SPONSOR: Rep. Paradee & Sen. Sokola
Reps. Hudson, Q. Johnson, Keeley; Sens. Hansen, Henry

HOUSE OF REPRESENTATIVES
149th GENERAL ASSEMBLY

HOUSE BILL NO. 350

AN ACT TO AMEND TITLE 6 OF THE DELAWARE CODE RELATING TO PERSONAL INFORMATION PRIVACY.

BE IT ENACTED BY THE GENERAL ASSEMBLY OF THE STATE OF DELAWARE:

Section 1. Amend Title 6 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underline as follows:

Chapter 12D. Biometric Privacy Protection.

§ 1201D. Short title.

This chapter shall be known and may be cited as the "Biometric Privacy Protection Act."

§ 1202D. Definitions.

For purposes of this chapter, the following definitions shall apply:

(1) "Biometric identifier" means a biologic or behavioral characteristic that can be used to identify a specific individual, including a finger or palm print, eye retina or iris scan, voice recognition, hand or face geometry, facial imaging or recognition, gait recognition, vein recognition, or other unique biological or behavioral characteristics. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191, as amended).

(2) "Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifier.

(3) "Personal information" shall have the meaning set forth in § 12B-101(7) of Chapter 12B of this title.

§ 1203D. Retention of biometric identifiers or biometric information.

A person in possession of biometric identifiers or biometric information of an individual must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying an individual's biometric identifiers and biometric information when the initial purpose for collecting or obtaining such biometric identifiers or biometric information has been satisfied, or within three years of the individual's last interaction

with the person, whichever occurs first. Absent a valid warrant, order, civil investigative demand, or subpoena issued by a court of competent jurisdiction, a person in possession of biometric identifiers or biometric information must comply with the retention schedule and destruction guidelines set forth in that person's written policy.

§ 1204D. Acquisition of biometric identifiers or biometric information.

A person shall not acquire, collect, or capture an individual's biometric identifier or biometric information unless that person:

(1) Provides timely, reasonable notice to the individual or the individual's legal representative of all of the following:

a. That the individual's biometric identifier or biometric information is being acquired, collected, stored, or captured.

b. The specific biometric identifiers or biometric information being acquired, collected, stored, or captured.

c. The specific purposes for which the biometric identifier or biometric information will be acquired, collected, captured, stored, or used.

d. The length of time the biometric identifier or biometric information will be retained.

(2) Obtains informed, affirmative consent from the individual or the individual's legal representative to the acquisition, collection, storage, or capture of a biometric identifier or biometric information.

§ 1205D. Prohibitions on the sale, lease, disclosure, or dissemination of biometric identifiers or biometric information.

(a) A person in possession of an individual's biometric identifier or biometric information shall not sell, lease, trade, or otherwise profit from that individual's biometric identifier or biometric information.

(b) A person in possession of an individual's biometric identifier or biometric information shall not disclose, redisclose, or otherwise disseminate that individual's biometric identifier or biometric information unless one of the following applies:

(1) The individual or the individual's legal representative gives informed, affirmative consent to the disclosure, redisclosure, or dissemination.

(2) The disclosure, redisclosure, or dissemination completes a financial transaction requested or authorized by the individual or the individual's legal representative.

(3) The disclosure, redisclosure, or dissemination is required by applicable federal or State law or regulation.

(4) The disclosure, redisclosure, or dissemination is required pursuant to a valid warrant, order, civil investigative demand, or subpoena issued by a court of competent jurisdiction.

§ 1206D. Protection of biometric identifiers or biometric information.

A person in possession of biometric identifiers or biometric information shall implement and maintain reasonable procedures and practices to store or transmit biometric identifiers and biometric information and to prevent the unauthorized acquisition, use, modification, disclosure, storage, transmission, or destruction of biometric identifiers or biometric information, provided that such procedures and practices are also no less protective than the manner in which the person stores, transmits, or protects other personal information.

§ 1207D. Enforcement.

The Consumer Protection Unit of the Department of Justice has enforcement authority over this chapter and may investigate and prosecute violations of this chapter in accordance with the provisions of Subchapter II of Chapter 25 of Title 29 of the Delaware Code.

§ 1208D. Construction.

(a) Nothing in this chapter shall be construed to apply in any manner to a financial institution or affiliate of a financial institution that is subject to Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. § 6801, et seq., as amended) and the rules and regulations promulgated thereunder.

(b) Nothing in this chapter shall be construed to impact the admissibility or discovery of biometric identifiers or biometric information in any action or proceeding in any court or administrative or arbitration tribunal, or before any governmental agency, board, or commission.

(c) Nothing in this chapter shall be construed to apply to the State, any political subdivision of the State, or any department, agency, board, or commission of the State, nor shall anything in this chapter be construed to apply to a contractor, subcontractor, or agent of the State or a political subdivision of the State, or any department, agency, board, or commission of the State or political subdivision thereof, when such contractor, subcontractor, or agent is working for and at the direction of the State or a political subdivision of the State, or any department, agency, board, or commission of the State or political subdivision thereof.

Section 2. Amend Title 6 of the Delaware Code by making deletions as shown by strike through and insertions as shown by underline as follows:

Chapter 12E. Geolocation Privacy Protection.

§ 1201E. Short title.

This chapter shall be known and may be cited as the "Geolocation Privacy Protection Act."

§ 1202E. Definitions.

For purposes of this chapter, the following definitions shall apply:

(1) "Geolocation information" means information which is all of the following:

a. Generated by or derived from, in whole or in part, the operation of a mobile device.

b. Sufficient to determine or infer the precise physical location of a mobile device.

c. Neither the contents of a communication nor an Internet protocol address.

(2) "Location-based application" means a software application that is downloaded or installed onto a mobile device and collects, uses, or stores geolocation information.

(3) "Mobile device" means a portable computing or electronic device, including a smartphone, cellular telephone, tablet computer, or laptop computer.

§ 1203E. Collection, use, storage, or disclosure of geolocation information.

(a) A person may not collect, use, store, or disclose geolocation information from a location-based application on an individual's mobile device unless the person first receives the individual's affirmative express consent after providing clear, prominent, and accurate notice that does all of the following:

(1) Informs the individual that the individual's geolocation information will be collected, used, stored, or disclosed.

(2) Informs the individual of the specific purposes for which the individual's geolocation information will be collected, used, stored, or disclosed, and, if the geolocation information will be disclosed to other persons, the identity of those persons.

(3) Provides the individual with a hyperlink or comparably easily accessible means to access the information specified in this subsection.

(b) A person may collect, use, store, or disclose an individual's geolocation information from a location-based application on an individual's mobile device without receiving that individual's affirmative express consent if the collection, use, storage, or disclosure is for any of the following purposes:

(1) To allow a parent or legal guardian to locate an unemancipated child.

(2) To allow a court-appointed guardian to locate a legally incapacitated individual.

(3) To provide fire, medical, public safety, or other emergency services.

(c) A person is not required to obtain an individual's affirmative express consent after the person has obtained the individual's initial affirmative express consent as described in subsection (a) of this section, unless the terms previously agreed to under paragraphs (1), (2), and (3) of subsection (a) are materially changed.

§ 1204E. Enforcement.

The Consumer Protection Unit of the Department of Justice has enforcement authority over this chapter and may investigate and prosecute violations of this chapter in accordance with the provisions of Subchapter II of Chapter 25 of Title 29 of the Delaware Code.

§ 1205E. Waiver; contracts.

(a) Any waiver of the provisions of this chapter is invalid and unenforceable.

(b) Any agreement created or modified after the effective date of this chapter that does not comply with this chapter is void and unenforceable. An agreement that is void and unenforceable under this section does not give rise to a private right of action under this chapter.

§ 1206E. Construction.

Nothing in this chapter shall be construed to apply in any manner to any of the following:

(1) A health care provider or other covered entity that is subject to the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191, as amended), and the rules and regulations promulgated thereunder.

(2) A financial institution or affiliate of a financial institution that is subject to Title V of the Gramm-Leach-Bliley Act of 1999 (15 U.S.C. § 6801, *et seq.*, as amended), and the rules and regulations promulgated thereunder.

(3) Internet, wireless, or telecommunications service providers.

(4) The State, any political subdivision of the State, or any department, agency, board, or commission of the State.

Section 3. This Act becomes effective January 1 following its enactment into law.

Section 4. If any provision of this Act or the application thereof to any person or circumstances is held invalid, the invalidity does not affect any other provision or application of the Act which can be given effect without the invalid provision or application; and, to that end, the provisions of this Act are declared to be severable.

SYNOPSIS

This Act will create the Biometric Privacy Protection Act and Geolocation Privacy Protection Act in Title 6 of the Delaware Code to give Delaware's citizens important protections with respect to the collection, storage, use, and disclosure of their unique biometric information (such as fingerprints, voiceprints, and retinal and facial scans) and, with respect to their use of mobile devices, geolocation information that can identify

Biometrics are biological and behavioral characteristics, such as fingerprints, voiceprints, and retinal and facial scans, that uniquely identify a person, and they are increasingly being collected from Delaware's citizens and used for a variety of purposes, including marketing, employment, and security. Biometrics are among our most sensitive personal information, potentially more valuable to identity thieves, hackers, and marketers than even Social Security numbers, and need to be protected as such. Currently under Delaware law, biometric information can be collected without an individual's knowledge or consent, and a person capturing or collecting biometric information is not required to identify what biometric information is being collected, why it's being collected, or how long it will be kept. Delaware law also contains no protections for individuals to prevent their biometric information from being sold or transferred to third parties. The use of biometrics offers great promise for improving the lives of Delaware's citizens in a variety of ways, but the sensitivity and

importance of biometric information requires that there be protections for Delawareans with regard to the collection and use of their biometric information.

The Biometric Privacy Protection Act will expand the legal protections available under Delaware law to individuals relating to the collection and use of their biometric identifiers and biometric information. Among its provisions, the Biometric Information Privacy Protection Act:

(1) Requires persons in possession of biometric data to develop and make publicly available written retention schedules and guidelines for keeping biometric information;

(2) Requires persons to provide timely, reasonable notice and obtain informed, affirmative consent before acquiring, collecting, storing, or capturing biometric data;

(3) Prohibits persons from selling or profiting from an individual's biometric data;

(4) Prohibits persons from disclosing or disseminating an individual's biometric data except under specified circumstances, which include an individual's informed, affirmative consent to the disclosure; and

(5) Requires persons in possession of biometric data to implement and maintain reasonable procedures and practices to protect the biometric data and prevent its unauthorized disclosure.

Geolocation information is data that can be used to determine the precise location of smartphones and other mobile devices and, by extension, the individuals carrying them. Such information can be used to track the users carrying those devices wherever they go. Location-based applications currently can make use of geolocation information on an individual's mobile device without explicitly informing the individual that the geolocation information is being collected, used, stored, or disclosed, why it is being collected, used, stored, or disclosed, or to whom it is being disclosed, and without obtaining the individual's consent to the collection, use, storage, or disclosure of the geolocation information.

The Geolocation Privacy Protection Act will create legal protections for Delaware's citizens relating to the collection, use, storage, or disclosure of the geolocation information on their mobile devices, by prohibiting persons from collecting, using, storing, or disclosing such information unless they first obtain an individual's affirmative express consent after providing the individual with clear, prominent, and accurate notice that:

(1) Tells the individual that the individual's geolocation information is being collected, used, stored, or disclosed;

(2) Informs the individual of the specific purposes for which the geolocation information is being collected, used, stored, or disclosed;

(3) Informs the individual of the identity of any third parties to whom the geolocation information is being disclosed; and

(4) Provides the individual with a hyperlink or other easy access to the geolocation information collected, used, stored, or disclosed.

Both the Biometric Information Privacy Protection Act and the Geolocation Privacy Protection Act give the Consumer Protection Unit of the Department of Justice the authority to investigate and prosecute violations. There is no private right of action under the Biometric Information Privacy Protection Act or the Geolocation Privacy Protection Act. Both the Biometric Information Privacy Protection Act or the Geolocation Privacy Protection Act provide that their provisions do not apply to certain specified persons or entities or in certain specific situations.

This Act provides that it will become effective January 1 following its enactment into law.