Privacy Act Exemptions

Employee and Business-to-Business Information Must Be Permanently Exempted from Privacy Rights Act to Avoid Unintended Consequences

In 2018, the Legislature enacted the California Consumer Privacy Act (CCPA). The CCPA is a comprehensive consumer privacy law that applies to businesses of all sizes and affects almost every industry. It created five privacy rights for consumers:

- Right to delete data.
- Right to know what data is collected.
- Right to opt-out of data being sold.
- Right against retaliation for exercising rights under the CCPA.
- Right to sue for data breaches.

Passage of the CCPA was contingent upon the revocation of a then-pending ballot initiative sponsored by Californians for Consumer Privacy. Negotiations to have the statute passed through the Legislature meant the CCPA was opened to input from a broader group of legislators and stakeholders, and generally faced a lower amendment threshold so that it could be updated over time. The result was the first comprehensive consumer privacy statute in the United States, and one of only a handful around the world.

Since then, similar statutes modeled after the CCPA have passed in Colorado and Virginia. Similar legislation has been proposed in more than 20 states, including New York and North Carolina.

California Privacy Rights Act

Following up on their success in 2018, proponents of the CCPA qualified and won voter approval of Proposition 24 in 2020, which created the California Privacy Rights Act of 2020 (CPRA). The CPRA revised CCPA by:

- Extending the exemptions for employee and business-to-business information until January 1, 2023.
- Creating a right to correct data.
- Expanding the right to delete data to any third parties, service providers, or contractors that accessed the data.
- Expanding the right to know what data is collected to include the right to access specific pieces of information and the purpose for which personal information is being sold or shared.
- Expanding the right to opt-out by creating a new category of information, called sensitive personal information (SPI) and the right to direct businesses to limit use of SPI.

CONTEXT BEHIND EMPLOYEE AND BUSINESS-TO-BUSINESS EXEMPTIONS

In order to understand the policy issues related to the employee and business-to-business exemptions, it is important to understand the context of this conversation against the text of the CCPA. Because employee-employer relationships and business-to-business relationships are fundamentally different from relationships between businesses and consumers, the drafters exempted information related to these relationships from the consumer rights created in the CCPA.

The CCPA was not designed to be applied to employee and business-to-business information, but because the definition of "personal information" was broad enough to capture these relationships, exemptions were drafted into the statute.

Why Employee Exemption Is Necessary

The CCPA was designed to apply only to consumer "personal information," defined as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly, or indirectly, with a particular consumer or household." The definition of "personal information" also includes a consumer's "professional or employment-related information."

Thus, the exemption exists to prevent this broad definition from capturing information that falls outside of the consumer context. For an employer, this means the CCPA does not apply

CalChamber

Agenda for California Recovery

2022 Business Issues and Legislative Guide

See the entire CalChamber 2022 Business Issues and Legislative Guide at www.calchamber.com/businessissues
Free PDF or epub available to download.

Special Thanks to the Sponsors
Of the 2022 Business Issues and Legislative Guide

Major

AUTOMOBILE CLUB • SOUTHERN CALIFORNIA • AAA

Silver

CSAA Insurance Group,
a AAA Insurer

to all the information found on an employee's computer or work phone, all information found in their physical office or workspace, all handwritten materials or Post-it notes, and any other information that potentially falls under the broad umbrella of "personal information" as defined in the CCPA.

Such broad application creates tremendous legal consequences for both employers and employees, and would cause the CCPA to conflict directly with existing laws and rights. In many cases, state and federal law require employers to collect employee information; thus, applying the CPRA's privacy rights is fundamentally inconsistent with existing laws and policies designed to protect workers.

Indeed, courts have even acknowledged limited rights to privacy when using employer-issued computers or email software. *See*, for example, *Holmes v. Petrovich Development Co., LLC*, 191 Cal. App. 4th 1047, 1068-70 (2011) (employee emailing personal attorney on her work computer was akin to talking to them in a "conference room[], in a loud voice, with the door open"). Accordingly, the employee exemption was placed in the CCPA.

Why Business-to-Business Exemption Is Necessary

Similarly, there is also a separate exemption for business-to-business information. Businesses that contract with one another for products or services need the flexibility to exchange relevant information in order to carry out contracts and daily business functions. The definition of "personal information" in CCPA and CPRA is broad enough that it captures much of this business-to-business information.

Thus, in order to avoid shutting down the daily operations of businesses with overwhelming compliance obligations, certain business-to-business information was exempted from much of the CCPA's application. The exemption applies to information that allows businesses to conduct business transactions with one another when no individual consumer is involved.

Specifically, the exemption applies to "personal information reflecting a written or verbal communication or a transaction" between the business and an employee or contractor of another business where the communication or transaction occurs in the context of a business conducting due diligence on another business, or the business providing or receiving a product or service to or from such organization. This would include, for example, information contained in emails between two companies regarding a purchase order or contract.

Small and large businesses rely on this exemption to carry out regular day-to-day operations and tasks, examples of which range from supply chain and logistics to retail operations to producers of digital media and content. This exemption also allows businesses to carry out philanthropic, good-will work with efficiency. Similar to the employee information, CCPA's framework does not make sense in this context and would give people the right to request access to proprietary information or delete pertinent documents.

Why the Sunsets Exist

For the above reasons, stakeholders agreed upon separate exemptions for employee and business-to-business information in order to avoid nonsensical results and conflicts with existing laws. An agreement was reached to include the current exemptions for employee and business-to-business information. Due to the nature of the negotiations, stakeholders added a sunset to both exemptions to give the Legislature time to address employer and employee data issues separately, but to date, no solution has been presented.

The CPRA extended the sunsets from January 1, 2021, to January 1, 2023. If the exemptions sunset, applying the CCPA to employee and business-to-business information will create serious issues for employers, workers, policymakers and the judiciary.

EVEN WITHOUT CCPA, EMPLOYEE DATA IS PROTECTED UNDER THE LABOR CODE

Even before passage of the CCPA, California law provided workers with certain rights regarding employment-related documents. These protections are memorialized in the Labor Code and are separate from the CCPA. This means that the exemption for employee data in the CCPA has no effect on employee data protections.

Thus, even if there was no sunset on CCPA's exemption for employee data, employees would retain these protections under the Labor Code. For example:

- **Right to Access**: payroll records (Labor Code Section 226), personnel records (Labor Code Section 1198.5), documents signed by employee (Labor Code Section 432).
- **Right Against Retaliation**: unlawful to retaliate for exercising rights (Labor Code Sections 1024.6, 1102.5; Government Code Section 12940(h)).
- **Right to Correct**: may correct contact information, employment status, Social Security number, etc. (Labor Code Section 1024.6).

CONSEQUENCES IF EMPLOYEE DATA NOT EXEMPTED

The CCPA does not apply to employees' "personal information" because the results would be untenable. An employee should not have the ability to request access to all their personal information, requiring the employer to go through thousands of electronic and physical documents, including every email ever sent or received by the employee or even containing their name; paper

files; payroll records; and notes and objects in physical offices. For any employer that has experienced electronic discovery for litigation, even limited electronic searches and reviews cost thousands of dollars and take hundreds of hours to complete. Putting this burden on employers is impractical and does not align with the true purpose of the CCPA: to provide consumers with more control over their personal information in their relationships with businesses.

For example, an employee considering filing a claim against their employer could use the consumer right to know as a means of side-stepping civil discovery rules. Use of the consumer right to know also could lead to the disclosure of proprietary information or communications that normally would be protected under privilege, such as the attorney-client privilege, because there are no limitations in the CPRA to protect that information from disclosure.

Additionally, the right to delete would be problematic as well. Granting this right to employees would create a nearly unfettered right to delete emails or other files. An employee who has acted inappropriately toward others in the workplace should not be allowed to demand deletion of any incriminating emails, texts, or instant messages. Continuing the exemption will assure that evidence will be retained in any future litigation or investigation.

Applying this right to delete in the employer-employee relationship conflicts with existing laws that require employers to maintain certain documents and records. Determining which law governs would become a question for the courts to decide. This would put judges in the position of policy makers. These layers of statutory conflict would also leave employers confused about their legal obligations under the CCPA as opposed to the California Labor Code, federal record-keeping requirements, and agency regulations.

Another example is the right to correct, which is not limited to information that can be factually verified. Without the exemption, employees would be allowed to correct any information they deem to be inaccurate. Whether a piece of personal information is "inaccurate" would be subjective to the employee and could conceivably include investigations or performance reviews.

The above issues are just examples of the consequences that affect both employers and workers. It is evident why other states with CCPA-styled privacy laws or pending bills have chosen to permanently exclude employee data. Because the CCPA's framework is inappropriate in the employee/employer context, the employee exemption should remain in place indefinitely.

CALCHAMBER POSITION

The California Chamber of Commerce supports extending the employee and business-to-business exemptions permanently. To the extent the State wishes to address the subject of employee privacy or employee data, that issue should be addressed through a separate statutory framework. Permitting the January 1, 2023 exemptions to expire would have serious unintended negative consequences that would harm both workers and employers.

Staff Contacts
Ashley Hoffman
Policy Advocate

ashley.hoffman@calchamber.com

Ben Golombek
Executive Vice President and Chief of Staff for Policy

ben.golombek@calchamber.com

January 2022