WRITTEN TESTIMONY IN SUPPORT OF HB 1220
Business Regulation – Data Broker Registry
House Economic Matters Committee
March 3, 2026 – 1:00 PM
Position: FAVORABLE

Chair Wilson and members of the Committee, thank you for the opportunity to submit testimony in support of HB 1220. My name is Emory Roane and I am the Associate Director at Privacy Rights Clearinghouse (PRC), a nonprofit consumer privacy advocacy and education organization based in San Diego, California. PRC has advocated for consumer privacy rights since 1992. We were co-sponsors of California's Delete Act, we maintain one of the nation's most comprehensive database sof publicly reported data breach, and for several years we've been conducting original research into data broker registration and compliance across every state that has enacted a data broker registry law.

Data brokers are the central infrastructure of the modern privacy crisis.

Data brokers are the invisible infrastructure around which nearly every major privacy concern of the past decade revolves. These are companies most people have never heard of that collect, aggregate, buy, and sell detailed personal information about hundreds of millions of Americans. The harms enabled by this industry are not theoretical and span targeted advertising that manipulates consumer behavior,[1] identity theft and fraud, stalking and harassment,[2] civil liberties abuses, and end-runs around the Fourth Amendment by law enforcement agencies that purchase personal data rather than obtain warrants.[3] Data brokers have national security implications: in recent years, researchers and journalists have demonstrated how easily foreign adversaries can purchase sensitive location data and personal dossiers on military personnel, government employees, judges and ordinary Americans.[4]

Data brokers also undermine democratic governance. They sell voter data enriched with behavioral profiles, enable micro-targeted political messaging at a scale that distorts public discourse, and create information asymmetries between institutions and the individuals those institutions are supposed to serve.[5] If there's one thing I want to underscore in this testiomny,

---

[1] Fed. Trade Comm'n, Press Release, FTC Takes Action Against Mobilewalla for Collecting and Selling Sensitive Location Data (Dec. 3, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-mobilewalla-collecting-selling-sensitive-location-data.
[2] Consumer Fin. Prot. Bureau, Press Release, CFPB Proposes Rule to Stop Data Brokers from Selling Sensitive Personal Data to Scammers, Stalkers, and Spies (Dec. 3, 2024), https://www.consumerfinance.gov/about-us/newsroom/cfpb-proposes-rule-to-stop-data-brokers-from-selling-sensitive-personal-data-to-scammers-stalkers-and-spies/.
[3] Am. Civ. Liberties Union, DHS is Circumventing the Constitution by Buying Data It Would Normally Need a Warrant to Access (Jan. 15, 2026), https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access.
[4] Justin Sherman et al., Data Brokers and the Sale of Data on U.S. Military Personnel: Risks to Privacy, Safety, and National Security, Duke Univ. Sanford Sch. of Pub. Pol'y (Nov. 2023), https://techpolicy.sanford.duke.edu/data-brokers-and-the-sale-of-data-on-us-military-personnel/.
[5] Elec. Frontier Found., How Political Campaigns Use Your Data to Target You (Apr. 2024), https://www.eff.org/deeplinks/2024/04/how-political-campaigns-use-your-data-target-you.

it's that this is not a partisan concern. When Americans learn what data brokers do and how much of their personal information is being bought and sold without their knowledge, the response is overwhelmingly bipartisan: people want a way to get their information out of these systems.

Unfortunately, existing consumer privacy frameworks are inadequate to address data brokers.

Consumer privacy laws, including the excellent Maryland Online Data Privacy Act, give individuals the right to request deletion of their data or opt out of the sale or sharing of their information, but these rights assume consumers know which businesses hold their data. That assumption fundamentally breaks down with data brokers. The defining feature of data brokers is that they operate almost entirely outside the awareness of the individuals whose data they collect and sell. A consumer cannot ask a company to delete their data if they do not know that company exists.

Even for consumers who learn about specific data brokers, the individual opt-out model is functionally impossible at scale. There are at least 750 known data broker groups operating in the United States, according to our research, and there are almost certainly many more that have not been identified. Requesting deletion from each of these companies individually, one at a time, is a burden no reasonable person can be expected to bear. And even when a consumer does successfully request deletion, data brokers oftenimmediately re-acquire the same information from other brokers, rendering the original deletion request effectively meaningless.

This dysfunction has spawned an entire pay-for-privacy industry. Companies, some of them even data brokers themselves,now offer subscription services to chase down data brokers on consumers' behalf, acting as authorized agents to submit deletion requests individually. But these services are costly, often incomplete, and frequently lack the mechanisms to verify that brokers have actually complied with deletion requests. Privacy should not be a luxury product available only to those who can afford to pay a monthly fee for it.

Registration is a necessary first step.

HB 1220 takes a straightforward and important step: it requires data brokers operating in Maryland to register with the Comptroller, identify themselves, and make that information publicly available. This is a basic transparency measure, and it is a prerequisite for everything else. How can Marylanders be expected to exercise their privacy rights if they do not even know these businesses exist? Right now, they do not.

This model works. California, Vermont, Texas, and Oregon have all enacted data broker registration requirements. In June 2025, PRC and the Electronic Frontier Foundation published original research analyzing all four state registries, compiling a unified database of over 750 unique registered data brokers operatingin the country. That research found significant compliance gaps, withEach state registry contained hundreds of brokers that appeared to be ignoring their registration obligations in other states. These findings demonstrate both that registration laws are generating valuable new information about this opaque industry and that

more states need to enact these laws to build the enforcement infrastructure necessary to bring data brokers into compliance.

Granular reporting requirements would strengthen the bill

HB 1220 already takes important steps in this direction by requiring data brokers to disclose whether they collect precise geolocation or consumer health data. We encourage the Committee to consider building on this foundation by expanding the disclosure requirements to cover additional types of sensitive personal information and who brokers sell it to.

California's recent amendments under SB 361 offer a model, requiring brokers to disclose whether they collect data types including biometrics, citizenship and immigration status, sexual orientation, and mobile advertising identifiers, and whether they have sold data to foreign adversaries, law enforcement, or AI developers. Texas similarly requires brokers to describe the categories of data they process, and both Texas and Vermont require additional disclosures when brokers possess children's data. Where states have required this kind of reporting, the resulting data has proven invaluable for understanding what these notoriously opaque businesses are actually doing.

For example, when PRC and the Electronic Frontier Foundation analyzed registration disclosures across state registries last year, we were able to identify 78 data brokers nationwide that reported selling the personal information of children. Twenty-five of those brokers were not registered in California despite appearing to meet the registration requirements there.[6] That kind of finding is only possible when registration forms require brokers to disclose what types of data they collect and from whom. Without granular reporting, a registry tells you that a data broker exists but not whether it is selling your kids' location data, your health conditions, or your biometric information to foreign governments or AI companies.

We urge Maryland to adopt similar granular reporting requirements as part of this registry.

We urge a favorable report, and encourage the Committee to consider strengthening the bill

PRC strongly supports the passage of HB 1220. Registration is an essential foundation. We also respectfully encourage the Committee to consider, whether through amendment to this bill or through subsequent legislation, two additions: first, expanded disclosure requirements so that Maryland's registry provides meaningful transparency into what data brokers are collecting and who they are selling it to; and second, data broker deletion requirements modeled on California's Delete Act, which would give Marylanders a practical mechanism to actually remove their information from these systems. Registration tells Marylanders who has their data. Granular reporting tells them what those companies are doing with it. And deletion gives them the ability to do something about it.

[6] Privacy Rights Clearinghouse & Elec. Frontier Found., Why Are Hundreds of Data Brokers Not Registering with States? (June 2025), https://privacyrights.org/resources-tools/reports/why-are-hundreds-data-brokers-not-registering-states.

Data brokers have operated in the shadows for too long, profiting from the personal information of millions of Marylanders who have no idea these companies exist. HB 1220 brings them into the light. We urge a favorable report.

Respectfully submitted,

Emory Roane
Associate Director of Policy
Privacy Rights Clearinghouse
3245 University Ave. #1101
San Diego, CA 92104
emory@privacyrights.org
619-610-9017