

Key Takeaways from the First Year of CCPA Enforcement

July 28, 2021

On July 19, 2021, California Attorney General Rob Bonta announced his [first-year enforcement update](#) on the California Consumer Privacy Act (“CCPA”), and unveiled a tool to help the Attorney General’s office (“CAAG”)—the primary enforcer of the CCPA until the [California Privacy Protection Agency takes over](#)—identify CCPA violations.

Over a year ago, on July 1, 2020, the first day of enforcement, the CAAG [sent a number of statutorily-required violation notices](#) to companies, making clear that the CAAG planned to aggressively enforce the statute. Last week’s update is a clear continuation of this trend, with the CAAG introducing a new tool that California residents can use to easily report violations to the Attorney General’s office. The CAAG also put the market on notice by providing enforcement statistics and examples of potential enforcement actions. Both the tool and examples provide much-needed guidance on the CAAG’s enforcement priorities for the CCPA.

Consumer Privacy Tool: Statutory Notice Generator?

The CAAG has launched a new online [Consumer Privacy Tool](#) that allows consumers to directly notify both businesses and the California Department of Justice of potential CCPA violations. Take note: notices created by the Consumer Privacy Tool likely satisfy [the statutory 30-day notice requirement](#), after which the Attorney General may bring an enforcement action if the company fails to cure during that window. Right now, Version 1.0 of the tool is limited to helping consumers send notices to businesses that do not post [an easy-to-find “Do Not Sell My Personal Information” link](#) on their website, but we expect the tool will be updated to include other potential CCPA violations in the future.

The tool walks consumers through a handful of questions on applicability and a company’s practices to determine whether a company is subject to, and potentially violating, the CCPA. If the answers indicate that there is a potential violation, the tool prompts the consumer to send the business name, contact information, and the date of the alleged violation to the Attorney General, who may leverage the tip to launch an

investigation or send a notice letter. The tool also generates a draft notice that the consumer can copy into an email or print and mail to the business that the consumer believes has violated the CCPA.

The creation of the Consumer Privacy Tool allows the CAAG to capitalize on vague language in the statute regarding who, exactly, is required to provide companies with notice of an alleged CCPA violation and thereby start the 30-day clock for the company to cure. The statute simply provides that a company is in violation of the CCPA “if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance.” Notably, the CCPA does not specify that the Attorney General must be the one to provide notice prior to beginning an investigation, and the instructions for the reporting tool state that a consumer’s notice may satisfy the notice requirement for an action by the Attorney General.

The new tool effectively deputizes consumers as the Attorney General’s eyes and ears in identifying violations for enforcement. Companies should be prepared for an increased number of notices and should assume that notices of alleged noncompliance received from consumers have also been provided to the Attorney General.

A Window into CCPA Enforcement.

In the update, the Attorney General also reported that upon receiving a notice of alleged violation, 75% of businesses took steps to come into compliance within the 30-day statutory cure period. The remaining 25% of businesses that received the notice were either currently in the 30-day period or are under active investigation at the time of this writing.

While the list of notice recipients is not publicly available, nor the total number of recipients known, the Attorney General’s office did [publish a list of 27 anonymized examples](#) where the CAAG’s notice letter prompted companies to come into compliance within the statutory timeframe. These examples provide an opportunity to read the tea leaves on how the CAAG will enforce the CCPA, while also identifying key considerations for covered businesses to reduce their CCPA enforcement risk.

Lessons Learned from CCPA Enforcement Examples.

- **Expect Broad Enforcement.** The examples included in the update suggest that the Attorney General is not prioritizing enforcement based on any specific sector or provision of the CCPA. Instead, the Attorney General has sent notices to a diverse

range of entities in the technology, marketing, and retail sectors. There are some notable exceptions; the publicly available examples do not include any healthcare or financial services sector entities, which is unsurprising given the exemptions available in these sectors. Similarly, all of the companies appear to be either consumer-facing or hold consumer data in the course of their business, suggesting that the CAAG is not focused on business-to-business or investor-oriented entities at this time.

The types of violations alleged in the examples touch on different areas of the CCPA, from privacy policies to notices of financial incentives and timely responses to consumer requests. While the tool currently focuses on the “Do Not Sell My Personal Information” link, this breadth of enforcement strongly suggests that it will be expanded to allow for reporting on other potential violations. Companies that sell data should ensure they are CCPA-compliant, and all companies should broadly evaluate when, where, and how they collect, share, or sell personal data, and assess CCPA compliance at each point. Taking a broad lens for compliance that mirrors the Attorney General’s approach can mitigate the risk of enforcement.

- **Getting the Basics Right.** While the Attorney General’s notices do not focus on any one particular area, they suggest that the Attorney General’s initial enforcement approach is centered on ensuring that companies are addressing the basic components of the CCPA. Of the 27 examples provided, 13 companies received notices of alleged violations for noncompliant privacy policies, among other alleged violations. Generally, the companies allegedly failed to inform consumers of the types of data that the company collected, the rights consumers have under the CCPA, and how they could exercise those rights. These are basic requirements of the CCPA that should be addressed proactively.
- **Potential Leniency for Best Efforts.** One case also suggests that, at this stage, the Attorney General may give companies a second chance at compliance where companies show they are making best efforts to comply. An online classified ads company received a notice of alleged violation for a number of issues with its privacy policy. After being notified, the business updated its privacy policy to include the key components of a privacy policy, but the CAAG found that, as revised, the privacy policy contained unnecessary legal jargon and was not understandable to the average consumer. The covered business received a second notice that the updated privacy policy did not comply with the CCPA regulations.

By giving the covered business an opportunity to cure on the second turn, this example suggests that the Attorney General may take best efforts into consideration prior to bringing an enforcement action even when the cure is imperfect.

- **Clarity Is Key.** A number of examples suggest that a clearer articulation of the company's data practices and role in processing personal information in the company's privacy policy or notice could have mitigated or prevented the notice. For example, in three cases, the covered companies received notices because, among other allegations, they "did not explicitly state whether or not [they] had sold personal information or transferred personal information for a business purpose in the past 12 months[,]" which is a statutory requirement. Similarly, multiple covered businesses also received notices of alleged violations where it was unclear that the business was acting as service provider rather than the party directly collecting personal information from consumers. The covered businesses were able to cure by updating their terms of service to reflect their role, and clarifying their practices with the Attorney General.
- **Make It Easy for Consumers.** The examples also provide insights into compliant methods for submitting requests to opt-out of the sale of personal information. For example, the Attorney General alleged a violation where a media conglomerate required consumers to submit multiple, separate requests to opt-out for each website in their profile rather than having a universal opt-out button ([which is required in other states](#)). Other potential violations included where a data broker's opt-out process directed consumers to their mobile device settings, and a mass-media company used a third-party trade association tool designed to manage advertising for the opt-out process.

Businesses should make it easy for consumers to effectuate their rights directly with the company. Any process that is confusing or cumbersome, like pushing the consumer to a third party, may be considered noncompliant.

- **Defining "Verifiable Requests."** The [CCPA regulations require](#) that a covered business create and comply with "a reasonable method for verifying" requests to know or delete, and provide a number of factors that should be considered when developing this methodology. Some of the CAAG's examples shed light on what may be considered unreasonable. A business required that consumers create an account to make the verifiable request—an action expressly prohibited by the CCPA—and produce identification and a bill showing the consumer's address. Upon receiving notice, the company stopped requiring that consumers take these steps. In another example, the covered business required a consumer's authorized agent to submit a notarized verification when invoking CCPA rights, a practice that it ceased after it received the notice of alleged violation.
- **Offline Collection Counts.** The CAAG appears to be looking at offline collection of personal information just as closely as online collections. This is a reminder that the CCPA extends to brick-and-mortar companies collecting information from

consumers in real life. An automotive company collected information of consumers signed up to test drive vehicles at the business, but failed to provide notice at the time of collection. After receiving notice, the business implemented notice at collection, regardless of whether the collection was completed online or in-person. Making one of its initial examples about offline collection emphasizes that the CAAG is not limiting its focus to webpages, but will investigate practices no matter the point or method of collection.

- **Don't Forget About Service Providers.** The CCPA requires that, where a covered business shares personal information with a service provider, the service provider's use of the personal information is limited by written contract. Three covered businesses received notices of alleged violation for failing to ensure that these contracts were in place. These examples are a good reminder that covered businesses should map their data flows both into and out of the company to ensure that the appropriate notices and contracts are in place at the time of collection and when the data is shared.
- **Have a Plan for Cure.** Taken together, the CAAG's examples show how a quick and complete response to a notice can effectively eliminate the risk of an enforcement action. Covered companies should have a clear plan in place setting out how they will respond to a CCPA notice from a consumer or the Attorney General. Establishing escalation pathways and creating a culture of CCPA awareness can help ensure that notices get to the right team members quickly so that companies have ample time to cure effectively.

To subscribe to the Data Blog, please click [here](#).

* * *

Please do not hesitate to contact us with any questions.

NEW YORK



Jeremy Feigelson
jfeigelson@debevoise.com



Jim Pastore
jjpastore@debevoise.com



Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

SAN FRANCISCO



David Sarratt
dsarratt@debevoise.com



H Jacqueline Brehmer
hjbrehme@debevoise.com



Christopher S. Ford
csford@debevoise.com