



June 26, 2025

Chair Thomas Umberg  
Vice Chair Roger Niello  
Committee on Judiciary  
California Assembly  
Legislative Office Building  
1021 O Street, Room 3240  
Sacramento, CA 95814

RE: AB 322 (Ward) – The California Location Privacy Act of 2025 – SUPPORT

Dear Chair Umberg and Vice Chair Niello,

Consumer Reports is proud to co-sponsor and support AB 322, legislation that would create commonsense protections around the collection and use of precise geolocation data, including banning the sale of it outright. Geolocation can be useful for pro-consumer applications such as turn-by-turn directions and finding a nearby restaurant; however, all too often this information is secretly collected and shared by dozens if not hundreds of ad networks and data brokers with whom consumers have no relationship or even awareness. This bill will provide straightforward, powerful, and critically important protections for the privacy, autonomy, and physical safety of Californians.

The location information market is a multi-billion-dollar industry<sup>1</sup> centered on collecting and selling people's everyday comings and goings, often collected from people's mobile devices and often without their knowledge or explicit consent. Location data is an extremely sensitive form of personal information. Researchers have shown that 95 percent of individuals can be uniquely identified from just four location points in time and 50 percent of individuals can be uniquely identified from just two spatio-temporal points; most companies that collect this information have orders of magnitude more data than that.<sup>2</sup>

Much of this information is amassed by data brokers, entities that compile extensive dossiers on virtually every American that include thousands of data points, including extremely granular information about people's behavior, as well as inferences about individuals based on their

---

<sup>1</sup> Jon Keegan and Alfred Ng, The Markup, There's a Multibillion-Dollar Market for Your Phone's Location Data, (September 30, 2021), <https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data>

<sup>2</sup> Yves-Alexander de Montjoye et al., Scientific Reports, vol. 3, art. no. 1376, Unique in the Crowd: The privacy bounds of human mobility, (March 25, 2013), <https://www.nature.com/articles/srep01376>

information.<sup>3</sup> Some companies collect and share consumers' location information as often as every three seconds.<sup>4</sup> This information is then sold and resold, often for marketing but for a variety of other purposes as well, eroding consumers' basic expectation of privacy in the process.<sup>5</sup> This activity poses a host of significant risks to California residents.

A few examples of location information-driven harms include:

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use location data brokers to target vulnerable individuals for scams, or otherwise use personal information to cause harm. For example, scammers can use commercially available location information to increase the specificity of their phishing or social engineering scams, such as by including location-specific details like mentioning a nearby business or the individual's recent activity.<sup>6</sup> Location data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.<sup>7</sup>
- *Predatory use of consumer data.* Data brokers sell location information about people who rarely even know the companies even exist—and who have rarely ever affirmatively, expressly consented to this information collection and sale. In some instances, this can result in financially disastrous consequences for consumers. Some data brokers sell lists of consumers sorted by characteristics like “Rural and Barely Making It” and “Credit Crunches: City Families,” which can be used to target individuals most likely to be susceptible to scams or other predatory products.<sup>8</sup> And a recent case brought by the Texas Attorney General alleged that Arity, a data broker owned by the insurance

---

<sup>3</sup> See, e.g., Joseph Cox, The Secret Weapon Hackers Can Use to Dox Nearly Anyone in America for \$15, 404 Media (Aug. 22, 2023),

<https://www.404media.co/the-secret-weapon-hackers-can-use-to-dox-nearly-anyone-in-america-for-15-tlo-usinfosearch-transunion/>;

Douglas MacMillan, Data Brokers are Selling Your Secrets. How States are Trying to Stop Them, Wash. Post (Jun. 24, 2019).

<https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-your-secrets-how-states-are-trying-stop-them/>.

<sup>4</sup> Federal Trade Commission, FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent, (January 14, 2025),

<https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-takes-action-against-general-motors-sharing-drivers-precise-location-driving-behavior-data>

<sup>5</sup> Big Data, A Big Disappointment for Scoring Consumer Credit Risk, Nat'l Consumer Law Ctr. at 15-16 (Mar. 2014),

<https://www.nclc.org/images/pdf/pr-reports/report-big-data.pdf>.

<sup>6</sup> Phishing Box, Tracking Data: Identifying the Anonymized,

<https://www.phishingbox.com/news/post/tracking-data-identifying-anonymized>

<sup>7</sup> Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, (October 30, 2023),

<https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs>

<sup>8</sup> Consumer Financial Protection Bureau, Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Rule; request for public comment, (December 3, 2024),

[https://files.consumerfinance.gov/f/documents/cfpb\\_nprm-protecting-ams-from-harmful-data-broker-practices\\_2024-12.pdf](https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf)

company Allstate, secretly harvested information from drivers, including their precise geolocation data, which it used in some cases to raise consumers' premiums or deny them coverage altogether.<sup>9</sup> They also sold the driving data to several other insurance companies without consumers' knowledge or consent.

- *Enhanced risks of data breaches.* Data brokers collect trillions of data points on Americans, so they are unsurprisingly a top target for hackers and cyber criminals. Location data broker Gravy Analytics, which has claimed to “collect, process and curate” more than 17 billion signals from people’s smartphones every day,<sup>10</sup> reportedly suffered a massive data breach that may have leaked the location information of millions of individuals.<sup>11</sup> This type of information makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.<sup>12</sup>

AB 322 will address the above described issues by updating CCPA to ensure that businesses only collect and use precise geolocation information to provide the products and services requested by consumers — and will prevent businesses from selling consumers’ location information outright. For the above reasons, we are proud to cosponsor AB 322 and urge the Legislature to pass it.

Sincerely,

Matt Schwartz  
Policy Analyst  
Consumer Reports

---

<sup>9</sup> Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans’ Driving Data to Insurance Companies, (January 13, 2025), <https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf>

<sup>10</sup> Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), [https://www.ftc.gov/system/files/ftc\\_gov/pdf/2123035gravyanalyticscomplaint.pdf](https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf)

<sup>11</sup> Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), <https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/>

<sup>12</sup> Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S. Military Personnel, (November 2023), <https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf>