CLIENT ALERTS & INSIGHTS

Privacy Points 2023: California and Colorado Will Soon Require Acceptance and Adherence to Universal Opt-Out Mechanisms

JANUARY 30, 2023

As Colorado and other US states join California in putting broad data protection laws and regulations in place, the ability for consumers to "opt-out" of certain collection and processing activities also expands—including a requirement that businesses adhere to universal opt-out mechanisms.

The Colorado Privacy Act ("**CPA**") was signed into law as Colorado's first broad data protection law in July 2021. Beginning July 1, 2023, the CPA will be effective and enforceable.

With that, Colorado will be joining the ranks of California and Virginia in states that have broad data protection laws in effect, with Connecticut and Utah also joining the ranks throughout 2023. To view our previous commentary on the effective dates and scope of the US state data protection laws, see here.

One of the biggest topics where the different US state laws diverge is on the topic of data subject rights. Most of the states have implemented a new category of information that receives greater protection: Sensitive Personal Information. However, the states differ on how businesses can collect Sensitive Personal Information, with Colorado, Connecticut, and Virginia requiring opt-in, prior consent; California allowing individuals the right to limit the use of their Sensitive Personal Information; and Utah allowing individuals the right to completely opt-out of the use of their Sensitive Personal Information.

This exemplifies the complicated web that is created by each US state setting up their own spin on a consumer data protection legal regime. The states also diverge on how many "opt-out" rights an individual has (e.g., to opt-out of the selling of their information; to opt-out of the sharing of their information; to opt-out of profiling; etc.). They also diverge in-where such opt-out rights are granted-how businesses are required to allow individuals to exercise those rights.

For example, in the latest version of the draft CPA's regulations and California regulations, businesses within the scope of each states' respective date protection law will need to configure their websites to recognize and honor a web user's universal opt-out signal. This requirement essentially changes the opt-out right into a requirement that an in-scope business obtain consent from individuals using universal opt-out mechanisms before enabling targeted advertising or the sale of personal information.

Colorado Data Privacy Rights

For purposes of explaining the universal opt-out requirement, we will focus on Colorado as an example; and to understand Colorado's universal opt-out requirement, a business must first understand the rights granted to individuals under the CPA.

Under the CPA, individuals have the following privacy rights to (i) opt-out of targeted advertising; (ii) opt-out of the sale of personal data; (iii) opt-out of profiling in furtherance of decisions producing legal or similarly significant effects; (iv) access the information collected about them; (v) correct inaccuracies in their information; (vi) delete information held about them; and (vii) to obtain their information in a portable and readily usable format and/or have it transmitted to another entity (e.g., data portability). The opt-out rights warrant further explanation.

The right to opt-out of targeted advertising only applies to cross-contextual behavioral advertising-meaning a business that creates personalized / targeted advertisements based on personal data obtained from an individual's activities across the Internet (outside of the business's specific website).

The right to opt-out of the sale of personal data largely tracks with similar, broad rights granted under other US state data protection laws. "Sale" is defined broadly to include any disclosure of personal information for monetary ***or other valuable consideration***.

Finally, the right to opt-out of profiling covers that processing by automated means (e.g., no human intervention) and for purposes of making decisions that result in the denial of financial or lending services, housing, insurance, education enrollment or opportunities, criminal justice, employment, healthcare, or access to essential goods and services.

The universal opt-out requirement under the CPA only applies to an individuals opt-out rights with regard to (i) the sale of their personal information; and (ii) targeted advertising.

Colorado Universal Opt-Out Requirement

Under the draft CPA regulations and beginning on July 1, 2024 (one year after the CPA's effective date), all in-scope business will need to (i) configure all of their websites to recognize any universal opt-out mechanisms (as identified by the Colorado Department of Law); (ii) treat all signals received from universal opt-out mechanisms as a valid request by an individual to opt-out of targeted advertising and/or the sale of their personal information (as applicable); and (iii) continue treating the individual as having opted-out until the individual opts-in to targeted advertising or sale of their personal information.

No later than January 1, 2024, the Colorado Department of Law will announce an initial list of universal opt-out mechanisms that businesses will need to accept as valid opt-out requests. However, the draft CPA regulations set forth technical specifications that any universal opt-out mechanism must meet in order to be recognized.

The mechanism must (i) allow for the automatic communication of their opt-out choice to multiple businesses (e.g., through commonly used coding formats such as HTTP or JavaScript); (ii) allow for the individual to clearly communicate their opt-out rights; (iii) store, process, and transmit the information necessary for the business to effectuate the opt-out request; (iv) must have in place

reasonable security measures for the transmission of such information; and (v) must not unfairly disadvantage the business (e.g., anti-competitive practices) or prevent the business's ability to verify the request or determine whether the individual is a resident of Colorado.

Additionally, it is important to note that a universal opt-out mechanism ***cannot be a default setting***. Meaning, the opt-out options cannot come pre-installed or pre-configured on a device, browser, or operating system. The opt-out setting still needs to be made by the individual's affirmative choice. This does not preclude an individual from exercising an opt-out right through the use of a browser add-on / plug-in, however.

Consent After Universal Opt-Out

It is important to note that a business can-after receiving a universal opt-out signal from an individual-enable that individual to later consent to targeted advertising or the sale of their personal information.

Therefore, for individuals who have enabled universal opt-out mechanisms, a business can present individuals with a link to ***opt-in to*** targeted advertising or the sale of their personal information, instead of merely providing an opt-out link.

This is a huge departure from previous US state laws that instead relied on individual, specific opt-out rights in order to give individuals more control over their information. Colorado's universal opt-out requirements flips that legal regime on its head as a business will now be required to obtain prior consent from those individuals with universal opt-out mechanisms implemented.

Comparison to California

The biggest difference between the Colorado and California universal opt-out requirement is that the requirement in Colorado is effective July 1, 2024, while the requirement is effective in California now, but enforceable beginning July 1, 2023.

Meaning businesses in the scope of California's data protection law will need to adhere to the universal opt-out requirement a full year before those businesses only subject to the CPA.

The California regulations also provide greater context and description on how a business is to proceed in the event a consumer has a universal opt-out mechanism in place, but has conflicting settings configured on a specific website. In such an event, the business is required to adhere to the universal opt-out, but can inform the individual of the conflict and the affect of their opt-out.

Finally, if a business subject to California's data protection law adheres to the universal opt-out requirement in a manner that is "frictionless"-does not charge a fee, does not change the individual's experience with the applicable product or service, and does not display a pop-up window in response to the opt-out signal-can forgo the traditional requirement of posting a link to a "DO NOT SELL OR SHARE MY PERSONAL INFORMATION" that is normally required where a business is selling personal information or using personal information for targeted advertising purposes.

Takeaway

As stated above, this is a departure from the standard US approach to privacy rights that traditionally relied on a "notice and choice" regime. The movement toward requiring acceptance of universal opt-outs-while still requiring some action to be taken by the individual-moves California and Colorado closer to a regime relying on consent.

Business's subject to the California or Colorado data protection laws will need to invest time and resources into building out the technical capabilities of their websites to ensure they meet the universal opt-out requirements.

As more states continue to implement their own variations of data protection laws and business juggle the various requirements, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.