Global Privacy Signaling: the trendsetting opt-out mechanism

September 19, 2022

By now, it is generally known that comprehensive privacy laws include requirements to allow consumers to opt-out of the sale of their personal information, including personal information collected through online behavioral advertising cookies. The California Consumer Privacy Act of 2018 ("CCPA") requires that covered businesses provide at least two mechanisms for allowing consumers to opt-out of the sale of their personal information. What has received less attention until recently is the use and recognition of a global privacy signal to communicate an opt-out.

Two states at least will ultimately require recognition of the Global Privacy Control ("GPC")—namely, California under both the CCPA and the California Privacy Rights Act ("CPRA") regulations and Colorado pursuant to the Colorado Privacy Act ("CoPA"). The GPC is a mechanism (*e.g.*, a browser setting) that allows consumers to opt-out of targeted advertisements and/or the sale of personal information through a pre-determined signal. The GPC allows consumers to make a *single* opt-out request that applies to all websites able to recognize the signal rather than manually electing this option on each website individually, which is the current default in the US and the EU.

Under the CCPA, CPRA, and CoPA, the GPC must be honored by covered businesses and must be treated as a valid consumer

Authors/Presenters

Christian M. Auty

US Data Privacy and Security Lead
Chicago
christian.auty@bclplaw.com

Gabrielle A. Harwell

Associate
Chicago
gabrielle.harwell@bclplaw.com

Paul B. Sudentas

request to opt-out of the sale or sharing of the consumer's personal information, subject of course to certain exceptions. Yet, the state of the technology surrounding GPCs is at best in flux. Mozilla Corp.'s Firefox browser was updated in December 2021 to include a GPC; but it remains unclear how or when other popular browsers—*e.g.*, Edge and Chrome—will integrate a GPC. Although not all browsers have an integrated GPC, standalone browser extensions are available from various developers including, *e.g.*, Abine and DuckDuckGo, which allow consumers to enable GPCs in some browsers that are not yet equipped with GPCs. But as of this writing, there is no universal solution to enable a GPC in all web browsers.

Associate
New York
paul.sudentas@bclplaw.com

Amy de La Lama

Chair - Global Data Privacy and Security
Boulder
amy.delalama@bclplaw.com

California

Under the California Attorney General's CCPA regulations, a business that "collects personal information from consumers online . . . shall treat user-enabled global privacy controls, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request submitted" under the CCPA.[1] Despite requiring covered businesses to recognize the GPC as a valid opt-out method under the CCPA, California regulators have not published clear guidance as to technical recognition and content of GPCs. The CCPA's implementing regulations merely explain that global privacy signals "shall clearly communicate or signal that a consumer intends to opt-out of the sale of personal information."[2] Regarding conflicting signals between a user's global privacy signal and a user's stated preference through a cookie preference center, the regulations require covered entities to respect the signal over any other user-stated preferences.[3] Beginning January 1, 2023, the CPRA goes into effect together with its own requirement to recognize the GPC. The issue is currently addressed in draft regulations, but substantively the requirements have not changed from CCPA: a business is required to recognize an opt-out signal for the browser and (if known) consumerin question and in the event of a conflict with other elections, the opt-out signal is given preference as a default matter. In fact, the CPRA regulations appear to go a step further by requiring businesses to acknowledge that a GPC has been processed to the consumer.

This is of particular importance given that the first monetary settlement under the CCPA alleged failure to honor the GPC. This settlement likely indicates that future enforcement will emphasize cookies, opt-outs and indeed recognition of the GPC. Businesses can and should address this issue now, if possible, utilizing technology that purports to recognize such signals automatically.

Colorado

Under CoPA (which goes into effect on July 1, 2023), controllers who process personal data for the purpose of targeted advertising or the sale of personal data "shall" allow consumers to exercise the right to opt out of processing for such purposes through a user-selected universal opt-out mechanism.[4] But unlike California's regulations which have immediate effect, this provision does not take effect until 2024. In addition, a consumer still may consent to the collection and use of their personal information for the purpose of targeted advertising or the sale of personal information.[5] Where the consumer consents to such processing, the consumer's consent "takes precedence over any choice reflected through the universal opt-out mechanism."[6]

Before the requirement to recognize a universal opt-out mechanism becomes operative on July 1, 2024, the Colorado Attorney General's office is expected to adopt rules detailing the technical specifications for one or more universal opt-out methods. These regulations must be finalized by July 1, 2023, and the regulations must contain certain limitations on use of the GPC.[7] Specifically, the universal opt-out mechanism:

- cannot unfairly disadvantage the controller;
- may not be a default setting and, instead, must clearly represent the consumer's affirmative, freely given, and unambiguous choice to opt-out of the processing of personal data;
- must be consumer friendly, clearly described, and easy to use by the average consumer; and
- must be consistent with any other similar mechanisms required by law or regulation in the US.[8]

In addition, the controller:

- must be required to inform consumers of the universal opt-out mechanism; and

- must be able verify the consumer's state residency and verify that the consumer has affirmatively opted out of the collection and use of personal information for targeted advertising or the sale of personal data.[9]

Forthcoming CoPA regulations should shed more light on operational requirements.

The emergence and adoption of global privacy signals will likely become critical to businesses' online operations in the near future, and as recent enforcement activity makes clear, this issue is a current priority for California regulators. At present, most businesses likely will need to rely on third party providers for technical assistance. Businesses should work with IT and other technical professionals to ensure GPC technology, however nascent, can be recognized if necessary.

---

[1] 11 CCR 7026(a), (c). Note that a global privacy signal must be treated as a request directly from the consumers, rather than as a request from an authorized agent. Id., at (f).

[2] 11 CCR 7026(c).

[3] Id., at (c)(2). Note, however, that the covered business may notify the consumer of any conflict and ask for confirmation of the consumer's interest in participating in any business-specific privacy setting or participation in a financial incentive program.

[4] Colo. Rev. Stat. § 6-1-1306(1)(a)(IV)(B).

[5] Colo. Rev. Stat. § 6-1-1306(1)(a)(IV)(C).

[6] Id.

[7] Colo. Rev. Stat. § 6-1-1313; Colo. Rev. Stat. § 6-1-1306(1)(a)(IV)(B).

[8] Colo. Rev. Stat. § 6-1-1313(2).

[9] Id.

RELATED PRACTICES

Data Privacy & Security

This document provides a general summary and is for information/educational purposes only. It is not intended to be comprehensive, nor does it constitute legal advice. Specific legal advice should always be sought before taking or refraining from taking any action.