Bloomberg Law®

bloombergbna.com

Data Protection

INSIGHT: Impact of the California Consumer Privacy Act on Employers

By Lothar Determann and Chetan Gupta

As of Jan. 1, 2020, companies around the world will have to comply with additional regulations related to processing of personal data of California residents. Pursuant to the California Consumer Privacy Act of 2018 (''CCPA''), covered companies have to observe restrictions on data monetization business models; accommodate rights to access, deletion, and porting of personal data; and issue or update privacy notices to provide detailed disclosures about data handling practices. For a general overview of the statute and its unusual history, *see* Lothar Determann, *The California Consumer Privacy Act of 2018: Broad Data and Business Regulation, Applicable Worldwide*, IAPP Privacy Tracker (Jul. 2, 2018).

1. Why the California Consumer Privacy Act Impacts Employees and Employers. The CCPA protects all California residents with respect to any personal information that relates to them. However, contrary to its title, the CCPA does not just protect Californians in their roles as consumers, but also as employees, patients, tenants, students, parents, children, etc. This is because Cal. Civ. Code § 1798.140(g) defines ''consumer'' as any ''natural person who is a California resident, . . . however identified, including by any unique identifier.'' That section specifies that the term ''resident'' is defined by Cal. Code Regs. Tit. 18, § 17014 as it read on Sept. 1, 2017, meaning it ''includes (1) every individual who is in the State for other than a temporary or transitory purpose, and (2) every individual who is domiciled in the State who is outside the State for a temporary or transitory purpose,'' subject to a number of clarifications and specifications. Therefore, employees in California fall within the definition of ''consumer'' under the CCPA.

2. Which Employers Are Covered by the California Consumer Privacy Act? Companies around the world have to comply with the CCPA if they receive personal data from California residents (including employees) and if they—or their parent company or a subsidiary—exceed one of three thresholds: (a) annual gross revenues of $25 million, (b) collection for commercial purposes of the personal information of 50,000 or more California residents, households, or devices annually, or (c) 50% or more annual revenue from selling California residents' personal information. Parent companies and subsidiaries using the same branding are covered in the definition of ''business,'' even if they themselves do not exceed the applicable thresholds. Cal. Civ. Code § 1798.140(c).

A. Companies must comply if they have annual revenues in excess of $25 million.

It is not clear whether this number includes only a company's California revenue or its global sales, as the CCPA does not specify the scope of this provision. For comparison, Cal. Civ. Code § 1714.43(a)(1) applies to companies according to their ''annual worldwide gross receipts,'' whereas the CCPA merely refers to ''annual gross revenues,'' Cal. Civ. Code § 1798.140(c)(1)(A). In contrast, Cal. Rev. & Tax. Code § 17942(a) applies only to income ''derived from or attributable to this state.'' Therefore, if a company with annual revenues over $25 million has even one employee in California (and therefore receives the employee's personal data), it is pos-

sible that the company would automatically be covered by the CCPA.

B. A company will need to comply if it obtains or sells personal information of at least 50,000 California residents annually for commercial purposes.

Given the broad scope of the CCPA, companies may reach this threshold more quickly than anticipated. Most notably, the Act defines ''[c]ommercial purposes'' as ''advancing a person's commercial or economic interests,'' Cal. Civ. Code § 1798.140(f), and ''[p]ersonal information'' as ''any information that . . . relates to . . . a particular consumer or household,'' specifically including employment-related information, Cal. Civ. Code § 1798.140(o)(1). Therefore, an employee's job description, details of an employee's compensation, performance reviews, and most HR records pertaining to the employee constitute ''personal information.'' Additionally, non-employee consumers would potentially count towards the threshold, and employers may inevitably gather related personal information by, for example, capturing IP addresses through operation of a website. Consequently, an employer may be subject to the CCPA if it has few employees in California but a large number of other ''consumers'' located there.

C. Companies can also be subject to the law based on whether they sell California residents' personal information.

A relatively small company in California may need to comply if it derives more than 50% of its annual revenue from selling California residents' personal information. ''Selling'' is defined broadly to mean any disclosing or making available for monetary or other valuable consideration, subject to a number of exceptions, including consumer-directed disclosures to third parties that do not sell the personal information; limited sharing with service providers; and business transfers in bankruptcy, M&A, and similar transactions. Cal. Civ. Code § 1798.140(t).

D. Out-of-state companies may be exempt from the CCPA.

The CCPA does not apply to collection or sale of personal information if ''every aspect of that commercial conduct takes place wholly outside of California,'' Cal. Civ. Code § 1798.145(a)(6), or if the company is not doing ''business in the State of California,'' Cal. Civ. Code § 1798.140(c)(1). Most companies with connections to California, however, will find proving either difficult. For one, commercial conduct will not be deemed taking place outside California if a company collects information about a consumer while the consumer is located in California, sells information collected when the consumer was located in California, or conducts any part of a sale in California. Cal. Civ. Code § 1798.145(a)(6). Additionally, under Cal. Rev. & Tax. Code § 23101(a), an out-of-state company is doing business in California if it actively engages ''in any transaction for the purpose of financial or pecuniary gain or profit'' in California. Employing or collecting information about California residents will usually satisfy either test.

3. What Rights do Employees Have under the CCPA?

■ Employees can ask employers to disclose the categories and specific pieces of information collected, and once a request is verified, this information must be provided free of charge. Cal. Civ. Code § 1798.100(a), (d). Since personal information is very broadly defined, and would cover most HR records, employees could potentially request confidential performance reviews or internal company correspondence relating to them. At present, the CCPA does not appear to provide any mechanism for denying such requests or withholding particular information. The Attorney General may, however, enact regulations to implement such measures before the CCPA becomes operative on Jan. 1, 2020. Specific regulations are already contemplated to provide exceptions with respect to trade secrets, for example. Cal. Civ. Code § 1798.185(a).

■ Employees must be informed at or before the point of collection about the categories of personal information collected and the purposes for which they will be used. No additional categories of information can be collected without prior notice. Cal. Civ. Code § 1798.100(b).

■ Employees can also ask for their personal information to be deleted, though an employer is allowed to retain the information if it is necessary, among other grounds, for performance of the employment contract or if it is required for solely internal uses aligned with the expectations of the employee. Cal. Civ. Code § 1798.105(a), (d).

■ Employees must also be informed if their personal information is being sold or being disclosed to third parties for a ''business purpose,'' and they can request information in this regard. Cal. Civ. Code § 1798.115. ''Business purpose'' is defined in Cal. Civ. Code § 1798.140(d) as use of personal information for operational purposes. This right would likely apply if employee information is shared in the context of a transaction, for example, and employees would have to be informed about such use (although it could be argued that an M&A transaction is not part of the operational purposes of a company). Although the definition of ''selling'' personal information in Cal. Civ. Code § 1798.140(t) excludes provision of information for transactions, there is no similar exclusion in the definition of ''business purpose.'' While specific information with respect to each transaction would not be required, employees would have to be generally informed that their personal information may be disclosed in relation to transactions. Similarly, ''business purpose'' would cover disclosures of employee information to payroll vendors, benefits providers, and other service providers and would require similar disclosures to employees. With respect to service providers, employers should be careful to enter into written agreements with such service providers that expressly forbid any sale or unauthorized use of the employee information save for specified processing purposes by the service providers. Otherwise, the employer could itself be construed as selling employee information. Cal. Civ. Code § 1798.140(t)(2)(C), (v).

■ Employees have the right to opt out of the sale of their personal information, subject to the very broad and somewhat counterintuitive definitions of ''sale.'' Cal. Civ. Code § 1798.120(a). For example, if an employer uses a free or freemium cloud service subject to standard terms and conditions that allow the provider to commercialize information received, this could qualify as a ''sale.''

■ Any California employee whose nonencrypted or nonredacted personal information is subject to unauthorized access and exfiltration, theft, or disclosure may institute a civil action under the CCPA. Cal. Civ. Code § 1798.150(a)(1). Unlike California's existing data

breach notification statute, Cal. Civ. Code § 1798.82(g), the CCPA does not contain an exception for ″[g]ood faith acquisition of personal information by an employee or agent.'' If a disclosure is unauthorized, it potentially triggers CCPA liability. A misdirected e-mail could trigger statutory damages in significant amounts—up to $750 per employee per incident. Cal. Civ. Code § 1798.150(a)(1)(A). Significantly, employees would not have to show any actual injury or harm to maintain such civil actions. However, ''personal information'' in this context covers only information relating to driver's licenses, social security numbers, and medical and financial information, in contrast to the broad definition of ''personal information'' in Cal. Civ. Code § 1798.140(o)(1). Cal. Civ. Code § § 1798.150(a), 1798.81.5(d)(1)(A). For an analysis of civil actions under the CCPA for data breaches, see Lothar Determann, *Be Wary of Liability for Statutory Damages under California Consumer Privacy Act*, Bloomberg Law: Privacy & Data Security (Jul. 9, 2018).

■ Employees enjoy broad anti-discrimination rights, and an employer cannot retaliate or discriminate against them for seeking to exercise any rights under the CCPA. Cal. Civ. Code § 1798.125(a).

■ Employees must be informed about their access, information, and anti-discrimination rights with respect to the collection, use, and sale of their personal information by way of a privacy policy. Cal. Civ. Code § 1798.130(a)(5). Employees also cannot be asked to contractually waive any rights provided by the CCPA, and any such contract is void against public policy. Cal. Civ. Code § 1798.192.

The CCPA prescribes rigid requirements regarding how consumers must be notified of and may exercise the rights guaranteed by the Act. For example, businesses must make available to consumers a toll-free telephone number for submitting requests for information required to be disclosed, and if a business sells personal information as contemplated under the CCPA, it must provide a clear and conspicuous link on its Internet homepage titled ''Do Not Sell My Personal Information.'' Cal. Civ. Code § 1798.130(a)(1), 1798.135(a)(1). These requirements apply even if they would not necessarily be the most appropriate means of communicating with employees.

4. *What Sanctions and Remedies Could Employers Face?*

■ The CCPA allows the California Attorney General to bring a civil action for violations of the Act. Companies that commit intentional violations are subject to penalties of up to $7,500 per violation. If a company commits an unintentional violation and fails to cure it within 30 days of receiving notice, it is liable for up to $2,500 per violation as provided by Section 17206 of the California Business and Professions Code. Cal. Civ. Code § 1798.155(a)-(b).

■ Under Cal. Civ. Code § 1798.150, companies that experience data theft or other data security breaches can be ordered in a civil class action to pay statutory damages between $100 to $750 per California employee per incident or actual damages, whichever is greater, and any other relief a court deems proper. Consumers, however, must notify the California Attorney General of any action, after which the Attorney General may choose to prosecute the company instead of allowing the civil action to proceed. Cal. Civ. Code § 1798.150(b)(3).

■ Companies, activists, associations, and others can be authorized to exercise opt-out rights on behalf of California employees according to Cal. Civ. Code § 1798.135(c).

5. *What Do Employers Need to Do?* Companies around the world will need to start working right away to assess the CCPA's impact on their businesses, systems, and data handling practices. A year and a half is not a lot of time, as anyone who has been working on EU GDPR compliance knows well. Companies will need to take a number of affirmative steps to comply with the new requirements, including the following:

■ **prepare data maps, inventories, or other records** of all personal information pertaining to California residents (including employees), households, and devices, as well as information sources, storage locations, usage, and recipients; to add newly required disclosures to privacy policies; to prepare for data access, deletion, and portability requests; and to comply with opt-out requests with respect to data sharing;

■ **update employee privacy policies or notices** with newly required information, including a description of California residents' rights per Cal. Civ. Code § 1798.130(a)(5);

■ **put in place written agreements with any service providers** receiving employee personal information pursuant to Cal. Civ. Code § 1798.140(v);

■ **make available designated methods for employees submitting data access requests**, including, at a minimum, a toll-free telephone number, pursuant to Cal. Civ. Code § 1798.130(a);

■ **fund and implement new systems, training, and processes** to comply with the new requirements, including to verify the identity and authorization of persons who make requests for data access, deletion, or portability; respond to requests for data access, deletion, and portability within 45 days; and avoid requesting opt-in consent for 12 months after a California resident opts out, per Cal. Civ. Code § 1798.135(a)(5); and

■ **monitor legislative developments,** as the California Legislature is working on corrections and improvements to the hastily passed CCPA and aligning the myriad existing California privacy laws (*see*, Lothar Determann, California Privacy Law - Practical Guide and Commentary, 3d Ed. 2018). Also, Congress may revive plans for federal privacy legislation that may preempt California laws partially or completely.

Author Information

Lothar Determann and Chetan Gupta practice law at Baker McKenzie LLP, Palo Alto, and advise clients on data privacy and employment law respectively. Chetan Gupta is admitted in California and India. Lothar Determann is admitted in California and Germany and is the author of Determann's Field Guide to Privacy Law (3d Ed. 2017) and California Privacy Law - Practical Guide and Commentary (3d Ed. 2018). The views expressed in this article are those of the authors and not necessarily those of Baker McKenzie or its clients, or of Bloomberg Law. The authors are grateful for valuable input from their Baker McKenzie colleagues Helena Engfeldt and Jonathan Tam.