WHITE PAPER

PARADIGM™ technology | Informatica™

California Consumer Privacy Act (CCPA): A Roadmap to Compliance

EXECUTIVE SUMMARY

The California Consumer Privacy Act (CCPA 2020), which went into effect earlier this year, is certainly not the first legislation in this area. Over the past few decades, numerous legislations have been enacted to protect the privacy and personal data of consumers. Most notably these include the Health Insurance Portability and Accountability Act (HIPPA 1996), Gramm-Leach-Bliley Act (GLBA 1999), Health Information Technology for Economic and Clinical Health Act (HITECH 2009), Family Educational Rights and Privacy Act (FERPA 1974), and Protection of Pupil Rights Amendment (PPRA 1978). While these are sectorial laws focused on specific industries, CCPA is focused on **all** California consumer data and includes a carve-out for GLBA and HIPPA.

In this white paper is a technical roadmap of primary capabilities that must be implemented to meet CCPA. We see these capabilities as:

- Track and act on consumer requests.
- Understand what information is captured and what categories it falls under based on CCPA guidelines.
- Capture and document the process for complying with the law.
- Document the purpose and use of the information captured.
- Communicate the information to the consumer and provide the ability to request the removal of information.
- Capture consent of the consumer for the storage and use of their personal information.

Through a combination of partner tools and products provided by companies such as **Informatica**, cataloging data and its processes can be combined in a modular way to address each of these needs.

While the focus here is on California, many other states have proposed, rejected, or enacted similar regulations including, but not limited to, New York (S00224), Washington Privacy Act (SB 6281), Texas Privacy Protection Act (HB 4390), Maryland, Mississippi, New Mexico, North Dakota, and Rhode Island. Other states have enacted CCPA-like features, such as Nevada, which has an amendment to its online privacy law requiring businesses to offer consumers a right to opt out of the sale of their personal information.

It's important to note regulations are evolving, making it necessary to keep up to date on legislative changes. The Washington Privacy law failed but passed a subset dealing with public and private facial recognition. The failed law - akin to GDPR or CCPA - would have allowed individuals to request companies delete their data and was different in that adornment data did not require identification.

OVERVIEW OF CALIFORNIA CONSUMER PROTECTION ACT (CCPA)[1]

CCPA in a nutshell is the next evolution of consumer privacy rights which impact certain types of organizations that conduct business with California residents.

Why

In 1972, California recognized "privacy" as "an inalienable right" for all people. Multiple measures have since then been adopted, including the Online Privacy Protection Act, Privacy Rights for California Minors in the Digital World Act, and Shine the Light - a law intended to give California consumers more control over how businesses use personal information. But these were deemed insufficient by the California Legislature given technology developments.

What

The California Consumer Privacy Act allows California consumers to own, control, and secure their personal information. The location of the business is not a factor. If the information is specific to California consumers, the law grants:

- The right to know what personal information is collected, used, shared, or sold, both as to the categories and specific pieces of personal information.
- The right to delete personal information held by businesses and by extension, a business' service provider.
- The right to opt-out of the sale of personal information. Consumers are able to direct a business that sells personal information to stop selling that information. Children under the age of 16 must provide opt-in consent, with a parent or guardian consenting for children under 13.
- The right to non-discrimination in terms of price or service when a consumer exercises a privacy right under CCPA.

When

The bill went into effect January 1, 2020. There are two milestones to note:

- July 1, 2020 is the proposed deadline for final regulations from the California Attorney General.
- Six months after final regulations are issued (which may be sooner than July 1, 2020), the California Attorney General may bring enforcement action.

New milestones may be created as the regulation changes over time.

Who

If a company (based anywhere in the world) captures personal information on any California resident and meets any of the following criteria, they are impacted by CCPA:

- Has $25 million or more in annual revenue; or
- Possess the personal data of more than 50,000 "consumers, households, or devices;" or
- Earns more than half of its annual revenue buying or selling consumers' personal data.

Impact

Intentional non-compliance includes fines of up to $7,500 per violation and is enforced by the California Attorney General. Consumers also can seek damages for unauthorized sharing of personal information which can be between $100 to $750 per incident per consumer. Enforcement is subject to a 30-day "cure" period prior to fine assessment.

[1] "California Consumer Privacy Act (CCPA) - Fact Sheet." California Department of Justice.

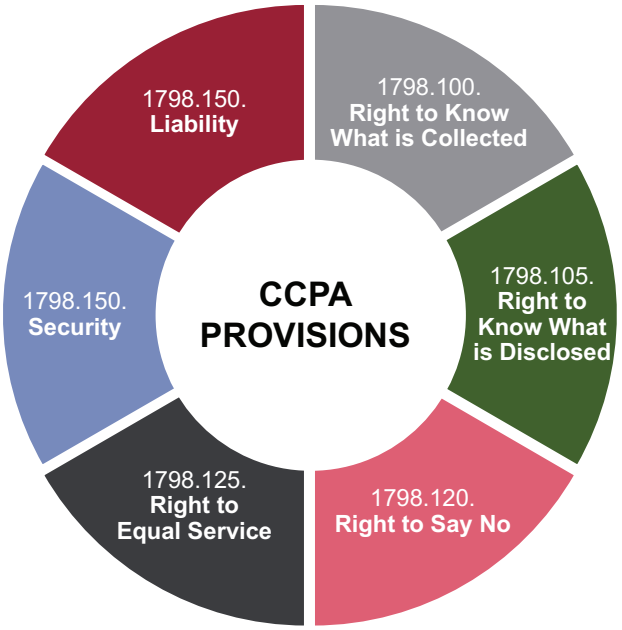
CCPA PROVISIONS[2]

The following is a high-level summary of key aspects of CCPA. The full regulation does change, and latest updates can be found within California's Legislative Information site.

Own Your Personal Information
CCPA empowers California consumers to know what information businesses are collecting about you, your devices, and your children including consumer personal identifiers, geolocation, biometric, internet browsing, and psychometric data.

Control Your Personal Information
Businesses cannot discriminate against consumers that have chosen not to have their personal information shared.

Secure Your Personal Information
Businesses are required to implement "reasonable" security measures. CCPA imposes additional fines over and above pre-existing legislation.



1798.100. Right to Know What is Collected
Consumers have a right to know the categories of personal data businesses have collected.

1798.120. Right to Say No
Consumers may "opt out" of allowing their personal information to be sold for any business purpose.

1798.150. Security
Businesses that own, license, or maintain personal information shall implement and maintain reasonable security procedures and practices to protect from unauthorized access, destruction, use, modification, or disclosure.

1798.105. Right to Know What is Disclosed
Consumers have a right to request disclosure from a business that sells personal information for a business purpose, including the category and identification of the person or business that received the information.

1798.125. Right to Equal Service
Businesses may not discriminate against any consumer that chooses to exercise their rights under CCPA. They may not charge different rates, deny goods or services, or deliver a different quality of goods or services.

1798.150. Liability
A business that suffers a breach involving consumers' personal information shall be in violation of the act and held liable.

ADDRESSING CCPA - TRIGGERS, RESPONSE, & CHALLENGES

Based on what is understood about the law, from a technical standpoint, identifying the information, processing requests, and identifying and cataloging the location and purpose behind the information's capture is necessary to begin to comply with the law. Key triggers prompting regulatory inquiry include:

- Data breaches: CCPA is not particularly nuanced about sensitive data and the California Department of Justice focuses on breaches/complaints and harm done.

[2] Title 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199]

- Number of complaints: An increase in the number of complaints.
- New technologies: Technologies like facial recognition require effective risk assessment for compliance.

Since the law came into effect, the California Attorney General has provided additional information including a second set of modifications to the proposed regulation. Even as rule-making activities move forward, there has not been a spike in what consumers request. This is an evolving space with a significant amount of uncertainty as new versions of CCPA are rolled out, including details around 'deletion' and what it means.

Receiving, Handling, & Tracking Requests

The most obvious need is the ability for the organization to interact and communicate with the consumer based on the requests. We are quite certain any company that must comply with the law already has a means to process consumers' requests. In processing said requests, statistics about the interactions and resolution, type, etc. can also be readily assembled and reported on. A dashboard to present the statistics, such as number and type of inquiry, the number of requests processed, and their current status would go a long way in satisfying a regulator's assessment of the organization's compliance with the law. The California Attorney General has built a data broker registry which supports the compliance check. Companies such as SayMine.com handle requests through a single process for data handling.

Operational Challenges

Successfully operationalizing the law involves verification of the individual for data identification, deletion, or enabling an opt-out request. Paradigm Technology has enabled this through data catalog development, such as **Informatica's Data Privacy Management**, which helps organizations identify Personally Identifiable Information (PII), Personal Health Information (PHI), and other sensitive data with ease. Additionally, our governance accelerator workflows - including defining a business rule, proposing new governance assets, and unsubscribing capabilities - enable our clients to further identify and handle data. Smaller companies that are unable to build a comprehensive infrastructure internally are managing this through service provider arrangements. Companies that hire third-party data brokers make managing requests an outsourced dialog between the consumers and the business with the service provider.

Whether handled in-house or through a third-party, some common challenges we've helped our clients overcome include:

- **Locating data:** It remains a difficult task for most organizations. Companies still struggle bringing the right data to the right person at the right time for activities such as analytics and marketing, let alone lawful compliance.
  - *Our experts helped a client identify, scan, and profile 200 data elements, 8.4 million variables, and 2.9 billion rows.*
- **Tracking and managing consent:** Usually this is nothing more than a webpage popup notifying the user of a website that their information is being captured and requesting an opt-in. What it does not necessarily do is capture that consent across the data and many systems that capture it.
  - *We simplified and automated a search for related information, reducing search time by 31%.*
- **Service level agreements (SLA's) and audit:** Documentation and proof that the request has been processed and completed are required for internal and external management of such data.
  - *Our data scientists enabled our client to track data lineage, perform data profiling, search data, and view data quality scores for a target quality increase of 28%.*
- **CCPA hotline messages:** Often they are unclear, and it can be difficult to identify the last name and email address which are essential with the obligation to follow up if the data isn't provided.
- **Data requests with specific look-back and restore needs:** These are different for varying industries and require clear policies covering data collection, data quality, management, purpose of usage, usage limitation, data security safeguards, openness, and individual roles and accountability.
  - *By enabling semantic search, the ability to search with meaning, we helped our client see an estimated 13% profitability increase.*

Capturing the Regulation & Process
What is less clear is how to capture more nuanced areas of the law, how they align with the data, and how to capture that information and associate the organization's policies as related to the law.

Fortunately, with greater focus on data governance, the tools related to handling and processing data can satisfy much of what is needed for CCPA. Products, such as **Informatica's Axon**, capture the policy and how it relates to the data collected by the organization. The law categorizes the types of data under its purview, such as Identifiers, select information in Customer Records, Legally Protected Characteristics, Commercial Purchasing Information, Biometric Information, Internet or Network Activity, ad Geolocation.

Mapping data captured across the organization's systems is a monumental task, but the ability to quickly track the location and type of information and where it is stored across the organization alleviates the regulator's concerns as to the organization's ability to understand and comply with the law.

CCPA vs. GDPR
Many of our global clients operating in both California and Europe are using governance and data cataloging products for CCPA and GDPR compliance. Below are areas where these products support both regulations:

- CCPA requires system level data identification. It's much smaller, with 21 sections versus 99 articles under GDPR.
- Shared components include data catalog, data provisioning processes, scan of systems and files, lineage, and effective data governance.
- GDPR is broader and focused on data governance and covering systems across multiple processes.
- GDPR contains international data transfer requirements and data control obligations.
- GDPR causes undue burden on smaller organizations; this is excluded in CCPA.
- CCPA has an exclusion to business information. GDPR does not differentiate between personal and business information.

Overall, both CCPA and the failed Washington Act pull from GDPR. California rulemaking is slowly evolving closer to GDPR.

PARTNER FOCUS - INFORMATICA

Pulling the information and statistics into a dashboard is a great way to track and present compliance. And, coupled with the data and organizational capabilities of Data Privacy Management and Axon, provides a quick means to link the consumer, their request, where their data is stored, and retrieve the exact information related to them from each system into a report. The report communicates back to the consumer as to what information the organization has and how it is used. Both the CEO and regulator benefit from a quick demonstration of the end-to-end compliance and that everything was done to adhere to the spirit of the law.

Master Data Management (MDM) and 360-degree views of the customer are desired by organizations to simplify and streamline their marketing and improve customer interactions. Products like **Informatica's Master Data Management** can pull together the organization's system view of the consumer and track their consent across all versions into a single, unified consent master. MDM adds another dimension to compliance and can easily link the consumer to all their data, though it may be captured differently across varying systems.

Axon's governance functionality allows both structured and unstructured data to be captured. Structured data is captured using automated scans such as **Informatica's Enterprise Data Catalog**, while unstructured or manual data is captured using a bulk uploads provision.

Axon can also capture business processes and manage process charts via BPML for owners and contacts who are responsible for the data under law, as well as document the process to provide and remove the information as required. In Axon Marketplace, data stewards and owners can publish datasets for users to search and browse the available data, then dive into the stored metadata descriptions and review the captured data files. Marketplace keeps an audit trail of requested information and data owner approvals thereby improving usage traceability over time.

CONCLUSION

There is no way to diminish the impact laws like CCPA and GDPR will have on companies that need to comply. Much of the data captured and used daily still needs to be brought under a consistent umbrella even before the law. A roadmap of technical capabilities along with products for data organization, identification, and mastering provide organizations the ability to comply with the law, and at the same time bring them closer to the data nirvana we would all like to achieve.

ABOUT THE AUTHORS

An award-winning end-to-end professional services organization, Paradigm Technology™ is a leader in digital and business transformation, working for 25 years with the Fortune 500. We partner with clients to understand and solve business problems through innovative, value-driven solutions and strategies. Our team leverages years of experience and leading-edge technologies to deliver intelligent insights to answer the hard questions to grow revenues, reduce costs, and avoid risk. We focus on delivering and communicating measurable value and impact above all else - that's the Power of Paradigm.

Informatica® is the only Enterprise Cloud Data Management leader that accelerates data-driven digital transformation. Informatica enables companies to fuel innovation, become more agile and realize new growth opportunities, resulting in intelligent market disruptions. Over 25 years, Informatica has helped more than 9,000 customers unleash the power of data. Data-driven digital transformations that Informatica can help businesses achieve include: Journey to Cloud, Reimagine Data Governance & Compliance, Deliver Intelligent Analytics Insights, and Unleash 360 Engagement.

PARADIGM™
technology

www.pt-corp.com | 480-473-7111 | info@pt-corp.com