GIBSON DUNN

December 13, 2019

CALIFORNIA CONSUMER PRIVACY ACT: COMPLIANCE HEADING INTO THE NEW YEAR

To Our Clients and Friends:

There are only 18 days left until the California Consumer Privacy Act of 2018 becomes effective on January 1, 2020, but many questions still remain. The California Attorney General's office just recently closed its comment period on its highly anticipated regulations, with several arguing that the regulations go beyond the scope of the CCPA. Companies are still grappling with whether—and to what extent—the law applies to their personal information practices, and news of additional privacy-related laws similar to CCPA raises further anxieties. As the effective date looms, we provide an update on the current status of the draft regulations and the recent hearings, priority compliance measures leading into the new year, and what to keep an eye out for in 2020 relating to CCPA.

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), the Attorney General's draft regulations (here), and the final amendments signed in October 2019 (here).

Draft Regulations and Hearings

From December 2, 2019, to December 5, 2019, the Attorney General's office held four public hearings designed to provide the public an opportunity to comment in person on the Attorney General's draft regulations released on October 10, 2019. The Attorney General will publish transcriptions of the hearing comments, and has already published many written comments submitted, available here. The window for public comments closed on December 6, 2019 (45 days after publication of the draft regulations) and there are no further public hearings scheduled at this time.

The Attorney General's representatives heard from many members of the public at the hearings, including on behalf of law firms, advertisers, technology companies, and credit unions. Many comments focused on the regulations' over-breadth compared with the CCPA, and the commenters spanned industries. Points of discussion included sector-specific issues, concern with § 999.315(c)'s alleged requirement for websites to honor do-not-track browser settings as an opt-out, the lack of a model opt-out button, the conflicting and potentially onerous verification standards, and the need for solutions for smaller and mid-sized companies collecting information solely for employment and legitimate business purposes.

Although the hearings are over, and the comment period has concluded, we do not expect the regulations to be finalized until well into the new year, including because there are various additional steps in California's regulatory process. The public must have *at least* 15 days to comment following changes to the draft regulations if *any* changes are made, and that period may be longer depending on the extent of

the revisions. The Attorney General's office must then prepare a summary of and response to each comment submitted orally or in writing, and that package must be submitted to the Office of Administrative Law for approval. The Office of Administrative Law has thirty (30) *working* days to approve the regulations, which will then be published.

We are keeping a close eye on any changes to the regulations based on the public comment period, and will update accordingly.

Priority CCPA Compliance Measures

While the regulations are not yet final, the statute itself becomes effective January 1, 2020 by its terms; practically, however, there are limits on what this may mean for companies. The Attorney General—largely responsible for enforcing the CCPA—will not start enforcing the statute or any regulations until July 1, 2020, and even then, may choose not to enforce all aspects of the regulations, if companies have little time to comply following the regulations' final release.[1] Nonetheless, the private right of action for certain data breaches begins January 1, 2020, and compliance with the statutory provisions is still expected by that date. As a result, we suggest that any compliance considerations begin with the following efforts as highest priority:

- **Analyze whether CCPA applies to your company as a "business."** Given the definition of "business," your company may not be covered by various of the obligations under CCPA, even if you collect personal information from California residents. This could be because of your size (measured by revenue, the number of consumers whose information your company has, and/or how your company uses such information), or because you solely operate as a service provider on behalf of a "business." The distinctions can lead to different obligations and compliance requirements.

- **Analyze whether CCPA applies to your company's personal information collection practices**. This could include analyzing whether the information falls under various exemptions based on sector-specific laws (e.g., GLBA, HIPAA), and whether the personal information falls under temporary and incomplete exemptions added to the CCPA by amendment (e.g., employment-related data, personal information collected in business-to-business transactions). Even if certain of the personal information collected falls into these categories, there may still be requirements (e.g., certain disclosures to employees are still required starting January 1, 2020).

- **Revise or draft privacy notices to relevant California residents.** Arguably most importantly, CCPA requires covered businesses to disclose information to California residents about the categories of personal information they collect, the purposes and uses of that information, whether they share and/or sell that information (and to whom), what rights California residents are granted under the statute, and how residents can exercise those rights (through two methods, one of which must include a toll-free number, unless the business operates wholly online). Provision of these key disclosures should be a business's number one priority, given that compliance with certain of the statute's other requirements can be performed by some companies on a just-in-time basis.

- **Review and bolster your cybersecurity program**. While the Attorney General's enforcement of CCPA is not expected to start until July 1, 2020, one thing is clear: as of January 1, 2020, California residents will have the right to sue for statutory damages based on a breach of certain personal information that results from a business's lack of "reasonable security procedures and practices appropriate to the nature of the information." The CCPA does not define what is "reasonable," but, for example, the 2016 Attorney General's California Data Breach Report's number one recommendation was that the Center for Internet Security's 20 controls constitute a "minimum level of information security that all organizations that collect or maintain personal information should meet."[2] It is important to strategize and build a defensible cybersecurity program now, to both prevent actionable breaches, and defend any suits that could result from this private right of action.

Prioritizing compliance efforts may be critical at this point. While certain aspects of the law remain somewhat in flux, and while more specificity may be provided when the regulations are finalized, the CCPA's core obligations are unlikely to change in any material way. Efforts spent toward these compliance measures are unlikely to be in vain, and companies subject to CCPA should consider these efforts (and others) as we begin the new year.

What to Watch Relating to CCPA in 2020

Among many issues related to CCPA, other states' related proposals, changes to or revamping of the CCPA itself, and the overlap between CCPA and other cybersecurity-related laws will be topics to watch in 2020. Many states other than California—including Illinois, Maine, Nevada, New York, Oregon, Texas, and Washington—passed some type of enhanced data privacy law this year. All have either gone into effect or will go into effect sometime before the end of July 2020. While none are as comprehensive as CCPA (though many include a right to delete and access personal information), and while certain other states' proposed consumer privacy laws are either still pending or have failed, we expect 2020 will bring more discussion and proposals of laws similar to CCPA.[3]

And though the CCPA has yet to go into effect, supporters of broader privacy rights are already attempting to strengthen it. Alastair Mactaggart, the real estate magnate who submitted the ballot initiative that eventually led to the CCPA, is attempting to introduce a new ballot initiative—the California Privacy Rights and Enforcement Act of 2020 (CPREA, and also known as "CCPA 2.0"). CPREA proposes many changes to the CCPA, including adding new rights around sensitive categories of personal information (including an opt-out right from use for advertising), a California Privacy Protection Agency to implement and enforce the law administratively (in addition to leaving civil enforcement with the Attorney General), a retention disclosure requirement, disclosures relating to automated profiling, and disclosures relating to use of personal information for political purposes. Mactaggart and his nonprofit group, Californians for Consumer Privacy, will need over 600,000 signatures to qualify for the ballot in November 2020.

In addition, companies should continue to monitor changes to the existing CCPA, where relevant, including the eventually sun-setting exemptions: business-to-business and employment-related data. It is unclear at this point whether the amendments will be renewed past January 1, 2021, whether category-

specific laws or amendments will be implemented, or whether the exemptions will indeed sunset. However, any changes will be significant for many of our clients.

Finally, the California Internet of Things (IoT) law, approved in September 2018 and starting enforcement on January 1, 2020, dovetails with the CCPA on the cybersecurity front, as it requires businesses selling connected devices offered for sale in California to include reasonable security features. We will see how companies address these requirements in the upcoming year, and how the Attorney General, city attorneys, county counsel, and district attorneys enforce the title's additional security requirements.

* * *

CCPA continues to challenge businesses' leadership and legal minds alike, with ambiguous requirements, yet-to-be-finalized regulations, and threats of new and changing legislation around the corner. Compliance efforts, however, can be tailored to fit the needs of particular businesses. We are happy to answer any questions relating to CCPA, and assist with any compliance measures as the CCPA goes into effect.

---

[1] The CCPA states that the Attorney General shall start enforcing either six months after issuing the final regulations, or July 1, 2020, whichever is earlier. Section 1798.185(c). Given the current status of the final regulations, we anticipate enforcement will not begin prior to July 1, 2020, and even then, enforcement with respect to certain aspects of the regulations may not begin at that time, if the regulations are released not too long prior.

[2] Those controls are available here: https://www.cisecurity.org/controls/cis-controls-list/.

[3] In addition to state laws, we may also see continuing movement based on CCPA at the federal level. As an example, two Democratic representatives (from California) have sponsored the Online Privacy Act, which would, among other things, create a Digital Privacy Agency (DPA), comparable to Data Protection Authorities established in the European Union for GDPR enforcement, and similarly allow users to access, correct, delete, and transfer their data.

The following Gibson Dunn lawyers assisted in the preparation of this client update: Alex Southwell, Eric Vandevelde, Cassandra Gaedt-Sheckter, Tony Bedel, and Isabella Sayyah.

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)
Debra Wong Yang - Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin - New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker - Denver (+1 303-298-5774, rbergsieker@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)

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)
Alejandro Guerrero - Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic - Paris (+33 (0)1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen - London (+44 (0)20 7071 4203, swazen@gibsondunn.com)

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