Insights, News & Events

3 TIPS FOR EMPLOYERS ON COMPLYING WITH THE CCPA'S RULES FOR OPT-OUT SIGNALS

Insights
Aug 18, 2022

Among the many privacy rights in California, state residents may opt-out of the sale of personal information under the California Consumer Privacy Act (CCPA) – and covered businesses cannot sell personal information after they receive a valid opt-out request. Recently, however, there's been confusion as to what constitutes a valid opt-out request. Businesses have been primarily concerned with requests made through opt-out preference signals, like a user-enabled global privacy control (GPC). This kind of request is typically made by the consumer's web browser, when enabled, and it acts as a "switch" to notify **every** owner of a website visited by the consumer that the consumer is exercising their right to opt-out of the sale or sharing of their personal information. The significant consumer benefit of this request is that it only needs to be enabled once before applying to all online webpages the consumer visits. However, businesses may be seeking clarity in light of recent changes to the CCPA made through the California Privacy Rights Act (CPRA) and proposed revisions to regulations. What is the current stance on opt-out preference signals? Here are three tips for covered businesses as you review your practices for compliance.

1. **Watch for Updates on Proposed Regulations**

   The CCPA went into effect in 2020 and became the first comprehensive consumer privacy bill in the United States. In August of that same year, regulations to the CCPA were enacted. Shortly thereafter, in November 2020, voters passed the CPRA through a ballot initiative.

Related People

Anthony Isola
Partner
415.490.9018

Service Focus

Consumer Privacy Team

Privacy and Cyber

Resource Hubs

U.S. Privacy Hub

Notably, the CPRA does not replace the CCPA but rather functions as an amendment to the CCPA. It will take effect on January 1, 2023.

Additionally, on May 27, 2022, the California Privacy Protection Agency released draft proposed regulations for the CPRA. These proposed regulations aim to update the prior CCPA regulations and provide guidelines for compliance with both the CPRA and CCPA. As of the date of this publication, the agency has commenced the formal rulemaking process for the proposed regulations, which is currently in the initial public comment stage.

2. **Understand Evolving Rules on Opt-Out Signals**

Opt-Out Signals Under the CCPA

Under the CCPA, a consumer has the right, at any time, to direct a business that sells personal information to not sell the consumer's personal information. The initial version of CCPA does not, itself, expressly require or mention opt-out preference signals.

Although opt-out preference signals are not discussed in the CCPA, the CCPA regulations do cover GPCs. In particular, the regulations require businesses to provide two or more methods for consumers to submit requests to opt-out. One method must be a clear and conspicuous link titled "Do Not Sell My Personal Information" on the business's website and mobile application. Most businesses have latitude to choose the second method for receiving opt-out requests, and the regulations mention several acceptable methods. However, the regulations require businesses that collect personal information from consumers online to treat user-enabled GPCs or other mechanisms that communicate an opt-out preference signal as a valid opt-out request. In other words, under the CCPA, businesses that operate online are required to take a GPC – or a similarly functioning universal opt-out mechanism – as a valid consumer request to stop the sale of their personal information.

Opt-Out Signals Under the CPRA

In contrast to the earlier iteration of CCPA, the CPRA does explicitly require that businesses recognize opt-out preference signals. The recently proposed regulations further clarify what attributes an opt-out preference

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills

signal must have to constitute a valid opt-out request, as follows:

- The opt-out preference signals should be in a "format commonly used and recognized by businesses." An example of this would be data in an HTTP header field.
- Consumers should be able to understand that the web browser or other mechanism that sends the signal is meant to convey an opt-out request.

The proposed regulations also outline other requirements related to opt-out signals including, among other things:

- The business must display on its website whether or not it has processed the consumer's opt-out signal. For example, the business may display on its website "Opt-Out Preference Signal Honored" when a browser using an opt-out preference signal visits the website.
- The business must treat the opt-out signal as a valid request to opt-out of the sale and sharing for that browser or device, as well as for the consumer, if known.
- The business must maintain a process to reconcile situations where the consumer's opt-out signal conflicts with the consumer's preferences previously shared with the business or the consumer's participation in a business's financial incentive program.

Businesses will need to update the functionality of their websites and mobile applications to comply with these additional requirements by 2023.

3. **Err on the Side of Caution**

As these regulations clearly demonstrate, an opt-out signal from a consumer-friendly, universal opt-out mechanism is something the law requires businesses to honor. Also, the proposed regulations require businesses to recognize signals in a "commonly used and recognized" format. While the scope of this phrase remains ambiguous, it is important to err on the side of caution when recognizing opt-out preference signals because the CCPA carries fines of $2,500 per violation, or $7,500 for each violation found to be intentional.

Conclusion

We will continue to monitor these developments, so make sure you are subscribed to Fisher Phillips' Insight system to keep up with the most up-to-date information. Please contact your Fisher Phillips attorney, the author of this Insight, any attorney in our Privacy and Cyber Practice Group, or any attorney in our California offices should you have any questions.