



Fact Sheet: AB 322 California Location Privacy Act

PROPOSED BILL

Assembly Bill (AB) 322, the California Location Privacy Act, modernizes the California Consumer Privacy Act (CCPA) to close dangerous loopholes in how precise location data is collected, retained, sold, and disclosed. It ensures that Californians' movements—especially in sensitive spaces like protests, clinics, houses of worship, and legal service centers—are not quietly tracked or weaponized against them.

BACKGROUND

Californians are more vulnerable to digital exploitation than ever before. Mobile devices are ubiquitous in our daily lives, with most consumers keeping their phones with them at all times. These devices have an incredible power to track a user's location, and generate a shockingly accurate record of a user's whereabouts and routines throughout the day.

Additionally, technologies like automated license plate readers, and facial recognition cameras have become ubiquitous in public spaces to provide services without the need for direct consent, or as a condition of entry into certain establishments. This means even if a consumer takes steps to reduce their personal device use, they are not able to avoid near constant surveillance while interacting in public spaces.

Precise location data can reveal deeply personal and constitutionally protected behaviors: attending a protest, seeking abortion care or legal services, visiting a place of worship, or organizing a union. Today, this data is quietly collected by apps and devices, traded by data brokers, and accessed by government agencies—often

without a court order or consumer knowledge.

In the last 5 years, the Federal Trade Commission (FTC) has filed numerous complaints and lawsuits exposing the conduct of large Location Data Brokers (LDB), with four high profile cases filed in 2024 alone. In their complaints, the FTC alleged LDBs collected billions of location data points linked to unique persistent identifiers and timestamps that could offer insights into people's movements. Once this data is shared with a third party data broker, there is little to no restriction on how and when it can be shared.

In a complaint filed on [Kochava Inc.](#), the FTC alleged they sold access to its data feeds on online marketplaces that are publicly accessible. Kochava typically charges a monthly subscription fee of thousands of dollars to access its location data feed but has also offered a free sample model. The FTC alleges that this behavior failed to adequately protect its data from public exposure. Kochava allowed anyone with little effort to obtain a large sample of sensitive data and use it without restriction.

In June of 2025, Immigration and Customs Enforcement (ICE) conducted coordinated raids across Los Angeles, detaining dozens and igniting fear in immigrant neighborhoods. In the days that followed, thousands of Angelinos took to the streets in protest, exercising their right to assemble and speak out. However, digital surveillance tactics—including geofencing and location tracking purchased from data brokers—now pose a direct threat to that right. Advocates warn that federal agents are increasingly using commercially acquired location data—

rather than warrants—to track people based on where they have been.

This disturbing trend, often described as “digital deportation,” has been the subject of mounting investigative reporting:

- The Department of Homeland Security (DHS) has purchased passenger data from airlines under [secretive programs](#), exposing millions to surveillance.
- ICE has built a “[vast surveillance dragnet](#),” buying geolocation, utility, and vehicle data from brokers to track and deport immigrants—without judicial review.
- Popular apps continue to sell location data to third parties, helping ICE target individuals for “[digital deportation](#).”

These practices threaten First Amendment rights, privacy, and public trust, and provide a legal loophole to get around local or state laws restricting cooperation with federal immigration enforcement.

While California is a leader in consumer privacy protection, much of our laws revolve around an opt-in/out model. Unfortunately, to the extent that consumers opt-in to the collection of precise location data, such opt-in processes typically do not explain to the consumer who will receive this data or how it will be used. Consumers are therefore unable to take reasonable steps to avoid exposure, and on the contrary often have no choice but to opt-in in order to receive services required for day-to-day activities.

Now more than ever it is imperative we protect the privacy rights of our communities, especially with increased attacks targeting our immigrant and minority community members, and individuals seeking legal health services, such as reproductive health and gender-affirming care. While the FTC has clearly outlined a the shocking violation

of consumer privacy by LDBs, it seems like further action from the federal government has been shelved indefinitely with the removal of FTC leadership, and the transition to a new administration.

SOLUTION

AB 322, the California Location Privacy Act, would safeguard the privacy of Californians by placing restrictions on the collection, use and sale of location data.

Specially, this bill would ban the sale, lease, or trade of precise location data to third parties; restrict the collection of such data to only what is strictly necessary to deliver a requested service; cap retention of location data; and require a valid California court order before any government agency can access this data. These provisions are specifically designed to protect sensitive spaces—including protests, clinics, places of worship, and legal service centers—from warrantless surveillance.

The FTC has made it clear in their reports that this conduct undermines our civil rights, and puts all consumers in danger from exploitation. Recent events have only further emphasizes the imminent danger these practices pose, and the urgent need for additional protections. Unfortunately, since the publication of their reports, all actions at the federal government level have seemingly stalled indefinitely and top officials removed with the transition to the new administration. AB 322 takes bold action at the state level to safeguard consumer privacy and ensure that the safety of all Californians is made a top priority.

SUPPORT

Consumer Reports (Co-Sponsor)
California Initiative for Technology
&Democracy (CITED) (Co-Sponsor)

Asian Americans Advancing Justice
Southern California (AJSOCAL) (Co-
Sponsor)

OPPOSITION

None at this time.

FOR MORE INFORMATION

Contact: Charles Loudon
Phone: (916) 319-2078
Email: Charles.Loudon@asm.ca.gov

Bill Version: Amended June 23, 2025