Summary: Worker Rights Under the CCPA/CPRA

November 21, 2023

UC BERKELEY LABOR CENTER

As of January 1, 2023, workers at large for-profit companies in California are covered by the California Consumer Privacy Act (CCPA/CPRA). The law covers employees, independent contractors, and job applicants.

This is the first time that workers in the U.S. have basic rights around their workplace data. They will know when employers are surveilling them and for what purpose. They will be able to get access to their data and ask to correct or delete it. They will know if employers are profiling them or buying data about them, like social media activity. And they will be able to opt out of employers selling their data. These provisions are an important first step in making sure that workers have the tools necessary to advocate for their rights in the 21st century data-driven workplace.

Workers have the right to know when their employers are collecting data on them

Employers must inform workers about any personal information they collect about them.

- Notice must be given **at or before** the point that the employer starts collecting the data.
- Personal information means any data that can be linked to an individual worker, like personal IDs, demographics, employment-related data, biometric data, social media data, geolocation data, audio data, and inferences made about the worker's characteristics and abilities.

Specifically, employers must give workers a notice describing:

- The categories of **worker data** they collect
- The specific **business purpose** for the data collection
- Whether the data is **sold or shared**, and how long they intend to keep the data
- What **rights** workers have under the CCPA/CPRA.

Employers can't collect data for purposes other than those stated in the notice, or change their purpose for the data collection, without first providing additional notice to workers.

Workers have the right to get access to their data

Workers have the right to request the data that their employer has collected about them.

- This includes data that the employer has sold, shared, or disclosed.
- The employer must comply with a request within 45 days, free of charge. If the employer has a website, workers must be able to make a request on it.

Specifically, employers must disclose:

- The categories of **data** it has collected about the worker in the last year
- The categories of **sources** from which that data has been collected
- The business **purpose** for the data collection, selling, or sharing
- The categories of worker data it **sold, shared, or disclosed** to third parties
- The categories of **third parties** to whom the employer has sold, shared, or disclosed the worker data
- The **specific pieces of data** it has collected about the worker in the last year, in an accessible format.

The employer must include worker data collected by third parties (like labor subcontractors).

Workers have the right to correct and delete their data

Workers have the right to request their employers delete their data or correct inaccurate data.

- The employer must comply with the request within 45 days, and notify all third parties to do so as well.
- If the employer denies a deletion or correction request, it must provide a detailed explanation to the worker.
- Note there are significant exceptions to the deletion requirement.

Workers have the right to opt out of employers' sale or sharing of their data

Workers have the right to opt out of employers selling or sharing their data to third parties such as data brokers.

- Similarly, **third parties** that control an employers' worker data can't sell or share that data unless the worker has received notice and been provided the opportunity to opt out.

Workers have the right to limit employers' use of their sensitive data

Workers have the right to direct their employer to limit use of their sensitive personal data to authorized business purposes. This right to limit is only for cases when the employer is using the data to profile the worker.

- Examples of sensitive worker data are Social Security numbers, union membership, genetic data, race/ethnic origin, health/medical data, biometric data, sexual orientation data, religious beliefs, and emails not meant for the employer.
- Authorized business purposes are identified in the regulations, but have not yet been specified for workplace applications. Some purposes do translate, like data security, physical safety, administrative data processing, and other concepts that could potentially include workplace functions such as performance monitoring.

If an employer uses or discloses workers' sensitive data for other purposes, it must first provide notice to the workers and give them the option to opt out.

General employer responsibilities

- Employers **must limit the collection, use, and sharing of worker data** to what is "reasonably necessary" to achieve the purposes for which the data was collected or processed.
- **Third parties (labor subcontractors and service providers)** that control the collection of an employers' worker data are bound by the same regulations as the employers.

Worker recourse and enforcement

- Workers can have an **authorized person or organization** make a data request on their behalf, **including unions or worker centers**.
- Employers can't retaliate against workers for exercising their rights under this law.
- Enforcement will be done by the California Privacy Protection Agency (CPPA) starting July 1, 2023, for violations occurring on that date forward. Workers do not have a private right of action for violations of the rights listed above (but they do have the right to sue the employer for negligent data breaches.)

This summary was prepared by the Technology and Work Program at the UC Berkeley Labor Center; it does not constitute a legal analysis. For more information, contact Annette Bernhardt, annette.bernhardt@berkeley.edu.