July 28, 2021

Don’t Sell Privacy Compliance Short; Why Now is the Time to Double-Check How Your Company Handles Consumers’ Opt-Out of Sale Requests

by Jon Neiditz

Most privacy eyes are currently focused on the new EU Model Clauses and forthcoming U.S. state laws that take effect in 2023. As the summer heats up, however, compliance professionals should look to the western U.S. states of Nevada and California.

(a) Expanded Rights for Nevada Consumers

This blog broadcast just over two years ago that many companies need not take any action to comply with what was then Nevada’s newly established consumer rights to opt out of information selling. Earlier this summer, the Nevada legislature updated that privacy law through SB 260 (which takes effect in October 2021) to profoundly expand the scope of (1) sales of which consumers may opt out and (2) types of entities subject to the law.

Nevada consumers will no longer have only the right to opt out of sales to data brokers. Under current law, a consumer may opt out of a sale only if the “purpose” of the sale is to allow the information’s recipient to further license or sell the information, i.e., sales to data brokers. As revised by SB 260, however, Nevada law defines “sales” to include exchanges of information for monetary consideration to any third party.

Data brokers, in addition to website operators, must now field opt-outs under Nevada’s updated law. As originally enacted, the law applied only to operators of commercial websites and online services. Come October (when SB 260 takes effect), data brokers must also comply with the law. (Unlike California and Vermont law, however, Nevada law does not create a data broker registry).

As we noted in 2019, exceptions abound under the Nevada law and SB 260 preserves and expands upon those exceptions. Given the expanded scope of sales, companies may need to now rely on such exceptions more substantially than they have been since 2019. A few of the key exceptions added by SB 260 ensure that the law does not apply to:

- Consumer reporting agencies and any agencies and entities subject to the GLBA;
- Any PII subject to the FCRA or GLBA;
- Entities that collect, maintain, or sell PII for fraud prevention purposes; and
- Any organization that does not collect, maintain, or sell covered information.

Given that Nevada's privacy law will soon apply to traditional selling, organizations should reassess their compliance positions under the law before October. Fortunately, organizations that find themselves subject to the revised Nevada law probably also sell personal information under the CCPA (the next subject of this blog post), so compliance may be as simple as expanding CCPA opt-out rights to Nevadans.

(b) CCPA Enforcement Updates

Lest its neighbor to the east steal the privacy spotlight, California's Attorney General introduced three important updates around "selling" under the CCPA, which, as many know, is broadly defined only in California to mean almost any type of sharing.

First, under CCPA regulations, businesses that collect and sell personal information from consumers online must accept opt-out requests through user-enabled privacy controls. The California Attorney General unequivocally clarified in online FAQs that the Global Privacy Control or "GPC" is one such control that companies must accept, writing that the GPC "must be honored by covered businesses as a valid consumer request to stop the sale of personal information."

Although the GPC will become optional in 2023 under the California Privacy Rights Act (or CPRA, an update to the CCPA), global privacy controls are here to stay. For example, the recently signed Colorado privacy law requires the Colorado Attorney General to issue regulations by July 2023 requiring businesses to comply with a "user-selected universal opt-out mechanism."

Second, newly released examples of CCPA enforcement also underscore the Attorney General's focus on consumers' right to opt out of sales, including through global privacy controls. Many of the enforcement actions that the Attorney General highlighted were centered around a business's failure to facilitate consumers' rights to opt out of CCPA sales. One enforcement action summary specifically mentioned a business's failure to comply with opt-outs submitted via a user-enabled global privacy control such as the GPC as a basis for the enforcement action. The example noted that the company resolved the enforcement action without penalty (as most CCPA enforcement actions are resolved) by working with its privacy vendors, underscoring many companies' growing reliance on outsourcing technical aspects of privacy compliance operations. Companies that launch online tracking controls for website users should check whether such controls respond to GPC signals.

Third, consumers may now scrutinize businesses' privacy compliance around selling personal information, as the California Attorney General launched a new privacy enforcement tool. Through the tool, consumers may draft notices to a business that does not post a conspicuous "Do not Sell" button on the business's website. Although developed by consumers, the notices generated through the tool are not without legal effect, and may trigger the CCPA's 30 day compliance cure period. As such, businesses should (1) check the prominence of the business's "Do not Sell" button(s) and (2) develop a process for flagging and escalating potential consumer notices.

Much like the European changes and updates, it seems that changes in state privacy laws and guidance will likely prevent privacy professionals from enjoying a relaxing summer.