



California Attorney General Focuses on Targeted Advertising and Disclosures in CCPA Enforcement

September 30th, 2021 | and [Webb McArthur](#)

The Office of the Attorney General of California began enforcing the California Consumer Privacy Act (“CCPA”) more than a year ago and recently released a set of enforcement case examples it has pursued against businesses. The examples are anonymous and not a complete list of all enforcement cases, but the descriptions may provide helpful guidance to business subject to the law. Even those businesses that generally deal in exempt personal information may find value in reviewing the examples because they demonstrate the AG’s enforcement strategy, enforcement priorities, and give some indication of how the AG interprets provisions of the law.

The AG’s release notes that businesses currently have 30 days to cure alleged noncompliance after receipt of a notice of alleged noncompliance. However, business should be aware that this 30-day cure period will end in 2023, when the CCPA changes as a result of the California Privacy Rights Act that was approved by California voters last year. Taking note of these examples now may help businesses get ahead of the game for their own CCPA compliance. Here is a quick summary of some important examples:

Relationship with the entity receiving data for online advertising and analytics – is it a “sale” to a third party or sharing with a service provider?

A striking number of the examples focus on the use of data for targeted advertising and analytics purposes. In several examples, the AG referenced businesses engaging in targeted advertising that involved the exchange of personal information the AG characterized as a “sale” of personal information requiring opt-out rights and disclosures. In one example in particular, the AG referred to a retailer using third-party tracking technology on its website that shared data with advertisers about consumers’ shopping activities. The AG faulted the business for not setting up a service provider relationship with the advertiser recipient.

Take-Away: Business should thoroughly analyze who is receiving their data and how the relationship is characterized, including for online marketing and analytics purposes. Businesses engaging service providers need to be reminded to enter into service provider agreements that contractually prohibit the service provider from retaining, using, or disclosing personal information outside of what is permitted by the law.

Third party trackers – what data is being analyzed and how can consumers decline their use?

One example referenced the use of third-party trackers employed for site analytics purposes. However, the AG does not provide details about the nature of the data that is of concern for this

example. In particular, how such data meets the definition of “personal information” under the CCPA is unknown at this point. Another example indicates that implementing a “global privacy control” browser extension that permits site visitors to decline to permit third-party online trackers, like cookies, to collect data might be required.

Take-Away: Businesses that have third-party trackers, like cookies, present on their websites should consider whether providing opt-out rights or setting up service provider relationships are appropriate responses.

Opt-out – what is an effective means?

In other examples, the AG implied that a business does not comply with opt-out requirements for online advertising simply by referring consumers to third-party trade association opt-out tools, perhaps referencing tools made available by the Network Advertising Initiative and the Digital Advertising Alliance.

Take-Away: Businesses subject to the CCPA sale opt-out rights should ensure that they do not employ verification procedures, like requiring government identification and a consumer bill, before granting an opt-out request.

The business is a financial institution under the GLBA – does the business still need to think about CCPA compliance?

Yes. For example, auto dealers should consider personal information they collect that is not regulated by the Gramm-Leach-Bliley Act and is subject to the CCPA, as one enforcement example references a dealer who collected personal information from consumers taking test drives without providing a Notice at Collection.

Take-Away: Financial institutions should conduct data inventories to assess whether they collect or disclose data sets that are subject to the CCPA.

Privacy program – what do the policies say?

In looking across the examples, it is clear that the Attorney General is focused on ensuring that privacy policies accurately and completely describe a business’ practices for processing personal information, including what information is collected, how it is used, and how it is shared.

Take-Away: Businesses should ensure that their privacy programs are integrated across the enterprise and capture all data practices, as well as changes to those practices. The examples also indicate that the AG pays attention to complaints submitted to it by consumers, so it is important that businesses have a good complaint management program and are responsive to consumer complaints.

The privacy program has been implemented – the business is done, right?

No, businesses should be reminded that they may not be able to set a CCPA compliance program in place and leave it alone. The CCPA will change in 2023 as a result of the California Privacy Rights Act, adding new requirements to businesses subject to the law and transferring enforcement authority to a new agency, the California Privacy Protection Agency. The agency is also beginning a rulemaking exercise to roll out regulations to reflect changes to the CCPA. And as time goes on,

as it the case with these enforcement examples, we will continue to learn more about CCPA interpretation by regulators and enforcement priorities.

Take-Away: As with all good compliance programs, businesses should implement routine review of their CCPA compliance program to ensure that legal updates are captured and adjustments are made for both changes to business practice and changes to the law, with appropriate consideration given to consumer complaints and requests.

Qualified counsel can help businesses walk through smart compliance approaches to address each of these questions as directly applicable to your business and its processes.

Businesses can find the enforcement case examples here: <https://oag.ca.gov/privacy/ccpa/enforcement>