California Consumer Privacy Act

On January 1, 2020, California will implement a sweeping new data privacy law that gives its residents the right to know (1) what "personal information" has been collected about them; (2) with whom it has been shared; (3) how it may be deleted; and (4) how to stop it from being sold. The California Consumer Privacy Act of 2018 (CCPA), is a significant shift in US privacy law and greatly impacts how covered businesses collect, use, store and share the "personal information" of all California residents.

The CCPA is expansive in scope, both in terms of substance and enforcement. It applies extraterritorially. The CCPA covers new forms of data such as IP addresses and internet browsing activity; defines "sale" broadly to include the exchange of "personal information" for not only monetary consideration, but for any "valuable" consideration; and provides for both regulatory enforcement and a private right of action. Certain provisions of the CCPA require covered businesses to update their external facing privacy notices with certain language and links. There are no express requirements for internal facing policies and procedures, risk management, or accountability. Compliance guidance is vague, leaving business leaders latitude in designing approaches that fit the business and customers.

"Personal information" defined

The CCPA defines "personal information" that which "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." The CCPA provides the following list of examples of personal information:

1. Identifier information, such as real name, alias, postal address, unique personal identifier, online identifier, IP address, email address, account name, social security number, driver's license number, passport number, signature, physical characteristics or description, telephone number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information, or other similar identifiers;
2. Characteristic information, such as race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status;
3. Commercial information, such as records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies;
4. Biometric information, such as fingerprint, iris scan, or geometric outline of face or body;
5. Internet or electronic network activity information, such as browsing history, search history, and information regarding a California resident's interaction with an internet web site, application, or advertisement;
6. Geolocation information, such as the location of the particular consumer or household;
7. Audio, electronic, visual, thermal, olfactory, or similar information;

8. Professional or employment-related information;
9. Education information; and
10. Inferences drawn from any of the above to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities and aptitudes.

For more information, please see the CCPA summary.