Published on *The National Law Review* https://natlawreview.com

No More Exceptions: What to Do When the California Privacy Exemptions for Employee, Applicant and B2B Data Expire on January 1, 2023

Article By:

Gregory (Greg) J. Krabacher

Brian G. Cesaratto

California's Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA) give consumers substantial rights regarding the disclosure and use of their personal information collected by businesses subject to the law. Significantly, CCPA/CPRA define the term "consumer" to mean any California resident. This broad definition extends not only a business's individual customers, but also its employees, job-applicants and even its business-to-business (B2B) contacts. We have previously discussed the compliance requirements of these data privacy laws on organizations doing business in California, and the moratoriums for B2B and employee/applicant data that that the Legislature had put in place exempting covered businesses from complying with certain requirements of the laws.[1] Unless extended by the Legislature (which appears unlikely) or preempted by federal privacy legislation (which appears even more unlikely), the moratoriums will sunset on January 1, 2023. Accordingly, covered businesses should begin preparing now to meet their upcoming expanded statutory obligations to protect consumers data privacy.

The compliance and operational challenges created by CCPA/CPRA's expansive definition of "consumer" are manifest. In the day-to-day course of operations, businesses may collect large amounts of personal information about current employees and job applicants, sourced from any number of locations and residing in any number of places or systems. Protected information can be generated from any division or department of a business and can be stored in the cloud, on local network drives, as hard copies or all three. Moreover, the information may be collected as structured data (*e.g.*, in databases and HRIS systems) or in unstructured form, such as in email. Added to this, data may be stored (and essentially shared) with third party vendors. Information exchanged day-to-day between businesses (whether they be competitors, vendors, customers, or partners) may be voluminous. Locating all this data and fulfilling an access, right to know or deletion request from employees, or other consumers, seeking to exercise rights their under the CCPA/CPRA will present significant complex and burdensome challenges that businesses will need to be prepared to meet. Failure to fulfill a request can lead to reputational – not to mention financial – consequences. Knowing where, how and why personal information is maintained is critical in evaluating how to comply with the CCPA's (*see, e.g.,* Cal. Civ. Code § 1798.145) data privacy notice and, employee request obligations, while balancing the business's other obligations (*e.g.*, to preserve evidence, defend legal

claims).

What are the existing employee and B2B data exemptions included in the California Consumer Privacy Act and the California Privacy Rights Act (CPRA)?

The CCPA contains a limited exemption for personal information collected by a business about an individual who is a job applicant or employee, owner, director, or independent contractor of the business. The employee exemption is limited, in part, in that it applies only when the information is collected and used "solely within the context of [the individual's] role or former role" as a job applicant, employee, owner, director, or independent contractor. In the context of a B2B relationship, businesses need not provide notice of the collection, and the "consumer" does not have a right to know or right to delete.

When do the exemptions currently expire and what attempts have been made to extend the exemptions?

The exemptions were included in the original version of the CCPA and were initially set to expire in January 2021. In September 2020, legislation was enacted to extend the exemptions by an additional year (as the COVID-19 pandemic had inhibited businesses' compliance efforts). Then, the CPRA, which passed as a ballot initiative in November 2020, extended the moratorium to January 1, 2023.

Although state legislators proposed a number of bills this year to further extend the exemptions they failed to pass before the August 31, 2022, close of the legislative session. Attempts to include an extension in a November ballot initiative have also fallen short. With the failure of further extensions, the exemptions will expire as of the New Year.

Given that it's unlikely the exemptions will be extended beyond the January 1, 2023 deadline, how should businesses be preparing?

Europe's General Data Protection Regulation (GDPR) applies to B2B and employee data; thus, businesses already subject to (and compliant with) GDPR should be in a good starting position to comply with the requirements of CCPA/CPRA. All businesses that are subject to CCPA/CPRA should consider the following compliance measures:

- Starting with the Human Resources, Benefits and Information Technology departments, employers should map the collection, use, and disclosure of personal data of California residents within the organization and any sharing or disclosure of that data with third parties.
- Document the commercial purposes for collection and use of each category of personal information collected or processed, including as required by applicable law (*g.*, laws that require the maintenance of certain employment and business records).
- Assess the value of personal information collected and follow sound data minimization principles (*e.*, do not collect what is not needed to achieve the commercial purpose).
- Update employee and/or job applicant notices beyond the currently required short form notice to provide additional required information, including communicating individual rights under CCPA/CPRA, information concerning any collection of sensitive information (e.g., race, ethnicity, government identifiers), any disclosure of personal information to third parties and

the business's information retention policies.

- Ensure that the business's mechanism and policies for responding to employees' requests to exercise their privacy rights (including expanded rights under CPRA) is expanded to include human resources and other personal data.

- Develop policies and operational procedures for responding to CPRA rights' requests (including right to know, delete, and access) in light of the organization's collection and use practices.

- Ensure that all employee and other personal information is reasonably safeguarded against hacking and other predictable cybersecurity threats.

- Review contracts with downstream service providers and contractors that hold employee or B2B data for cooperation and other downstream data protection clauses.

- Review contracts with business partners as to B2B information to address CCPA/CPRA compliance responsibilities.

FOOTNOTES

[1] *See* Businesses Should Begin Assessing Their Data Practices In Order to Meet the California Privacy Rights Act Requirements; Complying with Enhanced Cybersecurity Safeguards in California.

National Law Review, Volume XII, Number 251