GIBSON DUNN

October 16, 2019

CALIFORNIA CONSUMER PRIVACY ACT: 2019 FINAL AMENDMENTS SIGNED

To Our Clients and Friends:

The California Consumer Privacy Act of 2018 becomes effective in 77 days (January 1, 2020), and offers California residents several new privacy rights through obligations placed on covered businesses. For a more in-depth look at the CCPA, see our previous client alerts summarizing the statute (here), amendments from October 2018 (here), additional proposed amendments (here), and the Attorney General's regulations posted last week (here).

Over the last several months, and prior to the release of the regulations, the California legislature worked on several additional amendments to the law that at long last have been signed by Governor Gavin Newsom—less than three months before CCPA takes effect. Like the regulations, these amendments respond to concerns raised after the passage of the CCPA. The signed amendments do not critically change the original core requirements of the CCPA, but may offer some clarification and even reprieve in certain areas for many of our clients.[1]

Finalized Amendments

Partial and Temporary Employment-Related Exemptions – AB 25

AB 25 provides a one-year exception for employers who feared that the consumer protection law inadvertently crept into covering employment-related information. The bill clarifies that the CCPA *generally* will not apply to personal information that is collected about job applicants, employees, contractors, and other employment-related roles. The bill also creates exemptions for employee emergency contact information and personal information necessary to administer benefits. Importantly, the bill does not relieve employers of the "private civil action provision [for data breaches] and the obligation to inform the [employee] as to the categories of personal information to be collected."[2] And these exemptions only extend to "personal information [that] is collected and used by the business solely within the context of the natural person's role or former role . . .", which may create uncertainty for areas of potential business and personal overlap. The bill also only provides temporary relief for employers in that these exceptions become inoperative on January 1, 2021, absent further legislative action in the coming year.[3]

Redefinition of Personal and Publicly Available Information – AB 874

This bill clarifies the terms "publicly available" and "personal information." Most significantly, the bill *removes* the requirement that publicly available information must be compatible with the purpose for which the data is maintained and made available in order to be exempt. Information lawfully made

available in federal, state or local government records therefore will be considered "publicly available" and excluded from the definition of personal information, regardless of the purpose for which they are used; this may be a significant relief for companies using publicly available government-collected data, at least with respect to compliance relating to those categories of information. That said, the definition of "publicly available" remains narrow, and "personal information" covered by CCPA would still include non-governmental information posted publicly by the consumer.

This amendment also clarifies the definition of "personal information" by adding the term "reasonably"—again—to read 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." Under the CCPA, "personal information" is a key term for information that would be protected and subject to various requirements. The bill would also exclude deidentified or aggregated consumer information from the "personal information" definition (a similar clarification for deidentified information is also provided by AB 1355).

Business-to-Business Exceptions and Various Technical Amendments – AB 1355

AB 1355 creates a one-year exception for personal information collected in the course of certain business-to-business interactions, and makes various minor technical amendments. During the last several weeks of the legislative session, legislators added an exception for business-to-business transactions when considering "personal information . . . where the consumer is . . . acting as an employee, owner, director, officer, or contractor of a company . . . and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company. . . ." This exception would not apply to other circumstances (e.g., when the consumer's information is additionally used for other purposes), the consumer's right to "opt-out" of selling, the right to non-discrimination, or the data breach private right of action. And like AB 25, this is only a temporary reprieve. The exemption is only valid until January 1, 2021. Nonetheless, for the first year of CCPA, this amendment provides clarity for businesses who mostly function in a business-to-business capacity, and may collect personal information from business agents in that course.

This bill also makes a number of more minor clarifications, cross-reference corrections and conforming changes to the act. Among the notable changes, this bill, like AB 874, clarifies that deidentified or aggregated consumer information is excluded from the definition of personal information and also clarifies the CCPA's non-discrimination exception. Under the original Act, businesses could exercise certain discrimination if the differential treatment is reasonably related to value provided to the *consumer* by the consumer's data. The bill modifies this exception for differential treatment related to value provided to the *business* by the consumer's data.

Data Broker Registration – AB 1202

AB 1202 amends the CCPA to require that "data brokers" register with the California General's Office on an annual basis. The bill broadly defines "data broker" as any "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a

direct relationship." According to the bill's text, direct relationships may be created in a "variety of ways such as by visiting a business' premises or internet website, or by affirmatively and intentionally interacting with a business' online advertisements . . . ."[4]; however, many businesses that collect information from sources other than the consumer, and then use that information downstream for a business purpose (including "selling"), may be implicated.[5] Data brokers who fail to comply with the law are subject to injunctions, civil penalties, fees, and costs for actions brought by the Attorney General. Civil penalties include fines of $100 for each day the data broker failed to register.

Contact Information for Consumer Requests – AB 1564

Under the original act, businesses were required to have a toll-free phone number to facilitate consumer requests. This bill creates an exception for a business that operates exclusively online and has a direct relationship with a consumer data subject. These online businesses are required to make an email address available for requests (and based on the recently proposed regulations, also a web form), but are not required to add a toll-free phone number. Nonetheless, the Act and regulations still require *two* modes of contact.

Vehicle Information – AB 1146

This amendment creates sectoral exceptions for the auto industry. Under the CCPA, consumers have an opt-out right to ask businesses not to sell information to third parties and have the right to ask business to delete certain consumer information. This bill allows businesses to exclude vehicle information from the opt-out and deletion provisions for the "purpose of effectuating or in anticipation of effectuating a vehicle repair covered by a vehicle warranty or a recall . . . ."

Other Amendments that May Affect CCPA

The California legislature also has passed laws that can shape the CCPA, without being amendments to the law itself. Businesses should consider how these laws may expand liability under the CCPA for their companies.

Data Breach Amendments – AB 1130

On October 11, Governor Newsom signed a bill that would expand the definition of "personal information" in the state's data breach *notification* law by including "specified unique biometric data and tax identification numbers, passport numbers, military identification numbers, and unique identification numbers issued on a government document in addition to those for driver's licenses and California identification cards . . . ." While this law does not modify the CCPA directly, the amendment's expansion of personal information broadens the list of personal information subject to the data breach private right of action in CCPA, as the private right of action's definition of "personal information" depends on the definition in the data breach statute.

Police Body Cameras – AB 1215

On October 9, Governor Newsom signed a bill that will ban law enforcement use of facial recognition technology on body-worn cameras for three years. While this also does not modify any substantive provisions of the CCPA, the new law further regulates the collection of personal information, sounds in California's concern for overly broad collection of information, and may influence modifications to the CCPA regarding facial recognition (such as AB 1281, which would require businesses to give conspicuous notices where facial recognition technology is employed). Law enforcement entities must cease this application of the technology by January 1, 2020.

* * *

The foregoing amendments present several clarifications to businesses working to comply with CCPA, and under certain instances institute additional burden. We continue to monitor developments regarding the CCPA, including the recently released regulations from the Office of the Attorney General, and are available to discuss these issues as applied to your particular business.

---

[1] Also notable is a significant bill that did *not* pass this legislative session—SB 561—which would have greatly expanded potential liability for businesses by creating a private right of action for any CCPA violation. As a result, the only private right of action under the CCPA remains actions for certain data breaches. However, businesses should continue to monitor SB 561 (and any others like it) in the next legislative session (one may recall that the CCPA itself was retrieved from the inactive file).

[2] Legislative Counsel's Digest, A.B. 25 (CA 2019)

[3] Legislative action specific to employment-related data may well be expected, as the Senate amended the bill to exempt this information for only a year, as a compromise (whereas there was no limitation in the original bill), on the premise that there would be consideration of how to address employment-related information in particular during the next legislative session. During the public comment period a number of speakers addressed the concern for the CCPA becoming an employment law—attenuated from its original intent to protect consumers.

[4] The requirement will yield to certain federal laws; businesses covered by the federal Fair Credit Reporting act, Insurance Information and Privacy Protection Act and Gramm-Leach-Bliley Act are exempted from the data broker registration requirement.

[5] California's bill fits into a national tableau of increasing data broker regulation. Last summer, Vermont passed H. 764, which required data brokers to register with the state government and produce certain reports about their data collection. Like California, Vermont cast a wide net for covered entities through a capacious definition: "'Data broker' means a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship." 9 V.S.A. § 2430(4)(A).

The following Gibson Dunn lawyers assisted in the preparation of this client update: Alex Southwell, Mark Lyon, Cassandra Gaedt-Sheckter, Arjun Rangarajan and Tony Bedel.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, or any member of the firm's California Consumer Privacy Act Task Force or its Privacy, Cybersecurity and Consumer Protection practice group:

California Consumer Privacy Act Task Force:

Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Cassandra L. Gaedt-Sheckter - Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Arjun Rangarajan - Palo Alto (+1 650-849-5398, arangarajan@gibsondunn.com)
Alexander H. Southwell - New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)

Please also feel free to contact any member of the Privacy, Cybersecurity and Consumer Protection practice group:

United States

Alexander H. Southwell - Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
M. Sean Royall - Dallas (+1 214-698-3256, sroyall@gibsondunn.com)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Olivia Adendorff - Dallas (+1 214-698-3159, oadendorff@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Richard H. Cunningham - Denver (+1 303-298-5752, rhcunningham@gibsondunn.com)
Howard S. Hogan - Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen - Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
Kristin A. Linsley - San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon - Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson - Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde - Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner - Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong - San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)

GIBSON DUNN

Europe

Ahmed Baladi - Co-Chair, PCCP Practice, Paris (+33 (0)1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox - London (+44 (0)20 7071 4250, jacox@gibsondunn.com)
Patrick Doris - London (+44 (0)20 7071 4276, pdoris@gibsondunn.com)
Bernard Grinspan - Paris (+33 (0)1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden - London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Kai Gesing - Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)

Asia

Kelly Austin - Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Jai S. Pathak - Singapore (+65 6507 3683, jpathak@gibsondunn.com)