SENATE BILL 504

I3, S2, E4 6lr2052
CF HB 711

By: **Senator Lam**
Introduced and read first time: February 2, 2026
Assigned to: Finance

A BILL ENTITLED

AN ACT concerning

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

FOR the purpose of prohibiting a certain controller from selling the personal data of a consumer if the controller knew or should have known that the purchaser seeks to use the data for immigration enforcement; altering the manner in which certain provisions of law may be construed with respect to a controller's or processor's compliance with governmental actions; requiring a custodian of a public record to adopt reasonable rules and regulations that prevent unauthorized disclosure or inspection of a public record, and to take reasonable steps to determine whether a public record is accessed for enforcing immigration law; altering the reasons for which a public record may be denied from being disclosed or inspected; requiring an entity that operates a certain message switching system to take certain actions regarding system access; requiring certain procedures developed and published by certain governmental entities to account for data containing certain sensitive attributes; and generally relating to data privacy of individuals in the State.

BY repealing and reenacting, without amendments,
Article – Commercial Law
Section 14–4701(a), (w), and (y)
Annotated Code of Maryland
(2025 Replacement Volume)

BY repealing and reenacting, with amendments,
Article – Commercial Law
Section 14–4701(x), (cc), (gg), and (hh) through (jj), 14–4703(b)(8), 14–4707(a), and 14–4712(a)
Annotated Code of Maryland
(2025 Replacement Volume)

BY adding to

EXPLANATION: **CAPITALS INDICATE MATTER ADDED TO EXISTING LAW.**
[Brackets**]** indicate matter deleted from existing law.

Article – Commercial Law
Section 14–4701(hh)
Annotated Code of Maryland
(2025 Replacement Volume)

BY repealing and reenacting, with amendments,
Article – General Provisions
Section 4–201, 4–320(b) and (g)(2), and 4–320.1
Annotated Code of Maryland
(2019 Replacement Volume and 2025 Supplement)

BY repealing and reenacting, with amendments,
Article – Public Safety
Section 3–529
Annotated Code of Maryland
(2022 Replacement Volume and 2025 Supplement)

BY repealing and reenacting, with amendments,
Article – State Government
Section 10–1702
Annotated Code of Maryland
(2021 Replacement Volume and 2025 Supplement)

SECTION 1. BE IT ENACTED BY THE GENERAL ASSEMBLY OF MARYLAND, That the Laws of Maryland read as follows:

Article – Commercial Law

14–4701.

(a) In this subtitle the following words have the meanings indicated.

(w) (1) "Personal data" means any information that is linked or can be reasonably linked to an identified or identifiable consumer.

(2) "Personal data" does not include:

(i) De–identified data; or

(ii) Publicly available information.

(x) (1) "Precise geolocation data" means information derived from technology that can precisely and accurately identify**, WITHIN A RADIUS OF 1,750 FEET,** the specific location of a consumer **[**within a radius of 1,750 feet**], A MOBILE DEVICE, OR A VEHICLE**.

(2) "Precise geolocation data" includes global positioning system level latitude and longitude coordinates or other similar mechanisms.

(3) "Precise geolocation data" does not include:

(i) The content of communications;

(ii) Data generated by or connected to an advanced utility metering infrastructure system; or

(iii) Data generated by equipment used by a utility company.

(y) (1) "Process" means an operation or set of operations performed by manual or automated means on personal data.

(2) "Process" includes collecting, using, storing, disclosing, analyzing, deleting, or modifying personal data.

(cc) (1) "Publicly available information" means information that a person:

(i) Lawfully obtains from a record of a governmental entity**, IF THE PERSON PROCESSES THE INFORMATION IN ACCORDANCE WITH EACH RESTRICTION OR TERM OF USE PLACED ON THE INFORMATION BY THE GOVERNMENTAL ENTITY**;

(ii) Reasonably believes a consumer or widely distributed media have lawfully made available to the general public; or

(iii) If the consumer has not restricted the information to a specific audience, obtains from a person to whom the consumer disclosed the information.

(2) "Publicly available information" does not include biometric data collected by a business about a consumer without the consumer's knowledge.

(gg) "Sensitive **[**data" means personal data that includes**]** **ATTRIBUTE" MEANS**:

(1) Data revealing:

(i) Racial or ethnic origin;

(ii) Religious beliefs;

(iii) Consumer health data;

(iv) Sex life;

(v) Sexual orientation;

(vi) Status as transgender or nonbinary;

(vii) National origin; or

(viii) Citizenship or immigration status;

(2) Genetic data or biometric data;

(3) Personal data of a consumer that the controller knows or has reason to know is a child; or

(4) Precise geolocation data.

(HH) "SENSITIVE DATA" MEANS PERSONAL DATA THAT INCLUDES A SENSITIVE ATTRIBUTE OR ANY OTHER PERSONAL DATA PROCESSED FOR THE PURPOSE OF IDENTIFYING A SENSITIVE ATTRIBUTE.

[(hh)**] (II)** (1) "Targeted advertising" means displaying advertisements to a consumer or on a device identified by a unique identifier, where the advertisement is selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated websites or online applications that are unaffiliated with each other, in order to predict the consumer's preferences or interests.

(2) "Targeted advertising" does not include:

(i) Advertisements based on the context of a consumer's current search query, visit to a website, or online application;

(ii) Advertisements based on a consumer's activities within a controller's websites or online applications;

(iii) Advertisements directed to a consumer in response to the consumer's request for information or feedback; or

(iv) Processing personal data solely to measure or report advertising frequency, performance, or reach.

[(ii)**] (JJ)** "Third party" means a person other than the relevant consumer, controller, processor, or affiliate of the controller or processor of relevant personal data.

[(jj)**] (KK)** "Trade secret" has the meaning stated in § 11–1201 of this article.

14–4703.

(b) The following information and data are exempt from this subtitle:

(8) Personal data collected, processed, sold, or disclosed **[**in compliance**]** **TO THE EXTENT NECESSARY TO COMPLY** with the federal Driver's Privacy Protection Act of 1994;

14–4707.

(a) A controller may not:

(1) Except where the collection or processing is strictly necessary to provide or maintain a specific product or service requested by the consumer to whom the personal data pertains, collect, process, or share sensitive data concerning a consumer;

(2) Sell sensitive data;

(3) Process personal data in violation of State or federal laws that prohibit unlawful discrimination;

(4) Process the personal data of a consumer for the purposes of targeted advertising if the controller knew or should have known that the consumer is under the age of 18 years;

(5) Sell the personal data of a consumer if the controller knew or should have known that **[**the**]:**

(I) **THE** consumer is under the age of 18 years**; OR**

(II) **THE PURCHASER SEEKS TO USE THE PERSONAL DATA FOR THE PURPOSE OF IMMIGRATION ENFORCEMENT**;

(6) Discriminate against a consumer for exercising a consumer right contained in this subtitle, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer;

(7) Collect, process, or transfer personal data or publicly available data in a manner that unlawfully discriminates in or otherwise unlawfully makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, sexual orientation, gender identity, or disability, unless the collection, processing, or transfer of personal data is for:

(i) The controller's self–testing to prevent or mitigate unlawful discrimination;

(ii) The controller's diversifying of an applicant, participant, or customer pool; or

(iii) A private club or group not open to the public, as described in § 201(e) of the Civil Rights Act of 1964; or

(8) Unless the controller obtains the consumer's consent, process personal data for a purpose that is neither reasonably necessary to, nor compatible with, the disclosed purposes for which the personal data is processed, as disclosed to the consumer.

14–4712.

(a) Nothing in this subtitle may be construed to restrict a controller's or processor's ability to:

(1) Comply with federal, State, or local laws or regulations;

(2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by a federal, State, local, or other governmental authority**, EXCEPT TO THE EXTENT THAT AN INQUIRY, AN INVESTIGATION, A SUBPOENA, OR A SUMMONS PERTAINS SOLELY TO IMMIGRATION ENFORCEMENT**;

(3) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, State, or local laws or regulations;

(4) Investigate, establish, exercise, prepare for, or defend a legal claim;

(5) Provide a product or service specifically requested by a consumer;

(6) Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;

(7) Take steps at the request of a consumer before entering into a contract;

(8) Take immediate steps to protect an interest that is essential for the life or physical safety of a consumer or another individual and when the processing cannot be manifestly based on another legal basis;

(9) Prevent, detect, protect against, investigate, prosecute those responsible, or otherwise respond to a security incident, identity theft, fraud, harassment, malicious or deceptive activity, or any other type of illegal activity;

(10) Preserve the integrity or security of systems; or

(11) Assist another controller, processor, or third party with an obligation under this subtitle.

Article – General Provisions

4–201.

(a) (1) Except as otherwise provided by law, a custodian shall allow a person or governmental unit to inspect any public record at any reasonable time.

(2) Inspection or copying of a public record may be denied only to the extent provided under this title.

(b) To protect public records and to prevent unnecessary interference with official business, each official custodian shall adopt reasonable rules or regulations that, subject to this title**[**,**]:**

(1) govern timely production and inspection of a public record**; AND**

(2) PREVENT UNAUTHORIZED DISCLOSURE OR INSPECTION OF A PUBLIC RECORD, INCLUDING IN ACCORDANCE WITH § 4–320.1 OF THIS TITLE.

(c) Each official custodian shall:

(1) designate types of public records of the governmental unit that are to be made available to any applicant immediately on request; and

(2) maintain a current list of the types of public records that have been designated as available to any applicant immediately on request.

4–320.

(b) Except as provided in subsections (c) through (f) of this section, **AND SUBJECT TO § 4–320.1 OF THIS SUBTITLE,** a custodian may not knowingly disclose a public record of the Motor Vehicle Administration containing personal information.

(g) (2) A person receiving personal information under subsection (d), (e), or (f) of this section may not disclose the personal information to a **[**federal agent**]** **PERSON** or **[**federal**]** **GOVERNMENT** agency for the purpose of **[**federal**]** immigration enforcement unless the person is presented with a valid warrant issued by a federal court or a court of this State.

4–320.1.

(a) In this section, "facial recognition" means a biometric software application that identifies or verifies a person by comparing and analyzing patterns based on a person's facial contours.

(b) **A CUSTODIAN SHALL TAKE REASONABLE STEPS TO DETERMINE WHETHER A PERSON SEEKING ACCESS TO A PUBLIC RECORD IS DOING SO FOR THE PURPOSE OF ENFORCING IMMIGRATION LAW.**

(C) (1) Notwithstanding any other provision of this title**[**, an officer, an employee, an agent, or a contractor of the State or a political subdivision**]** **A CUSTODIAN** shall deny inspection of the part of a public record that contains personal information or inspection of a photograph of an individual by any **[**federal agency**]** **PERSON** seeking access for the purpose of enforcing **[**federal**]** immigration law, unless the **[**officer, employee, agent, or contractor**]** **CUSTODIAN** is provided with a valid warrant issued by a federal court or a court of this State **THAT CLEARLY IDENTIFIES THE RECORD TO BE ACCESSED**.

(2) Notwithstanding any other provision of this title**[**, an officer, an employee, an agent, or a contractor of the State or a political subdivision**]** **A CUSTODIAN** shall deny inspection using a facial recognition search of a digital photographic image or actual stored data of a digital photographic image by any **[**federal agency**]** **PERSON** seeking access for the purpose of enforcing **[**federal**]** immigration law, unless the **[**officer, employee, agent, or contractor**]** **CUSTODIAN** is provided with a valid warrant issued by a federal court or a court of this State **THAT CLEARLY IDENTIFIES THE RECORD TO BE ACCESSED**.

(3) On or before June 1, 2023, and each June 1 thereafter, the Motor Vehicle Administration, the Department of State Police, and the Department of Public Safety and Correctional Services shall, with respect to requests from **[**federal**]** **GOVERNMENT** agencies seeking access for the purpose of **[**federal**]** immigration enforcement for personal information, a photograph of an individual, or a facial recognition search, whether or not the request was initiated through a State or local law enforcement agency, report to the General Assembly, in accordance with § 2–1257 of the State Government Article, the following information for the immediately preceding calendar year:

(i) the number of requests received from any **[**federal**]** **GOVERNMENT** agency for personal information, a photograph of an individual, or a facial recognition search;

(ii) the number of requests received from any **[**federal**]** **GOVERNMENT** agency for personal information, a photograph of an individual, or a facial recognition search for which a valid warrant issued by a federal court or a court of this State was provided;

(iii) the number and purpose of facial recognition searches completed for any **[**federal**]** **GOVERNMENT** agency based on personal information or a photograph of an individual provided to the **[**federal**]** **GOVERNMENT** agency by the Motor Vehicle Administration, the Department of State Police, or the Department of Public Safety and Correctional Services; and

(iv) the number of individuals whose personal information or photograph was provided to any **[**federal**]** **GOVERNMENT** agency by, respectively, the

Motor Vehicle Administration, the Department of State Police, and the Department of Public Safety and Correctional Services.

(D) THE MOTOR VEHICLE ADMINISTRATION, THE DEPARTMENT OF STATE POLICE, AND THE DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL SERVICES SHALL ADOPT REGULATIONS AND PROCEDURES TO IMPLEMENT, ENFORCE, AND ENSURE COMPLIANCE WITH THIS SECTION.

Article – Public Safety

3–529.

(a) (1) In this section the following words have the meanings indicated.

(2) (i) "Database" means any database operated by State and local law enforcement agencies, including databases maintained for a law enforcement agency by a private vendor.

(ii) "Database" does not include a registry operated under Title 11, Subtitle 7 of the Criminal Procedure Article.

(3) (i) "Law enforcement agency" means a federal, state, or local agency authorized to enforce criminal laws.

(ii) "Law enforcement agency" includes the Maryland Department of Public Safety and Correctional Services.

(4) "MESSAGE SWITCHING SYSTEM" MEANS A LAW ENFORCEMENT COMMUNICATIONS PLATFORM THAT AUTOMATICALLY ROUTES, FORMATS, AND DELIVERS ELECTRONIC QUERIES AND RESPONSES BETWEEN LAW ENFORCEMENT AGENCIES AND DATABASES.

(b) An entity operating a database **OR A MESSAGE SWITCHING SYSTEM** shall:

(1) deny access to the database **OR MESSAGE SWITCHING SYSTEM** to any **[**individual**]** **PERSON** who is seeking access for the purpose of enforcing **[**federal**]** immigration law, unless the **[**individual**]** **PERSON** presents a valid warrant issued by a federal court or a court of this State; and

(2) require an individual accessing the database **OR MESSAGE SWITCHING SYSTEM** to provide to the entity:

(i) the individual's name;

(ii) the individual's contact information, including a telephone number, an e–mail address, and a physical address; and

(iii) unless the individual presents a valid warrant issued by a federal court or a court of this State, a statement by the individual, under penalty of perjury, that the individual is not accessing the database **OR MESSAGE SWITCHING SYSTEM** for the purpose of enforcing **[**federal**]** immigration law.

(C) EACH ENTITY OPERATING A DATABASE AND, WITH RESPECT TO A MESSAGE SWITCHING SYSTEM, THE DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL SERVICES SHALL ADOPT REGULATIONS TO IMPLEMENT THIS SECTION.

Article – State Government

10–1702.

(a) (1) In this section the following words have the meanings indicated.

(2) "Governmental entity" means a unit or instrumentality of State or local government.

(3) "Personal record" has the meaning stated in § 4–501 of the General Provisions Article.

(4) "SENSITIVE ATTRIBUTE" HAS THE MEANING STATED IN § 14–4701 OF THE COMMERCIAL LAW ARTICLE.

(b) (1) Subject to paragraph (2) of this subsection, on or before July 1, 2026, each governmental entity, in consultation with the Department of Information Technology, shall develop and publish procedures that prevent the sale and redisclosure of personal records and **[**geolocation**]** data **CONTAINING SENSITIVE ATTRIBUTES** provided or made available by the governmental entity in a way that harms the privacy of residents of the State.

(2) The procedures required and published under paragraph (1) of this subsection shall address:

(i) any possible contractual limitations on the sale or redisclosure of personal records or **[**geolocation**]** data **CONTAINING SENSITIVE ATTRIBUTES** that a governmental entity may place on a person who receives personal records or **[**geolocation**]** data **CONTAINING SENSITIVE ATTRIBUTES** that are provided or made available by the governmental entity;

(ii) considerations regarding:

1. the threat to privacy posed by data brokers who utilize personal records or geolocation data for commercial purposes; **AND**

2. the risk that personal records or **[**geolocation**]** data **CONTAINING SENSITIVE ATTRIBUTES** may be used for purposes other than the purposes for which the personal records or **[**geolocation**]** data **CONTAINING SENSITIVE ATTRIBUTES** were developed or collected; and

[3. geolocation, genetic, and other sensitive data; and**]**

(iii) any other considerations necessary to:

1. protect the privacy of residents of the State;

2. discourage the development of a secondary commercial market for personal records or **[**geolocation**]** data **CONTAINING SENSITIVE ATTRIBUTES** that are provided or made available by a governmental entity; and

3. limit a person who receives personal records or **[**geolocation**]** data **CONTAINING SENSITIVE ATTRIBUTES** that are provided or made available by a governmental entity from selling or redisclosing the data with other persons.

(c) On or before July 1, 2026, each governmental entity shall, in accordance with § 2–1257 of this article, submit to the General Assembly a copy of the procedures developed under subsection (b) of this section.

SECTION 2. AND BE IT FURTHER ENACTED, That this Act shall take effect July 1, 2026.