

February 21, 2025

The Honorable C.T. Wilson
House Economic Matters Committee
Room 231
House Office Building
Annapolis, MD 21401

Dear Chair Wilson and Members of the Committee:

EPIC writes in support of HB 1089, the Building Information Guardrails Data Act of 2025. 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 be doing all they can to make data brokering as limited as possible, and Maryland made great strides towards that with the passage of the Maryland Online Data Privacy Act last year, which banned the sale of sensitive data and limited the amount of data companies can collect about us. To further protect consumers from the harms of data brokers, the Committee should consider amending HB 1089 to give Marylanders the ability to use a centralized deletion mechanism to express their preference to data brokers that they want their data deleted. Together, these protections are critical to cut down on 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, DC, 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, 20224), <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>.

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 information about consumers that is often inaccurate, wrongfully denying them credit, housing, or even a job.

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, and cars and real estate owned. Data brokers also collect information on an individual's purchases, where they shop, and how they pay for their purchases. In addition, data brokers collect health information, the sites we visit online, and the advertisements we click on. 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; substance abuse disorder and addiction recovery centers; domestic violence shelters; children's schools; and even military bases. The sale of whereabouts and location data enables stalking, gendered violence, and threats to public officials, too.

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

To further protect consumers from the harms of data brokers, 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 2023.⁴ 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. The California Privacy Protection Agency is currently developing the system to implement California's DELETE Act and has indicated that it will make the system available to other states who are interested, 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.

B. Data Broker Registry Currently Lacks Enforcement Mechanism

EPIC would also suggest that the Committee amend the bill to ensure the data broker registry is complied with. Currently, HB 1089 contains no penalty for data brokers who fail to register. States

⁴ 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>.

who have previously passed data broker registries have a chronic problem with under-registration.⁵ Just this week, the California Privacy Protection agency brought an enforcement action against National Public Data, a Florida-based data broker, for failing to register and pay an annual fee as required by California law.⁶ Last year, National Public Data was breached, exposing the personal data of 2.9 billion people, including Social Security Numbers.⁷ Most of that breached information has been published for free online.

Maryland will have a difficult time determining data brokers who are required to file a data broker gross income tax return if they do not register in the first place. The Committee should amend HB 1089 to include penalties for failure to register, as other states have done.

* * *

EPIC encourages the Committee to ensure that Maryland is doing all it can to cut down on data brokers' harmful practices before it taxes data brokers' income to fund critical government services. The addition of DELETE Act provisions and penalties for non-registration will build on the protections in the Maryland Online Data Privacy Act to 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

⁵ Suzanne Smalley, *Delete-your-data laws have a perennial problem: Data brokers who fail to register*, The Record (Oct. 17, 2023), <https://therecord.media/state-data-broker-registries-california-vermont>.

⁶ Press Release, Cal. Priv. Protection Agency, *CPPA Brings Enforcement Action Against Florida Data Broker* (Feb. 20, 2025), <https://cppa.ca.gov/announcements/2025/20250220.html>.

⁷ Jon Healey, *Hackers may have stolen the Social Security numbers of every American. Here's how to protect yourself*, L.A. Times (Aug. 13, 2024), <https://www.latimes.com/business/story/2024-08-13/hacker-claims-theft-of-every-american-social-security-number>.