California's Latest Privacy Push: The Location Tracking Crackdown Businesses Can't Ignore

Insights
3.05.25

Businesses operating in California that rely on location tracking – whether for fleet management, employee monitoring, logistics, or marketing – should pay close attention to a bill that would dramatically alter the legal landscape. If enacted, the California Location Privacy Act would significantly impact employers that rely on GPS and other tracking tools to manage their workforce. And for websites, it may turn consumer privacy law on its head by requiring – for the first time in California – that websites provide for opt-in consent before collecting a user's IP address. What do you need to know as AB 1355 works its way through the legislative process? This article breaks down the bill's key provisions, how it fits into California's existing privacy framework, and what employers and businesses should consider doing now to prepare.

1. The Bill at a Glance

AB 1355 seeks to impose strict regulations on how businesses collect, use, and retain "location information" gathered from or about individuals in California.

What is location information?

The bill defines location information to include "information derived from a device or from interactions between devices, with or without the knowledge of the user and regardless of technological method used, that pertains to or directly or indirectly reveals the past or present geographical location or 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 definition includes, but is not limited to, GPS coordinates, IP addresses, cell-site location data, and information captured by automated license plate readers or facial recognition systems.

Who does AB 1355 cover?

AB 1355 would apply to virtually *all* private organizations, businesses, nonprofits, and individuals that collect or use location data, with narrow exceptions for healthcare data covered by HIPAA or similar laws. Government agencies are excluded but would be barred from selling location data to third parties.

What would AB 1355 change?

One of the bill's most controversial provisions is its express opt-in consent requirement— meaning businesses would need to obtain affirmative consent from individuals before collecting their location data. In addition, the bill limits how long businesses can retain location data and imposes a strict ban on selling, renting, or trading location data. This heightened regulatory framework goes well beyond California's current privacy laws.

California already regulates location tracking through a combination of criminal and consumer privacy laws. Under the California Penal Code, it is illegal to use an electronic tracking device to determine a person's location or movements without their consent. The statute does not explicitly carve out exceptions for location tracking via smartphones, computers, or software-based tools, leaving some ambiguity around how modern technologies fit into this framework.

The California Consumer Privacy Act (CCPA), as amended by the California Privacy Rights Act (CPRA), also treats geolocation data as "personal information." That means it is subject to disclosure requirements and consumer rights protections. The law defines "precise geolocation" to include any location data derived from a device that identifies a person's location within an 1,850-foot radius. This type of data is also considered sensitive personal information, giving consumers the right to limit its use and disclosure for certain purposes such as inferring characteristics about an individual.

Businesses subject to the CCPA must provide notice when they collect location data, along with options for consumers to access, delete, or opt out of the sale of that data. The CCPA does not require opt-in consent before collecting geolocation information. AB 1355 would layer even stricter obligations on top of these existing requirements, pushing California's privacy regime toward a far more restrictive, opt-in model.

AB 1355 would also apply to all businesses and nonprofits, without exception, as compared to the CCPA which generally only applies to for-profit businesses that meet the minimum revenue threshold (currently at $26,625,000 gross revenue in the prior calendar year as of January 1) or other criteria tied to selling personal information.

2. Key Provisions of AB 1355

AB 1355 would impose the following requirements on businesses that collect or use location data:

- ***Strict Opt-In Requirement.*** Businesses would be required to obtain clear, affirmative consent before collecting any location data. Implied consent would not be sufficient. This would go further than the CCPA, which only requires an opt-out process.
- ***Purpose Limitation.*** Location data can only be collected if necessary to provide a specific good or service requested by the individual. This "necessity" standard is extremely vague, potentially leaving employers uncertain as to whether common business practices (such as tracking company vehicles and monitoring remote work) meet this standard.

- ***Five-Mile Radius of Location Data.*** Location data includes data revealing a person's or device's location within a five-mile radius – broad enough to cover entire zip codes in densely populated areas. This overinclusive scope creates significant compliance hurdles for businesses of all sizes.
- ***Retention Limits.*** Businesses may only retain location data for as long as strictly necessary for the requested service. This vague standard could make it difficult for companies to defend lawsuits, respond to regulators, or ensure cybersecurity.
- ***Sale and Disclosure Ban.*** Selling, renting, trading, or leasing location data is prohibited. Sharing data with third parties is limited to situations directly necessary for the requested service.
- ***No Inference Rule***. Businesses are prohibited from inferring additional data from location information beyond what is necessary for the requested service. This could severely limit common employer practices like tracking employee productivity or monitoring for policy violations based on location patterns.
- ***Enhanced Notice and Policy Requirements.*** Businesses must prominently disclose when and by whom location data is collected, provide a phone number and a website where consumers can obtain more information, provide detailed privacy policies, and notify individuals at least 20 days before any changes are made to these policies.

Violations could trigger civil penalties of up to $25,000 per violation, injunctive relief, and an award of attorney's fees to prevailing plaintiffs. The bill permits enforcement by the California Attorney General, district attorneys, and certain public prosecutors. For small businesses in particular, these steep fines could be financially devastating, with even minor or unintentional violations quickly adding up to crippling penalties.

3. Concerns for Employers

AB 1355 raises particularly thorny issues for employers that frequently use location tracking for legitimate business and operational reasons, such as:

- Fleet management and logistics tracking for company vehicles
- Employee productivity monitoring for remote or field-based workers
- Workplace safety and incident response, including confirming an employee's presence during emergencies
- Asset protection, particularly for equipment in transit
- Cybersecurity monitoring, such as ensuring company systems are accessed only from approved locations

The bill's "necessary for service" standard does not neatly fit these employment-related uses, creating ambiguity about what location data employers can collect and retain. Additionally, requiring express opt-in from employees could complicate routine onboarding processes, and employees who

refuse consent could create conflicts over job requirements. This opens the door for potential retaliation claims if consent is a condition of employment or continued employment.

AB 1335's prohibition on making inferences from location data would seriously limit an employers' ability to monitor remote employees, prevent timecard fraud, or enforce attendance policies. For example, if an employee calls out sick but logs in from Hawaii, employers may be unable to question that discrepancy, as it would be based on an inference from the location data. For remote workforces, this restriction could make it harder to detect misconduct or enforce workplace rules.

AB 1355 is not the only pending legislation targeting employee monitoring – AB 1331 would prohibit employers from monitoring employees during off-duty hours, raising its own set of compliance challenges. To learn more, click here to read our FP Insight on AB 1331.

4. Issues for Businesses

For businesses more broadly – especially those operating online platforms or engaging in location-based marketing – AB 1355 also poses significant challenges. Notably, AB 1355 does not include any exemptions for small businesses or nonprofit organizations, meaning all entities that collect or use location data must comply, regardless of size or resources. This lack of exemptions could create substantial burdens for smaller organizations that may lack the infrastructure or expertise to implement complex opt-in mechanisms and data minimization processes.

Some of the most significant compliance challenges under AB 1355 include:

- ***Basic Internet Functionality.*** Many online services depend on basic location data, such as IP addresses, to operate. It is unclear whether AB 1355's opt-in requirement would cover these routine data exchanges, and if so, how businesses could realistically comply.
- ***Marketing and Personalization.*** Location data is crucial for targeted advertising, but AB 1355 would ban most uses unless strictly necessary for the requested service.
- ***Data Retention Conflicts***. Businesses often retain data for regulatory compliance, to defend in litigation, or for cybersecurity purposes. AB 1355's retention limits could conflict with these legal obligations.

In short, AB 1355 would dramatically shift California's privacy rules toward a highly restrictive, opt-in model – creating a compliance nightmare for any business that relies on location data for routine operations.

5. What Employers and Businesses Should Do Now

Although AB 1355 is still pending, businesses should consider taking proactive steps now to prepare:

- ***Track the Bill's Progress.*** Stay updated on amendments, committee hearings, and potential changes. Industry groups may also weigh in to shape the final language.

- ***Audit Current Practices.*** Review how your company collects, uses, retains, and shares location data for both employees and customers to ensure you are better prepared to navigate the new legal framework if AB 1355 passes. This includes identifying and reviewing agreements with third parties who collect location data on your company's behalf.
- ***Engage in Legislative Advocacy.*** Trade associations and industry groups may push for clarifications or exemptions, particularly for employee tracking. Employers should consider working through these groups to raise concerns about operational impacts.

Conclusion

California has long been a leader in privacy regulation, but AB 1355 marks a sharp departure from existing frameworks. If passed in its current form, the bill would dramatically reshape how businesses collect, use, and retain location data – creating a compliance nightmare for companies of all sizes. While aimed at enhancing consumer privacy, AB 1355's broad and far-reaching scope would not only restrict how businesses track customers, but also fundamentally alter how employers monitor and manage their own workforce.

Fisher Phillips will continue to monitor the bill's progress and provide timely updates as the situation develops. To stay informed, subscribe to our Insight System, and for further guidance, contact your Fisher Phillips attorney, the authors of this Insight, or any member of the firm's Consumer Privacy Team.

Related People

Risa B. Boerner, CIPP/US, CIPM
Partner
610.230.2132
Email

Usama Kahf, CIPP/US
Partner
949.798.2118
Email

Chelsea Viola
Associate
213.403.9626
Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Trending

U.S. Privacy Hub

Related Offices

Irvine

Los Angeles

Sacramento

San Diego

San Francisco

Woodland Hills