



**Testimony of Eric Null, Co-Director, Privacy & Data Program,
Center for Democracy & Technology, before the
Maryland House of Delegates Economic Matters Committee
Hearing Scheduled March 4, 2025
HB 1365 — Oppose
February 28, 2025**

About CDT

The Center for Democracy & Technology (CDT) is a nonprofit, nonpartisan organization fighting to advance civil rights and civil liberties in the digital age. For 30 years, CDT has worked on many issues touching on various aspects of privacy, civil rights, and related issues, both at the state and federal level. Privacy issues have been central to CDT’s work since its founding.

We Oppose Weakening the Data Minimization Standard in the Maryland Online Data Privacy Act

HB 1365 proposes a simple, but fundamental, change to the Maryland Online Data Privacy Act (MODPA): replace the language limiting the collection of data to what’s reasonably necessary to provide a product or service, with the weaker, more industry-friendly requirement that data collected be “adequate, relevant, and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer.” This change is a regression in privacy protections and should be rejected outright.

Data minimization ensures companies collect only data that is necessary to provide the product or service an individual requested. Data minimization requirements place the privacy-protecting burden primarily on companies that collect and exploit the data, rather than on the already overburdened consumer. U.S. privacy law has developed primarily through the Federal Trade Commission’s authority to [prevent “deceptive” practices](#), which has resulted in protections focused on when companies mislead people. For years, however, [most people have agreed](#) that [notice-and-consent has failed](#), in large part because we know that people [do not read or understand laborious](#), labyrinthian privacy policies.

Narrowing the categories of data that companies can collect is important because of the [variety of privacy-based harms](#) that come about simply from companies collecting and hoarding massive amounts of data: becoming a larger target for hackers or unauthorized access, breaches of that data that result in further downstream harms like identity theft, and subsequent use of data that is unknown or secretive, such as selling the data to third parties that compile detailed individual profiles and use that data (particularly sensitive data) for targeted advertisements.

Reducing data collected also protects against another significant harm: law enforcement access to data. Any data that a company has access to, law enforcement also has access. The Supreme Court’s decision in *Dobbs v. Jackson Women’s Health Organization* raised the

salience of this concern, as people realized that any data that could be used to identify whether a person sought or received an abortion (location data, communications data, among [many others](#)) could be accessed by law enforcement.

Last year, Maryland took an important step to address this fundamental problem and rejected the industry-friendly model that continues to place the privacy protection burden on consumers. MODPA limited the collection of data in the first instance, and placed that burden on the companies—the party that primarily benefits from the collection, processing, and transfer of consumer data. It did so by creating two tiers of minimization, limiting collection of non-sensitive data to what is “reasonably necessary” to provide the product or service, and limiting collection of sensitive data to what is “strictly necessary” to provide the product or service.

HB 1365, which seeks to amend the standard for non-sensitive data, would subvert these limits, place more burdens on the already-overwhelmed Marylander, and provide no benefit to the consumer overall. The only beneficiaries of this type of change would be companies, who would be free to continue listing every possible type of non-sensitive data collected in a long privacy policy that no one will read.

If anything, the minimization limits should be strengthened—they should apply not just to collection of data, but also the processing and disclosure of that data. Just because a company legitimately collects certain data to provide a service should not entitle them to disclose or sell that data for unrelated purposes.

We strongly urge the Committee to vote no on HB 1365, and on any other bill that further weakens Maryland’s strong data minimization standards.