DAE Client Alert

CCPA GAINING STEAM

Evan Ladd

eladd@dollamir.com

APRIL 2020

The California Consumer Privacy Act ("CCPA") is proving to be exactly what supporters and critics believed it would be—a sea change in privacy protections and expectations regarding how companies use personal data. Only a few months into its "live" date, the CCPA is spurring action on all fronts—litigation, regulatory, and legislative.

Litigation

In the first four months of this year, CCPA-based claims have appeared in a number of complaints. The examples below highlight key theories consumers are testing to broaden the application of the CCPA.

- CCPA as a predicate:
    - In the first of many complaints filed against Zoom, the increasingly popular video conferencing company (which has seen an almost 20X increase in usage this year), the plaintiff alleges violations of the CCPA as a stand-alone count and as a predicate under California's Unfair Competition Law ("UCL"), Cal. Civ. Code § 17200, *et seq*. *Cullen v. Zoom Video Commc'ns Inc.*, 5:20-cv-02155 (N.D. Cal. Mar. 30, 2020). The CCPA claim is twofold: (1) Zoom collected and used personal information without adequate notice and (2) Zoom failed to prevent consumer personal information from unauthorized disclosure as a result of failing to implement and maintain reasonable security measures. This is notable because there is no private right of action available for the first alleged violation (collection and use without disclosure). It appears the plaintiffs in *Cullen* are attempting to fold this allegation into their CCPA-based count, and also make this provision a predicate for their claim under the UCL. So far, a court has not had to weigh in on whether the CCPA can serve as a predicate for the UCL when the California Legislature did not provide for a private right of action, but *Cullen* may force the Northern District to opine on this issue. Recently, seven other cases against Zoom were consolidated into the *Cullen* case before U.S. District Judge Lucy H. Koh. *See Taylor*, 5:20-cv-02170; *Johnston*, 5:20-cv-02376; *Kondrat*, 5:20-cv-02520; *Lawton*, 5:20-cv-02592; *Jimenez*, 5:20-cv-02591; *Hartmann*, 5:20-cv-02620; *Henry*, 5:20-cv-02691.

- In *Hurvitz v. Zoom Video Commc'ns, Inc., et al.*, 2:20-cv-03400 (C.D. Cal. April 13, 2020), instead of taking the approach asserted in *Cullen* (folding two CCPA claims together into a UCL claim, one of which has a clear private right of action), the plaintiff in *Hurvitz* is boldly asserting that a violation of the CCPA's collection and use without disclosure is sufficient to support a claim under the UCL. Similar to *Cullen*, the court will likely have to weigh in directly on the UCL predicate question. Notably in *Horvitz*, Facebook and LinkedIn Corp. are also named as co-defendants—the former being a common target for privacy violation claims. (Interestingly, the court in *Hurvitz* issued an Order to Show Cause why venue is appropriate in the Central District of California and not another venue, such as the Northern District of California. Plaintiff filed his response on April 27, and Defendants Zoom, Facebook, and LinkedIn have until May 11 to respond. It is possible, therefore, that this matter may also be consolidated with *Cullen* in the near future.)

- In *Burke v. Clearview AI, Inc., et al.* (originally filed in the Southern District of California as 3:20-cv-00370-BAS, transferred to Southern District of New York as 1:20-cv-03104), the plaintiffs also allege a UCL claim based on an alleged violation of the CCPA's collection and use without disclosure protections. These allegations are similar to those in *Cullen*, however, in contrast to *Cullen*, there are no separate data breach allegations (for which there is a private right of action). Additionally, this case is pending in the Southern District of New York (where other similar cases are pending against the defendants), so any questions regarding the CCPA's private right of action may be examined by a New York federal judge interpreting California's brand new law.

- Retroactivity:

  - In *Barnes v. Hanna Andersson, LLC, et al.*, 3:20-cv-00812-DMR (N.D. Cal. Feb. 3, 2020), the plaintiff alleged several violations against Defendants Hanna Andersson and Salesforce.Com related to a data breach of Hanna Andersson customers in late 2019. The complaint alleges violations of the UCL and the CCPA's data breach provision, Cal. Civ. Code § 1798.150, which provides for a private right of action based on a business' failure to implement and maintain reasonable data security procedures to prevent unauthorized disclosure. Because the data breach occurred in 2019, the court will need to address the question of retroactivity of the CCPA to events prior to its effective date of January 1, 2020.

Regulatory

On February 10, 2020, the California Attorney General released revised proposed regulations in an attempt to provide further clarity on the CCPA. The revised proposed regulations expound on the requirements for data brokers and service providers, requirements for notice and website accessibility, methods for consumer requests and consumer verification prior to responding to requests, and examples of the "Do Not Sell" button and how loyalty programs can be run without running afoul of the CCPA's non-discrimination provision. These proposals garnered significant feedback, which led to revised regulations being released on March 11. The second set of revisions

make further clarifications regarding the duties of data brokers and service providers, duties for businesses that do not directly collect consumer personal information, and removal of the sample "Do Not Sell" button. However, critics have identified places where this second set of revisions fails to provide other badly-needed guidance—for example, a clear definition of "sale" and whether IP addresses are considered personal information.

Comments to the second set of revisions were due on March 27. In the meantime, however, California and many other states were essentially shut down in order to curb the outbreak of COVID-19. As a result, many industry groups requested a deferral on enforcement of the CCPA altogether given the state and nationwide shut down. These groups cited the unexpected challenge that compliance and IT teams at most companies are facing—accommodating a remote workforce, which has taken the focus away from business as usual preparations for the CCPA. Consumer groups responded that because the law has been on the books since 2018, there has been ample time to prepare for CCPA enforcement.

California Attorney General Becerra has recently stated that his office intends to push forward with a July 1, 2020 enforcement schedule. How this actually plays out will be interesting to see given that many companies doing business in California (either from within the state or out of state) are working from home and will likely continue to do so for some time. Therefore, how companies receive and respond to requests for information under the CCPA presents new operational challenges not originally contemplated. At a time when call center staff in almost every industry are already overburdened, fielding calls for requests for information or questions regarding personal data will likely cause even more strain. Furthermore, responding to requests for data presents an additional challenge given certain data storage elements may be unavailable to remote access. Companies will need to employ creative and flexible solutions to their CCPA compliance plans in order to ensure they are protecting and providing information regarding consumer privacy during the stay-at-home periods and beyond.

Legislative

With a new calendar year, we now have insight into proposed privacy laws in many other state legislatures beyond California. Many of these are renewed from last year's legislative sessions, but given the progress many of these laws saw last year in their respective state houses, it is possible that some of them may be signed into law this year. Some of these states include New York and Virginia. New York's version of a privacy bill could become more impactful on businesses (relative to the CCPA) by creating a fiduciary duty "to act in the best interests of the consumer," which would supersede a business' duty to itself, owners, or shareholders. (So far this year, the New York Privacy Act (A08526/S05642) has not moved from committee.) Virginia's legislation may also end up being more consumer-friendly than the CCPA due to the potential for a private right of action. (The Virginia Privacy Act, HB 473, has been tabled until 2021.) Washington State considered a number of privacy bills during the 2020 legislative session, but at the end of the session, the core privacy bill, the Washington Privacy Act, failed to become law. Sponsors of this bill intend to renew efforts to push through this legislation in 2021.

Furthermore, there is a ballot initiative in California, which if it obtains enough support, may appear on the November 2020 ballot. Interestingly, the same person who drove the first ballot initiative in 2018, Alastair Mcctaggart, is pushing this new initiative. This ballot initiative would

further boost the CCPA's protections and would create a new agency—the California Privacy Protection Agency—which would be responsible for administering, implementing and enforcing the CCPA, removing this from the AG's enforcement umbrella. Proponents of the initiative have until June 25, 2020 to gather the over 620,000 signatures needed in order to appear on the November 2020 ballot—a threshold many believe will be easily met.

While the requirements and prohibitions set forth in the CCPA are coming more into focus, what is evident is that the coming months and year will continue to present challenges to businesses attempting to comply with the CCPA. Until there is clear guidance from the AG, businesses will continue to wrestle with uncertainty around what disclosures need to be provided, what requests require responses, and what data needs to be deleted (and how). To protect against risk of exposure, businesses should continue to build processes for responding to consumer requests for information and deletion requests, as well as refining their internal knowledge about data collection and storage and ensuring privacy disclosures are accurate and up-to-date. As the landscape continues to evolve, businesses that invest now in developing a thorough process to comply with the known requirements, and a compliance management procedure to better ensure the success of the company's procedure, will be better positioned to navigate the scrutiny that is sure to come.