



HB711 Data Privacy-Consumer Data, Public Records, and Message Switching System (Data Privacy Act)

Position: Favorable

February 24, 2026

The Maryland Alliance for Racial Equity in Education (MAREE), a coalition of education advocacy, civil rights, and community-based organizations committed to eliminating racial disparities in Maryland's education system, **offers favorable testimony in support of House Bill 711, the Data Privacy Act.** This bill is the necessary complement to Maryland's historic decision last week to end 287(g) agreements between local law enforcement and federal immigration authorities. Ending those formal partnerships was essential. But in an era when data brokers, public records systems, and law enforcement communication networks can be weaponized to accomplish the same targeting goals through the back door, we must ensure that Maryland's commitment to protecting its communities extends to every avenue through which personal information can be used as an instrument of surveillance and enforcement. HB 711 does exactly that.

The Trump administration's immigration enforcement apparatus does not rely primarily on tips from local law enforcement. It relies on data — purchased from commercial brokers, extracted from public records systems, and accessed through interstate law enforcement communication networks. A person's name, address, driver's license record, cell phone location history, and vehicle registration can be assembled from commercially available sources into a targeting profile without a warrant, without probable cause, and without any of the constitutional protections that govern formal law enforcement activity. This is not a hypothetical vulnerability. It is the documented operational model of ICE and its data partners.

For Black, Latino, and immigrant communities in Maryland, the threat is compounded by the ways in which race, ethnicity, and national origin are embedded — explicitly or implicitly — in the data being collected and shared. The bill recognizes this by including race, ethnicity, health, sexual orientation, citizenship status, and precise location among the sensitive attributes that require heightened procedural protection. These are not incidental categories. They are the categories along which communities in Maryland have historically been surveilled, profiled, and targeted, and they are the categories that federal enforcement actors are most likely to exploit.

This bill must be understood alongside HB 293, the Maryland Longitudinal Data System expansion bill also before the General Assembly this session. In testimony supporting HB 293, we argued that Maryland's decision to expand the MLDS's research partnerships is the right one — and that its value depends entirely on the strength of the data privacy protections surrounding the system. HB 711 is the broader legislative context that makes that argument credible. A state that prohibits the sale of consumer data for immigration enforcement, that requires warrants before public records are disclosed to federal enforcement actors, and that limits warrantless access to law enforcement communication networks is a state with a coherent, comprehensive approach to data sovereignty.

Student data, consumer data, public records, and law enforcement databases are not separate silos. They are interconnected systems that, in the absence of comprehensive protections, can be assembled into a surveillance

architecture that disproportionately harms Black students, immigrant families, and communities of color. HB 711 treats data privacy not as a technical compliance requirement but as a civil rights imperative — and that framing is correct.

Opponents of this bill may argue that requiring warrants for immigration enforcement access to data systems obstructs legitimate federal law enforcement. That argument inverts the constitutional order. The Fourth Amendment's protection against unreasonable searches does not include an exception for civil immigration enforcement. The warrant requirement that HB 711 applies to public records access and message switching systems is not a novel restriction — it is the constitutional baseline that should already apply. Maryland is not obstructing federal enforcement. It is insisting that federal enforcement operate within the bounds of the Constitution.

This is precisely what Maryland's Senate argued when ending 287(g) agreements: that ICE agents conducting warrantless home entries and using unaccountable enforcement tactics were violating the Fourth Amendment, and that Maryland would not facilitate that violation. HB 711 extends that same constitutional logic to the data infrastructure that enables warrantless targeting in the first place.

The legislative work Maryland has undertaken this session — ending 287(g) agreements, protecting educational civil rights through HB 649, expanding the MLDS with robust privacy protections through HB 293, and now enacting the Data Privacy Act through HB 711 — represents a coherent state-level response to a federal government that has chosen to weaponize its power against the communities Maryland is committed to protecting. Each of these bills fills a different gap in the same wall of protection. Remove any one of them and the wall has a hole.

Black families, Latino families, and immigrant communities in Maryland need to know that when they drive to work, apply for benefits, enroll their children in school, or carry a cell phone, they are not generating a data trail that will be assembled into a targeting profile and handed to federal enforcement agents. HB 711 is Maryland's answer to that need. It is not a partisan measure. It is a constitutional one.

We urge this Committee and the full General Assembly to pass House Bill 711 without delay.

peace & truth,
sharlimar douglass
Education Justice Advocate & Analyst
Maryland Alliance for Racial Equity in Education (MAREE)