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

May 6, 2025

Senator Floyd Prozanski, Chair
Senator Kim Thatcher, Vice Chair
Oregon Senate Committee on Judiciary

Dear Chair Prozanski, Vice Chair Thatcher, and Members of the Committee:

EPIC writes in support of HB 2008. We appreciate the work of the Oregon Legislature and the working group led by the Oregon Attorney General in passing the Oregon Data Privacy Law, which built on existing laws from other states but included important consumer protections unique to Oregon – protections which other states are now emulating. The provisions in HB 2008 reflect the last few years of work on privacy legislation in other states, and passage would allow Oregon to continue in its role as a leader on data privacy.

HB 2008 would **put a stop to some of the worst data abuses happening today.** By banning the sale of precise geolocation data and data about minors, The Maryland Online Data Privacy Act, enacted last year, bans the sale of sensitive data, including precise geolocation data and data on minors (under 18 years old).[1] Oregon should follow Maryland's lead.

In my testimony I'll both rebut some of the points raised in opposition by Association of National Advertisers' and outline why Oregon should move forward on this important legislation.

A. The Arguments in the Association of National Advertisers' Opposition Testimony Fail to Stand up to Scrutiny

The Association of National Advertisers made three primary arguments in their opposition letter. First, they claim that the bill would prohibit businesses from using location data to send advertising to consumers in the right time and at the right place. Second, they claim it would impede the use of location data for emergency notices. And third, they claim that it would hinder effective fraud prevention. These arguments do not stand up to scrutiny.

First, advertisers do not need our ***precise*** geolocation data to effectively advertise to us. This bill prohibits the sale of precise geolocation data within a 1,750 ft radius. Advertisers would be free to use our course location data outside that radius to advertise to us, allowing customers to get ads for businesses, restaurants, events, and more near their location. If I have an app for my grocery store on my phone, there is no reason I can't always have access to that week's circular in the app – why do

[1] Md. Code Ann. Com. Law § 14-4607.

advertisers need to know I'm in the store before providing it to me? With no meaningful limits on the amount of data they can collect and monetize, they over collect and abuse our personal data.

Second, the advertisers claim that it would impede the use of location data for emergency notices. But Wireless Emergency Alerts, as these alerts are known, are not generally 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.[2]

So precise geolocation data is not used to send those types of alerts.

Third, they claim that it would hinder effective fraud prevention. But the Oregon Consumer Privacy Law, which HB 2008 amends, says:

> ORS 646A.570 to 646A.589 do not prohibit a controller or processor from:
>
> (e) Preventing, detecting, protecting against or responding to, and investigating, reporting or prosecuting persons responsible for, security incidents, identity theft, fraud, harassment or malicious, deceptive or illegal activity or preserving the integrity or security of systems;[3]

And nothing in the ban on sale of precise geolocation data prevents controllers from working with their processors to use this type of data to prevent fraud – they simply can't sell it.

The Association of National Advertisers' proposed amendment is not a reasonable proposal. Incentivizing data brokers and advertisers to parse through Oregonians' precise geolocation data to determine whether they've been to sensitive location such as domestic abuse shelters, rape crisis centers, protests, gay bars, and addiction treatment centers just so they can continue selling precise geolocation data is the opposite of the goal of this legislation.

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

Geolocation can be incredibly 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. Advertisers do not need to ***sell*** Oregonians'

[2] Fed. Emergency Management Agency, *Wireless Emergency Alerts*, https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system/public/wireless-emergency-alerts.
[3] ORS 646A.572(3)(e).

precise geolocation data in order to effectively advertise. This bill will provide straightforward, powerful, and critically important protections for the privacy, autonomy, and physical safety of Oregonians while still giving advertisers plenty of leeway to advertise.

Nearly every week there is a new story about how precise location data is being packaged and sold to the highest bidder. Location data can be combined with other data to reveal an individual's movements or to track them in real time, which can pose a significant threat to physical safety. Location data can also reveal sensitive information about individuals including their religious affiliation, their personal and political beliefs, their sexual orientation, their health status, or other sensitive categories. Despite common assurances from companies, precise location data is not "anonymous" and can in many cases be linked back to an individual. A top Catholic Church official was forced to resign a few years ago after a Catholic media site used cellphone data to show that the priest was a regular user of the queer dating app Grindr and visited gay bars.[4]

Many an app has likely prompted you to request access to your location. Sometimes, the app has a legitimate reason to access the information, like 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.

Apps are not the only way your location data ends up on the open market. Earlier this year, 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.

---

[4] Michelle Boorstein et al., *Top U.S. Catholic Church Official Resigns After Cellphone Data Used to Track Him on Grindr and to Gay Bars*, Wash. Post (July 21, 2021), https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/.

[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.

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 often 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 existing 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]

A few examples of location data-driven harms include:

1. ***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 data 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.[9] 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.[10]

2. ***Predatory use of consumer data.*** Data brokers sell data about people who rarely even know the companies even exist—and who have rarely ever affirmatively, expressly consented to this data 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 Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products.[11] And a recent case brought by the Texas Attorney General alleged that

---

[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] Phishing Box, *Tracking Data: Identifying the Anonymized,*
https://www.phishingbox.com/news/post/tracking-data-identifying-anonymized.

[10] Justin Sherman, *People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs*, Lawfare (Oct. 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs.

[11] Consumer Financial Protection Bureau, Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Rule Request for Public Comment (Dec. 3, 2024),

Arity, a data broker owned by the insurance company Allstate, secretly harvested information about consumers' driving behaviors (including their precise geolocation data), which it used in some cases to raise consumers' premiums or deny them coverage altogether.[12] They also sold the driving data to several other insurance companies without consumers' knowledge or consent.

3. ***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,[13] reportedly suffered a massive data breach that may have leaked the location data of millions of individuals.[14] This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.[15]

4. ***Exposure of sensitive location data.*** 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."[16] The FTC complaint aims to stop the data broker from selling sensitive location data and require it to delete the existing location data it has collected.[17]

---

https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf.

[12] Press Release, Office of the Texas Att'y Gen., *Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Dri-ving Data to Insurance Companies*, (Jan. 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf.

[13] Press Release, Fed. Trade Comm'n, *FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites* (Dec. 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf.

[14] Joseph Cox, *Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data*, 404Media (Jan. 7, 2025), https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/.

[15] Justin Sherman et al., *Data Brokers and the Sale of Data on U.S.Military Personnel*, Duke Sanford School of Public Policy (Nov. 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.

[16] 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.

[17] *Id.*

C. Entities Should Not Be Selling Minors' Data

From a very young age, minors participate in a wide range of activities online. These online activities can have many benefits—allowing kids to learn about an endless array of topics, participate in school during a pandemic, connect with loved ones around the world, play games, and explore their developing identities. They should be free to participate in these activities without worrying about their data being sold on the open market.

Last year, the College Board reached a settlement with the NY Attorney General and NY State Education Commissioner for collecting students' personal information when they were taking the PSAT, SAT, and AP exams in school and then selling that data to colleges, scholarship programs, and other customers who used it to solicit students to participate in their programs.[18] This was in violation of New York State student privacy laws, which require consent before such transfers. The investigation found that in 2019 alone, the College Board had improperly sold the personal information of more than 237,000 New York students.

Consent alone won't fix this problem. Parents and teens cannot be expected to read every lengthy privacy policy they are faced with in order to prevent their data from being sold. And even if they did read those policies, they are left with a take-it-or-leave it "choice." A teen would have to "choose" between taking the SAT and preventing their personal data from being sold. That is not a real choice.

Maryland banned the sale of personal data on consumers that the controller knew or should have known was a minor under 18 years of age in the Maryland Online Data Privacy Act, enacted last year. Banning the sale of minors data is a common sense amendment to the ODPA.

* * *

Privacy is a fundamental right, and it is time for business practices to reflect that reality. The Oregon State Legislature has an opportunity to continue to be a leader on data privacy. EPIC asks the Committee to support HB 2008.

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

Sincerely,

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)

[18] Press Release, N.Y. Att'y Gen. Letitia James, *Attorney General James and NYSED Commissioner Rosa Secure $750,000 from College Board for Violating Students' Privacy* (Feb. 13, 2024), https://ag.ny.gov/press-release/2024/attorney-general-james-and-nysed-commissioner-rosa-secure-750000-college-board.