HINSHAW

Alerts

# Here's How to Prepare for CPRA and Proposed VCDPA Requirements Concerning Sensitive Information

**February 11, 2021**
*Hinshaw Privacy & Cyber Bytes*

One of the most notable features of the new California Consumer Privacy Rights Act (CPRA) and the proposed Virginia Consumer Data Protection Action (VCDPA)—which has now passed both houses of the Virginia legislature—is the establishment of special categories of "sensitive" information. Those categories are broadly defined in both the CPRA and the proposed VCDPA, capturing a wide-ranging array of different types of information.

Under the CPRA, "sensitive personal information" is defined as:

(1) personal information that reveals:

> (A) a consumer's social security, driver's license, state identification card, or passport number;
> (B) a consumer's account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account;
> (C) a consumer's precise geolocation;
> (D) a consumer's racial or ethnic origin, religious or philosophical beliefs, or union membership;
> (E) the contents of a consumer's mail, email and text messages, unless the business is the intended recipient of the communication;
> (F) a consumer's genetic data; and

(2)

> (A) the processing of biometric information for the purpose of uniquely identifying a consumer;
> (B) personal information collected and analyzed concerning a consumer's health; or
> (C) personal information collected and analyzed concerning a consumer's sex life or sexual orientation.

The CPRA imposes additional requirements on organizations that collect or use sensitive personal information and grants special rights to consumers to limit the use of such information.

The proposed VCDPA states that "sensitive data means a category of personal data that includes:

## Service Areas

Privacy, Security & Artificial Intelligence

1. Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status;
2. The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
3. The personal data collected from a known child; or
4. Precise geolocation data."

Under the proposed law, organizations would be required to obtain consumer consent, defined as "a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement," before processing sensitive data.

The CPRA does not go fully into effect until January 1, 2023, the same date on which the VCDPA would go into effect, if signed by the Governor. Given the budgetary, operational, and organizational impacts associated with the implementing the requirements around sensitive information, however, organizations should begin taking steps to ensure timely compliance.

Here are some action items we encourage organizations potentially subject to these laws to implement:

- Understand current practices concerning the collection and use of sensitive information;
- Map current systems to understand where sensitive information resides and how it flows within the organization;
- Establish systems for quick retrieval and deletion of sensitive information;
- Ensure that appropriate cybersecurity safeguards are in place to protect sensitive information;
- Reevaluate whether the organization really needs to collect and/or utilize sensitive information in the first instance;
- Limit collection, use, and retention of sensitive information;
- Begin preparation of any required notices and consents;
- Implement systems to accurately track consumer consents;
- For CPRA-regulated organizations, prepare either a "Limit the Use of My Sensitive Information" link or a single, clearly-labeled linked that easily allows consumers to limit the use or disclosure of sensitive personal information.

The EU's General Protection Data Protection Regulation (GDPR), which went into effect on May 25, 2018, also contains additional requirements concerning the processing of "special categories of personal data," which is describe as "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."

Notably, the CPRA contains a lookback period for information collected after January 1, 2022.