

[Blogs](#)

February 07, 2023

California Attorney General Targets Popular Mobile Apps in CCPA Enforcement Sweep

As it did [last year](#), the California Attorney General's Office recognized Data Privacy Day by announcing its latest investigative sweep under the California Consumer Privacy Act (CCPA). This time, the Attorney General focused on companies that operate mobile apps allegedly without offering CCPA-compliant opt-out mechanisms.

According to its [press release](#), the California Attorney General's Office sent letters to businesses with "popular mobile apps in the retail, travel, and food service industries that allegedly 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" as well as to those that failed to process consumer requests submitted via an authorized agent, specifically [Permission Slip](#). In the announcement, the Attorney General made specific mention of global privacy controls and sensitive personal information in the context of honoring user choice in mobile apps.

Consumer Privacy Rights

While the CCPA was amended by the California Privacy Rights Act (CPRA), and those amendments took effect on January 1, this sweep was brought under the CCPA because the Attorney General cannot enforce the CPRA until July 1, 2023.

The CCPA grants California consumers numerous privacy rights, including the rights to opt out of "sharing" and "sales" activities.

- **Sharing.** "Sharing" occurs when a business discloses personal information to an external third party for the purpose of displaying ads to consumers on non-affiliated websites or apps. *See* Cal. Civ. Code § 1798.140(ah).
- **Sales.** Subject to limited exceptions, a "sale" occurs when a business discloses personal information to an external third party "for monetary or other valuable consideration." Cal. Civ. Code § 1798.140(ad(1)). What constitutes "valuable consideration" has been very broadly interpreted by the California Attorney General. Because of this broad interpretation, even disclosures of personal information to analytics services, ad measurement providers, and other third parties are likely to be considered sales, even though no money is exchanged for the personal information and even though the business providing the personal information is the one acquiring a service from the analytics or ad provider, *unless* the recipient of the personal information contractually agrees to be a "service provider" subject to a contract that meets the requirements of the CCPA. For some entities, having these terms in place requires the business to enable a restricted data processing or limited data use feature.
- **Browser-based opt outs.** California law requires businesses to look for and honor browser-based or other technical settings that communicate a consumer's opt-out preference. This includes the [Global Privacy Control](#) ("GPC"). When businesses see these signals, they must opt the consumer out in the same way they would if the consumer had clicked the opt-out link on the business's website. For websites, this means that when a user visits a website with GPC enabled, the business must stop any cookie-based sales/sharing and, if the consumer is logged in, opt the consumer out of non-cookie based sales and sharing as well.

Next Steps

This latest enforcement sweep, together with the California Attorney General's first CCPA settlement last summer, further signals the Attorney General's focus on user control in the context of online and mobile advertising practices under the CCPA.

It is imperative that businesses understand what cookies, pixels, software development kits, and similar technologies are collecting data on their websites and mobile apps. The inventory of third-party recipients should then be assessed to determine if such disclosures constitute sales or sharing under current interpretations of the CCPA. If a company wants to engage in data sharing for targeted advertising uses without offering an opt out, it must ensure that it has implemented limited or restricted data processing by recipients and has contractual terms in place that meet the CCPA's narrow definition of "service provider." If a business engages in sales or sharing through its websites and mobile apps, it must (1) prominently disclose such activity to consumers through its privacy policy and other required notices (transparency); (2) offer consumers the ability to opt-out of that activity (through an opt-out link and preference signals); and (3) effectuate opt-out requests. Companies that receive a CCPA notice from the Attorney General should consult experienced privacy counsel immediately.

Authors

Explore more in

[Privacy & Security](#)