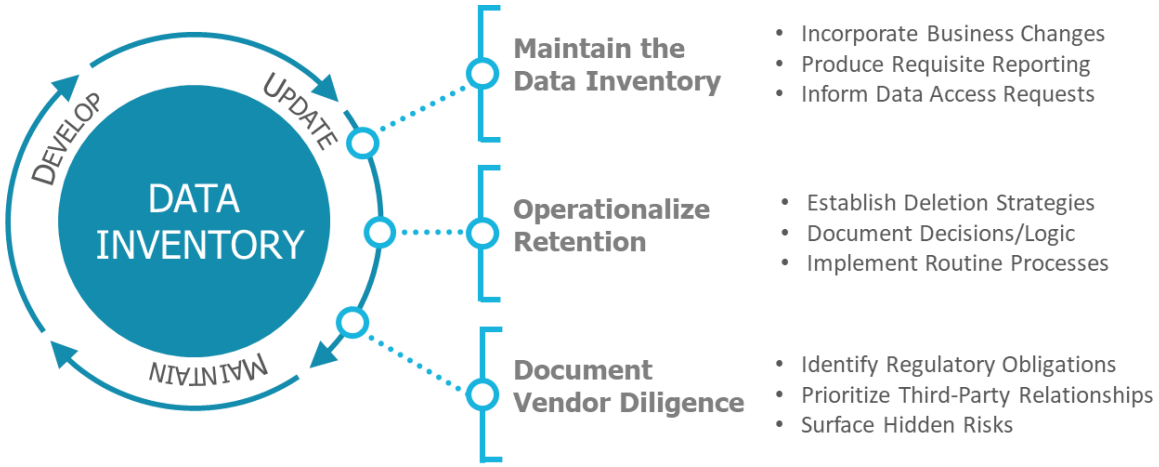
Develop and maintain a comprehensive and actionable data inventory that identifies personal and sensitive data across **all data sources** (not just what's in applications and databases). Identify and address where personal data are at risk and respond compliantly to data access demands.

2. KNOW YOUR VENDORS

Risk profile all third parties and vendors to identify those relevant to data privacy and cybersecurity regulations. Then assess those vendors' data security practices and ability to comply with data access and deletion requests. Demonstrate effective diligence, mitigate risks and avoid surprises.

3. ELIMINATE UNNECESSARY DATA

Connect personal data to retention requirements and operationalize deletion strategies across all data sources (email, paper, electronic) and eliminate unnecessary information. Personal data you don't have can't be breached and you don't have to produce it.



ABOUT US | Experienced. Trusted. Proven.

For over 30 years, Jordan Lawrence has been helping companies manage their information compliantly, defensibly and cost effectively. We work with many of the world's leading organizations to ensure they meet their obligations, mitigate risks, and reduce the costs of overall information compliance and control.

Legal, compliance, privacy and IT teams at the world's premier companies rely on us to help them meet domestic and international legal and regulatory obligations for data privacy and cybersecurity compliance, data retention and minimization, and third-party diligence. We leverage over three decades of deep domain knowledge, robust frameworks, proven standards, and a proprietary service delivery model to provide predictable, practical and defensible results for our clients.

Since 2005, Jordan Lawrence has been an ***ACC Alliance Partner of the Association of Corporate Counsel***. In 2018, we were appointed the exclusive ***ACC Alliance Partner for Data Privacy & Cybersecurity Compliance***.

Top law firms from around the world partner with us and leverage our services to provide clients the most comprehensive legal guidance available.

ACC ALLIANCE
Exclusive Savings for ACC Members

Exclusive ACC Alliance Partner for
Data Privacy &
Cybersecurity Compliance

CONTACT US FOR MORE INFORMATION

636.778.1700
services@jordanlawrence.com
JordanLawrence.com