Blogs
July 27, 2021
Perkins on Privacy

Recent Developments at the California Attorney General's Office Concerning the CCPA and Enforcement

There have been several notable developments this month at the California Attorney General's office relating to the CCPA. First, California Attorney General (AG) Rob Bonta held a press conference and issued a press release regarding CCPA enforcement in the past year. AG Bonta signaled that under his leadership, as under prior California Attorneys General, such as now Vice President Kamala Harris and United States Department of Health and Human Services Secretary Xavier Becerra, the AG's office will continue its focus on privacy. AG Bonta emphasized the importance of the CCPA at a time when so much of our lives has moved online due to the COVID-19 pandemic and that "there's more work to be done." He reported "great progress" in CCPA enforcement, noting that 75% of businesses that received a notice of violation came into compliance within the CCPA's 30-day cure period, while the remaining 25% are within the cure period or currently under active investigation. Second, AG Bonta revealed a new web tool, now available on the AG's website, which allows consumers to generate a notice of violation and send it to a business that they believe does not have a clear and conspicuous "Do Not Sell My Personal Information" link in violation of the CCPA. The Consumer Privacy Interactive Tool walks the user through a series of questions to determine whether the business is subject to the CCPA and may be selling consumers' personal information without a compliant opt-out link for sale of that information. Based on the user's answers, the tool generates a notice of noncompliance that can be mailed or emailed to the allegedly offending business. A business's receipt of this consumer-initiated notice of violation could potentially start the statutory 30-day cure period. The web page containing the tool explains to consumers that "while consumers cannot sue businesses for most CCPA violations, sending a notice of noncompliance is useful. The AG may sue businesses that violate the CCPA if they do not cure any CCPA violation within 30 days of being notified of noncompliance. The notice you send may satisfy that prerequisite." It is unclear whether there is a statutory basis for consumer-initiated notices to trigger the 30-day cure period for violations of the CCPA subject only to AG enforcement. The language in Cal. Civ. Code § 1798.155 generally refers to a business having 30 days to cure after "being notified of alleged noncompliance," but does not specify who can send that notice. This is in contrast to Cal. Civ. Code § 1798.150, which provides that consumers may only initiate a private action after *the consumer* sends the business a notice of alleged violation and gives the business 30 days to cure. It will likely be up to the courts to decide on this issue. Finally, the AG's office has also updated its FAQ to specifically address the Global Privacy Control (GPC), a user-enabled mechanism that sends a signal to websites via participating browsers that the user is electing to opt out of sales of their personal information. We previously discussed the GPC and noted that then-AG Becerra had expressed his support for the initiative via Twitter, previewing that the AG's office may be taking an official position on the GPC. Now, the AG's office has officially stated in its FAQ that the GPC must be honored under the CCPA as a valid opt-out request.[1] Industry might push back against the GPC FAQ changes but it remains to be seen whether the AG's office will change course. The AG's office has already instituted enforcement action against at least one business for failure to honor the GPC (see the last bullet in the CCPA Enforcement Case Examples below). As evidenced by these recent developments, the AG's office appears to be focusing its enforcement efforts on violations of the CCPA's opt-out sales provisions. Ad-tech companies in particular are likely to be affected by this enforcement focus due to the AG's position that the use of third-party cookies on a website is considered a "sale" under the CCPA. The AG's CCPA Enforcement Case Examples include at least five enforcement actions triggered by the use of online advertising, third-party tracking and even third-party analytics (highlights added for emphasis):

- **Media Conglomerate Updated Opt-Out Process and Notices** Industry: Mass Media and Entertainment Issue: Non-Compliant Opt-Out Process; Notices to ConsumersA mass media and entertainment business did not provide consumers with any methods to opt-out of the business's sale of their personal information. The business only directed consumers to a third-party trade association's tool designed to manage online advertising. The business's privacy policy and notice of right to opt-out also did not include required information about how consumers or their agents could exercise their opt-out rights. The business also did not have a notice at collection and lacked a "Do Not Sell My Personal Information" link on several of its digital properties. After being notified of alleged noncompliance, the business updated its opt-out process, privacy policy, and notices to address these issues, and added the "Do Not Sell My Personal Information" link to all of its digital properties.
- **Pet Industry Website Updated Its Opt-Out Web Form for Consumers to Opt Out of All Sales of Personal Information** Industry: Pet Industry Issue: Authorized Agent; Sales of Personal InformationA business that operates an online pet adoption platform required a consumer's authorized agent to submit a notarized verification when invoking CCPA rights. The business's disclosures regarding its sale of data were also confusing, and the business did not appear to provide a mechanism for consumers to opt-out of the sale of their personal information. The business also made consumers take additional steps to opt-out by directing consumers to a third-party trade association's tool designed to manage online advertising. After being notified of alleged noncompliance, the business removed the notarization requirement for agents, added a "Do Not Sell My Personal Information Link", and updated its opt-out web form that allowed consumers to fully opt-out of the sale of personal information, including personal information that was exchanged for targeted advertising.
- **Mobile App Game Stopped Selling Personal Information and Updated Protections for Minors** Industry: Online Gaming Issue: Sales of Personal Information; Sales of Minors' Personal InformationA business that operates a mobile app game installed software from a third-party mobile advertising platform that made available the personal information of its players, including minors aged 13 to 15 years old. The business did not provide an opt-out mechanism to adults or obtain an opt-in for minors. After being notified of alleged noncompliance, the business removed the ad software and instituted other privacy protections directed at younger users, including age-gating and parental verification features.
- **Social Media Company Stopped Selling Personal Information and Updated Privacy Policy** Industry: Social Media Platform Issue: Notices to Consumers; Sales of Personal InformationA business that launched a social media platform and advertised itself as being pro-privacy failed to inform consumers about their CCPA rights. The business also exchanged personal information about users' online activities with various third-party analytics providers but did not post the required notices or provide consumers with methods to opt-out of the sale personal information. After being notified of alleged noncompliance, the company updated its privacy policy and removed all third-party trackers from its app and website.
- **Manufacturer and Retailer Stopped Selling Personal Information** Industry: Consumer Electronics Issue: Sales of Personal InformationA business that sells electronics maintained third-party online trackers on its retail website that shared data with advertisers about consumers' online shopping. The business neither imposed a service provider contractual relationship on these third parties, nor processed consumers' requests to opt-out that were submitted via a user-enabled global privacy control, e.g., a browser extension that signaled the GPC. After being notified of alleged noncompliance, the company worked with its privacy vendor to effectuate consumer opt-out requests and avoid sharing personal information with third parties under conditions that amounted to a sale in violation of the CCPA.

Beyond the AG's own enforcement efforts, businesses are now at greater risk of receiving a notice of alleged violation with the introduction of the Consumer Privacy Interactive Tool. The AG's office seems to contemplate that such a notice could start the 30-day cure period under CCPA. Though this interpretation may be subject to challenge, companies should start preparing for how they might pivot and change their practices within 30 days if they do receive a notice. Companies currently offering a CCPA opt-out of sale mechanism should determine what technical and organizational changes are needed to comply with the GPC signal. [1] *See* CCPA FAQs B.7,

B.8. *See also* CCPA Regs at § 999.315(c) which provides, "If a business collects personal information from consumers online, the business shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted pursuant to Civil Code section 1798.120 for that browser or device, or, if known, for the consumer."

Explore more in

Privacy & Security
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field.

View the blog