GIBSON DUNN

California Privacy Protection Agency Rulemaking Begins and Heightened Privacy Focus Continues

Client Alert | November 23, 2021

As we head into a new year, and the California Privacy Rights Act ("CPRA") inches closer to its effective date of January 1, 2023 (with enforcement scheduled to begin six months later), the new California Privacy Protection Agency ("CPPA") has begun holding regular public meetings. The CPPA's chair and board members were appointed in March, and the tasks ahead are substantial: the board is charged with writing and revising a slew of new regulations to implement the sweeping privacy law under the pioneering agency's purview, before it turns to enforcing them. At the CPPA's recent meetings, board members have discussed the agency's goals and the steps they have taken to launch the new agency.

By way of background, the California Attorney General ("AG") already drafted rules under the CPRA's predecessor, the California Consumer Privacy Act ("CCPA"), and both the CCPA and its implementing regulations remain *enforceable* until *July 1, 2023*, when enforcement of the CPRA begins.[1] The CPRA will amend the CCPA when it takes effect, and the CPPA has the authority to update the current CCPA regulations, in addition to writing new regulations that will implement the CPRA.

The CPPA's first meeting took place in June 2021, and the board has met several times since then, including as recently as Monday, November 15. These initial meetings have given some clues about what to expect from its rulemaking—and when to expect it:

- **Impact of Hiring Delays**: The CPPA's five-member board noted that the pace of hiring has slowed the CPPA's ability to structure the organization, hold informational hearings, and conduct research to determine the focus of its rulemaking. That said, the pace may pick up soon—in October, the CPPA hired an executive director, Ashkan Soltani, a former FTC chief technologist who is now running the agency's day-to-day operations. Those operations include hiring much of the staff, with the board's input. The CPPA's board has also been tackling the minutiae of creating a new agency, from finding office space in Sacramento, to adopting a required conflict-of-interest code. In the meantime, the AG's Office has been providing the CPPA with administrative support as the agency gets off the ground.
- **Current Clues on Timing of the Draft Regulations**: The CPPA will soon replace the AG's Office in drafting implementing regulations, and could begin promulgating those rules as soon as April, though timing is still unclear. Under the CPRA, the CPPA will supersede the AG's *authority* to promulgate rules the later of July 1, 2021, or six months after the CPPA formally notifies the AG that it is prepared to issue rules. (Note that although the language in the CPRA initially stated that this deadline would be the *earlier* of the two, AB 694 clarified that it would be the *later* of the two, including in light of the delays noted above.) In its October meeting, the CPPA approved providing that notice to the AG's Office. Depending on when the notice was actually sent, and whether the CPPA will issue rules at the

Related People

Ashlie Beringer

Cassandra L. Gaedt-Sheckter

Abbey A. Barrera

Tony Bedel

time the authority is transitioned, the CPPA could issue rules around April 19, 2022. Interestingly, however, the final regulations must be adopted by July 1, 2022. As some may remember from CCPA's regulatory rulemaking process, there were various required comment periods, which would make meeting that deadline difficult even with promulgation of a draft on that day.

- **Considerations of Expedited Rulemaking or Delayed Enforcement**: In the November meeting, the board considered potential solutions for the challenges it is facing in connection with its rulemaking responsibilities, including the complexity of the issues and its limited staff. These potential solutions include (i) engaging in emergency rulemaking to write rules faster than the standard timeline, (ii) delaying enforcement of the CPRA, (iii) hiring temporary staff, and (iv) staggering rulemaking, many of which could have significant effects on companies' compliance programs and timing.
- **Public Comment Period**: In September 2021, the board called for public comment on its preliminary rulemaking activities, asking the public for feedback on "any area on which the [CPPA] has authority to adopt rules." Some of the specific areas it sought comments on included: when a business's processing of personal information creates a "significant risk" for consumers, triggering additional compliance steps for businesses; how to regulate automated decision making; what information should be provided to respond to a consumer's request for their information; how to define various terms; and specifics regarding effectuating consumers' rights to opt out of the sale of their information, to delete their information, and others. According to the board, it received "dozens" of comments to this initial open-ended call for comments by the November 8, 2021 deadline.
- **Rulemaking Priorities**: While the CPPA reviews its initial public comments, board members are also studying a number of areas for potential rulemaking and considering topics for informational hearings—presumably similar to what we saw in the CCPA rulemaking process—which are used to gather information on certain key issues. To tackle its many tasks, the CPPA board has divided itself into several subcommittees, including ones focused on updates to existing CCPA rules, new CPRA rules, and on the rulemaking process itself. Those subcommittees are considering for rulemaking areas such as defining the terms "business purposes" and "law enforcement agency approved investigation;" recordkeeping requirements for cybersecurity audits, risk assessments, automated decision making, and other areas; clarifying how the CPRA will apply to insurance companies; and prescribing how to conduct the rulemaking process itself. For informational hearings, the board highlighted areas such as automated decision-making technologies, profiling, and harmonization with global frameworks; and how the current rules governing consumer opt outs are operating "in the wild" for consumers and businesses.
- **Additional Goals**: Board members also noted they want to make sure they are educating Californians about their privacy rights and ensure that outreach is available to speakers of languages other than English.

Further Legislative Privacy Measures

The CPPA is not alone in crafting new data privacy requirements. In October, California Governor Gavin Newsom signed legislation that made technical changes in the CPRA through AB 694 (mentioned above), clarifying when the CPPA would assume its rulemaking authority.

Also in October, Governor Newsom signed the Genetic Information Privacy Act to impose new requirements on direct-to-consumer genetic testing companies and other companies that use the genetic data they collect. The new law requires those companies to, among other things, make additional disclosures to consumers, obtain express consumer consent for different uses of consumers' genetic information, and timely destroy consumers' genetic samples if requested. The law allows the AG to collect civil penalties of up to

$10,000 for each willful violation. Separately, the governor also signed a bill that adds "genetic information" to the definition of personal information in California's data-breach law.

Next Steps

Despite Governor Newsom's initiatives and all of the CPPA's efforts so far, we can expect months of uncertainty before companies have a clear sense of what rules may supplement the CPRA's language. But companies cannot wait until the CPPA completes its rulemaking to start thinking about their compliance programs, particularly in those areas not covered under existing regulations, such as automated decision making and profiling. Given the complexity of the CPRA and its new requirements—and important sunsetting provisions on employment and B2B data that may have left companies with opportunities to avoid compliance with CCPA on large swaths of data—companies should begin planning now for how they will comply with the enacted amendments to the CCPA. In particular, companies should, sooner than later:

- **(Re)consider collection and storage of personal information**: Even though the CPRA does not come into effect until January 2023, the CPRA will give consumers the right to request access to personal information collected on or after January 1, 2022, and for any personal information collected from January 1, 2023 forward, the CPRA may give consumers the right to request their historical information beyond the CCPA's 12-month look back. Companies should start thinking about how to collect and store personal information in a way that will allow them to respond to such a request (if such information is indeed subject to the right), and begin analyzing how new rights such as the right to limit the use of sensitive personal information, right to opt out of sharing, and right of employees to the same protections, may apply to your business. In particular, the distinction between personal information and sensitive personal information may affect how information should be collected and stored.
- **Design a plan to revise privacy-related documents**: In light of changes to service provider and contractor requirements, transparency and disclosure requirements (including relating to data subject rights), retention limitation requirements, and additional changes in the CPRA, it is a good time to start reviewing vendor contracts, privacy statements, data retention practices and policies, and other privacy-related documents.
- **Prepare for compliance with respect to employment and B2B data**: The CPRA extended until January 1, 2023, exemptions in the CCPA for business-to-business and employment-related data. To the extent companies have avoided bringing those categories of data into compliance so far, they may want to revisit those decisions as the exemptions near their end.
- **Don't neglect CCPA compliance**: Given that CCPA will continue to be enforceable until July 1, 2023, and the roll-out of regulations over the course of 2020 may have left some with outdated compliance programs that should be updated, it is a good time to revisit that compliance as well.
- **Remain nimble**: Rulemaking will clarify certain requirements. Companies should therefore be prepared to modify certain aspects of their compliance programs as those rules take shape.

Of course, businesses should also take heed that it's not just California they should be paying attention to: Colorado and Virginia have also implemented comprehensive privacy laws that will take effect in 2023, as our prior updates have detailed, and consideration of a national privacy program from the ground up may be most efficient.

We will continue to monitor developments, and are available to discuss these issues as applied to your particular business.

[1] Cal Civ. Code § 1798.185(d).

This alert was prepared by Ashlie Beringer, Alexander H. Southwell, Cassandra L. Gaedt-Sheckter, Abbey A. Barrera, Eric M. Hornbeck, and Tony Bedel.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity and Data Innovation practice group.

Privacy, Cybersecurity and Data Innovation Group:

United States
Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@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)
David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@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)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Deborah L. Stein – Los Angeles (+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)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)

Europe
Ahmed Baladi – Co-Chair, PCDI 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)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@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)
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)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

GIBSON DUNN

Related Capabilities

Privacy, Cybersecurity, and Data Innovation