February 12, 2025

Chair Cliff Hayes
Vice Chair Irene Shin
Committee on Communications, Technology and Innovation
Virginia House of Delegates
General Assembly Building
201 North 9th Street
Richmond, Virginia 23219

Re: S.B. 1023 (Perry) – *SUPPORT*

Dear Chair Hayes and Vice Chair Shin,

The undersigned organizations write in strong support of S.B. 1023, legislation that would ban the sale of consumers' precise geolocation information. 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*** Virginians' ***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 Virginians while still giving advertisers plenty of leeway to advertise.

The location data market is a multi-billion-dollar industry[1] 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 data. Researchers have shown that 95 percent of individuals can be uniquely identified

[1] 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

from just four spatio-temporal points; most companies that collect this information have orders of magnitude more data than that.[2] This activity poses a host of significant risks to Virginia residents.

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.[3] Some companies collect and share consumers' location data as often as every three seconds.[4] 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.[5]

A few examples of location data 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 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.[6] 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.[7]

- *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

---

[2] 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

[3] 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-yoursecrets-how-states-are-trying-stop-them/.

[4] 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

[5] 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.

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

[7] 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

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.[8] 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.[9] 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,[10] reportedly suffered a massive data breach that may have leaked the location data of millions of individuals.[11] This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.[12]

Unsurprisingly, the advertising industry that profits off this predatory use of consumer data strongly opposes threats to their ill-gotten gains. We offer some additional context on some of their key arguments here:

- *"SB 1023's proposed ban would ignore existing VCDPA protections, diverge from the approach to precise geolocation data used across all other effective state privacy laws, and stop Virginia consumers from receiving desired location-based services."*[13]

---

[8] 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

[9] 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

[10] 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

[11] 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/

[12] 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

[13] Letter from Association of National Advertisers, Interactive Advertising Bureau, Digital Advertising Alliance, American Association of Advertising Agencies, American Advertising Federation, and Digital Advertising Alliance on S.B. 1023, (February 3, 2025)

The bill simply raises the standard in VCDPA from an opt-in framework to an outright ban on sale of location, matching the standard in the recently passed Maryland Online Data Privacy Act of 2024, which bans the sale of *all* sensitive data (a fact that the letter from advertisers glosses over by saying that this rule diverges from all other "effective" state privacy laws – Maryland's law goes into effect this year).[14] Similar bans are currently being considered in the Massachusetts[15] and Washington[16] legislatures.

Opt-in frameworks, like the one currently in VCDPA, are not robust enough to prevent businesses from selling location data behind consumers' backs. While businesses must obtain opt-in consent to *process* location data under VCDPA, they are arguably not required to obtain separate consent for functionally necessary data collection (e.g. a weather app collecting location to provide an accurate forecast) versus unnecessary secondary sharing (e.g. a weather app selling location to data brokers). As such, under the current standard it isn't always clear to consumers what they are consenting to and they may in fact be *required* to consent to sales of their data simply to receive the service. Businesses have repeatedly leveraged this fact to their advantage.[17]

A ban on sale of precise geolocation data would also not stop consumers from receiving desired location-based services, such as ads for local businesses or coupons. Under this bill, businesses are still free to *collect* consumers' location data, with clear, affirmative consent, to advertise to them — they just can't *sell* that data to other businesses. Furthermore, businesses that wish to buy or sell consumers' location information for advertising purposes can ultimately still do so, albeit in a more privacy-protecting way. Precise geolocation is defined in VCDPA as information that directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet — close enough to identify someone's home address. Instead, businesses could still leverage data at the town, city, or zipcode level. Advertisers could still advertise based on a consumer's general location, such as "Richmond area," but they do not need the consumer's ***precise*** geolocation to do that.

- *"SB 1023 ignores the very valuable role that geolocation data plays in anti-fraud and law enforcement functions."*[18]

---

[14] Maryland Online Consumer Data Privacy Act, Section 14-4607(A)(2), https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/sb0541?ys=2024RS
[15] H.D. 2965/S.D. 501, The Location Shield Act, https://malegislature.gov/Bills/194/HD2965; H.D. 2135, Consumer Data Privacy Act, thttps://malegislature.gov/Bills/194/HD2135; H.D. 2110/S.D. 267, Massachusetts Data Privacy Act, https://malegislature.gov/Bills/194/HD2110
[16] H.B. 1671, the People's Privacy Act, https://app.leg.wa.gov/BillSummary/?BillNumber=1671&Year=2025&Initiative=false
[17] Oates et al., Consumer Reports, Companies Continue to Share Health Data Despite New Privacy Laws, (January 16, 2024), https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf
[18] Letter from Chamber of Progress on S.B. 1023, (January 31, 2025)

Nothing in this bill prevents anti-fraud or law enforcement functions. VCDPA already includes a number of exemptions for anti-fraud and law enforcement, including that "nothing in this chapter shall be construed to restrict a controller's or processor's ability to… [p]revent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity."[19] And once again, this bill is about the commercial sale of location data, not the collection of it. Anti-fraud entities and law enforcement that have lawfully collected precise geolocation data would still be able to leverage it for their own purposes.

- *"SB 1023 will burden low-income consumers. Monetizing user data is critical to the advertising-supported ecosystem that makes many apps free to users."*[20]

  Free iPhone apps that secretly sell consumers' location data is not a serious cost-of-living issue and, as demonstrated above, the *actual* costs to consumers of the unfettered sale of their location data are severe. Some types of data are simply too sensitive to allow commercial entities to buy and sell. Granular data about our everyday comings and goings — which reveals the location of our homes, friends' homes, places of worship, political causes we support, medical services we seek out, and more — should not be for sale on the open market.

For the above reasons, we are proud to support S.B. 1023 and urge the Legislature to pass it.

Sincerely,
Matt Schwartz
Policy Analyst
Consumer Reports

Ben Winters
Director of AI and Privacy
Consumer Federation of America (CFA)

Caitriona Fitzgerald
Deputy Director
Electronic Privacy Information Center (EPIC)

Katharina Kopp
Deputy Director
Center for Digital Democracy

Ruth Susswein
Director of Consumer Protection
Consumer Action

---

[19] VCDPA, Section 59.1-582 (A)(7), https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/
[20] Letter from Chamber of Progress on S.B. 1023, (January 31, 2025)

Eric Null
Co-Director, Privacy & Data Project
Center for Democracy and Technology

Emory Roane
Associate Director of Policy
Privacy Rights Clearinghouse

Hayley Tsukayama
Associate Director of Legislative Activism
Electronic Frontier Foundation

Ellen Hengesbach
Associate, Don’t Sell My Data Campaign
Public Interest Research Group (PIRG)

Eden Iscil
Senior Public Policy Manager
National Consumers League

Alex Marthews
National Chair
Restore the Fourth