

Will Employers Have More Obligations Beyond the CCPA if these California Privacy Bills Pass?

June 1, 2022 – *The TMCA*

by Melonie S. Jordan and Gabrielle Wirth



Related People

- Melonie S. Jordan
- Gabrielle Wirth

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

California employers have navigated the ever-changing privacy landscape when it comes to employee and personnel personal information (“human resources data”). For years, California employers’ obligations were narrow in scope compared to covered businesses’ broader obligations to consumers under the California Consumer Privacy Act (“CCPA”). The California Privacy Rights Act (the “CPRA”) expanded these obligations and set a deadline for employer compliance by January 1, 2023. Now, with two pending privacy bills on the horizon, California employers may need to meet additional obligations in 2023 and beyond.

As previously shared, employers already have existing obligations under the CCPA regarding human resources data – the personal information of a job applicant, employee, owner, director, officer, medical staff member, or contractor of a covered business collected and used (1) in the context of the covered business’s relationship with the employee or personnel, (2) to maintain emergency contact information on file, or (3) to administer benefits. Under the CCPA, California employers must provide a notice to employees and personnel describing the categories of human resources data to be collected and the purposes for which the categories shall be used.

By the time the CPRA goes into effect on January 1, 2023, California employers will need to have revised the notice to meet three broader obligations.

First, the notice must disclose whether the employer sold the human resources data. California employers should keep in mind that CPRA broadly defines “sale” – if a California employer receives monetary or “other valuable consideration” for “selling, renting, disclosing, disseminating, making available, or otherwise communicating” human resources to a third party, the notice must disclose this as action as a sale. *Second*, the notice must describe the retention period that applies to the human resources data. California employers can meet this obligation by describing either (a) “the length of time the business intends to retain each category of personal information, including sensitive personal information,” or (b) “the criteria used to determine that period” provided that the human resources data is not retained for longer than is necessary for the disclosed purpose. *Third*, the notice must disclose categories of “sensitive personal information” as a separate category if the information is collected or processed with “the purpose of inferring characteristics” about the employee or personnel. “Sensitive personal data” includes, among other things, a Social Security, driver’s license, state identification card, or passport number; an account log-in, financial account, debit card, or credit card number in combination with credentials needed for access to the account or cards; precise geolocation; racial or ethnic origin, religious or philosophical beliefs, or union membership; mail, email, or text messages contents unless the business is the intended recipient; and, genetic data (this would likely mean that the notice should disclose that certain sensitive personal information is submitted to the Department of Fair Employment and Housing should Senate Bill 1162 pass). California employers can meet the broader CPRA obligations by January 1, 2023 by taking steps now.

Aside from broadened obligations under the CCPA and the CPRA, California employers may need to account for two privacy bills when collecting and processing human

resources data should the bills become law.

Assembly Bill 1651 (“AB 1651”), coined as the “Workplace Technology Accountability Act,” seeks to build upon the CCPA and CPRA regarding human resources data. Introduced by Assembly Member Ash Kalra, AB 1651 seeks to “impose various duties on employers and their vendors regarding the ability to collect and use worker data, as defined.” The proposed definition of “worker data” includes “any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular worker.” “Worker data” includes some categories of data already covered by the CCPA and CPRA, such as biometric information, but also includes “human resources information” such as a personnel file or performance evaluation.

Like the CCPA and CPRA, AB 1651 would require California employers to provide a notice “at or before the point of collection” that informs workers about the specific categories of worker data to be collected, the specific purpose for which the specific categories of worker data are collected or used, and whether and how the data is related to the worker’s essential job functions. However, the AB 1651 enlarges the CCPA and CPRA by generally prohibiting “audio-visual monitoring of a workplace in a worker’s residence, a worker’s personal vehicle, or property owned or leased by a worker” unless that audio-visual monitoring is strictly necessary to accomplish compelling purposes. The bill also generally prohibits electronic monitoring systems that incorporate facial recognition, gait, or emotion recognition technology. AB 1651 further requires employers or vendors to submit to the labor agency a summary of its uses of algorithms, also referred to as “automated decision systems,” and to complete an algorithmic impact assessment before using the system to make or assist an employment-related decision. The bill has been met with criticism from several groups, including the California Chamber of Commerce. AB 1651 was referred to the California State Assembly Committee on Privacy and Consumer Protection last month, but was later withdrawn from consideration prior to a hearing in the Assembly’s Committee on Labor and Employment. The bill currently sits with the Committee on Privacy and Consumer Protection.

California employers may have additional obligations under Senate Bill 1189 (“SB 1189”), which also seeks to build upon the CPRA by further refining obligations for biometric information. Introduced by Senator Bob Wieckowski, SB 1189 seeks to require private entities in possession of biometric information, as defined, to develop and make available to the public a written policy. The proposed definition of “biometric information” includes a “faceprint, fingerprint, voiceprint, retina or iris image, or any other biological characteristic that can be used to authenticate the individual’s identity.” Human biological samples used for valid scientific testing or screening and information captured by a health care provider under the federal Health Insurance Portability and Accountability Act are not covered by the proposed bill.

Similar to the CPRA, SB 1189 would require California employers to develop a retention schedule and guidelines for destroying biometric information by earliest of (a) the date on

which the initial purpose for collecting or obtaining the biometric information is satisfied; (b) one year after the individual's last intentional interaction with the private entity; or (c) within 30 days after the private entity receives a verified request to delete the biometric information submitted by the individual or the individual's representative. Should the bill pass, California employers would need to develop this policy by September 1, 2023. SB 1189 was referred to California Senate Appropriations Committee last month. At the May 19, 2022 Appropriations Hearing, the bill was taken under submission.

Will California employers have more obligations beyond the CCPA and CPRA if AB 1651 and SB 1189 pass? Yes. In addition to supplementing the CCPA/CPRA required notice, California employers will need to expand the notice to include worker data as defined by AB 1651 and to assess workplace monitoring systems and any use of algorithms.

California employers will also need to revise retention schedules to set clear guidelines for destroying biometric information. For now, California employers will need to wait and see if these bills become law. In the meantime, the CCPA/CPRA-required notices should be revised in preparation for January 1, 2023. Additionally, other states have introduced similar legislation. National employers should monitor pending legislation in Minnesota, New York, Washington, and Virginia.