MAPPING GUIDE

Imprivata FairWarning mapping to CCPA

as of 11/12/19

What is CCPA?

The California Consumer Privacy Act (CCPA) was signed into law in June 2018 and goes into effect in January 2020. This act grants California residents the right to know what personal information is being collected about them, who has that information, who is selling the information, and the ability to prevent the sale of their personal information and have it deleted upon request. Any for-profit business that processes residents' personal information, sells or exchanges personal information, and has revenues over a certain amount will be required to comply with CCPA or face fines, sanctions, and/or lawsuits.

What is the purpose of CCPA?

CCPA is designed to restore a sense of autonomy over personal data and privacy by giving Californians more ownership, control, and security. The Act enables California residents to request that a business delete any of their personal information collected from them and refrain from selling their data. Certain exceptions apply to the rules, and the law contains broad definitions and verbiage that leave room for future amendments, but the Act is a significant step in granting consumers a right to their own privacy and information.

Under the new legislation, Californians can access information including the data a business has collected about them, how they use and disclose that data, and more. Personal information, as defined by the new law, may include identifiers such as names and phone numbers, biometric information, geolocation, employment information, education information, and internet/network activity, among others.

Who does CCPA apply to?

A FOR-PROFIT BUSINESS IF IT:

- Does business in California
- Collects personal information of California residents or has residents' information collected on the business' behalf
- Determines the purposes and means of processing that personal information

Companies must also meet one of three criteria: (a) have annual gross revenue in excess of $25 million; (b) buys, receives, or sells personal information of at least 50,000 California consumers and households; or (c) derives at least 50% of its annual revenue from selling California residents' personal information.

Note: a business does not need to be located in California to be subject to CCPA. To exempt themselves from CCPA, a business must demonstrate that its "commercial conduct takes place wholly outside of California." However, the California civil and tax codes define doing business very broadly as "any transaction for the purpose of financial or pecuniary gain or profit in California." Therefore, a non-California-based business that has reoccurring transactions in California would be subject to CCPA.

What are the penalties for noncompliance?

The California Attorney General may bring actions for penalties of $2,500 per violation, or up to $7,500 per violation if intentional. However, CCPA allows businesses a 30-day period to cure (resolve) violations. Consumers have a private right of action of $100 to $750 per violation (or actual damages if higher) if their unencrypted and unredacted information is subject to unauthorized access, theft, or disclosure.

What are key takeaways of CCPA?

CCPA represents the broadest and most comprehensive privacy legislation in the United States to date. It grants California residents significant control over their personal information and requires compliant businesses to fully understand and document how they obtain, process, exchange, and protect California residents' personal information. In addition, CCPA is likely to influence other states to follow with their own privacy protection laws, and, potentially, federal privacy legislation.

What are specific rights given to consumers?

- **Access** – A business must inform the consumer of the categories of personal information collected and the purpose for which it was collected.
- **Disclosure** – A business must disclose the information categories and specific information items it has collected, sold, or disclosed upon a verifiable consumer request. A business must disclose the source of the information and the categories of third parties with whom it shared the information. Businesses must disclose this information for the preceding 12 months.
- **Opt Out** – A consumer can direct a business not to sell their information to a third party. Businesses must conspicuously display a "Do Not Sell My Personal Information" link and a straightforward process for a consumer to make that request.
- **Opt In for Children** – A business must not sell information about consumers between the ages of 13 and 16 without the consumers' explicit opt-in (consent) and must obtain parental consent before selling information about a consumer under the age of 13.
- **Deletion** – A business must delete information collected on a consumer upon receipt of a verifiable consumer request. CCPA specifies deletion exemptions that include information pertinent to legal obligations, free speech, or needed to engage in research.
- **Nondiscrimination** – A business cannot discriminate against any consumer who exercises their CCPA rights.

What is exempt from CCPA?

Medical information governed by the California Medical Information Act (CMIA) or Protected Health Information (PHI) covered under the Health Information Portability and Accountability Act (HIPAA). Covered entities (as defined by HIPAA) or CMIA "provider of healthcare" are also exempted if they maintain patient information to the level of how PHI is protected. Personal information covered by the Fair Credit Reporting Act (FCRA), personal information covered by the Driver's Privacy Protection Act of 1994 (DPPA), and personal information governed by the Gramm-Leach-Bliley Act (GLBA) are also exempt.

How do I work towards CCPA compliance?

Compliance with CCPA can be a daunting task. An approach that focuses on laying a foundation for a business's "culture of privacy" and addresses CCPA-specific elements is a strong and sustainable methodology.

LAYING A FOUNDATION FOR A CULTURE OF PRIVACY INCLUDES THESE STEPS:

- Conduct a Risk Assessment to gain a comprehensive view of where your organization currently stands in relation to its privacy and security practices. Frameworks from ISO and NIST are publicly available and can assist businesses in focusing on privacy and security controls, identifying vulnerabilities, and organizing their privacy and security protection efforts.
- Identify and classify your current data into severity levels (e.g., confidential, private – nonpublic, public). You cannot protect assets if you are unaware of them and you want to focus on your most essential data assets first.
- Identify and document how data flows into, through, and from your business. Know who you exchange information with and what you do with that information in your business.
- Train staff to understand privacy and security practices that are a critical part of their job (regardless of job title).

COMPLYING WITH CCPA INCLUDES THESE STEPS:

- Identify and document what CA consumer personal information your business has. Note that CCPA has a very expansive definition of personal information that goes beyond traditional identifiers such as name, Social Security number, email address, and account name.
- Identify and document how your business sells or exchanges CA consumer personal information with third parties. Determining if information is "sold" by CCPA definitions is critical. Businesses that sell personal information are required to post a "Do Not Sell My Personal Information" button prominently on their websites and then ensure a consumer's personal information is not sold once a customer exercises this right.
- Be prepared to delete consumer information if a consumer exercises this right and deletion does not fall into exemption categories. Investigate how the deletion will impact your business processes and remaining data sources.
- Train your staff on how CCPA will impact their jobs and how they can assist the business in being CCPA compliant.

How does Imprivata FairWarning assist with CCPA compliance?

IMPRIVATA FAIRWARNING FULFILLS OR PARTIALLY FULFILLS UPON THE FOLLOWING ARTICLES FOR CCPA:

Section 1798.100	Section 1798.110	Section 1798.120	Section 1798.140	Section 1798.145	Section 1798.150	Section 1798.175
Consumer right to know the personal information the business has collected	Consumer right to know if businesses are selling or disclosing information and to whom	Consumer right to direct businesses not to sell personal information	Broad definitions of key terms in CCPA such as “personal information” or “sell” of personal information	CCPA’s obligations and exemptions	Businesses’ duty to implement and maintain reasonable security procedures and practices	Provisions that afford greatest protection to privacy Applies to the collection and sale of all personal information (not just electronic)

Section	Requirement	Requirement description	Imprivata FairWarning Platform	Full or Partial support
1798.100	Consumer right to know the personal information a business has collected	This requirement gives consumers the right to know what personal information of theirs businesses have collected.	Imprivata FairWarning helps customers identify what systems contain personal information and other confidential data. During onboarding, Imprivata FairWarning’s expertise with data sources assists customers in gaining a more in-depth knowledge of their information assets. With this knowledge, businesses may map out their data assets and respond effectively to verifiable consumer requests to know what personal information the business has collected.	Partial
1798.110	Consumer right to know if a business is selling or disclosing information and to whom	This requirement gives consumers the right to know if their personal information is being sold or disclosed and to the categories of third parties receiving the information.	Imprivata FairWarning’s solutions assist customers in regularly monitoring what information their users (and third-party service providers) are accessing in each application. The solutions give insights into how data is being processed within a business and with whom it is being shared. The Imprivata FairWarning platform can aid in determining who has accessed what (documenting) and provide evidence to support establishing and changing access control policies if third parties are receiving information unnecessarily.	Full

Section	Requirement	Requirement description	Imprivata FairWarning Platform	Full or Partial support
1798.120	Consumer right to direct businesses not to sell their personal information	This requirement gives consumers the right to direct businesses not to sell their personal information and delete any personal information held.	Imprivata FairWarning enables customers to regularly monitor who is accessing their information. With this capability, a customer can determine what third parties are accessing information. If a consumer exercises their “Do not sell” right, the FairWarning solution can verify the request is fulfilled and information is no longer available to third parties.	Partial
1798.140	Broad definition of protected entities, personal information, and selling of information in scope of CCPA	This requirement provides broad definitions of several key elements of CCPA: • Who is protected – A natural person who is a California resident and protected in various roles (e.g., consumer, parent, children) • What personal information is – “Any information…that relates to…a particular consumer or household” • What is considered a sale of personal information – selling is “any disclosing or making available for monetary or other valuable consideration”	Imprivata FairWarning’s platform is architected to be robust, flexible, and accommodating for expansive regulations like CCPA. The platform enables the integration of multiple applications so the many types of personal information to be tracked can be added into the platform. The platform contains multiple pre-built analytics and custom report wizards that assist in tracking the “selling” (i.e., disclosing, transferring, making available etc.).	Full
1798.145	CCPA’s obligations and exemptions	Healthcare information subject to HIPAA or CMIA or personal information subject to GLBA, FCRA, or DPPA is exempted from CCPA. HIPAA Covered Entities and CMIA Providers of Healthcare are exempted if they maintain patient information as though it was subject to CMIA or HIPAA. It is important to note that HIPAA business associates are not included in these exemptions.	Imprivata FairWarning’s platform provides monitoring for potential data breaches as well as incident response tracking and management for multiple forms of sensitive data (not just PHI) or data subject to GLBA and other specified Acts. HIPAA business associates can use the platform both to maintain HIPAA compliance and fulfill on the newer compliance obligation of CCPA.	Full

Section	Requirement	Requirement description	Imprivata FairWarning Platform	Full or Partial support
1798.150	Businesses' duty to implement and maintain reasonable security procedures	CCPA does not directly specify what are "reasonable security procedures". It does specify that a right of action is possible for certain data breaches if the business failed to implement and maintain reasonable security practices and procedures.	Imprivata FairWarning's platform is a full lifecycle privacy and security incident management solution. It assists customers in managing incidents from alerting to investigation to governance across multiple applications containing personal information and other sensitive data. Information from Imprivata FairWarning may also be integrated into SIEM or GRC solutions as part of an enterprise-level risk management strategy. Use of this platform supports a businesses' assertion that they have reasonable security procedures. Moreover, Imprivata FairWarning can demonstrate how use of its solution maps to multiple regulatory standards and security frameworks. Mapping guides are available for the CIS CSC, ISO 27001, and the NIST CSF.	Full
1798.175	The provisions of the law that afford the greatest protection the right of privacy shall control Applies to the sale and collection of all personal information (not just electronic)	This requirement specifies that if CCPA conflicts with other CA laws, the law providing the greatest privacy protection shall prevail. The requirement goes on to specify that CCPA applies to all personal information a business may collect on a consumer (not just electronic or Internet-based).	Businesses may be subject to CA laws that have stronger privacy protections than CCPA. Rather than a checklist approach to complying with CCPA, businesses need to fundamentally support a "culture of privacy" within their organizations. With this culture, a business can become a leader in privacy excellence and instill trust and confidence among customers. Imprivata FairWarning's platform helps instill this culture in these ways: - Deploying privacy policies and procedures by identifying and monitoring the users accessing personal data, identifying and remediating inappropriate access to that information, supporting governance controls to support and maintain a privacy program, and demonstrating to staff that privacy protection is important to the business through training, ongoing access monitoring and remediation or disciplinary actions on privacy violations as needed. Imprivata FairWarning data may also be exported into SIEM or GRC tools as part of a business-wide risk management program. Imprivata FairWarning's platform is not limited to electronic information. Its alerting, investigation, and governance modules can also support privacy controls around high printing of paper records or equipment theft.	Partial

*Imprivata FairWarning only fully or partially fulfills the requirements above for the data contained in the applications integrated with Imprivata FairWarning.