July 10th, 2023

New US Privacy Rules For Sensitive Data: Key Items To Consider For The Rest Of 2023

by Richard Eisert and Zachary Klein

U.S. state privacy laws are multiplying at a dizzying rate.

The Virginia Consumer Data Protection Act, which came into effect on January 1, 2023, will be followed by the Colorado Privacy Act and the Connecticut Data Privacy Act on July 1, 2023 ("VA/CO/CT Laws"), the same date that the new California Privacy Rights Act amendments to the California Consumer Privacy Act ("CCPA") will become enforceable.

Finally, the year will come to a close with the Utah Consumer Privacy Act, effective December 31, 2023.

Amidst the flurry of new legislation, there are several requirements for collecting and processing "sensitive" information that may not be receiving enough focus in the ad tech ecosystem as most participants scramble to achieve basic compliance.

Here are the key points to know for the collection and processing of sensitive information for the rest of 2023.

Opt-in consent for Virginia, Colorado, and Connecticut residents

The VA/CO/CT Laws require prior opt-in consent to collect and process "sensitive data," which includes:

- Personal data revealing racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status;
- The processing of genetic or biometric data for the purpose of uniquely identifying a natural person;
- The personal data collected from a known child; and
- Under the Virginia and Connecticut laws (but not Colorado), "precise geolocation data," meaning information derived from technology that directly identifies the specific location of an individual within a radius of 1,750 feet.

Before collecting the above categories of personal information, companies that are subject to the VA/CO/CT Laws will need to provide consumers with separate and clear disclosures regarding their intended processing activities. Consumers will then need to take active measures (e.g., via a checkbox, toggle switch, etc.) to indicate their consent.

Originally published on www.adexchanger.com. All rights reserved.

While this may be straightforward when companies request data directly from consumers that they have a relationship with, other situations may create unique challenges. For example, in cases where data is collected automatically – such as precise geolocation data that websites gather through tracking technologies – companies may need to use pop-up banners or similar methods to provide disclosures and get consents.

Additionally, downstream participants that receive sensitive data from another party will need to ensure the disclosing party has obtained the proper consents.

The CCPA's "right to limit"

Under the CCPA, businesses that collect "sensitive personal information" ("SPI") may be subject to a new "right to limit the use and disclosure of sensitive personal information."

The scope of SPI under the CCPA is slightly broader than "sensitive data" under the VA/CO/CT Laws and includes, for example, social security numbers, state-issued IDs and certain financial account, payment card and account log-in information.

Consumers can restrict processing of SPI to only what is "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests" them, in addition to other statutorily permitted uses.

Businesses that collect SPI from consumers online for purposes that are subject to the "right to limit" will need to add either a standalone "Limit the Use of My Sensitive Personal Information" link at the bottom of their website homepage or an "Alternative Opt-Out Link" that serves as a combined "Do Not Sell" and "Limit the Use" link in lieu of posting two separate links.

Additionally, businesses will need to configure their websites to recognize opt-out preference signals not just for selling and sharing data, but also for requests to limit.

Utah's opt-out rule

In addition to the CCPA's right to limit and the opt-in consent requirements under the VA/CO/CT Laws, businesses should be mindful of the Utah Consumer Privacy Act's opt-out provisions.

Before collecting and processing "sensitive data" – a term that largely mirrors similar definitions in the VA/CO/CT Laws – companies must first provide Utah residents "with clear notice and an opportunity to opt out of the processing." Companies that are on track to follow the VA/CO/CT Laws and the CCPA by July 1, 2023, should be in good shape to adapt their compliance programs to meet Utah's opt-out requirement.

Data protection assessments

Finally, companies that are subject to the VA/CO/CT Laws will have to conduct a data protection assessment prior to commencing any processing activities that involve sensitive data.

The assessment must "identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with such processing, as mitigated by safeguards that can be employed by the controller to reduce such risks."

Companies must keep such assessments on file and be prepared to submit them to the attorneys general of Virginia, Colorado or Connecticut, if requested.

California is in the preliminary rulemaking process for its own CCPA "risk assessment" requirements, which will likely share some similarities with the VA/CO/CT Laws. However, Utah's law makes no mention of assessments, and there is no indication that Utah will require them in the future.

The bottom line

In short, companies in the ad tech ecosystem need to carefully evaluate whether they collect and process sensitive information and be mindful of the above requirements – and the nuances under the various different state laws – if they do.

Richard Eisert is co-chair of the Advertising + Marketing Practice Group and a partner in the Privacy + Data Security and Intellectual Property + Media Practice Groups of Davis+Gilbert LLP. He may be reached at

Zachary Klein is an associate in the Privacy + Data Security and Advertising + Marketing of Davis+Gilbert LLP. He may be reached at

DAVIS + GILBERT

Follow Davis+Gilbert LLP and AdExchanger on LinkedIn.