THOMPSON HINE

Privacy & Cybersecurity Update

October 2023

Major Changes to California Privacy Laws

California has enacted some of the most comprehensive and stringent privacy laws in the United States, and it recently enacted a series of bills aimed at providing even greater data privacy rights and protections for California residents. Recently, California Governor Gavin Newsom signed into law a series of bills that expanded "data deletion" rights for California residents, established new obligations for data brokers, and broadened the scope and applicability of the California Consumer Privacy Act (CCPA).

The Delete Act and New Data Broker Obligations

The CCPA grants California residents (also known as "consumers") with various privacy rights, including the right to request that a business delete personal information about the consumer that the business has collected from the consumer. However, the CCPA does not specifically provide Californians with the right to request that a "data broker" delete their personal information and, the Delete Act, which was signed into law by Governor Newsom on October 10, is intended to address that scenario and other privacy issues related to data brokers.

A "data broker" is defined as a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." This definition, however, has several exceptions and excludes from its scope entities that are covered by certain federal and state laws governing healthcare, financial, and insurance industries.

The Delete Act requires the California Privacy Protection Agency (CPPA) to create an "accessible deletion mechanism" that, among other things, allows a consumer to request that every data broker that maintains any personal information about them to delete that personal information upon request. This mechanism must be accessible online without charge to consumers, and it must allow a consumer, or a consumer's agent, to submit a single verifiable deletion request that data brokers can access via the mechanism. In addition, consumers will have the option to customize their deletion request and "selectively exclude" data brokers when submitting a deletion request in the mechanism.

The Delete Act: Key Dates
• **January 31, 2024**: Data brokers must comply with enhanced registration, disclosure, and reporting requirements. • **January 1, 2026**: The CPPA must develop a "deletion system" that allows residents to make a single data deletion request to multiple data brokers. • **August 1, 2025**: Data brokers are required to access the deletion system at least once every 45 days to review and process new deletion requests and delete any new personal information collected about residents who have already submitted deletion requests. • **January 1, 2028**: Data brokers must undertake an independent external audit every three years to certify their compliance with the law. • **January 1, 2029**: Data brokers need to disclose their audit results while registering annually with the CPPA.

Data brokers must access the deletion mechanism at least once every 45 days to review and process deletion requests. All such requests must be completed within 45 days of receiving the request. The CPPA will also have the

option to charge a fee for data brokers to access the deletion mechanism "that does not exceed the reasonable costs of providing that access." If a data broker denies a deletion request as unverifiable, the data brokers must still process the request as a Do-Not-Share and Do-Not-Sell request. Data brokers will be required to direct all its service providers and contractors to take similar steps for deletion or opt-out processing.

Data brokers must register with the CPPA (as they previously had to register with the California attorney general), and they are now required disclose, among other areas, the following to the agency:

- Metrics related to the number of privacy requests it processes and to other compliance obligations under the law,
- Whether it collects personal information of minors, precise geolocation data, and reproductive health care data, and
- A link to its website privacy policy, which must address data privacy rights and processes.

Starting January 1, 2028, data brokers will be required to undertake an independent external audit every three years to certify their compliance with the law. Data brokers will need to maintain records of any compliance audit for at least six years and submit audit results to the CPPA within five business days after receiving a request. Data brokers also will need to disclose their audit results while registering annually with the CPPA, beginning January 1, 2029.

If data brokers fail to comply with the Delete Act, they could be liable for fines up to $200 per day plus expenses. The Delete Act does not provide for a private right of action.

Expanding the California Consumer Privacy Act

In 2020, California residents approved Proposition 24, known as the California Privacy Rights Act of 2020 (the "CPRA"). The CPRA sought to expand the privacy protections within the CCPA in several ways. For instance, the CPRA grants California residents the right to direct a covered business to limit its use of "Sensitive Personal Information" to only certain purposes set forth in the law and future regulations and requires these covered businesses to comply with certain notice and transparency obligations related to Sensitive Personal Information. The term "Sensitive Personal Information" is defined as personal information that reveals sensitive data about a consumer, such as their social security, driver's license, state identification card, or passport number; precise geolocation; racial or ethnic origin; religious or philosophical beliefs; and union membership.

With the recent enactment of California Assembly Bill 947 (AB 947), the definition of Sensitive Personal Information now includes a person's "citizenship or immigration status." Accordingly, disclosure by a consumer of information that reveals a consumer's citizenship or immigration status is afforded the same heightened protections under the CCPA as other Sensitive Personal Information.

The CCPA includes several exceptions to when an organization needs to comply with the CCPA's requirements. For instance, the CPRA amended the CCPA to provide that the CCPA shall not "restrict" an otherwise covered business's ability to "[c]ooperate with a government agency request for emergency access to a consumer's personal information if a natural person is at risk or danger of death or serious physical injury," provided however that (1) the request is approved by a high-ranking agency, and is based upon a "good faith determination" that the agency has a lawful basis to access the information on a nonemergency basis, and (2) the agency agrees to petition a court for an appropriate order within three days and to destroy the personal information it received if that court order is not granted. This is commonly known as the "Emergency Access" exception.

AB 1194 was recently enacted into law, and it provides that "a consumer accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including, but not limited to, abortion services" is not considered a person who is "at risk or danger of death or serious physical injury" for purposes of the Emergency Access exception.

AB 1194 also provides that business *cannot* rely on several of the exceptions and exemptions within the CCPA, including the Emergency Access exception, and therefore must comply with the CCPA's requirements with respect to personal information related to an individual accessing, procuring, or searching for services regarding contraception, pregnancy care, and perinatal care, including

abortion services. Although AB 1194 limits when businesses cannot invoke exceptions to the CCPA in these circumstances, it does not alter the CCPA's non-applicability framework with respect to personal information that is aggregated and deidentified.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)
216.566.5646, 202.263.4126
Steve.Stransky@ThompsonHine.com

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Marla M. Izbicky
Certified Information Privacy Professional/United States (CIPP/US)
312.998.4253
Marla.Izbicky@ThompsonHine.com

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com