Arielle Feger

# California privacy regulations have implications beyond the state

Article

Beginning January 1, 2023, the California Privacy Rights Act (CPRA) will take effect, though enforcement won't begin until July.

- This is an expansion of the California Consumer Privacy Act (CCPA), which took effect January 1, 2020.
- The aim of the CCPA is to give consumers more control over the personal information businesses collect.
- The CPRA expands aspects of the CCPA, including the types of businesses that must adhere to data privacy standards, the types of data that are protected, and the rights consumers have to alter or limit use of collected data. The CPRA goes into effect without exemptions January 1, 2023.
- The CPRA also establishes the California Privacy Protection Agency, which will take over enforcement from the California attorney general.
- "It's going to be a lot harder for companies to argue that consumer data practices are privacy-compliant if they are sharing any deterministic data for advertising purposes," said our analyst Evelyn Mitchell.

**What's covered?** CCPA regulations apply only to customer data that was sold by one company to another. The CPRA goes beyond the sale of data to regulate any data sharing, regardless of whether money is exchanged.

- Under the CPRA, businesses that collect consumer data (including third parties and contractors) must disclose what kinds of information they are collecting and whether it is sold or shared for the purpose of advertising.
- Consumers must also be given the choice to opt out of having their data shared.
- It also limits service providers' ability to combine consumers' personal information, which can make measurement quite tricky, according to Gary Kibel, partner at Davis+Gilbert LLP.

**No one is exempt:** Though the CPRA doesn't go into effect until January, all businesses should already be in compliance with the CCPA. However, some (mistakenly) believe that they are small enough to evade enforcement or otherwise don't need to comply.

But if the establishment of a new agency tells us anything, it's that enforcement has just begun.

- In August, Sephora agreed to pay $1.2 million in fines for allegedly failing to comply with the CCPA. (Though agreeing to pay the fines "does not constitute an admission of liability or fault by Sephora," said the company.)

- According to Arielle Garcia, chief privacy officer at media agency UM, this case served as both a "warning shot" and an "an effort to remove any potential residual doubt that an opt-out is and will be required—whether for sale or for sharing of data for targeted advertising."
- This has spurred a wave of small- to medium-sized businesses reviewing their privacy policies to ensure compliance.
- Even businesses outside of California need to stay vigilant, said Mitchell. "It's difficult to draw digital fences around California residents," she warned.

**Getting ready:** Last month, the Interactive Advertising Bureau made waves by stating that privacy regulation was advertising's greatest threat.

- While a comprehensive federal law hasn't come into play yet, a bevy of new privacy laws in states like California, Virginia, Colorado, Connecticut, and Utah will begin taking effect next year.
- In addition to reducing risk of legal action, becoming compliant with the CCPA and CPRA can help companies plan for any looming laws. "It's a way to work with something concrete that's in effect instead of preparing for something that's not real yet," said Mitchell.

**Brush up:** This is not a comprehensive list of the CPRA updates. Companies should familiarize themselves with the language of the CCPA and CPRA to ensure they're in compliance.

*This was originally featured in the eMarketer Daily newsletter. For more marketing insights, statistics, and trends, subscribe here.*