
California AG Announces Investigative Sweep of Mobile Applications for CCPA Compliance

JANUARY 31, 2023

In a [press release](#) on January 27, 2023, California Attorney General (“California AG”) Rob Bonta announced an investigative sweep focused on mobile applications’ compliance under the California Consumer Privacy Act (CCPA), particularly with respect to effective processing of opt-out provisions. Attorney General Bonta noted that his office “is working tirelessly to make sure that businesses recognize and process consumers’ opt-out requests,” reaffirming the office’s commitment to enforcement of CCPA opt-out provisions. To date, the California AG has sent investigative letters to businesses in the retail, travel, and food service industries, which control mobile apps that allegedly have failed to comply with the CCPA.

This press release from the California AG’s office comes at a time when the CCPA has recently been amended (and expanded) by the California Privacy Rights Act (CPRA) and when the California AG shares concurrent enforcement authority over the new law with the newly formed California Privacy Protection Agency (CPPA). The CPPA has been in the process of developing and finalizing rules for the CPRA, and neither the CPPA nor the California AG’s office can enforce the new provisions of the CPRA until July 1, 2023 (and only then for violations that occur after that date). Still, businesses should be aware that the CCPA is still in effect until that time and that the California AG is actively enforcing the law.

We have summarized key provisions from the press release and outlined potential compliance steps for businesses to consider as part of their CCPA/CPRA compliance programs. We are happy to answer any specific questions you may have.

Summary of Press Release

Opt-Out Rights. First, the California AG alleges that the targeted applications fail to comply with consumer opt-out requests or do not offer any mechanism for consumers who want to stop the sale of their data. The California AG’s focus on this issue comes as no surprise, as this past summer the [AG Announced its first public CCPA enforcement decision](#), against Sephora, over allegations that they failed to disclose to consumers that they were selling their personal information and failed to process opt-out requests via user-enabled global privacy controls in violation of the CCPA. This investigative sweep represents an expansion of the California AG’s focus beyond websites to

mobile apps and indicates the California AG is committed to enforcing consumer opt-out rights across varied platforms.

Authorized Agents. Second, the California AG alleges that the implicated mobile apps have failed to process consumer requests submitted via an authorized agent, as required under §1798.130 3(A) of the CCPA. The press release points specifically to the failure to process agent requests through agent services, such as the service created by Consumer Reports called “Permission Slip.”

[Permission Slip](#) is a mobile app that aims to provide an accessible manner for consumers to set general permissions for what companies can do with consumer data. Once a consumer sets their general permissions, Permission Slip contacts companies and facilitates data-related requests on consumers’ behalf. This example demonstrates the California AG’s continued focus on companies’ failure to process authorized agent requests. Further, it indicates an endorsement of methods of compliance that are consumer-controlled, which empower consumers to exercise their rights and promote business accountability under the CCPA. The California AG has even publicly hinted that the technology industry should “develop and adopt user-enabled global privacy controls for mobile operating systems” which would allow for consumers to have control over the collection of information.

Potential Compliance Steps

Following the press release, the California AG provided businesses with some insight into the motivation behind this continued focus by tweeting on the importance of a mobile device to an individual in today’s society, noting the nature of information stored on a mobile device, which Bonta describes as a “wide array of sensitive information.” Although, the California AG provided forewarning through investigative letters in this instance, businesses should be cognizant that the CCPA’s affirmative right to cure has expired, and that moving forward the CPRA only provides a discretionary 30-day cure period. Thus, neither the California AG nor the CPRA are required to provide non-compliant businesses with an opportunity to come into compliance with CCPA/CPRA provisions before they potentially fine them. Businesses subject to compliance under the CCPA/CPRA, including those which operate mobile applications, should ensure compliance when collecting, processing, and sharing consumer data. Most importantly, businesses should be sure that they:

- Provide consumers with an accessible format to submit CCPA/CPRA requests, particularly opt-out requests.
- Provide a “Do Not Sell or Share My Personal Information” link connected to mechanisms or processes which will stop the sale or “sharing” of a consumer’s personal information.
- Institute a process which will ensure that authorized agent requests, received in all compliant formats, including those received via agent services, are processed.
- Institute a process which facilitates consumer rights requests within the time period required under the law.

Authors



Kirk J. Nahra

PARTNER

Co-Chair, Artificial
Intelligence Practice

Co-Chair, Cybersecurity
and Privacy Practice

✉ kirk.nahra@wilmerhale.com

☎ +1 202 663 6128



Ali A. Jessani

COUNSEL

✉ ali.jessani@wilmerhale.com

☎ +1 202 663 6105



Genesis Ruano

ASSOCIATE

✉ genesis.ruano@wilmerhale.com

☎ +1 202 663 6154