DORSEY

DORSEY+WHITNEY LLP

Global Pandemic Raises Importance of Privacy and Security Compliance as California Attorney General's Office Signals No Delay on CCPA Enforcement

As much of America's work force shelters at home and many corporate offices shutter doors (for now) during the global COVID-19 pandemic, remote working becomes the new reality. Inevitably, even the tech savviest companies have found themselves facing privacy and security problems with digitized operations.

Tech giants have been plagued by privacy issues and resulting headlines leading to swift revisions to privacy policies and disclosures. And, as expected, class action California Consumer Privacy Act ("CCPA") lawsuits regarding unauthorized disclosure of personal information quickly followed. Unfortunately, the news is all too familiar given that the focus on consumer privacy rights has spread from Europe and General Data Protection Regulation ("GDPR") enforcement to the United States.

Heralded as the strictest privacy law in the country, the CCPA went into effect January 1, 2020, but Attorney General ("AG") enforcement looms as the office moves to finalize the draft regulations implementing the Act by July 1, 2020. On March 11, 2020, the AG's office released its third draft regulations, with the comment period ending on proposed modifications March 27, 2020. While maintaining these swift and multiple revisions, the AG has stated that enforcement will stay on its current timeline.

Consumers were able to begin exercising their rights as to data breaches under the CCPA on January 1, 2020, and quickly class action lawsuits pleading a cause of action under the CCPA, among other alleged violations, were filed. The CCPA makes clear that businesses are required to implement and maintain reasonable security procedures and practices to protect consumers' personal information. Consumers are authorized to institute a civil action if their personal information, as defined in Section 1798.81.5 of the Act is subject to an unauthorized breach as a result of a business's failure to reasonably secure this data. Dorsey expanded on what reasonable security entailed here.

The California AG recently stated, "Right now, we're committed to enforcing the law upon finalizing the rules or July 1, whichever comes first…We're all mindful of the new reality

Related Capabilities

- California Consumer Privacy Act (CCPA)
- Privacy & Social Media

created by COVID-19 and the heightened value of protecting consumers' privacy online that comes with it. We encourage businesses to be particularly mindful of data security in this time of emergency." The California AG even issued estimates for initial CCPA compliance costs here.

With enforcement only months away, it's more imperative than ever to address compliance measures, even remotely, because risk of noncompliance is high -- a civil penalty of up to $2,500 per violation or $7,500 per intentional violation and 30 days to become compliant. The emphasis being on "per" violation, which may prove costly.

This means technical resources need to be put in place to keep operations running on a global scale. As the AG's office has signaled, even despite the issues COVID-19 presents, companies use COVID-19 as an excuse for noncompliance. Indeed, if GDPR is a prelude to CCPA enforcement, we may see employee illness tracking and screening actions resulting in legal violations in the United States too. For companies, that means confirming legal review of key policies, revising protocols for consumer requests for information, implementing or continuing to improve data protection programs, and otherwise upping privacy and security measures.