

Privacy Points 2023: Different Sensitive Personal Information Rights & Requirements Emerge in New US State Data Protection Laws

JANUARY 23, 2023

Colorado, Connecticut, and Virginia landed on requiring opt-in, prior consent before a business can collect sensitive personal information; while California and Utah landed on different forms of opt-out rights that allow initial collection without prior consent.

At the dawn of 2023, California and Virginia both had new data protection laws take effect. Soon, Connecticut, Colorado, and Utah will join their ranks as US states are quickly filling the void left [by a lack](#) of Federal and Congressional action on omnibus data protection reform.

To view our previous commentary on the effective dates and scope of the US state data protection laws, see [here](#).

While each state data protection law undoubtedly has substantive differences-such as the rights they grant to individuals residing in their respective states-they all have one point of overlap: the introduction of “sensitive personal information” into the US data protection regime.

Each state’s data protection law places greater requirements on the collection and processing of sensitive personal information, while also granting, in some form, rights to individuals to grant them more control over businesses’ collection and processing of their sensitive personal information.

For specific information on the categories of information that each state considers “sensitive” and the rights they afford to individuals, see more below.

What Constitutes Sensitive Personal Information?

While each puts forth slightly different, specific definitions, “sensitive personal information” can generally be understood to cover information that if breached by unauthorized third parties or improperly used, would or could cause significant harm to the individual.

- Sensitive Identifiers: Social Security Numbers, driver’s licenses, state / government identification cards, passport numbers
 - California
- Financial Data: Account log-in, financial account number, debit or credit card number in combination with any required security or access code, password, or credentials allowing access to an account

- California
- Location Data: Precise Geolocation
 - California (to within a radius of 1,850 feet or less), Connecticut (to within a radius of 1,750 or less), Utah (to within a radius of 1,750 or less), Virginia (to within a radius of 1,750 or less)
- Demographic Information: Race, ethnicity, religious / philosophical beliefs, sexual orientation
 - California, Connecticut, Colorado, Utah, Virginia
- Job-Related Data: Union membership
 - California
- Private Communications: Contents of mail, email, and text messages
 - California (unless the business is the intended recipient)
- Medical Data: Genetic, biometric, and health data
 - California, Connecticut, Colorado, Utah, Virginia
- Immigration Information: Citizenship or citizen / immigration status
 - Connecticut, Colorado, Utah, Virginia
- Children Data: Children's' personal data (under 13 years old)
 - Colorado, Connecticut, Utah, Virginia

As shown above, there is large overlap between the states in what is considered “sensitive” and warranting of higher protections or greater conferring of rights-such as demographic information, biometric data, health data, precise geolocation etc. However, there are important nuances as well.

For example, only California covers union membership status and private communications that the business was not an intended recipient of under “sensitive personal information”. Additionally, California also includes large swaths of financial-relates information (e.g., credit or debit card numbers) if they are collected in tandem with access codes, passwords, or credentials that would allow access to the funds and/or accounts.

The other four states-Connecticut, Colorado, Utah, and Virginia-have substantively identical definitions. The difference between California and the other four states exemplifies the different approach the legal regimes took.

California (i) implemented their data protection law in tandem with an amended data breach notification law; and (ii) included employee-related data in the scope of the data protection requirements. Therefore, the definition of “sensitive personal information” in California largely tracks with the definition of personal information as defined under most US state breach notification laws (e.g., sensitive identifiers, financial data) and include employee-related categories (e.g., union membership).

The other four states largely followed a European model (largely reflected in the EU’s General Data Protection Regulation), which is exemplified in the states’ inclusion of immigration information and children’s personal data in the scope of “sensitive personal information”.

It is important to note that while California does not include children’s personal information in the definition, California does require the prior consent for the sharing or selling of child’s personal information (for those under the age of 16).

In terms of health data, it is also important to note that all five states’ data protection laws also include some form of exemption if a company is covered by and required to comply with HIPAA.

Practically, a business that falls-or might soon fall-within the scope of all or most of the five state data protection laws should build out a sensitive personal information compliance program that covers **all** the above categories of sensitive personal information. Additionally, businesses that rely on the collection and processing of sensitive personal information will need to analyze how the new data protection laws-and the related data subject rights discussed below-will impact their business model.

What Rights Are Granted Over Sensitive Personal Information?

Although the definitions of sensitive personal information in each state generally overlap, the states differ on how businesses can collect sensitive personal information.

In summary, Colorado, Connecticut, and Virginia require opt-in, prior consent; while California grants individuals the right to limit the use of their sensitive personal information. Utah falls somewhere in the middle, and grants individuals the right to completely opt-out of the use of their sensitive personal information.

- California Right to Limit the Use of Sensitive Personal Information

California grants individuals the right to limit the use of their sensitive personal information to only that which is necessary. Essentially, the California right boils down to a limited opt-out right-meaning an individual can only opt-out of uses that are outside of their reasonable expectations.

Specifically, within 15 days of receiving a request to limit the use of sensitive personal information, a business must cease the use and disclosure of such information for purposes ***other than*** the following purposes: (i) performing services or providing products reasonable expected; (ii) to detect security incidents and to protect transmitted information; (iii) to defend the businesses legal rights and make lawful claims; (iv) ensuring the safety of others; (v) short term, transient use provided the information is not used by and disclosed to a third party for purposes of building a profile; and (vi) maintaining the quality or safety of the services and products.

The first exception is illustrative of California's limited opt-out approach. If an employee exercises their right to limit the use of their sensitive personal information, it does not prevent an employer business from disclosing and/or using that sensitive information to provide employee benefits as such is reasonable expected in the employee-employer relationship.

Under the California draft regulations, businesses are also responsible for information any third parties or service providers that have access to or that are processing the sensitive personal information of the request to limit.

- Connecticut, Colorado, Virginia Opt-In Requirement

Connecticut, Colorado, and Virginia take a simpler approach-albeit an approach that is more onerous on a business that collects and uses sensitive personal information.

These three states prohibit the collection and processing of sensitive personal information unless the business first obtains that individual's consent. This is in contrast to California and Utah's opt-out rights that initially allow the collection and use of sensitive personal information and rely on the traditional "notice and choice" regime that built the foundation of US privacy law.

Connecticut, Colorado, and Virginia, instead, track closer to a European-style privacy regulation in requiring on affirmative consent.

- Utah Right to Opt-Out of the use of Sensitive Personal Information

Utah falls in between California and the other states. Utah's data protection law grants individuals the right to fully opt-out of the use of their sensitive personal information.

Specifically, prior to processing an individual's sensitive personal information, a business must present the individual with (i) clear notice; and (ii) the ability to opt-out of the processing of their sensitive personal information.

Practically, this means building out a privacy policy or notice that clearly indicates the sensitive personal information collected by the business and the specific purposes it is used for. In tandem with this notice, there will need to be a consumer-friendly mechanism that allows the user to opt-out-likely in the form of a linked to form or configuration for businesses operating online.

Considerations Moving Forward

If your business collects and/or uses sensitive personal information a comprehensive review of how such information is used will be required if your business falls within the scope of any of the five US state data protection laws.

Additionally, privacy policies and procedures will need to be expanded on to properly provide clear notice to individuals so as to meet the various state laws' transparency requirements and to either meet the necessary opt-in consent or opt-out requirements.

As more states continue to implement their own variations of data protection laws and business juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.