131st MAINE LEGISLATURE

FIRST SPECIAL SESSION-2023

Legislative Document	**No. 1705**
H.P. 1094	House of Representatives, April 18, 2023

An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data

Reference to the Committee on Criminal Justice and Public Safety suggested and ordered printed.

ROBERT B. HUNT
Clerk

Presented by Representative O'NEIL of Saco.
Cosponsored by Senator TIPPING of Penobscot, Senator HICKMAN of Kennebec and Representatives: BOYER of Poland, LIBBY of Auburn, MALON of Biddeford, POIRIER of Skowhegan, RIELLY of Westbrook, Speaker TALBOT ROSS of Portland, Senators: BENNETT of Oxford, KEIM of Oxford.

Be it enacted by the People of the State of Maine as follows:

Sec. 1. 10 MRSA c. 1057 is enacted to read:

CHAPTER 1057

PRIVACY OF BIOMETRIC IDENTIFIERS

§9601. Definitions

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

1. Affirmative written consent. "Affirmative written consent" means:

A. A specific, unambiguous and informed written consent given by an individual who is not under duress or undue influence at the time the consent is given; or

B. In the context of employment, a release signed by an employee as a condition of employment.

2. Biometric identifier. "Biometric identifier" means information generated by measurements of an individual's unique biological characteristics, including a voiceprint or imagery of the iris, retina, fingerprint, face or hand, that can be used to identify that individual. "Biometric identifier" does not include:

A. A writing sample or written signature;

B. A photograph or video, except for measurable biological characteristics that can be generated or captured from a photograph or video;

C. A biological sample used for valid scientific testing or screening;

D. Demographic information;

E. A tattoo description or a physical description, such as height, weight, hair color or eye color;

F. A donated organ, tissue or other body part, blood or serum stored on behalf of a recipient or potential recipient of a living or cadaveric transplant and obtained or stored by a federally designated organ procurement organization;

G. Health care information, as defined in Title 22, section 1711-C, subsection 1, paragraph E, obtained for health care, as defined in Title 22, section 1711-C, subsection 1, paragraph C;

H. An x-ray, computed tomography, magnetic resonance imaging, positron emission tomography, mammography or other image or film of the human anatomy used to diagnose or treat an illness or other medical condition or to further validate scientific testing or screening; or

I. Information collected, used or disclosed for human subject research.

3. Human subject research. "Human subject research" means a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalized knowledge and that is conducted in accordance with the federal

policy for the protection of human subjects under 45 Code of Federal Regulations, Part 46, the protection of human subjects under 21 Code of Federal Regulations, Parts 50 and 56 or security and privacy under 45 Code of Federal Regulations, Part 164, or other similar research ethics laws, or with the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or successor organization.

4. Personal information. "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with or could reasonably be linked, directly or indirectly, with a particular individual, household or electronic device.

5. Private entity. "Private entity" means an individual acting in a commercial capacity, partnership, corporation, limited liability company, association or other group, however organized. "Private entity" does not include:

A. A state or local government agency;

B. A state court judge, justice or clerk of the court; or

C. An entity acting as a processor for another entity.

6. Processor. "Processor" means a private entity that collects, processes, stores or otherwise uses biometric identifiers on behalf of another private entity.

§9602. Applicability

This chapter does not apply to:

1. Admission or discovery of biometric identifier. The admission or discovery of a biometric identifier in any action of any kind in any court or before any government tribunal, board or agency;

2. Personal health information subject to HIPAA. Personal health information subject to the federal Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, and applicable regulations;

3. Personal information pursuant to Gramm-Leach-Bliley Act. Personal information collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act, Public Law 106-102, and implementing regulations; or

4. Facial surveillance. Information governed by Title 25, chapter 701.

§9603. Biometric identifier policy requirements

1. Development of policy. Except as provided by subsection 3, a private entity in possession of biometric identifiers shall develop and make available to the public a written policy that establishes a retention schedule and guidelines for permanently destroying a biometric identifier of an individual on the earliest of:

A. The date on which the initial purpose for obtaining the biometric identifier has been satisfied;

B. One year after the individual's last intentional interaction with the private entity in possession of the biometric identifier; and

C. Thirty days after receiving a request to destroy the biometric identifier submitted by the individual or the individual's representative. A request received under this paragraph is not valid unless the private entity can verify using commercially

reasonable methods that the individual who is the subject of the request is the individual whose biometric identifiers are in the possession of the private entity.

2. Adherence to policy. A private entity shall comply with the policy developed by the private entity under subsection 1, except for an action taken in response to a state or federal law or compulsory request or demand issued in an investigation conducted pursuant to state or federal law or taken to comply with a valid warrant, subpoena or other order issued by a court of competent jurisdiction.

3. Exception. A private entity is not required to make available to the public a written policy that:

A. Applies only to the employees of the private entity; and

B. Is used solely within the private entity for the operation of the private entity.

§9604. Affirmative written consent

1. Release or user agreement. For purposes of this chapter, the execution of a general release form or affirmation of a user agreement does not constitute affirmative written consent.

2. Uses of affirmative written consent. A private entity may only use the affirmative written consent regarding a biometric identifier of an employee of the private entity to permit access to a secure physical location or secure computer hardware or software and to record the beginning and end of the employee's work day and meal or rest breaks. The private entity may not retain a biometric identifier related to access for the purpose of employee tracking.

3. Electronic affirmative consent. Affirmative written consent may be given by electronic means. A user interface may not influence an individual toward giving affirmative written consent, and any default settings in a user interface must be designed to have as a default setting the option not to give affirmative written consent.

§9605. Storage, transmission and protection

1. Standards. A private entity or processor that collects or possesses a biometric identifier shall store, transmit and protect from disclosure that biometric identifier in a manner that is:

A. Consistent with the reasonable standard of care used in the private entity's or processor's industry; and

B. As protective or more protective than the manner in which the private entity or processor stores, transmits and protects from disclosure other confidential and sensitive information.

2. Confidential and sensitive information. For purposes of this section, "confidential and sensitive information" means personal information that can be used to identify an individual or an individual's account or property, including:

A. Genetic testing information;

B. A unique or personal identification number;

C. An account number;

D. A passcode;

E. A driver's license number; and

F. A social security number.

§9606. Required disclosure

1. Disclosure required. On the request of an individual, a private entity that collects or possesses a biometric identifier shall disclose to that individual, free of charge, any biometric identifier associated with that individual and the information required by subsection 2.

2. Required information. The information disclosed as required by subsection 1 must include all the relevant information for the period beginning 12 months before the biometric identifier was collected by or entered into the possession of the private entity and ending on the date of disclosure under this section, including:

A. The type of biometric identifier;

B. All personal information related to the biometric identifier;

C. The types of sources from which the private entity obtained the biometric identifier and personal information linked to the biometric identifier;

D. The use of the biometric identifier and personal information linked to the biometric identifier;

E. The type of 3rd party with which the private entity has shared the biometric identifier; and

F. The type of personal information linked to the biometric identifier that the private entity has disclosed to a 3rd party.

§9607. Prohibitions

1. Collection, storage or dissemination without consent. A private entity may not collect, store, purchase, receive through trade or otherwise obtain, use, disclose, transfer or otherwise disseminate an individual's biometric identifier unless the private entity first:

A. Informs the individual in writing that a biometric identifier is being collected, stored, purchased, received through trade or otherwise obtained, used, disclosed, transferred or otherwise disseminated;

B. Informs the individual in writing of the specific purpose and length of time for which a biometric identifier is being collected, stored, purchased, received through trade or otherwise obtained, used, disclosed, transferred or otherwise disseminated; and

C. Receives affirmative written consent from the individual.

This subsection does not apply to a disclosure of a biometric identifier if the disclosure completes a financial transaction requested or authorized by the individual, is required by state or federal law or is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

2. Sale, lease or trade prohibited. A private entity that collects a biometric identifier may not:

A. Sell, lease or trade that biometric identifier; or

B. Permit an entity to which the private entity transfers, shares or provides a biometric identifier to sell, lease or trade that biometric identifier.

3. Discrimination. A private entity may not:

A. Condition a sale of goods or the provision of a service on the collection, use, disclosure, transfer, sale, retention or processing of a biometric identifier unless the use of a biometric identifier is strictly necessary to the sale of the goods or the provision of the service;

B. Charge a different price or rate for goods or the provision of a service to a customer that does not provide affirmative written consent to providing a biometric identifier; or

C. Provide a different quality of goods or a service to a customer that exercises a right described by this chapter.

4. Processors. A processor may not sell, lease or trade a biometric identifier. A processor may not collect, store, process, use, disclose or conduct any action for profit or otherwise on or with biometric identifiers, except as authorized by a contract with a private entity that legally possesses the biometric identifiers.

A. A contract between the processor and the private entity described by this subsection must expressly prohibit the processor from disclosing, retaining or using the biometric identifiers outside of the direct contractual relationship with the private entity.

B. A private entity that contracts with a processor to process or store biometric identifiers may not allow the processor to collect, store, process, use, disclose or conduct any action for profit or otherwise on or with biometric identifiers, except for purposes for which the private entity received express affirmative written consent from the individual.

§9608. Remedies for violation

1. Private right of action. An individual alleging a violation of this chapter may bring a civil action against an offending private entity. If the individual prevails in the action, the individual is entitled to:

A. For a violation of this chapter:

(1) As a result of negligence, actual damages or $1,000 per violation, whichever is greater; or

(2) As a result of recklessness or intentional misconduct, actual damages or $5,000 per violation, whichever is greater;

B. Reasonable attorney's fees and court costs, including expert witness fees and other litigation expenses; and

C. Other relief, including injunctive or equitable relief, as the court determines appropriate.

2. Unfair trade practice. In addition to subsection 1, any violation of this chapter constitutes prima facie evidence of a violation of the Maine Unfair Trade Practices Act.

3. Enforcement by Attorney General. The Attorney General may bring an action against a private entity for a violation of this chapter and seek any form of relief available to any other plaintiff, including the collection of damages as a civil penalty.

§9609. Effective date

This chapter takes effect January 1, 2025.

SUMMARY

This bill provides for an individual's privacy regarding the collection and use of biometric identifiers of the individual and personal information connected to the biometric identifiers. The bill requires a written release from an individual before a private entity may obtain or use biometric identifiers and requires the private entity to establish a policy for retention and destruction of the biometric identifiers. The bill provides for a private right of action for an aggrieved individual who has had biometric identifiers obtained or used in violation of the provisions related to biometric identifiers, as well as civil penalties and enforcement by the Attorney General. The bill also provides that violations of provisions related to biometric identifiers constitute violations of the Maine Unfair Trade Practices Act.