PUBLICATION

Location Data Practices Targeted by California Lawmakers and Regulators

Authors: Alisa L. Chestler, Matthew George White, Alexander Frank Koskey, III, David J. Oberly
March 14, 2025

In late February, California lawmakers introduced new legislation that would impose sweeping restrictions on the use of location and tracking data. Known as the California Location Data Act (CLDA), this legislation goes a step beyond the current body of law governing location data – which generally only requires informed consent – by imposing substantive, strict limitations and prohibitions on certain location tracking activities, even where data subjects acquiesce. Just weeks later, California Attorney General Rob Bonta (California AG) announced an ongoing investigative sweep of companies using location data for compliance with the California Consumer Privacy Act (CCPA).

Taken together, companies that collect or use location data should review (and, if necessary, modify) their current privacy practices immediately, as legal requirements and restrictions, regulatory scrutiny, and class action risk arising from this particular type of sensitive data will continue to increase as we move further into 2025 and beyond.

CLDA Overview and Compliance Obligations

If enacted, the CLDA would apply to "covered entities," broadly defined to mean "any individual, partnership, corporation, limited liability company, association, or other group, however organized," as well as their agents. Data subjects, referred to as "individuals" in the CLDA, are likewise defined in an expansive fashion to encompass all individuals "located" within the state of California – thereby extending the CLDA's protections beyond residents of the state.

The scope of covered data under the CLDA is likewise sweeping, with "location information" defined to include any information that directly or indirectly reveals the present or past geographic location of an individual or device within the state of California with sufficient precision to identify street-level location information within a range of five miles or less.

The CLDA would also impose significant monetary penalties for any covered entity that violates or otherwise *facilitates* a violation of the CLDA, including: (1) actual damages; (2) civil penalties of $25,000 per person; (3) attorney's fees; and (4) exemplary damages. Importantly, however, the CLDA does not include a private right of action allowing for class action litigation. Instead, enforcement authority would rest exclusively with the California AG and its district, county, and city equivalents.

In terms of its compliance obligations, the CLDA would first require covered entities to obtain prior, express consent before collecting location information. Separate consent would also be needed before a covered entity uses location data in a manner that departs from what was disclosed to individuals at the initial time of collection.

Second, the CLDA would impose strict data minimization obligations on covered entities, limiting the collection, retention, use, and disclosure of location information to only that which is necessary to provide goods or deliver services. In addition, the law would also impose an across-the-board, blanket ban on all selling, renting, trading, or leasing of location information.

Third, covered entities would be required to disclose certain details regarding their processing of location information to individuals at or before the time of collection.

Fourth, covered entities would be required to maintain specific location-information policies setting forth detailed disclosures that include, among other things: (1) the identities of all service providers with which the covered entity contracts concerning location information; (2) the covered entity's data management and data security policies governing location information; and (3) its retention schedule and guidelines for permanently deleting location information.

California AG Launches Probe Into Use of Location Data

On March 10, 2025, the California AG announced its ongoing investigative sweep into companies using location data and their compliance with the CCPA. Given that "[t]he risk posed by the widespread collection and sale of location data has become immediately and particularly relevant given federal threats to California's immigrant communities, and to reproductive and gender-affirming healthcare." The AG's enforcement sweep focuses on how covered businesses offer and effectuate consumers' right to stop the sale and sharing of personal information and the right to limit the use of their sensitive personal information, which includes geolocation data.

As part of its initiative, the AG has issued letters to advertising networks, mobile app providers, and data brokers putting them on notice of potential violations of California's comprehensive consumer privacy statute. In addition, the AG's letters also seek additional information regarding recipients' location data-related business practices.

Other Recent Developments

The CLDA mirrors similar restrictions and limitations imposed on location data under Maryland's consumer privacy statute, the Maryland Online Data Privacy Act (MODPA). Both are reflective of the emerging trend whereby lawmakers are moving away from the traditional "notice and consent" privacy model in favor of more concrete, robust privacy protections.

At the same time, regulators have also increased their focus on investigating and rooting out improper tracking practices at both the federal and state levels. In 2024, the Federal Trade Commission (FTC) pursued four separate enforcement actions against companies that used location data in an unfair or deceptive fashion. For years now, state AGs and other state privacy regulators have targeted companies deemed to have used location data in an unfair or deceptive manner as well. In 2022, for example, Google paid just shy of $400 million to settle an enforcement action brought by a collation of 40 states arising out of the company's purportedly improper location data practices. At the start of 2025, the Texas AG sued insurance giant Allstate for unlawfully collecting, using, and selling location data in violation of the Texas Data Privacy and Security Act (TDPSA) – marking the first lawsuit filed to enforce a comprehensive state consumer privacy statute.

Recently, even those states without a comprehensive consumer privacy statute on the books have entered the fray, pursuing civil enforcement actions under Unfair or Deceptive Acts and Practices (UDAP) laws, which exist in some form or fashion across all 50 states. As just one example, in February 2025 the Arkansas AG sued a Fortune 50 company for allegedly improper location data practices under the Arkansas Deceptive Trade Practices Act (ADTPA).

It comes as no surprise, then, that the California AG has ramped up its efforts to scrutinize location data practices for potential CCPA violations. The AG has carried out several other investigative sweeps in its enforcement of the CCPA, including those targeting employers, loyalty programs, streaming services, and connected vehicles. Notably, the AG's investigative sweep of companies operating in the connected vehicle space singled out how businesses used and shared location data generated by "today's connected computers

on wheels." More than that, previous investigative sweeps have resulted in CCPA enforcement actions and significant settlements with large monetary and broad remedial components.

The Final Word

While it is yet to be seen whether the CLDA makes its way into law, the California AG's current investigative sweep should serve as a reminder of the significant legal risks and liability exposure that exists in connection with location data and related tracking activities. Companies should work closely with outside privacy counsel to thoroughly review their current location data practices and assess their level of compliance with federal and state law. By starting the compliance check process now, companies can afford themselves sufficient time to remediate any compliance gaps and head off the prospect of being the target of a future investigative sweep, enforcement action, or class action litigation.

If you have questions or concerns regarding this alert, please reach out to Alisa L. Chestler, CIPP/US, QTE, Matthew G. White, CIPP/US, CIPP/E, CIPT, CIPM, PCIP, Alexander F. Koskey, CIPP/US, CIPP/E, PCIP, David J. Oberly, or any member of Baker Donelson's Data Protection, Privacy, and Cybersecurity team.