

What we've learned from a year of CCPA enforcement

Article

The news: The California Office of the Attorney General (OAG) issued a **press release** last month summarizing the **first year of enforcement of the California Consumer Privacy Act (CCPA)**, which came into effect on July 1, 2020.

- The release provided **27 examples of enforcement actions** the OAG has taken in the past year, shedding light on what behavior is—and is not—permitted when it comes to personal

data collection.

Here's what we learned:

The OAG is taking privacy policies very seriously. Fourteen of the 27 examples focused on **noncompliant privacy policies**, including use of “unnecessary legal jargon,” failure to disclose what information a company has sold in the past 12 months, and failure to notify customers of their right to opt out.

Third-party opt-out sites are noncompliant.

- The CCPA requires companies to give consumers the ability to opt out of selling their personal information to be used for targeted ads. But rather than provide that ability directly on their sites, **some companies had been using pre-existing opt-out tools** created by popular trade associations, such as the **Digital Advertising Alliance** or the **Network Advertising Initiative**.
- “It seems like the problem is that the **tools don't necessarily cover the totality of what a given site might do with your personal information**, and CCPA requires a clear opt out from everything for every site,” said Nicole Perrin, eMarketer principal analyst at Insider Intelligence.
- Essentially, they don't provide a truly blanket opt-out. That didn't fly with the OAG, which ruled that **publishers have to provide their own “Do Not Sell My Personal Information” link** on their sites.

Consumers can send noncompliance notices that have the same weight as a notice from the OAG. The press release encouraged consumers to use its **interactive privacy tool**, which helps average users send notices to businesses that may have violated the CCPA.

- The OAG stressed that notices from consumers start the 30-day window that businesses are given to fix noncompliance issues before they can be sued.

More on this: These recent clarifications aren't the first time the OAG has shown how strict it can be.

- In March, it **issued** a ban on “dark patterns,” or user interfaces on websites and apps designed to misdirect or otherwise nudge consumers into doing actions that benefit the business, such as allowing said businesses to sell their data. The OAG said that consent given under these circumstances doesn't count.

What it means for marketers: Though the CCPA's opt-out rules are considered better for the ad industry than opt-in rules, it's becoming increasingly clear that **the California OAG won't settle for anything less than the most stringent compliance.**

- There's little room for businesses to try to get around the rules, even with more subtle means like unclear legal language or a confusing user interface.
- Ultimately, while the OAG's strictness is good for privacy, it may come as bad news for marketers hoping the CCPA wouldn't disrupt business-as-usual too much.