HWG | HARRIS, WILTSHIRE & GRANNIS LLP

CLIENT ADVISORY

November 4, 2020

Post-Election Update | California Privacy Ballot Initiative Passes

As commentators endlessly reminded us last night, the U.S. election was not just about the presidency: it was also about Congressional representatives, state and local government seats, and increasingly ubiquitous state and local ballot initiatives. While we may not yet know who won the presidency, we do know that one of those initiatives, the California Privacy Rights and Enforcement Act of 2020 (CPRA), passed in a landslide. If your organization has not yet begun planning for the CPRA, here is our high-level primer on why many organizations should start planning now.

Didn't California just put a broadly applicable consumer privacy law into place?

Yes, but the legal landscape is changing yet again. In 2018, in response to a ballot initiative, the California legislature adopted the Consumer Privacy Act of 2018 (CCPA), a data protection law that imposed certain obligations on organizations collecting personal information from California residents, where the organization has annual gross revenues above $25 million or processes personal information on 50,000 individuals, households, or devices. Most provisions of the CCPA went into effect on January 1, 2020. Regulations implementing the CCPA went into effect on July 1, 2020, and proposed regulatory amendments are currently under consideration.

Does the CPRA overlap with other privacy laws?

Somewhat, but far from entirely. U.S.-only companies may be surprised by the European-style approach of the CPRA. For example, the CPRA grants Californians a number of privacy-related rights that did not previously exist in the United States, outside of narrow, highly-regulated contexts (like healthcare). Among other rights, a consumer has a right to request that a business correct inaccurate personal information about the consumer. Businesses that collect personal information also must inform consumers of the length of time the business intends to retain each category of personal information.

Companies that have already faced non-U.S. privacy obligations (such as the European Union's General Data Protection Regulation and Brazil's recently enacted data protection law, the Lei Geral de Proteção de Dados Pessoais) may also see new obligations and new definitions. For example, under the CPRA, consumers have the right to direct a business which collects sensitive personal information to limit its use of that information to the use necessary to perform services or provide goods to the consumer. Though similar rights exist under non-U.S. laws, the CPRA defines "sensitive personal information" more broadly than other data protection laws—to include information that reveals government-issued identifier numbers, such as a social security number, passport number, or driver's license number; account log-in credentials in combination with any required credentials allowing access to an account; precise geolocation; and the contents of mail, email, and text messages (unless the business is the intended recipient of the message).

How will the CPRA be enforced?

The CPRA establishes the California Privacy Protection Agency, governed by a five-member board, with full implementation and enforcement authority. The Privacy Protection Agency will be the first independent government enforcement agency in the United States dedicated solely to privacy, and will have subpoena and audit powers.

The CPRA also expands on the CCPA's private right of action against businesses that fail to maintain reasonable security procedures, allowing consumers to sue without showing actual damages when an email address, in combination with a password or security question and answer that would permit access to the account, is subject to unauthorized disclosure or theft.

How long until the CPRA goes into effect?

The CPRA will come into effect on January 1, 2023. Like other data protection laws, complying with the CPRA may require changes to an organization's internal operations, vendor relationships, and public disclosures. These changes can take some time. Moreover, some changes may need to be partially or entirely in place before January 1, 2022, when the organization begins to collect personal information that will be covered by the CPRA when it comes into effect a year later. We encourage companies to begin reviewing the impact of the CPRA and planning for compliance as soon as possible and, in any event, in advance of 2022.

In addition to these ongoing work product and privilege updates, our firm has gathered state and local corona virus advisories being issued by the government. Here is a link to that webpage: https://www.hwglaw.com/state-and-local-covid-19-orders/.

* * * * *

For more information on the California Privacy Rights Act or HWG's data privacy, security, and governance practice, please contact Adrienne Fowler* (afowler@hwglaw.com), Becky Burr (bburr@hwglaw.com), Deepika Ravi (dravi@hwglaw.com), or the HWG lawyer with whom you regularly work.

*Admitted in New York only. Practice limited to matters before federal departments, agencies, and courts.