

Universal Opt-Out/Global Privacy Control: Preparing for the New Online World

December 21, 2022 – *The TMCA*

by Jamie Nafziger and Katherine Chaves



2022 has been a whirlwind year for cybersecurity, data, and privacy counsel who are navigating an expanding regulatory landscape and unique sets of legal requirements from numerous jurisdictions. This trend is likely to continue and grow more complex in the new year as additional states

adopt and implement privacy laws. A growing trend across privacy legislation is requiring company websites to respond to universal opt-out mechanisms, also known as “Global Privacy Control.” If ignored, a business exposes itself to liabilities that can result in legal and financial consequences. As businesses look toward 2023, we encourage them to examine their compliance obligations in connection with universal opt-out mechanisms and if applicable, develop an implementation plan.

Universal Opt-Out – The Basics

For those who are unfamiliar with the term, universal opt-out is a mechanism by which consumers can exercise their right to “opt out” of a platform or technology processing their personal data for targeted advertising or of the sale of their personal data. In practice, a consumer sets their preferences in their browser or with a plug-in to “opt out” of data sharing. Once the preference is set, a signal indicating the consumer’s preference is automatically sent each time they visit a website. If required, the website operator must respond to that signal by opting the person out of targeted advertising, the sharing of their personal data, or other sharing limited by statutes and regulations. The website operator also must inform its vendors and other third parties with which the consumer’s information has been shared of the opt-out request and they must honor it as well.

Related Capabilities

- Trademark, Copyright + Advertising
- Intellectual Property Litigation

Current Legal Requirements

The most time-sensitive legal requirements come from California. On January 1, 2023, California's Privacy Rights Act (CPRA) will be in effect. Under the current *draft* implementing regulations, businesses that interact with consumers online are required to respond to opt-out preference signals as well as to offer another opt-out option. While the CCPA previously included a 30-day cure period for violations, this is no longer available come January 1.

Colorado's Privacy Act ("CoPA") goes into effect on July 1, 2023, and contains a similar requirement to respond to universal opt-out signals by July 1, 2024. Colorado's *draft* regulations anticipate that a universal opt-out could be achieved in other ways than through a browser or plug-in signal, such as through a do not sell list that website operators would be required to query. The Colorado Department of Law plans to release a list of approved universal opt-out mechanisms no later than April 1, 2024.

Connecticut's Data Privacy Act ("CTDPA") includes a universal opt-out requirement that goes into partial effect July 1, 2023, and into full effect July 1, 2025. Other states are considering similar provisions in their data privacy legislation.

While only time will tell how these regulations will play out and how companies will manage to comply with the requirements, the [Sephora case](#) highlights the ease by which a regulator can allege legal violations and the monetary and reputational consequences this can have. This past August, the California Attorney General's office announced a settlement with Sephora, Inc. alleging, among many things, that Sephora failed to process users' requests to opt out of the sale of their data through the Global Privacy Control. The AG's office lauded its settlement with Sephora and AG Rob Bonta emphasized that, "I hope today's settlement sends a strong message to businesses that are still failing to comply with California's consumer privacy law. My office is watching, and we will hold you accountable."

Technical and Legal Challenges

Currently, only certain internet browsers (DuckDuckGo, Brave, Mozilla Firefox) or a separately installed plug-in enable universal opt-out signals. Notably, Google Chrome and Apple's Safari do not enable such signals. Without support from major browsers, the technical implementation of responding to universal opt-out signals is naturally haphazard. Without more consumers opting to opt out in this way, the business pressure on companies to conform with opt-out requirements may not be omnipresent. The regulatory pressure to conform with the rules, however, remains and cannot be ignored (*see, e.g., Sephora*). Consent management platforms such as [OneTrust](#) are working on helping their customers integrate universal opt-out into their existing consent management program.

Effects of Consumers Opting Out and How to Plan for the World of Universal Opt-Out

In the short term, consumers opting out of sharing their personal data can have immediate strategic and financial consequences for business. The growth of importance of first party data may also present new business opportunities. It is critical, therefore, to bring together key company stakeholders to best address these changes and properly prepare. No one wants to be caught off guard, and the sooner companies can bring together their legal, business, and data privacy teams to discuss these changes, the more time they will have to pivot, adapt accordingly, and strongly position themselves. As the industry navigates this “new normal,” companies can no longer rely on previous advertising and consumer data business models. This is a time to think creatively and utilize the collective knowledge of company decision makers to implement new solutions. Dorsey’s Cybersecurity, Privacy and Social Media Practice Group would be happy to assist in these discussions.