PAUL HASTINGS

STAY CURRENT

May 2020

Follow @Paul_Hastings

CCPA Enforcement Is Coming July 1–Here's What to Know

By Sherrese Smith, Andrew Erber & Jacqueline Cooney

Although the California Consumer Privacy Act ("CCPA") has been in effect since January, the California Attorney General ("AG") is set to begin enforcement in earnest on July 1, 2020. Despite the effects of COVID-19 and the lack of final implementing regulations, the AG is undeterred and has clearly indicated that enforcement will begin on time. With AG actions looming, companies should be finalizing their CCPA compliance in the coming weeks to avoid searching regulatory scrutiny. Companies that ensure they are doing their best to comply with the law as written, as well as the tentative guidelines in the draft regulations, will be better positioned to avoid regulatory fines and potential law suits related to the law.

Enforcement Commencing Without Final Regulations and Clear Guidance

First published in October 2019 the CCPA's implementing regulations have undergone multiple revisions in February and March 2020. With less than seven weeks remaining before enforcement begins, the regulations remain in draft form, creating significant uncertainty regarding how the AG's office will enforce the CCPA, come July.

These delays are exacerbated by the requirement under California law that the California Office of Administrative Law ("OAL") conducts a review of the draft regulations once they are finalized by the AG, but before they go into effect. Under normal circumstances, OAL has 30 working days to complete that review after which they could go into effect. However, due to COVID-19 disruptions, Governor Newsom has extended the OAL's review timeline by an additional 60 days. Given this additional review time, it is highly uncertain whether OAL's review would be complete in time for a July 1 effective date—even if the AG released final regulations today.

Of course, business planning must move forward in the face of such uncertainty. Companies should look to the current draft regulations for guidance, on the understanding that specific requirements could change on the margins before they become final. We have discussed the various iterations of the regulations elsewhere (here and here), so will only recap a few key practical points that arose in the last draft of the regulations.

- **Broadened Ability of Service Providers to Use Personal Information for Business Purposes**: The draft regulations permit service providers to use personal information for internal use to build or improve quality of services.

- **Clarification on Accessibility of Privacy Policies and Notices**: Access to privacy notices for the disabled must be in compliance with the Web Content Accessibility Guidelines.
- **Allowable Collection of Personal Information through Mobile Devices**: Mobile devices and applications shall utilize links to privacy notices, including just-in-time notices for collections that the consumer would not reasonably expect (e.g., a flashlight app that collects geolocation data).

You can access the updated draft regulations here: Text of Second Set of Modified Regulations–Comparison Version, pdf.

California Attorney General's Aggressive Stance on Enforcement

The foremost risk for companies is the likelihood that AG Becerra will take an aggressive stance in bringing enforcement actions against companies that have not made "reasonable" efforts to comply with the law. Unlike the limited private right of action—only available for data breaches—the AG is able to bring statutory actions for any CCPA violation. Civil penalties can range from $2,500 for a non-intentional violation to $7,500 for an intentional violation. While the CCPA does provide a 30-day "cure" period once a company is notified of a potential violation, AG penalties can add up if a cure is not possible.

Further, AG Becerra's intention to pursue non-compliant companies has not been softened by the current health and economic crisis related to COVID-19. Although his office has been lobbied by industry groups to delay the enforcement date, he has confirmed that July 1 is the deadline for compliance. Nonetheless, he has indicated that his enforcement priorities will be focused on those companies that made little to no effort to comply with the law. In December, he stated in relation to small companies that may have difficulty with compliance that they will likely not be the target of initial enforcements, but that "ignorance of the law is not an excuse for not following it" and businesses should comply because they "do not want to be the poster child" for enforcement[1]. What this means for California companies, large and small, is that a clear effort to comply with the law, including updating privacy notices and responding to consumer requests, is expected for all companies.

What Private Rights of Action Under CCPA May Mean for Companies

Despite efforts to expand the CCPA's private right of action during the amendment process, the final text of the statute provided a fairly limited right arising from a failure of a business to implement and maintain reasonable security practices.[2] The CCPA even contains a statutory bar against expanding the private right of action, providing that "[n]othing in this title shall be interpreted to serve as a basis for a private right of action under any other law."[3]Nonetheless, plaintiffs are already experimenting with legal theories that would circumvent this prohibition and expand the private right of action to all CCPA violations.

- **Unfair Competition Claims**: In *Barnes v. Hanna Andersson LLC*[4], a California sub-class part of a nationwide class action suit related to a data breach included a cause of action under California's Unfair Competition Law, Cal. Bus. & Prof. Code §17200 ("UCL") that relies on the CCPA as a predicate for the claim that Hanna Andersson engaged in unfair competition by not meeting the requirements of that statute.

- **Claims Related to "Unauthorized Disclosures"**: In *Sheth v. Ring*[5], the plaintiff argues, among other things, that while there was no specific data breach, certain data collection and disclosures or "sale" to third parties were not disclosed in the defendant's privacy notice in violation of CCPA. Similar claims have been brought in other suits that allege CCPA violations based on companies' unauthorized disclosures of personal information.[6]

Defendants have reasonable arguments against these non-breach claims, but no court has ruled on their validity, so litigation continues. As a result of these uncertainties, it is more important than ever to ensure that your notices are clear and meet the requirements of both the CCPA and consumer expectations, as well as reflect your actual data collection practices and uses. In addition, protecting the personal information you collect continues to be an important priority – companies need to make sure their security practices are in line with industry standards.

Additional Requirements for Employee and Business Data Coming January 1, 2021

In addition, it is important to remember that the scope of the CCPA is set to change again on January 1 when moratoria on the enforcement of certain rights for employees and individuals whose "business" data may be collected in California expire. Access and deletion rights for individuals whose data is collected in either an employment capacity or a business capacity will go into effect on January 1. It is important for companies to be preparing now for these expanded rights.

Currently, under CCPA, while companies must provide updated privacy notices for employees and business contacts, they can refuse to honor access and deletion requests for these individuals. Looking forward to January, companies should be expanding their ability to respond to such requests by:

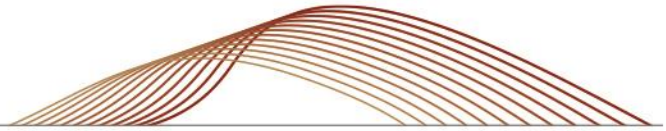
- Expanding existing data maps to include employee and business data if that has not already been done.
- Creating internal mechanisms for responding to access and deletion requests.
- Planning to update employee and external-facing privacy policies to reference these new rights.

What Companies Should Be Doing Now to Prepare for July 1

Post Updated Privacy Notices. You should review and update current privacy notices to conform to specific CCPA requirements, including the provision of clear and concise language that describes how you collect, use, share, and dispose of personal information. These should be made available to any California residents from whom you collect personal information and should be posted prominently on your website(s). Ensure the notice is compliant with WCAG 2.0 accessibility requirements.

Create a "Webform" to Respond to Individual Access Requests. The draft regulations include specific guidance regarding how individuals should be provided the ability to submit access and deletion requests. Specifically, companies that operate a website should include a "webform" on their websites that allow consumers to submit requests to receive a copy of the personal information collected about them or have their information deleted by the company. You should also ensure you have internal procedures for responding to these requests within 45 days.

Create a Mechanism to Verify Individuals' Identities. The CCPA and accompanying draft regulations require companies to verify the identity of individuals who submit access or deletion requests. Specific acceptable verification methods are provided in the draft regulations and companies



are required to ensure that they do not respond to access requests without first reasonably confirming that the requester's identity is confirmed.

Include on Your Homepage a "Do Not Sell" Button (if you do sell data). You should review your data collection and sharing practices to determine whether you "sell" data as defined under CCPA. If you do, you must develop procedures to enable individuals to opt-out of the sale of their personal information, including placing a link on your website where individuals can easily opt-out of such sale.

Review Your Security Practices. The CCPA provides California consumers with a private right of action for data breaches. There is also the potential for claims such as *Sheth*, which could potentially allow consumers to bring a private action against a company for unreasonable security measures that result in an "unauthorized disclosure." Companies should conduct assessments of their security practices against common industry standards, such as the Center for Internet Security ("CIS") Critical Security Controls ("CSC"), which Becerra has indicated he considers a "reasonable" security framework.[7]

Watch for CCPA 2.0. As if present uncertainties were not enough, on May 4, 2020, Californians for Consumer Privacy confirmed that their proposed ballot initiative to expand the CCPA had enough signatures to qualify for the November 2020 election. The new ballot initiative would represent another overhaul of California's privacy laws—creating a new data correction right, a new agency to enforce privacy law, and extending the employee and business-to-business exemptions through 2022.

The regulatory landscape in California continues to evolve and uncertainty abounds. Businesses need to be prepared for continual change, including the tightening of consent and sharing standards. The attorneys and experienced consultants in our Privacy and Cybersecurity practice group help clients navigate these issues every day. We are available and ready to help you navigate the privacy landscape in this time of unprecedented change and uncertainty.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

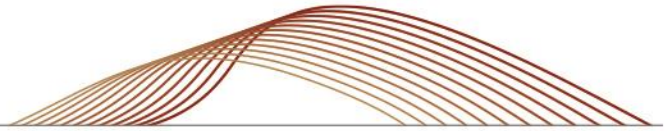
Washington, D.C.

Sherrese Smith
1.202.551.1965
sherresesmith@paulhastings.com

Jacqueline Cooney
1.202.551.1236
jacquelinecooney@paulhastings.com

Atlanta

Andrew J. Erber
1.404.815.2289
andrewerber@paulhastings.com



[1] https://www.bizjournals.com/sacramento/news/2019/12/16/california-to-start-enforcing-privacy-law.html.

[2] *See* Cal. Civ. Code § 1798.150.

[3] *Id.* § 1798.150(c).

[4] *Barnes v. Hanna Andersson LLC and Salesforce.com Inc.*, Case No. 4:20-cv-00812 (N.D. Cal.).

[5] *Sheth v. Ring LLC*, Case No. 2:20-cv-01538 (C.D. Cal.).

[6] *See*, *Burke v. ClearviewAI, Inc.*, Case No. 3:20-cv-00370 (S.D. Cal.); *Cullen v. Zoom Video Communications*, Inc., Case No. 5:20-cv-02155 (N.D. Cal.).

[7] https://www.oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.