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

March 4, 2026

Dear Governor Spanberger:

EPIC writes to urge you to sign S.B. 338, a bill that amends the Virginia Consumer Data Privacy Act to ban 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 Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization in Washington, DC, established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[1] EPIC has long advocated for enhanced protections for precise geolocation data.[2] In my testimony, I'll both outline why EPIC urges you to sign this important legislation and rebut some of the points raised in the opposition letter by the Association of National Advertisers, American Advertising Foundation, Digital Advertising Alliance, and American Association of Advertising Agencies.

A. A Ban on the Sale of Precise Geolocation Data Will Prevent Some of the Worst Data Abuses Happening Today

The location data market is a multi-billion-dollar industry focused on collecting and selling people's daily movements, often gathered from mobile devices without their knowledge. Many apps have probably asked you to grant access to your location. Sometimes, there is a valid reason, such as showing your local weather. Other times, there isn't. In either case, the app might be selling your location data to third parties.

Consumers are often unaware that their precise location data is being collected. Apps frequently gather location information through third-party Software Development Kits, or "SDKs," which are pieces of code that data aggregators create and provide to app developers to easily add functionality to their apps—and to build a data pipeline back to the data aggregator. SDK developers pay app developers who use their SDKs based on the number of active users—the more people who use the app, the more location data the developer supplies to the aggregator's dataset, increasing its value. A single SDK can be integrated into hundreds of different apps, giving the data aggregator location data on thousands or even millions of individuals. This data could later 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 decide which ad to display to the device. This means that every

[1] EPIC, *About EPIC*, https://epic.org/about/.
[2] *See* e.g. EPIC, *EPIC v. AccuWeather*, https://epic.org/documents/epic-v-accuweather/.
[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.

time you see an ad on your smartphone, there is an invisible auction for your attention where companies compete to have their ads shown to people who match certain demographics. However, this also means that your personal data, including your location, is broadcast to thousands of companies you've never heard of, hundreds of times each day.

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."[4]

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 purchased software that allows the agency to track millions of Americans via their cellphones.[5] 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.[6] It was recently reported that ICE is exploring how it can use the "bidstream" type data broadcast in ad auctions for investigations.[7]

B. The Arguments in the Advertisers' Opposition Letter Fail to Stand up to Scrutiny

The advertising lobby made three primary arguments in their opposition letter. First, they claim that Virginia's existing privacy law already safeguards location data. Second, they say that a majority of states follow Virginia's current approach. And third, they highlight some particular "unintended consequences" to the ban. These arguments do not stand up to scrutiny.

First, current Virginia law requires opt-in consent to collect or process precise geolocation data. But opt-in consent does not adequately protect Virginians. A prohibition on selling precise geolocation data allows companies to transfer this data for legitimate business purposes while eliminating data sales that serve only to increase profits rather than to benefit consumers. Under existing Virginia law, companies aren't typically required to separate their request for consent for necessary processing (e.g. data collection) from unnecessary processing (e.g. data sales), so consumers are still often presented with take-it-or-leave-it choices.

This weakness became apparent to many consumers when TikTok's transfer to a U.S. entity prompted a new pop-up notice for TikTok users in January. Upon opening the app, users were

---

[4] 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.

[5] 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.

[6] 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/.

[7] 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.

presented with a notice that TikTok was updating its Terms of Service and Privacy Policy to reflect changes including "new types of location information (including device geolocation) we may collect from you, with your permission" as well as changes to advertising practices. There was no "disagree" button—instead users had to agree or simply delete the app.[8] That's not a real choice, particularly for other apps that may be required for work, school, or other life necessities.

Second, the advertisers note that a majority of states follow Virginia's current approach in regulating precise geolocation data. But other states have already enacted or are considering similar protections. The Maryland Online Data Privacy Act, enacted in 2024, bans the sale of sensitive data, including precise geolocation data,[9] and Oregon amended its data privacy law last year to protect its residents from the sale of precise geolocation data and minors' data.[10] Similar legislation is currently being considered in Massachusetts, Maine, Vermont, and Connecticut.

Third, the advertisers claim that this law would impede the use of location data for severe weather warnings and AMBER alerts. But Wireless Emergency Alerts, as these alerts are known, are not sent using precise geolocation data, but rather to all cell phones connected to certain cell phone towers. As the Federal Emergency Management Agency describes:

> Wireless Emergency Alerts (WEAs) are short emergency messages from authorized federal, state, local, tribal and territorial public alerting authorities that can be broadcast from cell towers to any WEA-enabled mobile device in a locally targeted area. Wireless providers primarily use cell broadcast technology for WEA message delivery. […] WEAs do not track your location. They are broadcast from area cell towers to mobile phones within the defined geographic location. Every WEA-capable phone within range receives the message.[11]

So precise geolocation data is not used to send those types of alerts, and S.B. 338 would have no impact on their use.

* * *

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 urges you to sign S.B. 338 into law.

Sincerely,

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)

---

[8] Aimee Picchi, *TikTok's new privacy policy is sparking a backlash. Here's what to know,* CBS News (Jan. 28, 2026), https://www.cbsnews.com/news/tiktok-new-terms-of-service-privacy-geolocation-personal-information/.
[9] Md. Code Ann. Com. Law § 14-4607.
[10] 2025 Or. Laws Chapt. 251.
[11] Fed. Emergency Management Agency, *Wireless Emergency Alerts*, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public/wireless-emergency-alerts.