Privacy & Data Security Law News

INSIGHT: California Privacy Rights Act—Key Takeaways for Businesses

By Mark Brennan, Bret Cohen, Tim Tobin, and Filippo Raso

July 15, 2020, 4:01 AM

The July 1 California Consumer Privacy Act's enforcement start date just passed, and there's a new law to focus on ahead of Election Day, the California Privacy Rights Act, which recently received enough signatures to make it onto the November ballot. Hogan Lovells attorneys break down everything businesses need to know.

Just days before California Consumer Privacy Act (CCPA) enforcement began on July 1, the California Privacy Rights Act (CPRA) qualified to be on California's Nov. 3 ballot. Drafted by the proponents behind the ballot that spurred the CCPA's enactment, the CPRA might find support among voters based on past polling.

While the CPRA has cleared significant procedural hurdles, it should not distract businesses from focusing on compliance with the CCPA and the California Attorney General's final CCPA regulations. Businesses should, however, track and be mindful of privacy developments that impact their privacy programs, such as the CPRA's ballot results and legislative action in California, other states, and in Congress.

What Is the CPRA?

The CPRA is a consumer privacy ballot initiative from Californians for Consumer Privacy, a non-profit privacy advocacy organization that spurred the enactment of the CCPA in 2018. On June 25, the CPRA qualified to be on California's ballot in the upcoming general election.

If California voters approve the measure, the CPRA would establish and fund the California Privacy Protection Agency (Agency), a state agency dedicated to enforcing privacy. The CPRA also would extend the CCPA's business-to-business and human resources exceptions until Jan.1, 2023.

The CPRA incorporates the CCPA, which will continue in effect. CPRA's additional substantive obligations would take effect Jan. 1, 2023, with enforcement of CPRA-related obligations beginning July 1, 2023.

The CPRA would greatly expand the CCPA and impose novel obligations on businesses, grant consumers new rights, and modify the CCPA's enforcement provisions. Below are just a few of the notable changes the CPRA would make to the CCPA:

- Prohibits service providers from combining personal information collected as a service provider with information received from other businesses or collected in the service provider's "business" capacity (subject to certain exceptions).
- Imposes data security, storage limitation, and data minimization requirements.
- Requires businesses to enter into contracts with third parties to which the business sells or "shares" personal information, with "sharing" referring to transfers for cross-contextual advertising.
- Mandates the Agency to promulgate rules governing audits and risk assessments from entities that conduct certain processing activities.
- Allows consumers to:
  - Request that a business use commercially reasonable efforts to correct inaccurate personal information in response to a verifiable request;
  - Opt out of "sharing," which the CPRA would define as disclosures of personal information for cross-contextual advertising;
  - Limit a business's use and disclosure of the consumer's "sensitive personal information," which includes a wide range of data elements;
  - Subject to a rulemaking proceeding, opt out of automated decision making and profiling.

- Eliminates the 30-day "cure" period before an instance of non-compliance results in a "violation" of the CCPA.
- Expands the CCPA's private right of action to include unauthorized access or disclosure of an email address and password or security question that would permit access to the account if the access or disclosure resulted from a failure to implement reasonable security measures.

What Should Businesses Do Now?

The CPRA does not change much immediately, even if approved by voters. Importantly, businesses should keep their CCPA compliance efforts moving forward.

As of July 1, the California attorney general can enforce the CCPA's statutory provisions. The final regulations will become enforceable soon thereafter, and the CCPA's requirements will remain enforceable even if the CPRA is approved.

If California voters approve CPRA, businesses can begin planning compliance efforts leading to Jan. 1, 2023. This might include re-evaluating data inventories and data maps to determine if they are sufficient under the CPRA, determining what existing CCPA and GDPR compliance processes can be leveraged, and assessing whether existing technology be configured or adapted in response to CPRA.

Businesses should also monitor privacy developments closely in California, in other states, and at the federal level. Businesses should watch for federal legislation—with the CPRA, it is possible that Congressional appetite for comprehensive federal privacy legislation will increase, especially if other states enact privacy legislation with differing requirements.

If California voters do not approve CPRA, businesses should prepare for the Jan. 1, 2021, expiration of the CCPA's temporary exceptions for employee and business-to-business (B2B) information. California's state legislature could extend the exceptions even if CPRA does not pass, but it would have a short window of opportunity to do so between the November election and Jan. 1, 2021.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

Mark Brennan is the global Lead Innovation partner for Hogan Lovells and the head of its Technology & Telecoms Industry Sector Group. He represents a wide range of clients on a variety of matters including privacy, communications, and artificial intelligence.

Bret Cohen is a partner in Hogan Lovells Privacy and Cybersecurity practice group based in Washington, D.C. With a practice focused on the internet and e-commerce, He has advised extensively on legal issues related to cloud computing, social media, mobile applications, online tracking and analytics, and software development.

Tim Tobin is a partner in Hogan Lovells Privacy and Cybersecurity practice. His two decades of legal experience involve advising clients on privacy matters ranging involving marketing and advertising, contracting and deals, the development of new products and technologies, cross-border data sharing, and within the workplace.

Filippo Raso is a Washington, D.C.-based associate in Hogan Lovells' Privacy and Cybersecurity practice. His practice focuses on helping clients traverse the evolving privacy, security, and data protection landscape so they can keep delivering innovative products.