CalCPA Evolves – US Chamber Supports Federal Standard

by Joseph Lynyak

The California Legislature has passed a bill to amend the California Consumer Privacy Act of 2018 (the "CCPA") that eliminates Attorney General's gate keeping function, and fixes various drafting errors. Senate Bill No. 1121 now awaits the Governor's signature.

Attorney General's Gate Keeping Removed From Private Rights of Action.

Most notable among the proposed amendments, consumers exercising the CCPA's private right of action would no longer be required to wait up to six months for the Attorney General to assume responsibility for prosecuting the claimed violations. This accomplishes two important objectives: it relieves anticipated pressure on the AG to act as a gate keeper tasked with reviewing the merits of various claims to determine whether the AG's office itself should become involved, and lowers the bar for potential claimants. Counter-balancing that expansion, the bill clarifies that the private right of action applies only to claims related to data breaches, and reserves to the Attorney General alone the authority to prosecute other violations of the CCPA.

The bill further clarifies the maximum penalty for a business's failure to "implement and maintain reasonable security procedures and practices." The original language of the CCPA arguably authorized a fine of up to $7,500 for *any* violation. The enhanced fine level is now clearly limited to *intentional* violations, rather than simply negligent ones.

The bill also relieves pressure on the Attorney General's office by postponing the deadline for issuing implementing regulations until July 1, 2020. Consistent with that amendment, the Attorney General would not be authorized to commence enforcement actions until July 1, 2020, or six months after the regulations are issued, whichever occurs first. The recent amendments do not, however, delay the CCPA's effective date from January 1, 2020, which theoretically would allow the Attorney General to bring enforcement actions commencing on July 1, 2020, for claimed violations that occurred starting in January.

Related People

- Joseph Lynyak

Related Capabilities

- Privacy & Social Media
- Consumer Financial Services
- Securities & Financial Services Litigation & Enforcement

Scope of “Personal Information” Redefined; Medical and Financial Exemptions Clarified.

The bill narrows the definition of “personal information” to step back from what many viewed as unnecessary overreach concerning information that could not, without more, actually be linked to any individual. Identifiers such as IP addresses, geolocation data, or purchasing history are “personal information” *only if* they can be “reasonably linked, directly or indirectly, with a particular consumer or household.” The revised CCPA still breaks new ground by applying privacy protections to data associated with “households,” and “devices”, even though neither are actually ‘personal’ information.

Also of significant import, the bill now expressly limits the CCPA’s applicability to exclude covered entities and health care providers covered under HIPAA and California’s Confidentiality of Medical Information Act. Similarly, the amendments limit the scope of the CCPA to avoid duplicate regulation of entities already covered by GLBA and the California Financial Information Privacy Act. Businesses and privacy advocates have raised numerous other concerns about the CCPA, some substantive, others more mechanical, not addressed by the legislature, although potentially open for further discussion in the 2019 legislative session.

US Chamber of Commerce Releases Privacy Principles

The impact of CCPA unquestionably transcends far beyond California’s borders, and other similar state initiatives are already in the works. Acknowledging that the privacy genie is not going back into the bottle, the US Chamber of Commerce and various tech companies have shifted their focus from opposing aspects of the CCPA considered objectionable to a uniform national privacy approach. Traditionally thought impossible in an era of Congressional gridlock, a single, preemptive national approach advocated in the Chambers’ Privacy Principles signals a dramatic shift in the tactics of companies concerned about the impact and potential unintended consequences of ever-more ambitious privacy initiatives. Translating the principles (set forth below) into detailed legislation will be challenging enough, but even if the substantive provisions could be agreed upon, any attempt to preempt state law is sure to ignite impassioned debate.

Proposed Privacy Principles

- Nationwide Privacy Framework
- Privacy Protections Should be Risk-Focused and Contextual
- Transparency in collection and use of personal data with consumer notifications
- Industry Neutrality
- Flexibility
- Harm-Focused Enforcement
- Enforcement Should Promote Efficient and Collaborative Compliance
- International Leadership
- Encouraging Privacy Innovation
- Tailored Security Obligations but Uniform Breach Notification

What's Next

Given the dynamic nature of the regulatory environment, many small-to-medium sized companies may be tempted to 'wait and see how it all shakes out.' While that reaction is understandable, it may be short-sighted. Basic principles of information governance are not going to change, and regardless of how the next chapter of privacy protection laws may ultimately be written, companies need to know what personal information they are collecting, how they are sharing and using it, and be transparent in their disclosures to their customers and clients.