GIBSON DUNN

As California Consumer Privacy Act Enforcement Commences, a Tougher New Data Privacy Law Will Go Before California Voters in November

Client Alert | July 1, 2020

Today marks the date that the California Consumer Privacy Act ("CCPA") becomes enforceable. Just one week ago, however, on June 24, 2020, a new and tougher proposed privacy law, the California Privacy Rights Act ("CPRA"), cleared the final hurdle to appear on the November 3, 2020 ballot in California. The CPRA ballot initiative represents an effort to address the perceived inadequacies of the CCPA, which, according to some, was hastily enacted into law by the California state legislature to avoid its enactment as a ballot initiative. Further, the ballot initiative reflects a fear by its proponents that the California legislature will make compromises that are, by its own standards, unacceptable. Hence, unlike the CCPA, if the CPRA is enacted by California voters in November, it could not be amended by the state legislature. Given the significance of the proposed privacy provisions (one of which would create a new state privacy enforcement agency to replace the Attorney General as the police of privacy rights), the prospects of the CPRA on the November ballot should be monitored.

Below we highlight a few notable aspects of the CPRA, including important dates.

Background

In September 2019, before the CCPA even went into effect, Alastair Mactaggart and the Californians for Consumer Privacy (the non-profit group behind the original CCPA initiative in 2018), filed the new ballot initiative, CPRA (referred to by many as "CCPA 2.0"). If enacted in November, the CPRA would become state law as written, and could be amended only by another ballot initiative, not the state legislature, as noted above.

By mid-march 2020, the Californians for Consumer Privacy reported that it had collected more than enough signatures (roughly 930,000) to appear on the November 2020 ballot. Though delays in the counties' official signature counting process nearly derailed the CPRA as a viable ballot initiative (prompting Californians for Consumer Privacy to file a motion for writ of mandate to order the Secretary of State to direct the counties to complete the process by the deadline), two of the final three counties alone reported 718,233 verified signatures, which is more than the required number of 675,000 signatures to put the initiative on the November 2020 ballot. This final verification occurred just one day before the June 25, 2020 deadline.

Brief Overview of CPRA and its Interaction with CCPA

If the CPRA is approved by California voters in November, it will go into effect on January 1, 2023. Until that time, the CCPA will remain in full force and effect, and compliance with the CCPA will be critical. Indeed, under Section 1798.185(c) of the CCPA, the California Attorney General is authorized to enforce the CCPA starting today, July 1,

Related People

Benjamin Wagner

Cassandra L. Gaedt-Sheckter

2020.[1]

The CPRA would impose new obligations that would only apply to personal information ("PI") collected after January 1, 2023, except the right to access personal information would extend to personal information collected on or after January 1, 2022. The CPRA would grant the California Attorney General the power at the outset to adopt regulations to expand upon and update the CCPA until July 1, 2021, at which point a newly created California Protection Agency would assume responsibility for administering the law. In addition, the final regulations arising from the CPRA would need to be adopted by July 1, 2022, a full year before the CPRA goes into effect.

Importantly, the CPRA would also extend the current moratoria on the application of CCPA to PI collected in the employee/job applicant and business-to-business contexts until January 1, 2023, allowing the legislature time to consider addressing those categories in a separate bill. This extension would be effective immediately, should the ballot measure pass, and the extended timeline should give businesses the time necessary to prepare for the compliance challenges that might arise with respect to these categories of PI.

Among the other significant changes that the CPRA would effectuate are: clarification of the definition of "sale" of PI and related obligations (e.g., to explicitly include the "sharing" of PI for monetary or other valuable consideration, and clarifying obligations regarding "cross-context behavioral advertising"); the expansion of consumer rights to include the right to correct PI and limit the use of sensitive PI (the definition of which the CPRA seeks to amend); data retention limitation requirements; service provider obligations to assist businesses with CPRA compliance; and the expansion of the private right of action to cover breach of an email address in combination with a password and security question and answer permitting access to the email account. Notably, the CPRA does *not* add a comprehensive private right of action for any other violations, leaving that enforcement to the proposed California Protection Agency.

Looking Forward

Because the initiative has only been certified for four days, the prospects for the initiative in the November election are unclear. It can be expected that the initiative will garner significant support, however. The CPRA joins nearly a dozen other initiatives that will also be on the ballot in California in November.

As the possibility of the CPRA moves closer to reality, we will provide additional information on how it will change data privacy and cybersecurity regulation in California. In the meantime, if you are interested in hearing more about the most notable provisions, and their application to your particular concerns, we are happy to discuss. Please do not hesitate to contact anyone in the list below with your questions.

---

[1] California Attorney General Xavier Becerra recently denied requests to consider a 6-month enforcement delay to January 2, 2021, due to challenges and disruptions presented by the coronavirus pandemic, including a request from a coalition of more than 60 businesses led by the Association of National Advertisers. Attorney General Becerra's office noted in an email to *Forbes*, "Right now, we're committed to enforcing the law upon finalizing the rules or July 1, whichever comes first. . .We're all mindful of the new reality created by COVID-19 and the heightened value of protecting consumers' privacy online that comes with it. We encourage businesses to be particularly mindful of data security in this time of emergency." *See* Marty Swant, "Citing COVID-19, Trade Groups Ask California's Attorney General To Delay Data Privacy Enforcement," Forbes (Mar. 19, 2020), available at: https://www.forbes.com/sites/martyswant/2020/03/19/citing-covid-19-trade-groups-ask-californias-attorney-general-to-delay-data-privacy-enforcement/#1ecf88de5c30.

GIBSON DUNN

The following Gibson Dunn lawyers assisted in the preparation of this client update: Alexander Southwell, Benjamin Wagner, Cassandra Gaedt-Sheckter, and Lisa Zivkovic.

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)
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)

GIBSON DUNN

Related Capabilities

Privacy, Cybersecurity, and Data Innovation