# California Consumer Privacy Act mapped to NIST Big Data Public Working Group Privacy Fabric (Version 3 Volume 4 Page 34)

## CCPA: Individual Rights

**Disclosures about Sharing/Sale:** Individuals may request an accounting of the disclosures, including sale, of personal information made to third parties; this significantly expands upon the existing California “Shine the Light” law

**Opt Out:** Individuals may object to the sale of personal information about them

**Opt In:** Minors or their guardian must affirmatively authorize the sale of the minor’s personal information

maps to

## NIST Privacy Fabric:

INTERFACE BETWEEN BIG DATA APPLICATION PROVIDER →DATA CONSUMER

Data, including aggregate results delivered to data consumers, must preserve privacy. Data accessed by third parties or other entities should follow legal regulations such as HIPAA. Concerns include access to sensitive data by the government.

***Notes:*** *The Privacy Fabric does not explicitly describe the mechanisms and/or level of control that the data provider retains over the distribution of private data by the application provider. (HIPAA is only one use case.) The CCPA provides more details .*

## *CCPA: Individual Rights*

**Access:** Individuals may request disclosure of the specific data elements of personal information collected about them, categories of personal information collected, categories of sources, purposes for collecting or selling, and categories of recipients with whom the personal information has been shared

**Data Portability:** If the specific data elements of personal information are provided to the requestor electronically, to the extent technically feasible, they must be provided in a readily transferable electronic format

**Deletion:** Individuals may request to have their personal information deleted

maps to

## NIST Privacy Fabric:

INTERFACE BETWEEN DATA PROVIDERS → BIG DATA APPLICATION PROVIDER

Data coming in from data providers may have to be validated for integrity and authenticity. Incoming traffic may be maliciously used for launching DoS attacks or for exploiting software vulnerabilities on premise. Therefore, real-time security monitoring is useful. Data discovery and classification should be performed in a manner that respects privacy.

***Notes:*** *The Privacy Fabric interface is more focused on security than privacy. The CCPA provides more details about the capabilities needed to "respect privacy".*

## CCPA Transparency:

The online privacy policy or other web-based notice must disclose the categories of data collected, sources from which data is collected, purposes for which the data is used, categories of third parties with whom data is shared, information about individual rights and how to exercise them, as well as the data collected, sold, or disclosed within the prior 12 months. It is expected that policies in scope of CCPA will need to be updated annually.

## and CCPA Implement:

Implement individual rights mechanisms to effectively manage incoming requests

maps to

## NIST Privacy Fabric:

INTERFACE BETWEEN DATA PROVIDERS → BIG DATA APPLICATION PROVIDER

Data coming in from data providers may have to be validated for integrity and authenticity. Incoming traffic may be maliciously used for launching DoS attacks or for exploiting software vulnerabilities on premise. Therefore, real-time security monitoring is useful. Data discovery and classification should be performed in a manner that respects privacy.

***Notes:*** *The Privacy Fabric does not explicitly describe the feedback and request interfaces supplied by the application provider to the data provider.*

## Conclusion: All of the above notes are relative small but useful extensions to the Privacy Fabric to cover CCPA use cases. They could possibly be added as a future appendix.