CCPA Enforcement Remains on Track Despite COVID-19 Pandemic

May 21, 2020

Just a few months ago, compliance with the California Consumer Privacy Act (the CCPA) was at the top of many businesses' priority lists for 2020. With the COVID-19 pandemic, many businesses put privacy compliance and the CCPA on the backburner, thinking the July 1, 2020 enforcement date would be postponed. The California Attorney General has maintained the current enforcement date, however, stating businesses must remain vigilant about consumers' privacy during the pandemic. Private lawsuits under the CCPA for security breaches of Californians' personal information are not limited by the July 1 enforcement date, and some plaintiffs have already filed suit. Businesses need to initiate, continue or resume their CCPA compliance efforts.

The CCPA has a broad reach. It applies to any for-profit business that collects personal information from California residents and meets at least one of the following: a) annual gross revenues of $25 million or more; b) buys, receives, sells or shares the personal information of at least 50,000 California residents, households or devices annually; or c) derives a minimum of 50% of its annual revenue from selling California residents' personal information.

A business subject to the CCPA must evaluate how it collects, uses and shares the personal information of California residents. The first step is data mapping, to determine what data the business collects and for what purpose. Next, compliance typically involves updating website privacy policies, revising third-party and vendor agreements, and - if necessary - putting a "Do Not Sell" button on websites. To succeed in a CCPA private right of action, a plaintiff must show that the defendant business failed to maintain reasonable data security, so it is important that a business can show that has in place a written information security program and incident response plan.

As expected, CCPA and other privacy litigation is on the rise, increasingly in the form of class actions. Some lawsuits have alleged poor security practices and inadequate disclosures by communication services like Zoom and Houseparty, beneficiaries of remote work arrangements and stay-at-home orders. Other suits, independent of the pandemic, highlight pressing issues of first impression. Ring, the home security company, faces class action litigation that implicates the CCPA notice provisions, private rights of action and whether arbitration provisions are valid under the CCPA.

CCPA 2.0 is on the horizon. The new ballot initiative from Alastair MacTaggart, the founder of the privacy nonprofit Californians for Consumer Privacy and catalyst for the original CCPA, now appears to have garnered enough signatures for the November general election in California. If passed, it would likely take effect in 2023. CCPA 2.0 includes a new right to correct personal information and the creation of a new California privacy law enforcement agency. The ballot initiative would also extend the CCPA exemptions for employee and business-to-business data for two years; otherwise these exemptions expire on January 1, 2021. Following this trend, Washington, New York and other states have introduced new privacy laws and we will continue to monitor these legislative initiatives.

If you have questions regarding CCPA compliance, please contact any of the following members of Lathrop GPM's Privacy Team: Tedrick Housh, Michael Cohen, or Reid Day.