epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

January 28, 2026

Chair Adam Ebbin
Senate General Laws and Technology Committee
Senate Room B, General Assembly Building
201 N 9th St
Richmond, VA 23219

RE: Support for S.B. 338 (Perry)

Dear Chair Ebbin:

EPIC writes in support of S.B. 338, a bill that amends the Virginia Consumer Data Privacy Act to ban the sale of precise geolocation data. By banning the sale of precise geolocation data, S.B. 338 would **put a stop to some of the most harmful abuses of our personal data happening today**. The Maryland Online Data Privacy Act, enacted in 2024, bans the sale of sensitive data, including precise geolocation data,[1] and Oregon amended its data privacy law last year to protect its residents from the sale of precise geolocation data and minors' data.[2] Similar legislation is currently being considered in Massachusetts, Maine, Vermont, and New Hampshire.

Many apps have likely prompted you to request access to your location. Sometimes, the app has a legitimate reason to access your information, such as displaying your local weather. Sometimes, it doesn't. In either case, the app may be selling your location data to a third party.

Apps often capture your location information through third-party Software Development Kits, or "SDKs", which are pieces of code that data aggregators write and make available to app developers to easily add functionality to their apps—and to create a data pipeline back to the data aggregator. SDK developers pay app developers that use their SDKs based on their app's number of active users—the more people who use the app, the more location data the developer contributes to the aggregator's dataset, and the more valuable the dataset. A single SDK can be found in hundreds of different apps, providing the data aggregator with location data on thousands or even millions of individuals. This data could subsequently be breached, as happened with Gravy Analytics in 2025.[3]

Apps are not the only way your location data ends up on the open market. Mobile ad companies also sell location data collected through a "bidstream," which is data sent from a mobile device to an ad company and used to determine which ad to serve to the device. This means that any time you see an ad on your smartphone, there is an invisible-to-you auction for your eyeballs in which companies vie to have their ad shown to people who fit certain demographics – but this also

[1] Md. Code Ann. Com. Law § 14-4607.
[2] 2025 Or. Laws Chapt. 251.
[3] Pieter Arntz, *Massive breach at location data seller: "Millions" of users affected*, MalwareBytes Lab (Jan. 2025), https://www.malwarebytes.com/blog/news/2025/01/massive-breach-at-location-data-seller-millions-of-users-affected.

means that your personal data, including your location data, is broadcast to thousands of companies you've never heard of hundreds of times every single day.[4]

In 2025, General Motors (GM) and its subsidiary OnStar agreed not to sell drivers' location data for five years following an investigation by the Federal Trade Commission. "GM monitored and sold people's precise geolocation data and driver behavior information, sometimes as often as every three seconds," said FTC Chair Lina M. Khan.[5] The FTC's complaint alleged that GM and OnStar were selling drivers' precise geolocation to consumer reporting agencies and other third parties.

The location data market is a multi-billion-dollar industry[6] centered on collecting and selling people's everyday comings and goings, often collected from people's mobile devices and without their knowledge or explicit consent.

Much of this data is amassed by data brokers, entities that aggregate extensive dossiers on virtually every American that include thousands of data points, including extremely granular information about people's behavior, as well as their inferences about individuals based on this data.[7] 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.[8]

Because data brokers collect so many data points about each of us, sensitive location data that can reveal whether someone is seeking reproductive or gender-affirming health care, where a person attends religious services, or if a person has visited a domestic violence shelter. The FTC recently took action against the data broker Kochava for selling exactly this type of sensitive location information, noting, "Where consumers seek out health care, receive counseling, or celebrate their faith is private information that shouldn't be sold to the highest bidder."[9]

The harms of the overcollection and widespread sale of precise geolocation data have also come to the forefront recently amid reports that Immigration and Customs Enforcement (ICE) has

---

[4] *See* Irish Council for Civil Liberties, *America's Hidden Security Crisis* (Nov. 2023), https://www.iccl.ie/wp-content/uploads/2023/11/Americas-hidden-security-crisis.pdf.

[5] Press Release, Fed. Trade Comm'n, *FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent* (Jan. 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.

[6] Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, The Markup (Sept. 30, 2021), https://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data.

[7] *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 (June 24, 2019), https://www.washingtonpost.com/business/2019/06/24/data-brokers-are-getting-rich-by-selling-yoursecrets-how-states-are-trying-stop-them/.

[8] *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.

[9] Press Release, Fed. Trade Comm'n, *FTC Sues Kochava for Selling Data that Tracks People at Reproductive Health Clinics, Places of Worship, and Other Sensitive Locations* (Aug. 29, 2022), https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-sues-kochava-selling-data-tracks-people-reproductive-health-clinics-places-worship-other.

purchased software that allows the agency to track millions of Americans via their cellphones.[10] Bypassing Fourth Amendment protections, ICE has purchased access to a social media and phone surveillance product that allows the agency to monitor specific areas for mobile phones and track the movements of those devices (or their owners) over time.[11] And just this week, it was reported that ICE is exploring how it can use the "bidstream" type data broadcast in ad auctions for investigations.[12]

Nothing in this bill would prevent companies from using precise geolocation data for legitimate business purposes. It simply says they should not sell that very sensitive data for profit.

Privacy is a fundamental right, and it is time for business practices to reflect that reality. EPIC asks the Committee to support S.B. 338.

I am happy to be a resource to the Committee as it navigates this issue and can be reached at fitzgerald@epic.org.

Sincerely,

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)

[10] Joseph Cox, *ICE to Buy Tool that Tracks Locations of Hundreds of Millions of Phones Every Day* (Oct. 2025), https://www.404media.co/email/0ba0f6a2-9195-4ced-9c40-92bb72367e7a/?ref=daily-stories-newsletter.
[11] Joseph Cox, *Inside ICE's Tool to Monitor Phones in Entire Neighborhoods* (Jan. 8, 2026), https://www.404media.co/inside-ices-tool-to-monitor-phones-in-entire-neighborhoods/.
[12] Wendy Davis, *ICE Issues RFI For 'Ad Tech Compliant' Data* (Jan. 2026), https://www.mediapost.com/publications/article/412314/ice-issues-rfi-for-ad-tech-compliant-data.html.