

GROUND LABS WHITEPAPER

How Businesses Can Meet CCPA Compliance Requirements

The Index

01

What is the California Consumer Privacy Act?

- What types of businesses does CCPA apply to?
- What rights does CCPA give consumers?
- What personally identifiable information (PII) does CCPA protect?

02

Upcoming Updates with CPRA

03

Consequences of Noncompliance

- Financial consequences
- Early CCPA violation

04

Common Compliance Challenges

- COVID-19 implications
- Resources required for compliance

05

First Step to Achieving Compliance: Data Discovery

- The Power of Glass™

06

Importance of Establishing Ongoing, Widespread Compliance

- States that have enacted or are considering privacy laws
- Achieve compliance at scale

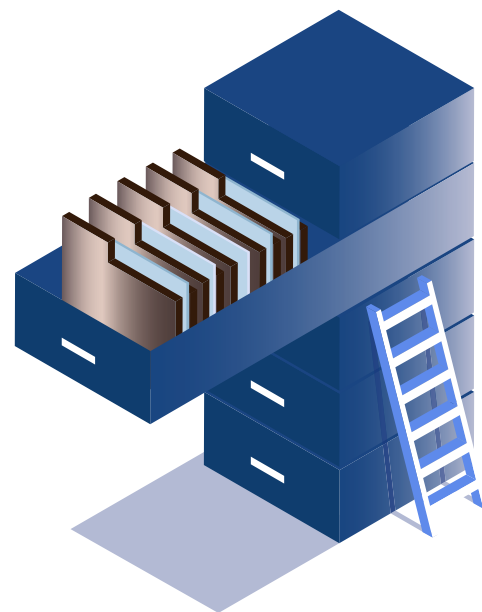
07

Data Mapping and Customer Trust

- The cost of trust

08

Conclusion



What is the California Consumer Privacy Act?

The California Consumer Privacy Act (CCPA) is a California state statute intended to enhance California residents' privacy rights. The state government passed CCPA in June 2018 and began enforcing it on July 1, 2020. Although several high-profile companies have already made headlines for violating this law, and California has been imposing fines, many companies are still not prepared to comply with CCPA.¹

On November 3, 2020, California voters approved Proposition 24, establishing the new California Privacy Rights Act (CPRA), the most comprehensive consumer data privacy law in the United States. Commonly referred to as the CCPA 2.0, the law amends the CCPA, and will be discussed in more detail in this whitepaper.

What types of businesses does CCPA apply to?

CCPA applies to for-profit businesses that do business in California and meet one or more of the following criteria:



Have a gross annual revenue of **over \$25 million;**



Buy, receive, or sell the personal information of **50,000 or more** California residents, households, or devices, or;



Derive **50% or more** of their annual revenue from selling California residents' personal information.²



Before you can achieve CCPA compliance, you need to understand the law's basics — what companies it applies to, what kind of information it protects, and what types of businesses need to comply. In this white paper, you'll find everything you need to know to understand CCPA and the compliance journey.

What rights does CCPA give consumers?

CCPA gives California residents the right to:



Know about the personal information a business collects about them and how it is used and shared



Opt-out of the sale of their personal information



Delete personal information collected from them (with some exceptions)



Non-discrimination for exercising their CCPA rights ³

What personally identifiable information (PII) does CCPA protect?

CCPA considers all of the following to be PII:

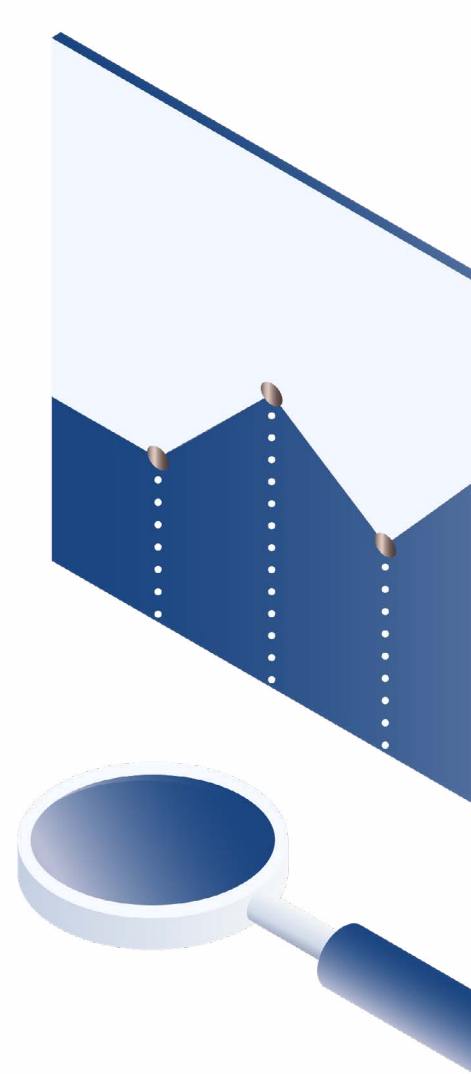
- Name & Social Security Numbers
- Driver's license numbers, tax identification numbers, passport numbers, military identification numbers, or other unique identification numbers issued on a government document commonly used to identify a person's identity
- Financial account numbers, credit card numbers, or debit card numbers if combined with any required security code, access code, or password that would allow someone access to your account
- Medical or health insurance information
- Fingerprint, retina or iris image, or other unique biometric data used to identify a person's identity ⁴



Upcoming Updates with CPRA

While the CPRA won't take effect until January 1, 2023, there are a number of changes that organizations will need to become familiar with. Here are some specific changes to pay attention to:

- **Employee and Independent Contractor Data:** Under the CPRA, the obligations of companies and organizations to protect the privacy rights of their employees and independent contractors is delayed until January 1, 2023. Originally supposed to be in effect in 2021, the CPRA expands the moratorium on employee and contractor data, providing the governing body and organizations to prepare
- **Redefining of Key Words:** One of the major changes is the redefinition to key words that focus on the meaning and scope of “business” and “breach” to apply to remove some of the ambiguity the CCPA had been criticized for
- **Establishment of California Privacy Protection Agency (CPPA):** The CPPA would create the first agency in the United States dedicated solely to privacy — the California Privacy Protection Agency. Comprising a five-member board, with expertise in privacy and data security, the CPPA will be in charge of creating public awareness about the upcoming amendment, as well as provide guidance to businesses and consumers. This governing body will be key to keeping privacy laws up to date over time enabling the law to remain current and applicable
- **Power of the CPPA:** The CPRA grants the governing body the authority to prevent future attempts by businesses to avoid or not comply with the CPRA. One of the major reasons for the creation of the CPRA was that the CCPA was targeted by businesses and lobbyists in an attempt to remove some of the “teeth” the law had. This nuance addresses this in the hopes of preventing business interference in the future ⁵



Consequences of Noncompliance

Businesses that violate CCPA could face significant consequences — both financially and reputationally. Although California enacted CCPA relatively recently, several large brands have already been fined and sued for not adhering to the regulations.

Financial Consequences

Fines range from \$2,500 to \$7,500 per violation, depending on whether the violation was intentional.⁶ The consequences of a data breach could be even more significant. After a data breach, under some circumstances, CCPA allows consumers to sue a company. They can file suit if their first name (or first initial) and last name were stolen along with any of the above PII, provided the company stored the PII in a non-encrypted and non-redacted form. Under CCPA, any consumers who are victims of this kind of data breach can sue the businesses for the amount of monetary damages they suffered from in the breach, or up to \$750 per incident.⁷



CCPA fines can range from
\$2,500 - \$7,500
per violation

Early CCPA Violations

Many high-profile companies have already received CCPA fines and lawsuits, such as Salesforce. In January 2020, a clothing company called Hanna Andersson announced hackers had stolen PII that it had hosted on Salesforce's e-commerce platform. Following this announcement, a Sacramento resident filed a lawsuit against both Salesforce and the clothing company, claiming they failed to secure and protect customers' PII.⁸

Another high-profile case occurred in early July 2020. A man in San Francisco filed a class-action lawsuit against Walmart in July 2020, just ten days after CCPA enforcement began. The man claimed Walmart was hacked and that his and hundreds of other Walmart customers' credit card numbers were stolen.⁹

Common Compliance Challenges

Although the July 1, 2020 CCPA enforcement deadline has already passed, many companies are still struggling to comply. A report published in mid-July found that 56% of companies were still not CCPA compliant, even after the July 1, 2020 deadline had come and gone.¹⁰

COVID-19 implications

COVID-19 could be one of the reasons why many companies might be struggling to comply with CCPA. In March 2020, the Association of National Advertisers (ANA) co-wrote a letter with more than 30 California and national trade associations. The organizations asked the California Attorney General to delay enforcement of CCPA, citing the COVID-19 pandemic as one obstacle impeding compliance.¹¹



The Attorney General's office responded to the letter the next day, saying it did not plan to extend the deadline.¹²

Resources Required for Compliance

CCPA is complicated, and meeting all of its requirements requires significant resources that some companies might lack. In a report, the California Department of Finance (DOF) estimated that initial CCPA compliance costs would equal \$55 billion across all companies.¹³ The DOF predicted initial costs would range depending on company size, and broke down the costs as follows:

Estimated initial compliance costs by company size



Less than 20 employees:
\$50,000



20-100 employees:
\$100,000



100-500 employees:
\$450,000



Greater than 500 employees:
\$2 million¹⁴

Businesses are lacking data awareness

Many companies assume that all of their customers' PII data is stored in one or two databases, but this assumption is typically incorrect. For example, if an employee emails a file that contains customer data, that data will be stored in multiple places: the original database, Excel, the employee's email outbox, the inbox of whoever the file was emailed to, and even backup databases, which organizations often forget about. If that customer requests that the company delete his or her PII, the company might only delete the data from the original database. However, the company will still have the consumer's PII saved in that employee's Excel file and email. This discrepancy could lead to CCPA violation fines, and even a lawsuit if the data is ever breached.

Companies unknowingly store PII in several locations



Cloud Storage
Providers



Databases
+ Servers



Email



Workstations

“

If that customer requests that the company delete his or her PII, the company might only delete the data from the original database. However, the company will still have the consumer's PII saved in that employee's Excel file and email.

This discrepancy could lead to CCPA violation fines, and even a lawsuit if the data is ever breached.”

Beginning Your Compliance Journey With Data Discovery

Once your business acknowledges it needs to gain compliance, you need to build a plan that outlines how you'll achieve and maintain compliance on an ongoing basis. Once you have this plan in place and have allocated the necessary resources and budget, you need to develop a baseline understanding of what data you have and where it resides: this is a process known as data discovery.

Understanding where your data lives will help you identify where your vulnerabilities are and what actions need to be taken to protect and remediate. In addition, data discovery can help you implement process changes to prevent sensitive or personal data from being misplaced in the future. None of this can be achieved without a full data discovery within the organization.

With Enterprise Recon by Ground Labs, organizations can find and remediate sensitive information across the broadest range of structured and unstructured data, whether it's stored on your servers, on your employees' devices, or in the cloud. Enterprise Recon enables organizations worldwide to seamlessly discover all of their data and comply with not only CCPA, but other important regulations as well, such as GDPR, PCI DSS, HIPAA, Australian Privacy, and more.

With Enterprise Recon, organizations can:



Identify more than **300 data types** of structured and unstructured data including pre-configured, CCPA-specific PII patterns



Accurately **map data across networks**, servers, and platforms to keep tabs on PII and more easily respond to consumer requests



Scan **immediately and fast** thanks to a low-impact distributed design, complementing and strengthening your data loss prevention strategy



Easily build custom data types and search platforms to locate and remediate unique data types to address **your organization's unique needs**



Demonstrate CCPA compliance with custom reporting and analytics **available in the Enterprise Recon**



Search within both structured and unstructured data sources including **files, databases, emails, cloud, big data** and more



Easily view and analyze the access permissions for sensitive data locations and **immediately take action to minimize risk** by managing and controlling access to those locations



Establish a 'Risk Profile' based on a **Risk Scoring feature**, enabling the tagging of high, medium and low data risks across your network




Execute a proactive approach to data security — as opposed to a reactive approach that relies on damage control post-breach — to **build a stronger foundation** of trust within your organization

The power of GLASS™

Enterprise Recon is powered by Ground Labs' proprietary discovery and pattern matching engine, GLASS™ Technology. GLASS™ Technology drives Enterprise Recon's industry-leading performance, versatility, and accuracy. The proprietary technology enables the most accurate data discovery across the broadest set of platforms, allowing organizations to find data they didn't even know existed, while easily and quickly deploying the solution in their environments and reducing false positives.

Traditionally, this level of comprehensive data discovery would take an organization years to accomplish and millions of dollars in resources to achieve manually. Even with a manual process, there's a high likelihood of missing data during scans. With Enterprise Recon, organizations can quickly and seamlessly get started on their first step to achieving data compliance.

	REGEX	GLASS™ TECHNOLOGY
Email Scan 	<code>\b[A-Z0-9._%+]+@[A-Z0-9]+\.[A-Z]{2,}\b.</code>	REFER 'PII_MISC_EMAIL'
Credit Card Scan 	<code>^(?:4[0-9]{12}(?:[0-9]{3})? # Visa (?:(?:5[1-5][0-9]{2} # MasterCard 222[1-9]22[3-9][0-9]2[3-6][0-9]{2} 27[01][0-9]2720)[0-9]{12} 3[47][0-9]{13} # American Express 3(?:0[0-5][68][0-9])[0-9]{11} # Diners Club 6(?:0115[0-9]{2})[0-9]{12} # Discover (?:(?:21311800 35\d{3})\d{11}) # JCB)\$</code>	REFER 'CHD_AMERICANEXPRESS' REFER 'CHD_DINERSCLUB' REFER 'CHD_MASTERCARD' REFER 'CHD_VISA' REFER 'CHD_DISCOVER' REFER 'CHD_JCB'

“After exhaustive due diligence and market alliance, we choose to partner with Ground Labs for meeting our PCI DSS obligations, through unmatched accuracy. Based on their expansive data discovery features in Enterprise Recon, we're also able to meet our growing needs for PII as well.”

— Angel Galvez Caballero, *Global IT Security Head at Dufry*

Importance of Establishing Ongoing, Widespread Compliance

CCPA will not be the only regional privacy law that companies need to manage. California has historically been a pioneer in progressive lawmaking, setting the example for many other states. For example, after California adopted low- and zero-emission vehicle regulations, many states, including Nevada, Washington, and Minnesota, followed its lead and set similar standards.¹⁵ Several states, including New York and Oregon, have also followed California's footsteps and adopted privacy regulations like CCPA.¹⁶

States that have enacted or are considering privacy laws



California



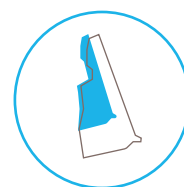
Illinois



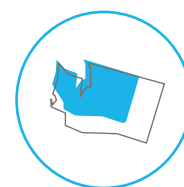
Nevada



New York



New Hampshire



Washington¹⁷

**Source: National Law Review*

Achieve compliance at scale

This trend means that staying privacy regulation-compliant is not a one-time checkmark; it's an ongoing obligation. CCPA regulations will change over time, and new states will continue to enact their own, separate privacy laws. Companies need to maintain compliance as regulations change and develop, or they will face hefty fines.

Enterprise Recon allows companies to reduce the overall time and investment required to reach and uphold CCPA compliance, even as regulations change over time. Ground Labs' tools enable companies to achieve compliance at scale, not just in California but with all users everywhere. If you're investing in tools to help you achieve compliance, it makes sense to use them at scale. For example, in November 2019, Microsoft decided to follow CCPA guidelines in every U.S. state.¹⁸

Data Mapping and Customer Trust

Ground Labs' Enterprise Recon allows companies to execute a proactive approach to data security instead of relying on a reactive strategy that involves post-breach damage control.

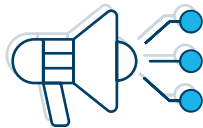
The cost of trust

When a company experiences a data breach, many customers lose trust and stop investing in the business. This customer loss adds up: a report found that, on average, the cost of lost business due to a data breach in 2020 was \$1.52 million.¹⁹

A CCPA fine might seem insignificant if the number of violations is low, but losing your customers' trust can have a devastating impact on your brand and shareholder and stock value. One report found

that more than 80% of customers in the U.S. said they would stop spending money at a business for several months after a security breach, and more than 20% said they would never return.²⁰

When your business is proactive about privacy and security and maintains an ongoing awareness of where data is stored, it builds a strong foundation of trust.



In 2020, the average cost of business loss due to a data breach was \$1.52 million.

Conclusion

Compliance is a journey, and maintaining it and approaching it holistically will positively impact your business' processes and workflows. Privacy regulations will continue to expand and change in the coming years. At the same time, the amount of data we need to manage, and our reliance on it will grow exponentially. As our data dependence grows, our need for data governance will amplify and become increasingly important for the success of organizations.

Data discovery is a cornerstone to knowing your risk and gaining compliance; an ongoing understanding of where all your data is stored is critical for achieving compliance with CCPA and will help you prepare for future privacy laws. California's recent amendments to CCPA and the upcoming CPRA deadline prove that compliance regulations are a moving target: your organization needs to have the proper tools and processes in place to keep up with regulations and stay compliant in the long term.

Your business has an obligation to your shareholders and customers. Proactive, ongoing compliance will mitigate risk and help you maintain that obligation, building stronger, trusting relationships with your employees, partners, and customers.

For more information on how to get started in your journey to CCPA compliance, please visit www.groundlabs.com

Sources & References

- ¹ Scott Ikeda, "New Report Shows That Most Companies Are Still Not Prepared for CCPA," CPO Magazine, July 17, 2020, <https://www.cpomagazine.com/data-protection/new-report-shows-that-most-companies-are-still-not-prepared-for-ccpa/>.
- ² "California Consumer Privacy Act (CCPA)," State of California Department of Justice, Section A5, <https://oag.ca.gov/privacy/ccpa>.
- ³ "California Consumer Privacy Act (CCPA)," State of California Department of Justice, <https://oag.ca.gov/privacy/ccpa>.
- ⁴ "California Consumer Privacy Act (CCPA)," State of California Department of Justice, Section A3, <https://oag.ca.gov/privacy/ccpa>.
- ⁵ Stephen Cavey, "CPRA and the Evolution of Data Compliance Risks," Risk Management, November 2, 2020, <http://www.rmmagazine.com/2020/11/02/cpra-and-the-evolution-of-data-compliance-risks/>.
- ⁶ Cynthia J. Larose, "CCPA QOTD: What Are the Penalties for Non-Compliance with the CCPA?," National Law Review, December 18, 2019, <https://www.natlawreview.com/article/ccpa-qotd-what-are-penalties-non-compliance-ccpa>.
- ⁷ "California Consumer Privacy Act (CCPA)," State of California Department of Justice, Section A7, <https://oag.ca.gov/privacy/ccpa>.
- ⁸ Daniel R. Stoller, "Salesforce Data Breach Suit Cites California Privacy Law," Bloomberg Law, February 4, 2020, <https://news.bloomberglaw.com/privacy-and-data-security/salesforce-data-breach-suit-cites-california-privacy-law>.
- ⁹ Aaron Nicodemus, "Walmart latest hit with CCPA-related lawsuit," Compliance Week, July 15, 2020, <https://www.complianceweek.com/data-privacy/walmart-latest-hit-with-ccpa-related-lawsuit/29192.article>.
- ¹⁰ Scott Ikeda, "New Report Shows That Most Companies Are Still Not Prepared for CCPA," CPO Magazine, July 17, 2020, <https://www.cpomagazine.com/data-protection/new-report-shows-that-most-companies-are-still-not-prepared-for-ccpa/>.
- ¹¹ "ANA and Others Ask for CCPA Enforcement Extension," Association of National Advertisers, March 18, 2020, <https://www.ana.net/blogs/show/id/rr-blog-2020-03-ANA-and-Others-Asks-for-CCPA-Enforcement-Extension>.
- ¹² David M. Stauss and Malia Rogers, "INSIGHT: Responding to CCPA Requests During the Coronavirus Pandemic," Bloomberg Law, March 27, 2020, <https://news.bloomberglaw.com/privacy-and-data-security/insight-responding-to-ccpa-requests-during-the-coronavirus-pandemic>.
- ¹³ "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," State of California Department of Justice: Office of the Attorney General, August 2019, http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.
- ¹⁴ "Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations," State of California Department of Justice: Office of the Attorney General, August 2019, http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf.
- ¹⁵ David Shepardson, "Nevada to join other states in adopting California zero emission vehicle rules," Reuters, June 22, 2020, <https://www.reuters.com/article/us-autos-emissions-usa/nevada-to-join-other-states-in-adopting-california-zero-emission-vehicle-rules-idUSKBN23U005>.
- ¹⁶ Issie Lapowsky, "New York's Privacy Bill Is Even Bolder Than California's," WIRED, June 4, 2019, <https://www.wired.com/story/new-york-privacy-act-bolder/>; Daniel J. Moses, "Oregon Amends Data Breach Notification Law to Include Vendor Obligations," National Law Review, June 12, 2019, <https://www.natlawreview.com/article/oregon-amends-data-breach-notification-law-to-include-vendor-obligations-expanded>.
- ¹⁷ Gretchen A. Ramos and Darren Abernethy, "Additional U.S. States Advance the State Privacy Legislation Trend in 2020," National Law Review, January 27, 2020, <https://www.natlawreview.com/article/additional-us-states-advance-state-privacy-legislation-trend-2020>.
- ¹⁸ Julie Brill, "Microsoft will honor California's new privacy rights throughout the United States," Microsoft, November 11, 2019, <https://blogs.microsoft.com/on-the-issues/2019/11/11/microsoft-california-privacy-rights/>.
- ¹⁹ "Cost of a Data Breach Report: 2019," IBM, 2019, <https://www.ibm.com/downloads/cas/ZBZLY7KL>.
- ²⁰ "Businesses facing post breach financial fallout by losing customer trust," Help Net Security, September 18, 2019, <https://www.helpnetsecurity.com/2019/09/18/post-breach-financial-fallout/>.