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

February 27, 2026

Maryland General Assembly
House Economic Matters Committee
House Office Building
6 Bladen Street
Annapolis, MD 21401

Dear Chair Valderrama and Members of the Committee:

EPIC writes in support of H.B. 1220, the Data Broker Registry. The data broker industry builds profiles on millions of Americans at great cost to our privacy, civil rights, national security, and democracy.[1] States should do all they can to make data brokering as limited as possible, and Maryland made great strides toward that with the passage of the Maryland Online Data Privacy Act in 2024, which banned the sale of sensitive data and limited the amount of data companies can collect about us. On top of those limitations, a data broker registry is an important transparency measure to allow enforcers and individuals insight into who data brokers are and what types of data they collect and sell. Together, these protections are critical to curtail data brokers' harmful practices as the state considers tying data brokers' income to critical government services.

The Electronic Privacy Information Center (EPIC) is an independent nonprofit research organization in Washington, D.C., established in 1994 to protect privacy, freedom of expression, and democratic values in the information age.[2] EPIC has a long history of advocating for safeguards and rules to limit the harms caused by data brokers.[3]

---

[1] *See e.g.* Dell Cameron, Dhruv Mehrotra, *Google Ad-Tech Users Can Target National Security 'Decision Makers' and People With Chronic Diseases*, WIRED (Feb. 20, 2025), https://www.wired.com/story/google-dv360-banned-audience-segments-national-security/; Justin Sherman et al., *Data Brokers and the Sale of Data on U.S. Military Personnel,* (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.

[2] EPIC, *About EPIC*, https://epic.org/about/.

[3] EPIC, *FCRA Rulemaking: A Path to Reining in Data Brokers* (2024), https://epic.org/documents/fcra-rulemaking-a-path-to-reining-in-data-brokers/; EPIC Comments to DOJ Regarding ANPRM on Access to Americans' Bulk Sensitive Personal Data and Government Related Data by Countries of Concern (Apr. 19, 2024), https://epic.org/documents/epic-comments-to-doj-regarding-anprm-on-access-to-americans-bulk-sensitive-personal-data-and-government-related-data-by-countries-of-concern/; EPIC, *Data Broker Threats: National Security* (2024), https://epic.org/wp-content/uploads/2024/05/Data-Broker-One-Pager-National-Security-2.pdf; EPIC, *CFPB Fair Credit Reporting Act Rulemaking* (2024), https://epic.org/cfpb-fair-credit-reporting-act-rulemaking.

A. Data Brokers Collect Massive Amounts of Personal Data Behind the Scenes

Data brokers pose a threat to us all through the vast range, depth, and scale of the personal datasets and products they market. Thousands of data brokers in the United States buy, aggregate, disclose, and sell billions of data elements on Americans with virtually no oversight. As the data broker industry proliferates, companies have enormous financial incentives to collect consumers' personal data, while data brokers have little financial incentive to protect consumer data. For these companies, consumers are the product, not the customer. Companies also maintain inaccurate information about consumers, resulting in wrongful denials of credit, housing, and jobs.

Data brokers collect and aggregate many types of personal information: names, addresses, telephone numbers, e-mail addresses, gender, age, marital status, children, education, profession, income, political preferences, religion, sexual orientation, race, ethnicity, cars and real estate owned, and much more. Data brokers also collect information about the sites we visit online, the advertisements we click on, our purchases, where we shop, and how we pay for our purchases. Data brokers also compile and sell sensitive information, including health information, biometric and genetic information, and immigration or citizenship status.

And thanks to the proliferation of smartphones and wearables, data brokers collect and sell real-time location data, including data that reveals visits to churches, mosques, and synagogues; medical facilities; protests and political events; substance abuse disorder and addiction recovery centers; domestic violence shelters; children's schools; and even military bases. The sale of this kind of location data enables serious physical harms, including stalking, domestic and intimate partner violence, threats to public officials, and even murder.

In today's political moment, there are also many clear—and horrific—examples of information collected by data brokers being used to discriminate against immigrants. Federal officials are relying on the vast troves of information—especially location data—compiled by data brokers to cause harm.[4] Agencies like ICE and CBP purchase extensive personal data on immigrant communities from brokers for use in enforcement campaigns.[5] Last month, ICE issued an official request for information on how "Big Data" providers "can directly support investigations activities."[6]

Despite how much data brokers know about each one of us, without a transparency measure like a data broker registry, we know almost nothing about them. Most Marylanders would not be able to name a single data broker.

---

[4] EPIC, *How Data Brokers Harm Immigrants* (2024), https://epic.org/wp-content/uploads/2024/10/12.4-Data-Broker-Harms-to-Immigrants-One-Pager.pdf.
[5] *Id.*
[6] U.S. General Services Administration, *Request for Information on Big Data & Ad Tech*, https://sam.gov/workspace/contract/opp/411452e8b3614944b9c50cc3aa24fb42/view.

Some states have started taking steps to regulate the data broker industry. California, Vermont, Texas, and Oregon have all passed laws establishing data broker registries, similar to what H.B. 1220 would do in Maryland. EPIC would urge the Committee to pass this bill and put Maryland on the path toward protecting its residents against the harmful practices of data brokers.

B. Marylanders Should Be Able to Tell Data Brokers to Delete Their Data

Marylanders should have the right to tell data brokers to delete their personal data. The Committee should consider amending this bill to give residents a deletion right and to make it as straightforward as possible for people to access this right. While the Maryland Online Data Privacy Act allows Marylanders to request that companies delete their personal data, the data broker industry operates behind the scenes, largely hidden from the view of everyday people. Marylanders cannot exercise their right to ask companies to delete their data if they don't know those companies exist. To this end, the Committee should consider amending the bill to give Marylanders the ability to use a centralized deletion mechanism to express their preference to data brokers that they want their data deleted.

California passed a similar law, the DELETE Act, in 2023.[7] Delete Act provisions would make it simple for Marylanders who do not want their information collected, sold, or retained by data brokers to express this preference. It would require the state to create a website providing access to a universal deletion mechanism that allows consumers, via single request, to delete their personal information from every data broker that has collected it. Fortunately, CalPrivacy has recently developed such a system, the Delete Request and Opt-out Platform (DROP), to implement California's Delete Act.[8] California's DROP implementation has been wildly successful since it launched on January 1 of this year—215,000 Californians signed up for the deletion platform in its first month of operation.[9] Importantly, the agency has indicated that it will make the system available to other interested states, cutting down on Maryland's implementation costs considerably.

We would be happy to work with the Committee to suggest language to give Marylanders' the right to express their preferences to data brokers.

* * *

EPIC encourages the Committee to support this bill because it is a critical first step toward reducing data brokers' harmful practices and giving Marylanders more control of their personal data.

---

[7] Thomas Germain, *California's New Delete Act Is One of the World's Most Powerful Privacy Laws*, Gizmodo (Oct. 11, 2023), https://gizmodo.com/governor-newsom-signs-delete-act-into-law-1850918011.
[8] California, *Delete Request and Opt-out Platform (DROP),* https://privacy.ca.gov/drop/.
[9] Jedidiah Bracy, Intn'l Ass'n of Privacy Professionals, *California Privacy Enforcement in 2026: A Discussion with CalPrivacy's Tom Kemp* (Feb. 6, 2026), https://iapp.org/news/a/california-privacy-enforcement-in-2026-a-discussion-with-calprivacy-s-tom-kemp.

The addition of DELETE Act provisions would build on the protections in the Maryland Online Data Privacy Act and this bill to further protect Marylanders from the harms of data brokers.

Thank you for the opportunity to speak today. EPIC is happy to be a resource to the Committee on these issues.

Sincerely,

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Deputy Director

/s/ *John Davisson*
John Davisson
EPIC Deputy Director

/s/ *Kara Williams*
Kara Williams
EPIC Counsel