March 20, 2025

Representative Nathan Sosa, Chair
Representative Farrah Chaichi, Vice Chair
Representative Virgle Osborne, Vice Chair
Oregon House Committee on Commerce and Consumer Protection

Dear Chair Sosa, Vice Chair Chaichi, Vice Chair Osborne, and Members of the Committee:

EPIC and Consumer Reports write in support of HB 3899, An act relating to requirements that apply to persons that process consumer personal data, with the forthcoming dash-1 amendment. 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 3899 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.

The key provisions of HB 3899 include:

- **Prohibiting some of the worst data abuses happening today.** By banning the sale of precise geolocation data and data about minors, HB 3899 (dash-1 amendment) would put a stop to some of the most harmful abuses of our personal data happening today. 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.

- **Strong Data minimization:** HB 3899 (dash-1 amendment) establishes meaningful limits on the unfettered processing of personal data by setting a baseline requirement that entities only collect, use, and transfer data that is reasonably necessary and proportionate to provide or maintain a product or service requested by the individual. The Maryland Online Data Privacy Act, enacted last year, includes similar data minimization rules,[2] as does legislation filed this session by the original sponsor of the Connecticut Data Privacy Act to update that law.[3]

[1] Md. Code Ann. Com. Law § 14-4607.
[2] *Id.*
[3] S.B. 1356, 2025 Gen. Assemb., Reg. Sess. (Conn. 2025).

- **Strong protections for sensitive data:** HB 3899 (dash-1 amendment) sets heightened protections for sensitive data (i.e., biometrics, location, health data) such that its collection and use must be strictly necessary for the product or service the consumer is asking for. This provision was also included in the recently enacted Maryland Online Data Privacy Act.[4]

In our testimony we will discuss the importance of a ban on the sale of precise geolocation data and data about minors, as well as the current weakness of "data minimization" rules in current state privacy laws and how HB 3899 (dash-1 amendment) adds necessary consumer protections to limit data collection and abuse.

A. 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' ***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.[5]

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.

[4] Md. Code Ann. Com. Law § 14-4607.
[5] 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/.

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.[6] 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[7] 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.[8] 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.[9]

---

[6] 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.

[7] 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.

[8] *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/.

[9] *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.

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.[10] 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.[11]

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.[12] And a recent case brought by the Texas Attorney General alleged that 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.[13] 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

---

[10] Phishing Box, *Tracking Data: Identifying the Anonymized,* https://www.phishingbox.com/news/post/tracking-data-identifying-anonymized.
[11] 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.
[12] Consumer Financial Protection Bureau, Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Rule Request for Public Comment (Dec. 3, 2024), https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf.
[13] 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' Driving Data to Insurance Companies*, (Jan. 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf [hereinafter "Texas Allstate action"].

curate" more than 17 billion signals from people's smartphones every day,[14] reportedly suffered a massive data breach that may have leaked the location data of millions of individuals.[15] This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.[16]

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."[17] 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.[18]

B. 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.[19] This was in violation of New York State student privacy laws, which

---

[14] 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.
[15] 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/.
[16] 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.
[17] 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.
[18] *Id.*
[19] 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),

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.

C. Current State Privacy Laws Don't Do Enough To Limit Data Collection and Abuse

Companies should not have a limitless ability to decide how much personal data to collect. Unfortunately, this is what all state laws — other than California's and Maryland's — allow. Most existing state privacy laws, including Oregon's, only limit collection to what is adequate, relevant and reasonably necessary to "serve the purposes the controller specified [in its privacy notice]," meaning businesses can collect data for whatever purposes they want, as long as they state that purpose in their privacy policies.[20]

This reinforces the failed status quo of "notice and choice" — businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them. The focus on notice has led to longer and more complicated privacy policies that users do not read and could not change even if they did. Technology's prevalence in our work, social, and family lives leaves us with no "choice" but to accept. And online tracking is too complex and opaque for the vast majority of internet users to understand or control.

Advertisers and data brokers track our every move online, and our data is used against us in ways that harm our wallets, opportunities, and rights. **At a time when policymakers are concerned about cost-of-living issues for their constituents, the impact of mass data collection and abuse on those costs cannot be ignored.** A few examples of these harms include:

1. **Increased insurance premiums.** Earlier this year, Texas Attorney General Ken Paxton sued insurance giant Allstate and its subsidiary Arity for unlawfully collecting, using, and selling data about the location and movement of Texans' cell phones

https://ag.ny.gov/press-release/2024/attorney-general-james-and-nysed-commissioner-rosa-secure-750000-college-board.

[20] *See id.*

through secretly embedded software in mobile apps, such as Life360 and GasBuddy. Paxton alleged that Allstate and other insurers then used the covertly obtained data to justify raising Texans' insurance rates.[21]

2. **Increased pricing on consumer goods**. Last month, the Federal Trade Commission released initial findings from a study on surveillance pricing, a practice that uses data about consumers' characteristics and behavior to alter prices. "Initial staff findings show that retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage," said then-FTC Chair Lina M. Khan.[22]

   Grocery stores are adopting "Electronic Shelving Labels" to allow them to use "dynamic" pricing "in which the price of basic household goods could surge based on the time of day, the weather, or other transitory events."[23]

3. **Targeted advertisements can be predatory and harmful.** Targeted ads can be predatory and harmful, using people's online behavioral data to reach vulnerable consumers who meet specific parameters. People searching terms like "need money help" on Google have been served ads for predatory loans with staggering interest rates of over 1,700%.[24] An online casino targeted ads to problem gamblers, offering them free spins on its site.[25] A precious metals scheme used Facebook users' ages and political affiliations to target ads to get users to spend their retirement savings on grossly overpriced gold and silver coins.[26]

Small businesses are harmed by these systems as well. For years, they've been told that success hinges on pouring money into online behavioral advertising, controlled by a handful of tech giants. They enter bidding wars against corporate behemoths. This isn't a

---

[21] Texas Allstate Action, *supra* note 13.
[22] Press Release, Fed. Trade Comm'n, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (Jan. 17, 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.
[23] Letter from Sen. Elizabeth Warren to Rodney McMullen, CEO and Chairman, The Kroger Co. (Aug. 25, 2024), https://www.warren.senate.gov/imo/media/doc/warren_casey_letter_to_kroger_re_electronic_shelving_and_price_gouging.pdf.
[24] Shanti Das, *Google Profiting from 'Predatory' Loan Adverts Promising Instant Cash*, The Guardian (Mar. 13, 2022), https://www.theguardian.com/technology/2022/mar/13/google-profiting-from-predatory-loan-adverts-promising-instant-cash.
[25] Rob Davies, *Online Casino Advert Banned for Targeting Problem Gamblers*, The Guardian (Oct. 9, 2019), https://www.theguardian.com/society/2019/oct/09/casumo-ad-banned-for-targeting-people-trying-to-stop-gambling.
[26] Jeremy B. Merrill, *How Facebook Fueled a Precious-Metal Scheme Targeting Older Conservatives,* Quartz (Nov. 19, 2019), https://www.yahoo.com/video/facebook-fueled-precious-metal-scheme-110044886.html.

level playing field. It's a digital black hole—swallowing resources and crushing entrepreneurial spirit, all to facilitate targeted advertising that is of dubious efficacy.

4. Data Minimization: The Key to a Strong Privacy Law

HB 3899 (dash-1 amendment) relies on a concept that has long been a pillar of privacy protection: data minimization.

When consumers interact with a business online, they reasonably expect that their data will be collected and used for the limited purpose and duration necessary to provide the goods or services that they requested. For example, a consumer using a map application to obtain directions would not reasonably expect that their precise location data would be disclosed to third parties and combined with other data to profile them. And indeed, providing this service does not require selling, sharing, processing, or storing consumer data for unrelated secondary purposes. Yet these business practices are widespread. Nearly every online interaction can be tracked and cataloged to build and enhance detailed profiles and retarget consumers. Even offline, credit card purchases, physical movements, and "smart" devices in homes create countless data points that are logged and tracked without consumer awareness or control.

HB 3899 (dash-1 amendment) sets a baseline requirement that entities only collect, use, and transfer data that is "*reasonably necessary and proportionate*" to provide or maintain a product or service requested by the consumer. **This standard better aligns business practices with what consumers expect.**

Data minimization is essential for both consumers and businesses. Data minimization principles provide much-needed standards for data security, access, and accountability, assign responsibilities with respect to user data, and restrict data collection and use. Indeed, a data minimization rule can provide clear guidance to businesses when designing and implementing systems for data collection, storage, use, and transfer. Data security will be improved because personal data that is not collected in the first place cannot be at risk of a data breach.

The Maryland Online Data Privacy Act, which was enacted last year, and the California Consumer Privacy Act also include provisions requiring a form of data minimization. The key with a data minimization provision is to ensure it is tied to the specific product or service requested by the individual, not simply to whatever purpose the collecting entity decides it wants to collect data for and discloses in its privacy policy.

Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data.

* * *

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 3899 with the forthcoming dash-1 amendment.

We are happy to be a resource to the Committee as it navigates this complex topic and can be reached at fitzgerald@epic.org and matt.schwartz@consumer.org.

Sincerely,

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)

Matt Schwartz
Policy Analyst
Consumer Reports