CCPA enforcement begins now and most companies aren't ready

The California Consumer Privacy Act (CCPA) went into effect on January 1, 2020 with a six-month enforcement grace period. That end date is now here.

The basics. As a refresher, CCPA explicitly applies to companies that qualify under one or more of the following statutory criteria:

- Have gross annual revenues in excess of $25 million;
- Possess the personal information of 50,000 or more consumers, households, or devices; or
- Earn more than half of their annual revenue from selling consumers' personal information

A number of categories of businesses are explicitly exempted from CCPA compliance, including certain industries covered by federal regulations. However, most publishers will need to be ready to enable U.S. consumers to opt-out of third-party data transfers and demonstrate compliance to regulators in the event of an investigation or complaint.

Attorney Aaron Tantleff, a partner at law firm Foley & Lardner, offers a sliver of hope that CCPA may not apply to everyone, while cautioning that the law has few geographic boundaries. "We have spoken with many clients that have called in a panic to discover that CCPA does not apply. The applicability of the CCPA, like the GDPR, is not limited to only those organizations based in California. It may apply to organizations that lack any physical presence in the State."

Broad application to businesses globally. As a practical matter the statute will broadly apply to most commercial

enterprises, whether or not they explicitly target California residents. For example, an early analysis of the legislation by the IAPP says:

> *Companies may pass [the personal information of 50,000 consumers] threshold more quickly than anticipated because the scope of personal information is broad. Most companies operate websites and inevitably capture IP addresses. Notably, companies need to comply regardless of whether the website targeted businesses or individual customers in California given that the term "consumer" is defined to mean any "resident." Even individual bloggers and relatively small businesses outside California may find it difficult to ensure that they do not receive personal information of more than 50,000 California resident visitors to their website annually, simply from having it be passively accessible from there, and, within California, most retailers, fitness studios, music venues and other businesses will meet this threshold.*

Risks of non-compliance. The California Attorney general can impose financial penalties up to $2,500 for non-willful violations and $7,500 for intentional violations. But these numbers can multiple quickly if thousands or millions of users are implicated. In most cases there will be no liability where the violation is "cured" within 30 days of receiving notice. There is also a private or individual right of action when personal information is wrongfully disclosed under CCPA. (The first CCPA class action lawsuit [.pdf] was filed in February against Hanna Andersson and Salesforce.)

According a recent Ethyca survey of 218 general counsels of technology companies, 56% said they were "unprepared for new privacy regulations coming in around the globe," which includes CCPA. During the months leading up to the enforcement deadline, 43% of respondents said they had deprioritized privacy preparedness because of COVID-19. The survey also

found that lack of resources or cost was the greatest challenge in complying.

What to do now. "For businesses still looking to button up on compliance, the essential – and only – first step is to figure out the personal data you possess and where it lives," says Cillian Kieran, CEO of Ethyca. "After you've built a data map that has a thorough and complete record of the data you hold, and where it lives, you can worry about putting the structures in place to address various compliance tasks. But it all starts with the map."

Attorney Tantleff adds, "Document everything. By now, organizations should have a robust set of security measures in place. However, under the CCPA, an organization must demonstrate that it has implemented reasonable security measures designed to protect personal information based upon the nature and sensitivity of that information."

According to Lisa Rapp, VP of Data Ethics at LiveRamp, "No company should try to do this on their own. The best thing to do is to obtain as much information as possible by reading what industry leaders are saying, staying up-to-date on the materials that groups like the IAPP and IAB are putting out, and reaching out to prominent law firms that deal with data privacy to gain their legal counsel and interpretations of the law."

Julie Rubash, VP of Legal at Nativo, recommends that publishers read the Attorney General's final regulations "to ensure that current [privacy] plans are in line with the Attorney General's interpretation." She adds that "Tools like the IAB CCPA Framework are a step in the right direction to prepare for an inquiry and limit revenue disruptions. Publishers that leverage the IAB CCPA Compliance Framework tool and sign the limited service provider agreement are unlikely to experience a significant impact to their business models."

Abby Matchett, Enterprise Analytics Lead at Bounteous, says, “Because CCPA takes a much broader view of personal data than Europe’s GDPR guidelines, most companies must undertake a significant internal inventory of any data that may be linked, directly or indirectly, with a consumer or household. Conducting such an inventory places a heavy burden on IT organizations, legal departments, and data analysts who may already be dedicated to other internal priorities. Overcoming this obstacle is one of the first steps towards compliance but is often the most challenging to coordinate and fully document.”

Matchett further explains, “If you are concerned that you may not have time to build a home-grown digital solution for this purpose, consider reaching out to third-party Cookie Consent Manager software companies that specialize in maintaining CCPA & GDPR ready solutions. Some common Consent Managers include TrustArc, OneTrust, and Quantcast, among others.”

Here comes CPRA. Even as many companies are struggling to comply with CCPA, a new November California ballot initiative could impose even tougher privacy rules if passed. According to the Future of Privacy Forum’s Katelyn Ringrose, “While companies may have begun, and in some cases, finalized strong compliance programs and efforts addressing the CCPA—the California Privacy Rights Act (CPRA), recently certified for the 2020 ballot, could have an enactment date as early as 2023, placing additional obligations on covered entities. The CPRA would create a sensitive data classification, place additional obligations on processors, and require the establishment of a California Privacy Protection Agency.”

Why we care. Large numbers of consumers have expressed concerns about how their data are being handled online. But there’s evidence that “privacy forward” companies are seeing both brand and financial benefits, in terms of greater consumer trust and even stronger revenue growth.

It’s foolish to delay taking the necessary steps to prioritize privacy and data security. As Tom O’Regan, CEO of Madison Logic put it, “Ultimately, complying with the CCPA controls will be far less expensive than penalties from non-compliance.”

Thursday’s Live with Search Engine Land will be a special CCPA and privacy discussion featuring ***Lisa Rapp,*** *VP Data Ethics,* ***LiveRamp, Abby Matchett,*** *Enterprise Analytics Lead,* ***Bounteous, Katelyn Ringrose,*** *attorney,* ***Future of Privacy Forum****.*

It starts at 1:00 p.m. EDT and will allow up to 100 people into the meeting to experience the discussion live and ask questions. If you’re a digital marketer you can’t afford to miss this. Sign up here.

About The Author

Greg Sterling is a Contributing Editor to Search Engine Land, a member of the programming team for SMX events and the VP, Market Insights at Uberall.
http://feeds.searchengineland.com/~r/searchengineland/~3/q9be3OqiVtg/ccpa-enforcement-begins-today-and-most-companies-arent-ready-337041