

# MAINE STATE LEGISLATURE

The following document is provided by the  
**LAW AND LEGISLATIVE DIGITAL LIBRARY**  
at the Maine State Law and Legislative Reference Library  
<http://legislature.maine.gov/lawlib>



Reproduced from electronic originals  
(may include minor formatting differences from printed original)



# 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.

A handwritten signature in cursive script that reads "Robert B. Hunt".

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.

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

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

3 **CHAPTER 1057**

4 **PRIVACY OF BIOMETRIC IDENTIFIERS**

5 **§9601. Definitions**

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

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

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

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

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

17 A. A writing sample or written signature;

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

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

21 D. Demographic information;

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

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

27 G. Health care information, as defined in Title 22, section 1711-C, subsection 1,  
28 paragraph E, obtained for health care, as defined in Title 22, section 1711-C, subsection  
29 1, paragraph C;

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

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

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

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

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

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

13 A. A state or local government agency;

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

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

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

18 **§9602. Applicability**

19 This chapter does not apply to:

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

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

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

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

30 **§9603. Biometric identifier policy requirements**

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

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

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

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

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

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

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

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

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

12 **§9604. Affirmative written consent**

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

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

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

26 **§9605. Storage, transmission and protection**

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

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

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

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

38 A. Genetic testing information;

39 B. A unique or personal identification number;

40 C. An account number;

41 D. A passcode;

1           E. A driver's license number; and

2           F. A social security number.

3           **§9606. Required disclosure**

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

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

12           A. The type of biometric identifier;

13           B. All personal information related to the biometric identifier;

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

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

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

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

22           **§9607. Prohibitions**

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

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

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

32           C. Receives affirmative written consent from the individual.

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

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

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

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

3 **3. Discrimination.** A private entity may not:

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

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

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

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

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

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

#### 24 **§9608. Remedies for violation**

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

28 A. For a violation of this chapter:

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

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

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

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

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

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

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13

**§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.