As CCPA Effective Date Draws Nearer, Hearings Highlight Potentially Increased Liability Risks

The U.S. privacy law scene continues to become more complex. In the lead-up to the California Consumer Privacy Act's (CCPA) January 1, 2020 effective date, at least seven additional states have pending comprehensive privacy legislation. The number of Federal and California hearings and forums have reached fever pitch. The California Attorney General's Office supports an even greater private right of action. Multiple new California bills have been introduced. What's a company to do?

We provide updates below on the recent flurry of activity surrounding the CCPA, detailing the California Assembly Hearing on the CCPA, the U.S. Senate and House hearings concerning preemptive federal legislation, the introduction of CCPA-clarifying legislation, and the explosion of CCPA-analogous state privacy laws. The time is now to begin efforts at complying with the CCPA. Privacy laws are coming, and in the absence of a federal or multivariate state network, businesses should ready themselves for the law on the books come 2020 - the CCPA.

California State Assembly Hearing

On February 20, 2019, the California Privacy and Consumer Protection Committee heard from witnesses concerned about definitions, logistics, and consequences, intended and otherwise for both businesses and consumers, under the CCPA. Of particular note was the testimony by Stacey Schesser, Supervising Deputy Attorney General on Consumer Protection. Schesser criticized the Act's 30-day cure period as a "get out of jail free" card, eschewed the entitlement of individual businesses to seek compliance guidance from the Office, citing a diversion of resources away from enforcement, and proposed broadening the private right of action to cover the entire CCPA, as opposed to merely data breaches.

The time and expense necessary to satisfy impending CCPA obligations is compounded by somewhat nontransferable efforts to comply with last year's EU General Data Protection Regulation (GDPR). According to witness Tanya Forsheit, Partner and Chair of the Privacy & Data Security Group at Frankfurt Kurnit Klein & Selz, "88% of companies

Related Capabilities

- Privacy & Social Media
- Trademark, Copyright + Advertising
- Technology Commerce
- Technology
- California Consumer Privacy Act (CCPA)

spent more than $1 million on preparing for the GDPR," an implementation for which they had two years to prepare. And yet, "[d]espite that longer runway under the GDPR and these considerable investments in time and expense, many if not most US companies are still not in compliance because the undertaking is so significant." Implementing the CCPA will be more complex than the GDPR in some respects (and on a truncated timeline). Thus, unsurprisingly, stakeholders have reinvigorated calls for a preemptive federal privacy law.

Federal Hearings

To that end, the Senate and the House held separate hearings to conceptualize the contours of a federal privacy law. The House hearing took place on February 26, 2019, before an Energy and Commerce subcommittee, and included witnesses from advocacy groups such as Color of Change and the Center for Democracy & Technology, as well as witnesses from IAB, the American Enterprise Institute, and Business Roundtable. For its part, the Senate held a hearing before the Commerce, Science, and Transportation Committee on February 27, 2019, receiving testimony from representatives of such groups as the Internet Association, the Retail Industry Leaders Association, BSA - The Software Alliance, the Interactive Advertising Bureau, and the 21st Century Privacy Coalition.

In a post-GDPR, multijurisdictional privacy landscape, interested parties, like Google, Microsoft, and Apple, are championing federal privacy legislation to salve state-by-state fragmentation, and its attendant compliance demands. And yet, to actualize a federal privacy law, compromise will be necessary. Key issues outstanding include the scope of preemption of state laws, a previous point of contention between industry stakeholders and privacy advocates, the appropriate mechanism, locus, and sanction of enforcement, the characteristics of the data to be protected, the entitlements of businesses to make use of that data, and the rights of consumers to define the parameters of that use.

Additional California Legislation

Where Stacey Schesser characterized the CCPA's current iteration as beset by "unworkable obligations and operational challenges," the bipartisan obstacles to federal lawmaking might make preemptive legislation of the kind imagined above all but infeasible. In light of that situation, California lawmakers have begun introducing legislation aimed at remedying CCPA infirmities. Of note, California Attorney General Xavier Becerra and State Senator Hannah-Beth Jackson have introduced a bill to actualize Stacey Schesser's recommendations to the Committee on Privacy and Consumer Protection. Senate Bill 561 relieves the Attorney General's Office from issuing advisory opinions to individual businesses, eliminates businesses' 30-day right to cure preceding penalization, and expands the private right of action to cover any violation of the CCPA.

Furthermore, California lawmakers recently introduced AB 846 and AB 950, which respectively empower consumers under the CCPA to participate in incentive-generating customer loyalty programs, and obligate businesses collecting data from California

consumers to disclose the average monetary value to the business of that data, and, in cases where the business sells consumer data, to disclose, upon receipt of a verifiable request, the actual price it commanded for that data.

Analogous State Privacy Laws

California is not the only state endeavoring to legislate on behalf of its residents. Various other states have introduced CCPA-derivative legislation, characterized by differences large and small, including Hawaii (S.B. 418), Maryland (S.B. 613), Massachusetts (S.D. 341), New Mexico (S.B. 176), and Rhode Island (S.B. 234). Other states , such as New York (S.B. 224), have introduced bills addressing, though not replicating, the legislative imperatives of the CCPA. For its part, Washington has introduced a privacy bill, S.B. 5376, more closely modeled on the GDPR. Unlike the CCPA, the aforementioned initiatives remain uncodified. However, they portend a patchwork privacy regime with which businesses may soon have to reckon.

Actions Needed

As indicated above, privacy legislation is on the horizon. While the futures of federal and many state initiatives remain uncertain, the CCPA is upon us. Therefore, it is imperative that businesses begin readying themselves to comply with the CCPA come January 1. Where the threat of private litigation, particularly in light of the California Attorney General's recent calls for expansion of that right, looms large, the most important step businesses can take now is assessing, strengthening, and documenting their data security regimes. In the event of breach, businesses need to provide evidence of "reasonable security procedures," necessitating written security policies and incident response plans, data protective vendor agreements, appropriate insurance coverage, personnel training, and adherence to industry standards, among other best practices.

Furthermore, some aspects of compliance will require development time. Businesses should begin effecting the required opt-out and opt-in functionality. As part of the opt-out right under the CCPA, businesses must enable a link with the phrase "Do Not Sell My Personal Information" on their websites, as well as provide a toll-free telephone number to field opt-out requests. Businesses should start to consider now whether they will ultimately create a separate California version of their websites, or whether they will afford the same rights to all consumers, and begin to actualize the technological demands of that choice.