California Privacy Rights Act

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

- California Consumer Privacy Act (2018) created eight core privacy rights for consumers, with various exemptions.
- California Privacy Rights Act (2020), a voter-approved initiative, revised/expanded rights enacted by the 2018 law.
- Privacy law exemptions for employees and business-to-business transactions were part of both the original law negotiated in 2018 and the 2020 initiative.
- Reinstating the exemptions permanently provides certainty to employers that "consumers" are not "employees" and can prevent negative unintended consequences harmful to workers and employers.

HISTORY OF PRIVACY ACTS

In 2018, the Legislature unanimously passed AB 375 (Chau et al., Chapter 55, Statutes of 2018), enacting the California Consumer Privacy Act (CCPA), to increase transparency and consumer control over the collection and sale of their personal information (PI), and to supplant a pending ballot measure, as discussed below.

The CCPA is a landmark, comprehensive, technology-neutral, and industry-neutral consumer privacy law, meaning that it applies to businesses of all sizes, across all industries, and irrespective of the specific technology (if any) used to collect or sell consumer PI. Modeled in part on the European Union's General Data Protection Regulation (GDPR), which took effect in May 2018, the CCPA was the first comprehensive consumer privacy statute of its type in the United States.

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.

The CCPA created roughly eight core privacy rights for consumers, subject to various exemptions:

1. **Right to be told** (right to disclosure, for example, per a privacy policy) the following:
   a. A description of a consumer's rights under the CCPA (Civil Code Section 1798.130(a)(5)(A)).
   b. The categories of personal information (PI) that a business collects about consumers, and the purposes for which they will be used, at or before the point of collection (Civil Code Section 1798.100).
   c. Specified categories of information relating to the collection and/or sale or disclosure of PI for a business purpose, such as the categories of sources from which the PI was collected, the categories of third parties with whom information is disclosed, and the business or commercial purposes for collecting/selling consumer PI (Civil Code Sections 1798.110 and 115).
2. **Right to know/request access to** certain categories of information from a business that *collected* PI about a particular consumer in the preceding 12 months (Civil Code Section 1798.100 and .110), and/or *sold or disclosed PI for a business purpose* about a particular consumer in the preceding 12 months (Civil Code Section 1798.115), upon receipt of a verifiable consumer request. Among other things, the consumer also has the right to know the categories of sources from which the PI is collected and categories of third parties to whom the business discloses PI (Civil Code Section 1798.110), as well as the third parties to whom the business sold its particular information, including the category or categories of PI sold to each category of third party (Civil Code Section 1798.115). The consumer also has the right to **request access to specific pieces of information** collected about them, from a business that collects PI about the consumer (Civil Code Section 1798.110).

3. **Right to request deletion** of data collected *from* that consumer, subject to additional exceptions. (Civil Code Section 1798.105).

4. **Right to opt-out** of the "sale" of PI, or opt-in if under the age of 16. (Civil Code Section 1798.120).

5. **Right against discrimination** for exercising rights under the CCPA. (Civil Code Section 1798.125).

6. **Right to a limited private right of action** for specified statutory damages for certain data breaches involving non-encrypted, non-redacted PI. (Civil Code Section 1798.150).

7. **Right of notice and opportunity to opt-out of sales of PI sold to third parties**. A third party is prohibited from selling PI about a consumer that was sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise their opt-out rights. (Civil Code Section 1798.115).

8. **The right to portability of PI,** if delivered in electronic form (Civil Code Section 1789.100).

In creating the CCPA in 2018, however, stakeholders were explicit in ensuring that the law exempted employee and business-to-business information from these rights, as stakeholders recognized there already were existing regulations in these areas and that this data is used in a very different way than consumer data.

The CCPA had a delayed operative date of January 1, 2020, contingent upon the withdrawal of a then-pending ballot initiative (initiative measure No. 17-0039, Consumer Right to Privacy Act of 2018) sponsored by Californians for Consumer Privacy. This ensured that the CCPA would not become operative at all if the initiative was not withdrawn from the ballot as its proponents promised (Civil Code Section 1798.198).

All parties involved in the negotiations and passage of the CCPA recognized that the law had flaws, but generally felt it was the preferred alternative to the initiative for two key reasons.

• First, by negotiating to have the statute passed through the Legislature, the CCPA was opened to input from a broader group of legislators and stakeholders.

• Second, the law also ensured that the CCPA could be amended in the future based on a majority vote of the Legislature, as opposed to the two-thirds requirement mandated in the competing initiative.

CALIFORNIA PRIVACY RIGHTS ACT

Following up on their legislative success in 2018, proponents of the CCPA qualified and passed Proposition 24 in 2020, enacting the California Privacy Rights Act of 2020 (CPRA). Among other things, the CPRA revised, or otherwise expanded, the rights afforded under the CCPA by:

• Extending the exemptions for employee and business-to-business information until January 1, 2023.

• Requiring additional disclosures/notices at or before the point of collection.

• Adding a new right to correct data.

• Expanding the right to delete so that it extends to any third parties, service providers, or contractors to whom a covered business discloses the consumer's data.

• Applying existing CCPA consumer rights, including the right to opt-out, to the sharing of a consumer's PI, and not just selling or sharing PI for monetary or valuable consideration.

• Providing the consumer an expanded right of access to all their data (starting on January 1, 2022), not just data collected or disclosed in the last 12 months.

• Incorporating the concept of data minimization, defining a new category of PI, called sensitive personal information (SPI), and establishing a consumer's right to direct businesses to limit use of SPI.

WHY EMPLOYEE EXEMPTION IS NECESSARY

An employee exemption is necessary to ensure that records which employers are required to maintain are not inappropriately disclosed or destroyed. For example, an employee facing a human resources complaint could have information destroyed that would be essential in an internal or criminal investigation.

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 being interpreted to capture information that falls outside of the consumer context.

As a practical matter, for an employer, this provided assurance that the CCPA does not apply to all information found on an employee's computer or work phone, information found in their physical office or workspace, 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 would not only be inconsistent with legislative intent, but it would create tremendous legal consequences for both employers and employees

and cause the CCPA to conflict directly with existing laws and rights under the Labor Code or other employment laws.

For example, in many cases, employers are *required* by state and federal law to collect employee information; thus, the application of CPRA's privacy rights would be 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, years before the CCPA was even enacted. *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, the CCPA was designed to apply only to PI collected in the context of a consumer transaction or communication. Naturally, businesses that contract with one another for products or services will exchange information to carry out contracts and daily business functions — information that would invariably include the PI of any employee(s) involved in that exchange of business-to-business information based on the breadth of the CCPA and CPRA definition of "personal information."

Thus, to prevent the disclosure of confidential information and to avoid interference with the daily operations of businesses with overwhelming compliance obligations, certain business-to-business information was exempted expressly from much of the CCPA's application. As part of the compromise, however, it was clarified that such information still is subject to the new, limited private right of action for data breaches.

The exemption applied to information that allows businesses to conduct business transactions with one another when no individual consumer is involved. Specifically, it applied 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 included, for example, information contained in emails between two companies regarding a purchase order or contract.

Small and large businesses relied upon 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. The exemption also allowed businesses to carry out philanthropic, good-will work with efficiency. Similar to employee information, CCPA's framework was not intended for and does not make sense in this non-consumer context but could be misinterpreted to give people the right to request access to proprietary information or delete pertinent documents.

CONTEXT BEHIND EMPLOYEE AND BUSINESS-TO-BUSINESS EXEMPTIONS

To understand the implications of and policy issues related to the expiration of the employee and business-to-business exemptions, it is important to consider the context of this conversation against the text of the CCPA.

- **First, business, labor and the Legislature saw the exemptions as entirely consistent with how the Legislature interpreted the existing CCPA, where these exemptions originally were enacted.** It never intended for the term "consumer" to encompass employees. Given the rushed nature of passing the CCPA in time for the competing initiative to be pulled off the ballot, significant clean-up legislation was warranted and work on that began immediately upon the passage of the CCPA.

The Legislature was clear in its intent not to weaken any of the CCPA rights in passing clean-up legislation, which included the "employee" and "business-to-business" exemptions. Stated another way, implicit in the genesis of these clarifying, "clean-up" amendments to the CCPA was that the Legislature was providing clarity on these issues. It was not changing how the law would have operated in the absence of those express statements.

- **Second, the exemptions turned on the reality that an individual could be wearing one of two hats when interacting with a business: one as a consumer, and one as an employee.** Whereas the former clearly was captured by the CCPA as the focus of the new consumer privacy law, the latter was not. The exemptions also centered on the potential misreading of incredibly broad definitions used throughout the act.

Specifically, the term "consumer" was drafted broadly under the CCPA to mean a natural person who is a California resident, however that person might be identified (such as by way of a unique identifier). While it generally was understood that "consumers" are not "employees," many entities wanted additional certainty in the plain text of the law to avoid any incorrect interpretations of that term in the future.

This ultimately led to the "employee" exemption. Although a sunset was added to this exemption, it was done solely to bring stakeholders back to the negotiation table for conversations around that data, specifically — not to imply that applying the CCPA only to consumers would be temporary. To further aid in those future conversations, a narrow limitation also was placed on this exemption to ensure that businesses provided their employees disclosures as to what data is collected per Civil Code Section 1798.100.

WHY THE SUNSETS EXISTED

For the above reasons, stakeholders agreed upon separate exemptions for employee and business-to-business information to avoid the problematic results that would ensue, as well as conflicts with existing laws. Due to the timing of the negotiations, stakeholders agreed to a sunset to both exemptions in order to encourage discussions around how best to address employer and employee data privacy issues, but to date no solution has been enacted by the Legislature. Those sunsets initially were set to expire on January 1, 2021, but were extended by way of Proposition 24, the CPRA, to January 1, 2023. In the event that Proposition 24 did not pass, the January 1, 2021, sunsets also had been extended by way of legislation with unanimous approval of the Legislature and without any objection from stakeholders. (*See* AB 1281 (Chau; D-Monterey Park; Chapter 268, Statutes of 2020.)

The expiration of the sunsets on January 1, 2023 has created issues and unnecessary complications for employers and workers and is likely to cause unnecessary litigation if conflict were to arise over the interpretation of the privacy law, in the absence of these express exemptions.

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 CCPA exemption for employee data does not diminish existing employee data protections.

Thus, even if there was no sunset on CCPA's exemption for employee data, employees would retain these same 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).

The CCPA does not, and should 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 try to use the consumer right to know as a means of side-stepping civil discovery rules. Use of that consumer right by an employee also could lead to the disclosure of proprietary information or communications that normally would be protected under privilege, such as the attorney-client privilege, depending on how the CCPA exemptions are interpreted, such as the exemption for exercising or defending legal claims.

In addition, the right to delete could be problematic as well. Despite specific exemptions to this right under the CCPA, granting this right to employees could be interpreted by some as creating a nearly unfettered right to delete emails or other files. An employee who has acted inappropriately toward others in the workplace (for example, sexual harassment) should not be allowed to demand deletion of any incriminating emails, texts or instant messages. Continuing the exemption would have assured employers that, even under the CCPA, they can retain evidence for 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 ultimately become a question for the courts to decide. This would not only create unnecessary litigation (given the implicit understanding of how the CCPA operated even before the inclusion of the express exemptions), but it

also would put judges in the position of policymakers. These layers of statutory conflict also would leave employers confused about their legal obligations under the CCPA as opposed to the California Labor Code, federal record-keeping requirements, and agency regulations. The impact would not be just to covered businesses; it also would affect other businesses that serve as contractors, service providers or the like in engaging in communications or transactions with covered businesses.

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

The above issues are just examples of the potential consequences and confusion 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 be reinstated and remain in place indefinitely, consistent with the underlying intent of the Legislature when passing the CCPA and subsequent clean-up legislation, as well as with the voter-approved CPRA, which maintained those exemptions.

CALCHAMBER POSITION

CalChamber supports reinstating 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 exemptions to expire could have serious unintended negative consequences that would harm both workers and employers.

Staff Contacts
Ashley Hoffman
Senior Policy Advocate

ashley.hoffman@calchamber.com

Ronak Daylami
Policy Advocate

ronak.daylami@calchamber.com
January 2024