California Regulator Signals New Era in Privacy Enforcement

April 30th, 2025 | and Erik Kosa

Last month, the California Privacy Protection Agency announced a consent order with an auto manufacturer alleging multiple violations of the California Consumer Privacy Act and imposing a $632,500 fine for alleged failure to strictly comply with the CCPA's provisions. In other words, there is no *de minimis* exception to CCPA enforcement; 90% compliance is not enough.

The regulator alleged the manufacturer collected more data than it needed, made it difficult for consumers to use authorized agents to act on their behalf to assert their rights under the CCPA, made it difficult for consumers to understand how to control what information was being collected, and failed to maintain contracts with advertising technology vendors containing adequate privacy protections.

This is the first finalized order entered into by the CPPA, which has to-date only been enforced by the Attorney General, and it marks a shift in the enforcement landscape. Up until now, California prioritized enforcement of major deficiencies in businesses' privacy practices, but the violations identified here are incredibly specific. While this action is part of a larger privacy sweep against manufacturers with connected vehicle technology, the order itself makes no mention of this specific technology. The privacy violations at issue are not unique to auto manufacturers and apply across industries. Below are some lessons businesses can take away.

- **Regulators don't like dark patterns.** Not all privacy rights requests should require the same number of steps to complete. The cookie consent management interface here required one click to opt-in and two clicks to opt-out, which the CPPA considered a violation of the CCPA's "symmetry in choice" requirement. Symmetry in choice means that the path for a consumer to exercise a more privacy-protective option cannot be longer or more difficult or time-consuming than the path to exercise a less privacy-protective option. Privacy choices must be symmetrical to comply with the CCPA.
- **Keep things as simple as possible for consumers.** Collecting too much information to process rights requests can violate the CCPA's data minimization principles. With respect to the rights to know, correct, and delete, the order suggests that verifying a consumer's identity should only require the collection of two data points. Here, the company required consumers to verify their identity by providing their first name, last name, address, city, state, zip code, preferred method to receive updates, email, and phone number before their requests could be processed, and this constituted a CCPA violation.
- **Pay close attention to what the CCPA does *not* require.** Under the CCPA, consumers have the

right to opt out of the sale or sharing of their personal information to third parties, as well as the right to limit the use of sensitive personal information. Unlike the rights to know, correct, and delete, these opt out rights do not *require* you to verify the consumer's identity before complying with the request. Because verification was not strictly required by the law, the Privacy Protetion Agency alleged that requiring it here was a violation. In addition, when consumers appointed authorized agents to exercise their rights to opt out of sale or sharing and to limit the use of sensitive information for them the company required consumers to independently confirm that they appointed the authorized agent. The CCPA permits this for requests to delete, request, or correct by providing "[w]hen a consumer uses an authorized agent to submit a request to delete, request to correct, or a request to know, a business may require the authorized agent to provide proof that the consumer gave the agent signed permission to submit the request." Cal. Code Regs. tit. 11, § 7063(a). The provision allowing consumers to opt out of the sale or sharing of their personal information and limit the use of sensitive information does not specifically prohibit a business from independently verifying with the consumer, but does state a business's process here "shall be easy for consumers to execute" and "shall require minimal steps[.]" Cal. Code Regs. tit. 11, § 7026(b). That this constituted a CCPA violation shows how strictly the Privacy Protection Agency intends to enforce its provisions.

- **Watch over vendors.** Every comprehensive state privacy law, including the CCPA, requires covered entities to have contracts in place with vendors who process personal information on their behalf with specific provisions protecting that data. Having a third-party risk management process in place will ensure your vendors are complying with the CCPA and other state privacy laws. Businesses should regularly review all contracts with vendors who access customer data to make sure they have the required language governing the exchange of data.

CCPA compliance requires a very strict and detailed reading of the law's requirements, paying as much attention to what is *not* said, as what is said.

Right now, regulators are particularly interested in the use and collection of geolocation data, a kind of "sensitive data" subject to heightened protections for its collection and use under state comprehensive privacy laws. California Attorney General Rob Bonta has announced an investigative sweep into the location data industry by sending letters to certain advertising networks, mobile app providers, and data brokers that the AG believes are in violation of the CCPA. You need an "opt-in" approach to gather this data rather than the "opt-out" approach that governs most data. And you don't need to use sophisticated connected vehicle technology before triggering these heightened protections. It can be as simple as having someone's IP address plus one other data field. Any company collecting location data should take a close look at how it handles this data.

While this action involved a vehicle manufacturer and not its finance company, remember that the CCPA's exemption for financial institutions regulated by Gramm-Leach-Bliley is narrow: it only applies to *data* regulated by the GLBA, not the entire financial institution, leaving significant categories of personal information—such as data used for marketing—subject to the CCPA's requirements. And while most states' privacy laws do exempt entire entities subject to GLBA,

there has been increased talk of narrowing these exemptions. Regulated entities would do well to incorporate the lessons from this settlement into their privacy compliance programs.