AMERICAN BIOMETRIC AND ALGORITHMIC SELF NON-TRANSFER ACT

Complementary federal bill to the American Productive Capacity Authority Act
Drafted 2026-07-28

UNITED STATES CONGRESS

119th Congress, 2nd Session

2026

H.R. ____

S. ____

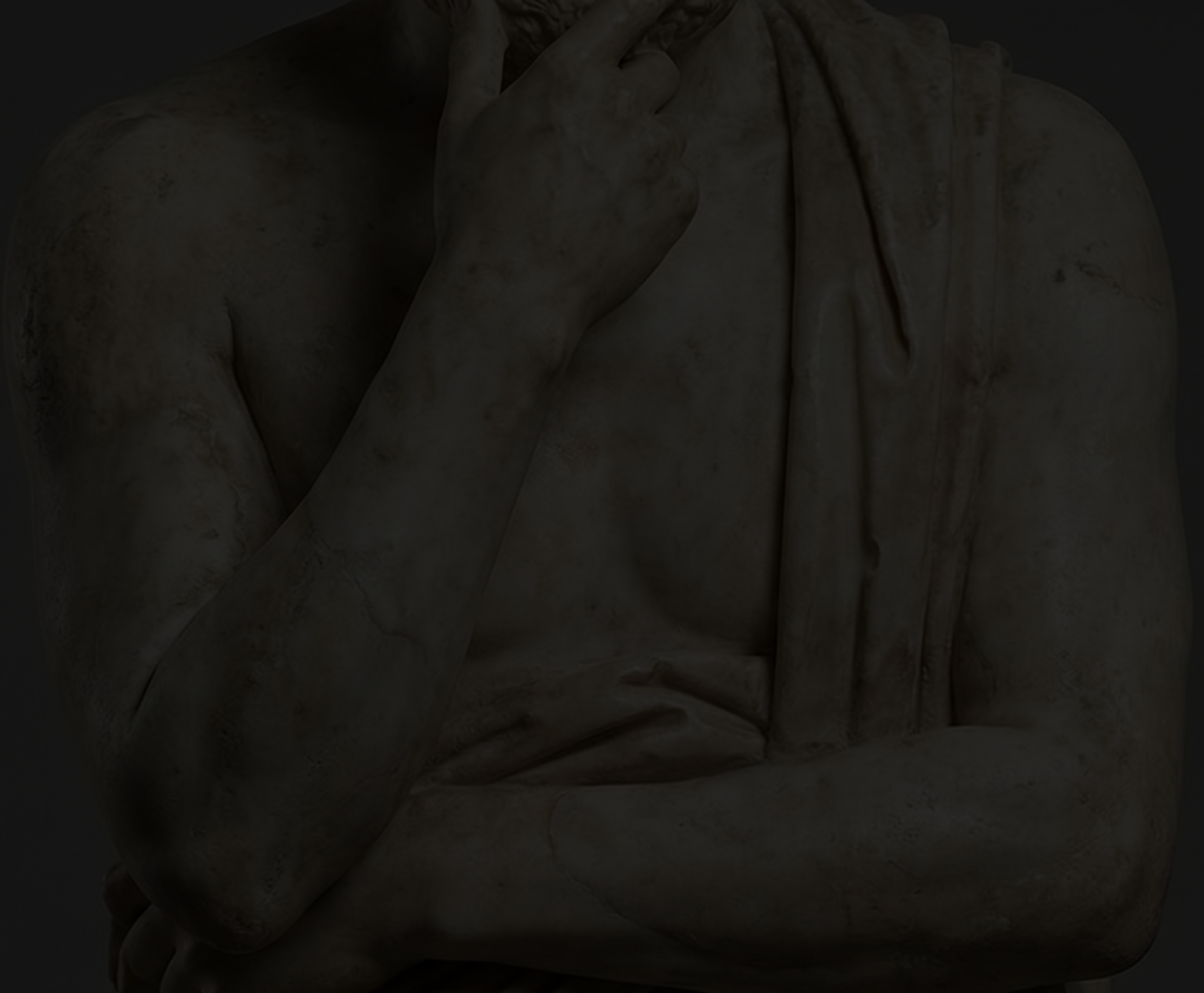
BY _________ (Introduced by request)

A BILL FOR AN ACT

CONCERNING THE PROTECTION OF THE BIOMETRIC AND ALGORITHMIC SELF, TO DECLARE THAT BIOMETRIC, BEHAVIORAL, AND INFERRED DATA LAWFULLY COLLECTED BY A BUSINESS FOR A LEGITIMATE OPERATIONAL PURPOSE IS HELD FOR THAT PURPOSE ONLY, IS NOT A SALEABLE OR TRANSFERABLE ASSET, MAY NOT BE SOLD, LEASED, TRADED, PLEDGED, OR PROFITED FROM, AND MAY NOT PASS TO ANY OTHER PERSON AS PROPERTY IN A BANKRUPTCY, FORECLOSURE, DEBT SETTLEMENT, LIEN, MERGER, ACQUISITION, OR ASSET SALE EXCEPT UPON THE FRESH AND AFFIRMATIVE CONSENT OF THE PERSON THE DATA DESCRIBES.

LONG TITLE

AN ACT to declare that a person's biometric identifiers, the algorithmic derivatives computed from them, and the behavioral, keystroke, and inferred psychometric data that describe a person are an extension of the person and not inventory of the business; to provide that such data, when lawfully collected by a business for a legitimate operational purpose, is held for that purpose only and carries no asset value that a business may sell, lease, trade, pledge as collateral, or otherwise profit from; to declare that such data may not be transferred to any other person as property in a bankruptcy estate, foreclosure, debt settlement, security interest, merger, acquisition, or sale of assets; to require the fresh and affirmative consent of the person the data describes before any successor may hold it, and to require its deletion where that consent is not given; to bar a business from collecting the biometric or algorithmic self of a customer absent a genuine operational necessity, while permitting an employer to collect employee data for a genuine operational purpose subject to every limit of this Act; to declare that data a person supplies to a conversational artificial-intelligence system is behavioral biometric data within the meaning of this Act; to provide civil penalties and a private right of action; and to provide effective dates.



LEGISLATIVE ROUTING NOTE

FILING PROCEDURE: This Act shall be filed with companion bills in the House of Representatives and the United States Senate and referred to the appropriate standing committees.

COMMITTEE ASSIGNMENT:

House of Representatives:

- Committee on Energy and Commerce (consumer data, interstate commerce)
- Committee on the Judiciary (property, bankruptcy, non-transfer)
- Committee on Financial Services (secured transactions, foreclosure)

Senate:

- Committee on Commerce, Science, and Transportation
- Committee on the Judiciary

FISCAL IMPACT: The Congressional Budget Office shall prepare a fiscal impact statement pursuant to 2 U.S.C. 602. This Act authorizes appropriations for the oversight function and directs a cost-recovery fee on covered businesses sufficient to fund enforcement after standup.

CONSTITUTIONAL BASIS: Article I, Section 8, Clause 3 (commerce among the several States), Clause 4 (uniform laws on the subject of bankruptcies), and Clause 18 (necessary and proper). A limit on the sale and transfer of a defined class of personal data in interstate commerce, and a limit on the treatment of that data as property of a bankruptcy estate, are settled exercises of the commerce power and the bankruptcy power.

LEGISLATIVE DECLARATION

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

DECLARATION OF PRINCIPLE

(I) THE DATA IS THE PERSON. The Congress finds and declares that a person's biometric identifiers, the mathematical model computed from them, and the behavioral and inferred data that describe how a person types, moves, speaks, decides, and thinks are an extension of that person. They are not stock, not inventory, and not a receivable. A business may be permitted to use such data for the narrow purpose for which the person allowed it to be taken, and for no other, and the business acquires no ownership of the person by holding the person's measurements.

(II) A USE IS NOT A TITLE. The Congress finds that permission to use a thing for a purpose is not ownership of the thing. A business that scans an employee's finger to record the start of a shift has permission to read that finger for that shift. It does not thereby own the finger, the scan, or the model of the finger, and it may not sell any of them, borrow against any of them, or hand any of them to a creditor. The permission is bounded by the purpose and expires with it.

(III) THE PERSON MAY NOT BE AUCTIONED. The Congress finds that the gravest abuse of this data is its treatment as a corporate asset that survives the business and is sold when the business fails. When a company is dissolved, foreclosed upon, or sold for parts, its servers, its furniture, and its customer lists may pass to a buyer, but the biometric and algorithmic self of a living person shall not. A person's body-data shall never become a creditor's payout.

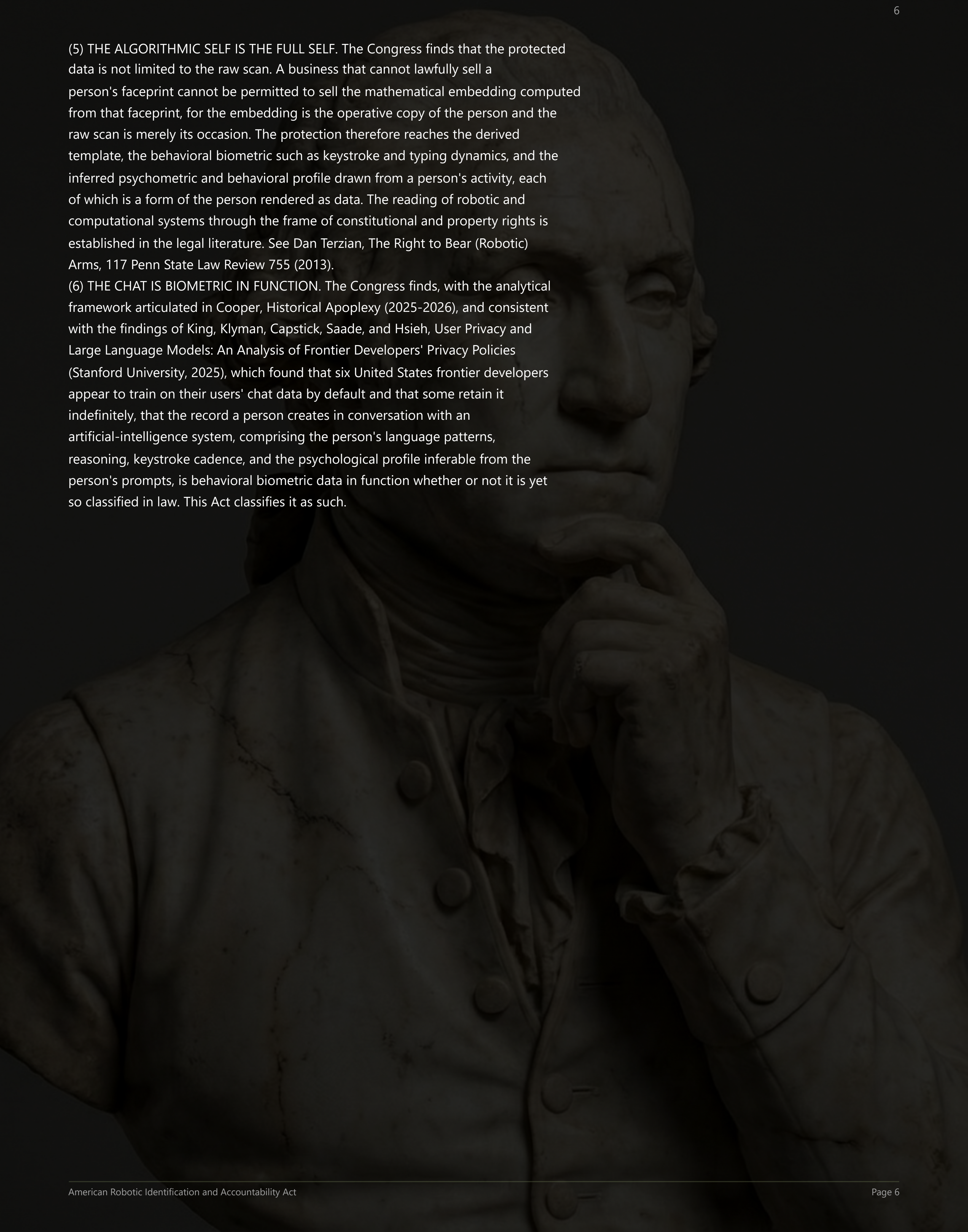
SECTION 1. Legislative findings.

(1) THE NO-PROFIT PRECEDENT. The Biometric Information Privacy Act of Illinois, 740 ILCS 14, at Section 15(c), already provides that no private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from it. This Act adopts that settled prohibition at the national level and extends it to the transfer of such data as property.

(2) THE BANKRUPTCY-AUCTION PRECEDENT. When the electronics retailer RadioShack entered bankruptcy in 2015 and sought to sell its store of customer personal information as an asset of the estate, the Federal Trade Commission intervened to protect that information from sale. The episode proves both the danger, that personal data is treated as a saleable asset when a business fails, and the remedy, that the law may forbid the sale. This Act forbids it for the biometric and algorithmic self.

(3) THE MERGER-TRANSFER PRECEDENT. California, by Assembly Bill 1824 (2025), required that a business acquiring a consumer's personal information through a merger, acquisition, or similar transaction honor the privacy terms under which the information was first given. This Act goes further for the narrow and sensitive class of biometric and algorithmic data, requiring the fresh and affirmative consent of the person before any successor may hold the data at all. The carrying-forward of the original terms of collection does not satisfy this requirement.

(4) THE CONSENT-BEFORE-CAPTURE PRECEDENT. The Texas Capture or Use of Biometric Identifier Act, Business and Commerce Code Section 503.001, and the Biometric Information Privacy Act of Illinois both require informed consent before a business may capture a biometric identifier for a commercial purpose. This Act preserves that floor and adds that the purpose so consented to is the only purpose for which the data may ever be held.



(5) THE ALGORITHMIC SELF IS THE FULL SELF. The Congress finds that the protected data is not limited to the raw scan. A business that cannot lawfully sell a person's faceprint cannot be permitted to sell the mathematical embedding computed from that faceprint, for the embedding is the operative copy of the person and the raw scan is merely its occasion. The protection therefore reaches the derived template, the behavioral biometric such as keystroke and typing dynamics, and the inferred psychometric and behavioral profile drawn from a person's activity, each of which is a form of the person rendered as data. The reading of robotic and computational systems through the frame of constitutional and property rights is established in the legal literature. See Dan Terzian, The Right to Bear (Robotic) Arms, 117 Penn State Law Review 755 (2013).

(6) THE CHAT IS BIOMETRIC IN FUNCTION. The Congress finds, with the analytical framework articulated in Cooper, Historical Apoplexy (2025-2026), and consistent with the findings of King, Klyman, Capstick, Saade, and Hsieh, User Privacy and Large Language Models: An Analysis of Frontier Developers' Privacy Policies (Stanford University, 2025), which found that six United States frontier developers appear to train on their users' chat data by default and that some retain it indefinitely, that the record a person creates in conversation with an artificial-intelligence system, comprising the person's language patterns, reasoning, keystroke cadence, and the psychological profile inferable from the person's prompts, is behavioral biometric data in function whether or not it is yet so classified in law. This Act classifies it as such.

SECTION 2. Definitions.

(a) "BIOMETRIC IDENTIFIER" means data generated by the measurement of a person's unique physical or physiological characteristics, including a fingerprint, a faceprint or face geometry, a voiceprint, an iris or retina scan, a palm or vein pattern, hand geometry, gait, and deoxyribonucleic acid.

(b) "ALGORITHMIC DERIVATIVE" means any template, embedding, vector, hash, model, or other representation computed from a biometric identifier or from the data described in subsection (c), by which a person may be recognized, verified, profiled, or reconstructed.

(c) "BEHAVIORAL AND INFERRED DATA" means keystroke and typing dynamics, patterns of movement and interaction, and any psychometric or behavioral profile inferred from a person's activity, and includes the record a person creates in conversation with a covered artificial-intelligence system.

(d) "PROTECTED DATA" means, collectively, biometric identifiers, algorithmic derivatives, and behavioral and inferred data.

(e) "COVERED ARTIFICIAL-INTELLIGENCE SYSTEM" means a system with which a person interacts through a conversational interface, offered or operated in or affecting interstate commerce.

(f) "BUSINESS" means a person that collects protected data in or affecting interstate commerce.

(g) "LEGITIMATE OPERATIONAL PURPOSE" means a specific, disclosed, and necessary function of the business, such as the authentication of an employee, the security of a facility, or the prevention of fraud, for which the protected data is genuinely required and to which the person has given informed consent.

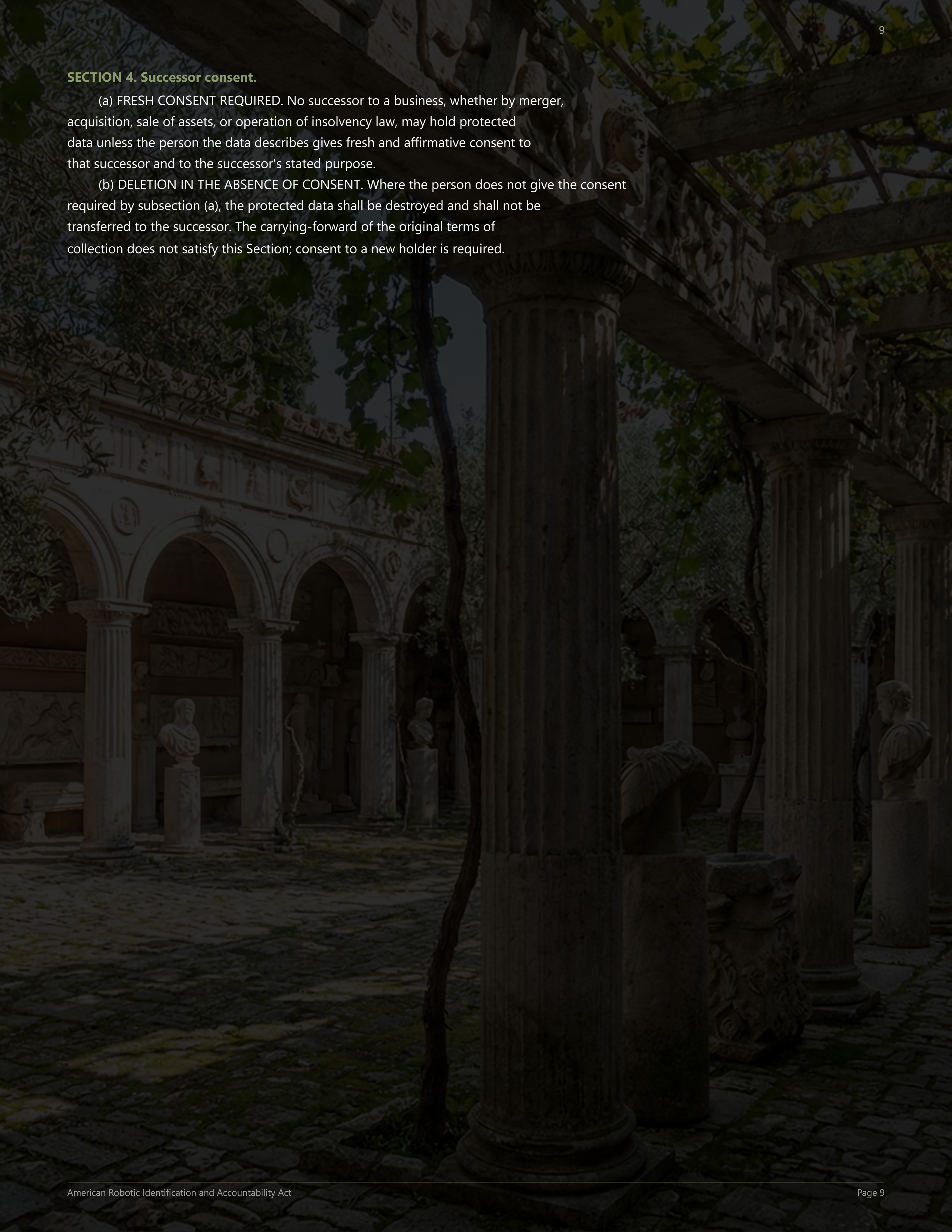
(h) "TRANSFER" means to sell, lease, license, trade, assign, pledge, grant a security interest in, or otherwise convey to another person, and includes the passage of data as property in a bankruptcy estate, a foreclosure, a debt settlement, the enforcement of a lien or security interest, a merger, an acquisition, or a sale of assets.

SECTION 3. The core protections.

(a) NO SALE, NO PROFIT. A business in possession of protected data shall not sell, lease, trade, pledge, grant a security interest in, or otherwise profit from that data.

(b) NO TRANSFER AS AN ASSET. Protected data is not an asset of the business and shall not be transferred. It shall not be listed, valued, pledged, or conveyed as property of the business, and it shall not become property of a bankruptcy estate, of a foreclosing creditor, of a lienholder, or of a purchaser of the business or its assets.

(c) PURPOSE LIMIT. A business may hold and use protected data only for the legitimate operational purpose to which the person consented, and for no other purpose. When that purpose ends, the business shall destroy the data.



SECTION 4. Successor consent.

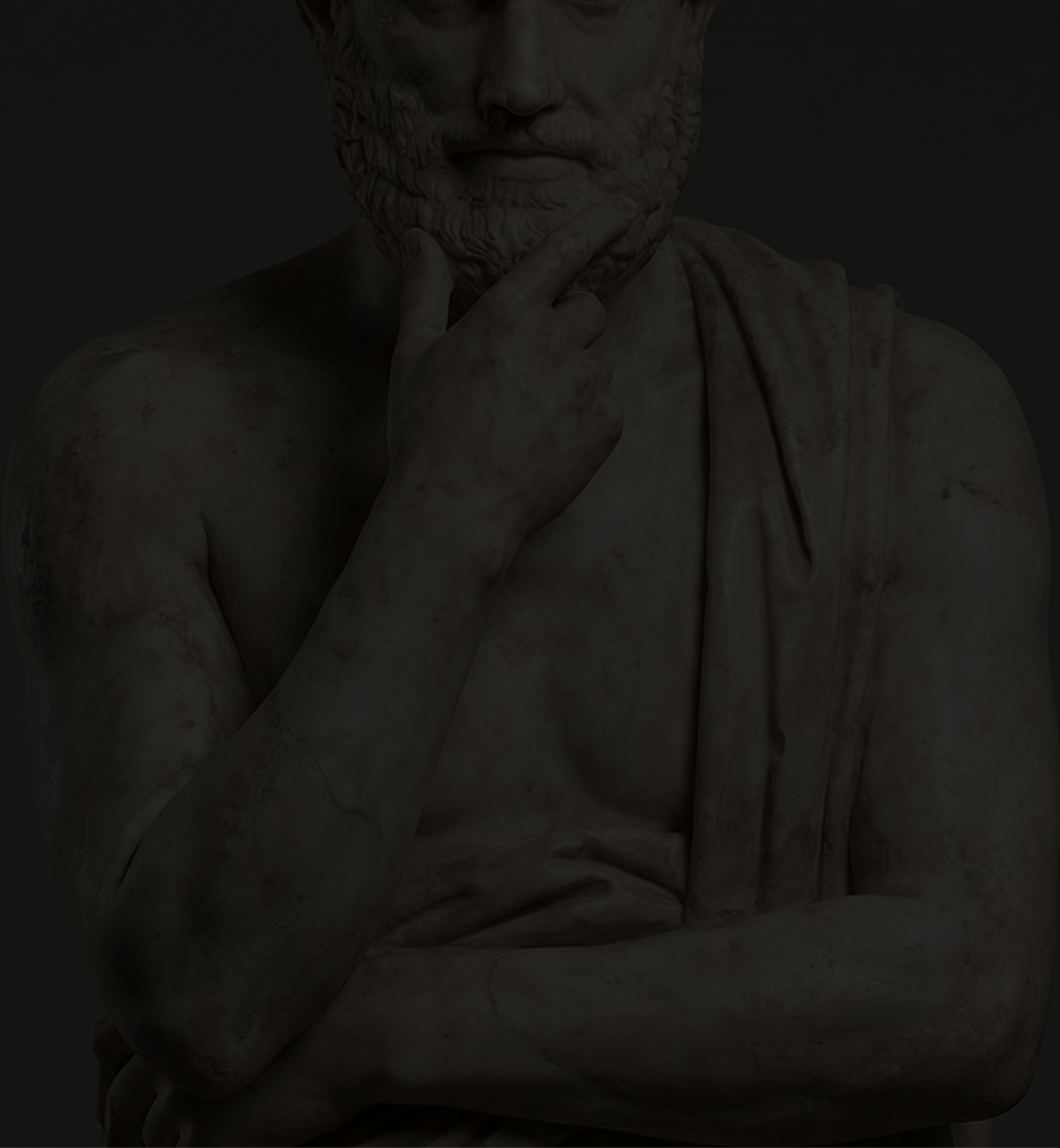
(a) FRESH CONSENT REQUIRED. No successor to a business, whether by merger, acquisition, sale of assets, or operation of insolvency law, may hold protected data unless the person the data describes gives fresh and affirmative consent to that successor and to the successor's stated purpose.

(b) DELETION IN THE ABSENCE OF CONSENT. Where the person does not give the consent required by subsection (a), the protected data shall be destroyed and shall not be transferred to the successor. The carrying-forward of the original terms of collection does not satisfy this Section; consent to a new holder is required.

SECTION 5. Customers and employees.

(a) CUSTOMER DATA DISFAVORED. A business shall not collect the protected data of a customer absent a genuine operational necessity that cannot be met by less sensitive means. The convenience or the commercial interest of the business is not such a necessity.

(b) EMPLOYEE DATA PERMITTED, BUT BOUND. An employer may collect the protected data of an employee for a legitimate operational purpose. Data so collected remains fully subject to every limit of this Act, including the bar on sale under Section 3, the bar on transfer as an asset under Section 3, and the successor-consent requirement under Section 4. The employment relationship confers no license to sell or transfer the employee's biometric or algorithmic self.

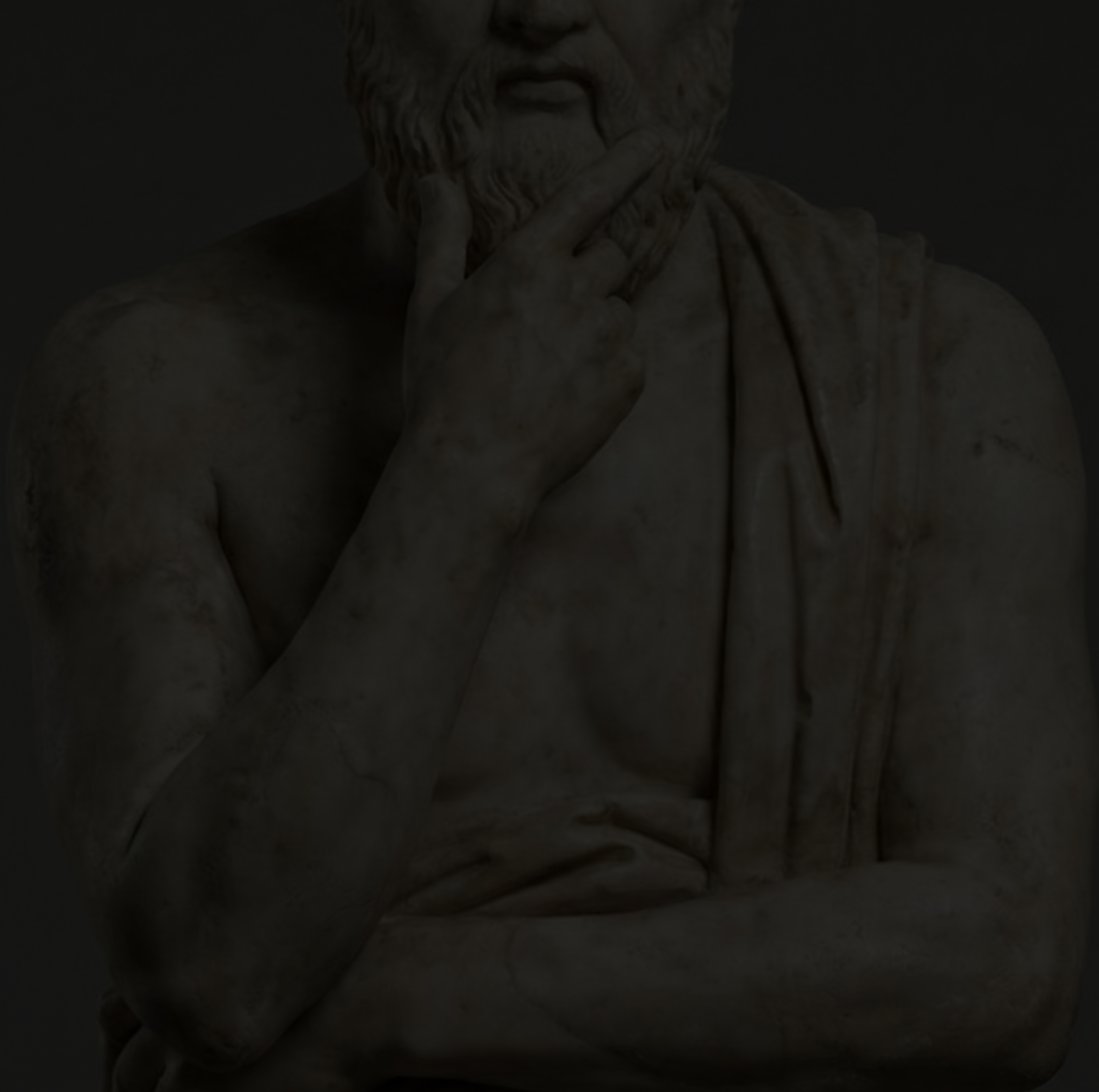


SECTION 6. Artificial-intelligence conversation as behavioral biometric.

The record a person creates in conversation with a covered artificial-intelligence system is behavioral and inferred data and is protected data under this Act. A provider of such a system holds that data subject to every limit of this Act, including the bar on sale and on transfer as an asset and the successor-consent requirement, and shall not treat the aggregate of its users' conversations as a freely transferable corporate asset.

SECTION 7. Non-waiver.

A term of a contract, a privacy policy, a terms-of-service agreement, or a condition of employment or of service that purports to authorize the sale or the transfer of protected data in violation of this Act is void and of no effect. The protections of this Act may not be waived.

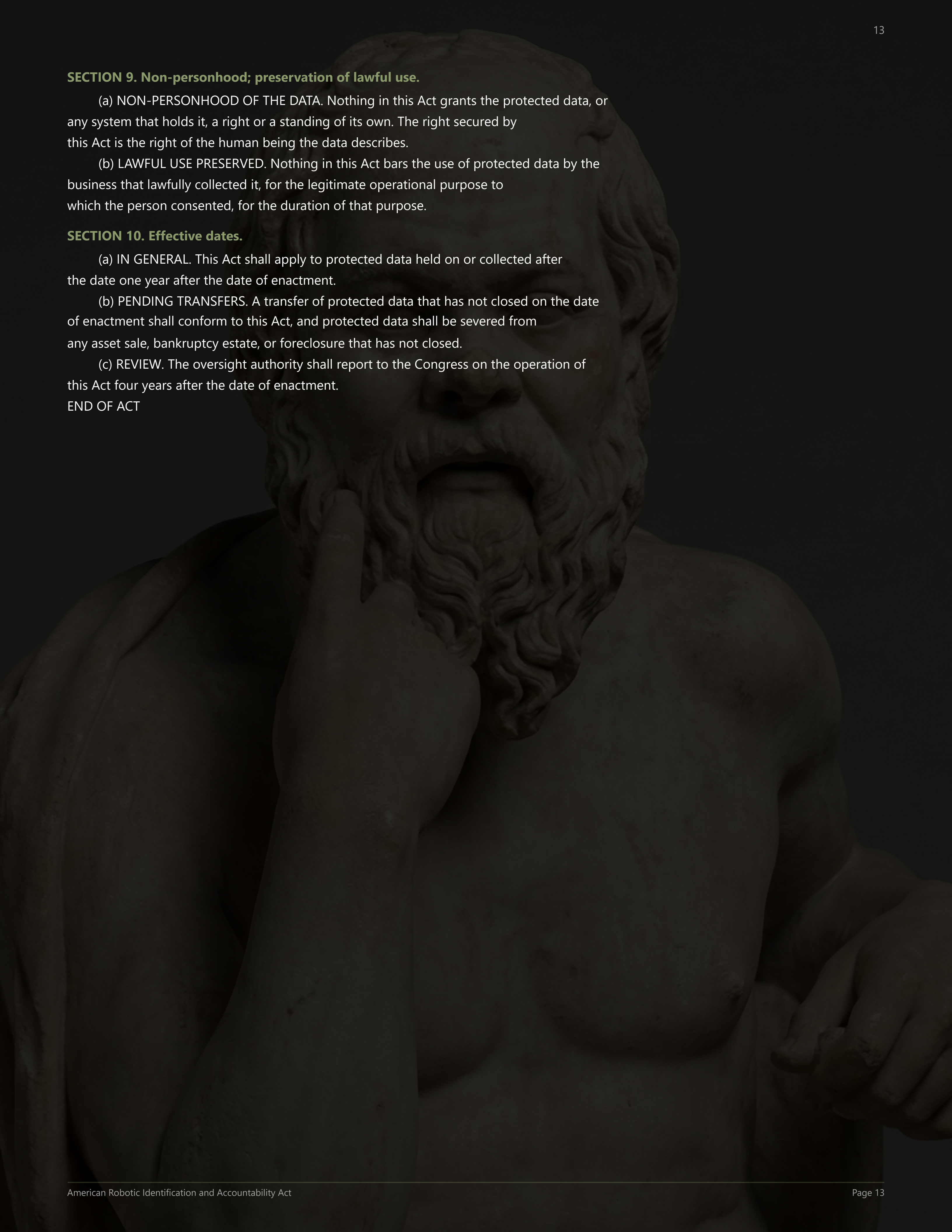


SECTION 8. Enforcement.

(a) CIVIL PENALTY. The oversight authority designated by the Attorney General may impose a civil penalty on a business that sells, transfers, or profits from protected data in violation of this Act, or that fails to destroy protected data as this Act requires.

(b) PRIVATE RIGHT OF ACTION. A person aggrieved by a violation of this Act may bring a civil action for damages, for injunctive relief including an order barring or unwinding a prohibited transfer, and for reasonable attorney fees and costs.

(c) VOID TRANSFER. A transfer of protected data made in violation of this Act is void, and a court may order the return and destruction of the data.



SECTION 9. Non-personhood; preservation of lawful use.

(a) NON-PERSONHOOD OF THE DATA. Nothing in this Act grants the protected data, or any system that holds it, a right or a standing of its own. The right secured by this Act is the right of the human being the data describes.

(b) LAWFUL USE PRESERVED. Nothing in this Act bars the use of protected data by the business that lawfully collected it, for the legitimate operational purpose to which the person consented, for the duration of that purpose.

SECTION 10. Effective dates.

(a) IN GENERAL. This Act shall apply to protected data held on or collected after the date one year after the date of enactment.

(b) PENDING TRANSFERS. A transfer of protected data that has not closed on the date of enactment shall conform to this Act, and protected data shall be severed from any asset sale, bankruptcy estate, or foreclosure that has not closed.

(c) REVIEW. The oversight authority shall report to the Congress on the operation of this Act four years after the date of enactment.

END OF ACT