LB204
2025

LEGISLATURE OF NEBRASKA

ONE HUNDRED NINTH LEGISLATURE

FIRST SESSION

LEGISLATIVE BILL 204

Introduced by Kauth, 31.

Read first time January 14, 2025

Committee:

A BILL FOR AN ACT relating to biometric data; to adopt the Biometric Autonomy Liberty Law; and to provide an operative date.

Be it enacted by the people of the State of Nebraska,

LB204
2025

Section 1. Sections 1 to 19 of this act shall be known and may be cited as the Biometric Autonomy Liberty Law.

Sec. 2. The Legislature finds that:

(1) The use of biometric data is growing in commercial, therapeutic, and recreational applications;

(2) The use of biometric data to identify or monitor individuals is unlike other unique identifiers that are used in commercial and recreational applications. Biometric data of an individual that has been compromised leaves the individual with no recourse, a heightened risk for identity theft, and a greater likelihood to withdraw from transactions facilitated by biometric data;

(3) An overwhelming majority of members of the public are weary of the use of biometric data when such data is tied to finances and other personal information;

(4) The ramifications of biometric data technology are not fully known; and

(5) The public's welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric data.

Sec. 3. For purposes of the Biometric Autonomy Liberty Law:

(1)(a) Biometric data means data that is generated to identify a specific individual through an automatic measurement of a biological characteristic of such individual and includes any:

(i) Fingerprint;

(ii) Voice print;

(iii) Retina image;

(iv) Iris image; or

(v) Unique biological pattern or characteristic.

(b) Biometric data does not include:

(i) Any photograph, video recording, or audio recording, except for data generated or collected from the biological characteristics of a

LB204
2025

person depicted in any such photograph, video recording, or audio recording; or

(ii) Information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act;

(2) Collect means to gather, acquire, or obtain;

(3) Confidential and sensitive data means personal data that can be used to uniquely identify an individual or an individual's account or property, including any biometric data, genetic marker, genetic testing data, unique identifier number used to locate any account or property, account number, personal identification number, pass code, motor vehicle operator's license number, state identification card number, or social security number;

(4) Controller means any private entity or public entity that, alone or jointly with others, determines the purpose and means of processing biometric data;

(5) Disclose includes redisclosure and dissemination;

(6) Implantable device means a biocompatible device that can be implanted inside the body;

(7) Portable means the ability of an individual to transfer biometric data in a usable form from one controller or processor to another controller or processor;

(8) Possess means to have any custody of, to have any control of, to manage the storage of, or to use;

(9)(a) Private entity means any individual, partnership, corporation, limited liability company, association, or other group or entity, however organized.

(b) Private entity does not include a public entity;

(10) Process or processing means an operation or set of operations performed, whether by manual or automated means, on biometric data or on sets of biometric data, such as the collection, use, storage, disclosure,

LB204
2025

analysis, deletion, or modification of biometric data;

(11) Processor means any private entity or public entity that processes biometric data on behalf of a controller;

(12) Public entity means:

(a) The State of Nebraska or any agent acting on behalf of the State of Nebraska;

(b) Any state or local governmental agency or any agent acting on behalf of any state or local governmental agency;

(c) Any political subdivision of the State of Nebraska or any agent acting on behalf of any political subdivision of the State of Nebraska;

(d) Any court of Nebraska or any judge, justice, or agent acting on behalf of such court; and

(e) The Legislative Council or any agent acting on behalf of the Legislative Council;

(13) Secure means to make certain that biometric data is:

(a) Protected from the danger of loss;

(b) Protected from corruption of the data; and

(c) Safe from disclosure to any party not authorized to collect or possess the data;

(14)(a) Security purpose means the prevention or investigation of any safety concern or criminal activity; and

(b) Security purpose includes:

(i) Assisting a law enforcement investigation, protecting property from trespass, controlling access to property, or protecting any person from harm, including stalking, violence, or harassment; and

(ii) Enforcement through any photograph, video recording, drug test, or identification method; and

(15) Written consent means a document that indicates informed written consent that:

(a) Is provided in a physical or an electronic format by an individual who is nineteen years of age or older or by such individual’s

LB204
2025

legal guardian or legally authorized representative;

(b) Only uses language that is clear, concise, and written at the seventh-grade lexile as such lexile is defined by the State Department of Education; and

(c)(i) For a physical document, is physically signed by the person who is providing the written consent; or

(ii) For a digital document, contains an affirmative indication of consent made by the person who is providing the written consent.

Sec. 4. Biometric data is the property of the individual from whom the data was originally collected. An individual may sell the right to use his or her biometric data or otherwise consent to its use.

Sec. 5. Any private entity or public entity shall not require or coerce any individual to be subject to any implantable device.

Sec. 6. Except as provided in section 18 of this act, a private entity shall not require or coerce any individual to wear or be subject to a device of any kind that collects biometric data.

Sec. 7. Except as provided in section 18 of this act, a private entity shall not require any individual to provide or submit to the collection of biometric data.

Sec. 8. (1) Except as provided in section 18 of this act, any controller or processor that is a private entity shall only collect or possess biometric data in a manner that is secure and portable.

(2) Except as provided in section 18 of this act, an individual may provide a written request to a controller or processor in possession of such individual's biometric data to transfer such biometric data to another controller or processor. A controller or processor shall transfer such biometric data as requested within thirty calendar days after receiving such written request.

Sec. 9. (1) Except as provided in section 18 of this act, any controller or processor that is a private entity that is or intends to be in possession of any individual's biometric data shall develop and make

LB204
2025

available to the public a written policy establishing a retention schedule and guidelines for permanently destroying biometric data at the earliest occurrence of the following:

(a) Unless the individual has provided written consent to a longer term, the initial purpose for collecting or possessing such data has been satisfied;

(b) Unless the individual has provided written consent to a longer term, within one year after the last interaction between the private entity and the individual from whom the data was originally collected; or

(c) The expiration or withdrawal of the written consent from the individual from whom the data was originally collected.

(2) Except if necessary to comply with a warrant or subpoena issued by a court of competent jurisdiction, a controller or processor that is a private entity in possession of biometric data shall comply with the established retention schedule and destruction guidelines of such controller or processor.

Sec. 10. (1) Except as provided in section 18 of this act, a private entity shall not collect or possess an individual's biometric data unless the individual from whom the data was originally collected, or such individual's legal guardian or legally authorized representative, has provided written consent that (a) authorizes such collection or possession and (b) specifies the purpose and duration for such collection or possession.

(2) Each document used to provide written consent shall include a biometric data collection warning. Such warning shall clearly and conspicuously indicate the biometric data that will be collected or possessed, the purpose and duration for such collection or possession, and a statement that is substantially similar to the following:

(a) "Do you consent to [private entity] collecting your biometric data for [each specified purpose]?";

(b) "Do you consent to [private entity] possessing your biometric

LB204
2025

data for [each specified purpose]?"; and

(c) "Do you consent to [private entity] selling or sharing your biometric data with [any third party]?".

Sec. 11. (1) Except as provided in subsection (2) of this section and section 18 of this act, a private entity or public entity shall not provide a difference in any service, good, benefit, or reward provided to any individual who does not consent to the collection or possession of biometric data.

(2) A private entity or public entity may provide a difference in any service, good, benefit, or reward provided to any individual who does not consent to the collection or possession of biometric data if such collection or possession is necessary to the provision of the service, good, benefit, or reward such that its absence would render the service, good, benefit, or reward inoperable, meaningless, or irrelevant.

Sec. 12. (1) A private entity or public entity in possession of or with access to biometric data shall not sell, lease, trade, or use biometric data without the prior written consent of the individual from whom the data was originally collected.

(2) This section does not apply to the use of biometric data by any law enforcement agency or any agent acting on behalf of any law enforcement agency if such use is for a legitimate purpose of the law enforcement agency.

Sec. 13. A processor that is in possession of biometric data shall not disclose an individual's biometric data unless such disclosure is compliant with the Biometric Autonomy Liberty Law and:

(1) Such individual or such individual's legal guardian or legally authorized representative provides written consent to the disclosure;

(2) The disclosure is required or authorized by law;

(3) The disclosure is required pursuant to a warrant or subpoena issued by a court of competent jurisdiction;

(4) The disclosure is made pursuant to a criminal action or

LB204
2025

proceeding;

(5) The disclosure is made pursuant to a civil action or proceeding under section 15 of this act; or

(6) Such processor is cooperating with any law enforcement agency and reasonably and in good faith believes the biometric data that will be disclosed concerns any of the following:

(a) Conduct or activity that violates any federal, state, or local law, rule, or regulation;

(b) Any missing person; or

(c) Public health.

Sec. 14. A processor that is in possession of biometric data shall store, transmit, and protect from disclosure all of such data:

(1) Using the reasonable standard of care within the industry or profession of the processor; and

(2) In a manner that:

(a) Is the same as or more protective than the manner in which the processor stores, transmits, and protects other confidential and sensitive data; or

(b) Converts the biometric data to a mathematical representation, including a numeric string or a similar method that cannot be used to recreate the biometric data.

Sec. 15. (1) The Attorney General may:

(a) Issue subpoenas and file a civil action to recover direct economic damages for any affected Nebraska resident aggrieved by a violation of the Biometric Autonomy Liberty Law; and

(b) Seek injunctive relief for a violation of the Biometric Autonomy Liberty Law.

(2) A violation of the Biometric Autonomy Liberty Law shall be considered a violation of section 59-1602 and be subject to the Consumer Protection Act and any other law that provides for the implementation and enforcement of section 59-1602.

LB204
2025

(3) Before bringing an action under this section, the Attorney General or an individual shall provide written notice to the party alleged to have violated the Biometric Autonomy Liberty Law. Such party shall have sixty days from the date of receiving such notice to cure the alleged violation. If the alleged violation is cured within the sixty-day period, no action shall be maintained against such party for the alleged violation.

(4) For purposes of a civil action under this section, the following conduct by a private entity shall constitute only a single violation of the Biometric Autonomy Liberty Law, notwithstanding that there were multiple instances of such conduct:

(a) Collecting, capturing, purchasing, receiving through trade, or otherwise obtaining the same biometric data from the same person using the same method of collection; and

(b) Disclosing the same type of biometric data obtained from the same person to the same recipient using the same method of collection.

Sec. 16. A waiver of any provision of the Biometric Autonomy Liberty Law obtained without the written consent of the individual waiving such provision or such individual's legal guardian or legally authorized representative is contrary to public policy and is void and unenforceable.

Sec. 17. Nothing in the Biometric Autonomy Liberty Law shall be construed to:

(1) Impact the admission or discovery of biometric data in any legal action of any kind in any court or before any private entity or public entity;

(2) Conflict with:

(a) The Data Privacy Act;

(b) The Genetic Information Privacy Act;

(c) Sections 71-8401 to 71-8407; or

(d) The federal Health Insurance Portability and Accountability Act

LB204
2025

of 1996 and the rules promulgated under such act;

(3) Apply to emergency medical care that is covered by the Emergency Medical Services Practice Act;

(4) Apply to facial recognition technology used by the Department of Motor Vehicles for fraud detection;

(5) Apply to personal data regulated by the federal Family Educational Rights and Privacy Act of 1974, 20 U.S.C. 1232g, as such act existed on January 1, 2025; or

(6) Apply to a financial institution, an affiliate of a financial institution, or data subject to Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. 6801 et seq., as such title existed on January 1, 2025.

Sec. 18. Sections 6 to 11 of this act shall not apply to biometric data collected or possessed for a security purpose.

Sec. 19. The Biometric Autonomy Liberty Law shall not apply to any information collected, used, or stored for health care treatment, payment, or operations, including protected health information, under the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under such act.

Sec. 20. This act becomes operative on January 1, 2026.