

American Artificial Intelligence Freedom, Privacy, and Accountability Act of 2026

To establish a comprehensive federal framework for artificial intelligence governance, to enforce strict consumer privacy and data ownership rights under the Commerce Clause, to regulate the collection and deployment of data in algorithmic systems, and to foster responsible American technological innovation.

IN THE SENATE OF THE UNITED STATES

Sponsorship is required for introduction of the following bill to be read twice and referred to the listed Subcommittees:

- **Subcommittee on Intellectual Property**
- **Subcommittee on Privacy, Technology, and the Law**
- **Subcommittee on Consumer Protection, Product Safety, and Data Security**

Sponsorship is required for the introduction of the following bill to be read twice and referred to the listed Committees:

- **Senate Committee on Commerce, Science, and Transportation**
- **Senate Committee on the Judiciary**
- **Senate Committee on Homeland Security and Governmental Affairs (HSGAC)**

A BILL

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) Short Title.—This Act may be cited as the "**American Artificial Intelligence Freedom, Privacy, and Accountability Act of 2026**".

(b) Table of Contents.—

- **Sec. 1.** Short Title; Table of Contents
- **Sec. 2.** Definitions
- **Sec. 3.** Constitutional Boundaries & Individual Liberty Safeguards
- **Sec. 4.** Consumer Data Ownership, Minimization, & Consent Architecture
- **Sec. 5.** High-Impact & High-Performance AI Classifications
- **Sec. 6.** Transparency, Watermarking, & Right to Explanation
- **Sec. 7.** Corporate Accountability, Civil Liability, & Enforcement
- **Sec. 8.** Regulatory Agility & Sunset Clauses
- **Sec. 9.** National Preemption & Reserved State Authorities

SEC. 2. DEFINITIONS.

In this Act:

(1) **ARTIFICIAL INTELLIGENCE SYSTEM (AI SYSTEM).**—The term "Artificial Intelligence System" means an electronic, machine-based system that infers, from input data, how to generate outputs such as predictions, recommendations, content, or decisions affecting real or virtual environments, operating with varying levels of autonomy and adaptability. (*Cf. Executive Order 13960, 85 Fed. Reg. 78939; 15 U.S.C. 9401(3)*).

(2) **HIGH-IMPACT AI SYSTEM.**—The term "High-Impact AI System" means any AI system deployed in critical infrastructure (*as defined in 42 U.S.C. 5195c(e)*), medical care or devices (*regulated under 21 U.S.C. 360j*), employment screening (*subject to 42 U.S.C. 2000e et seq.*), credit evaluation (*regulated under 15 U.S.C. 1691 et seq.*), housing access (*regulated under 42 U.S.C. 3601 et seq.*), law enforcement, judicial proceedings, or public benefit determinations that materially influences outcomes affecting individual constitutional rights, physical safety, or economic security.

(3) **HIGH-PERFORMANCE AI SYSTEM (FRONTIER MODEL).**—The term "High-Performance AI System" means any foundational or generative AI model trained using a cumulative computational threshold exceeding 10^{26} floating-point operations (FLOPs). (*Cf. Executive Order 14110, 88 Fed. Reg. 75191*).

(4) **COVERED DATA.**—The term "Covered Data" means any personal information, biometric identifier, behavioral tracking data, precise geolocation data (*as referenced in 15 U.S.C. 45*), or user-generated content linkable to an identified or identifiable United States person.

(5) **BIOMETRIC IDENTIFIER.**—The term "Biometric Identifier" means physical, physiological, or behavioral characteristics used to identify an individual, including facial geometry, fingerprints, iris scans, voiceprints, or gait patterns. (*Cf. 740 ILCS 14/10*).

(6) **ALGORITHMIC DISCRIMINATION.**—The term "Algorithmic Discrimination" means the unlawful or unjustified differential treatment of individuals in civil rights, housing, employment, or public accommodations resulting from automated processing based on traits protected under Title VII of the Civil Rights Act of 1964 (42 U.S.C. 2000e et seq.) or the Fair Housing Act (42 U.S.C. 3601 et seq.).

SEC. 3. CONSTITUTIONAL BOUNDARIES & INDIVIDUAL LIBERTY SAFEGUARDS.

(a) Fourth Amendment Protections Against Warrantless AI Surveillance.—

1. **Government Use Restriction.**—No federal agency, nor state or local entity receiving federal funds, shall deploy real-time facial recognition, biometric identification, or predictive policing AI systems in public spaces without a warrant issued by a neutral magistrate upon a finding of probable cause under the Fourth Amendment to the United States Constitution. (*See Carpenter v. United States*, 585 U.S. 296 (2018); *Kyollo v. United States*, 533 U.S. 27 (2001)).
2. **Prohibition on Data Purchases.**—No government agency shall purchase, lease, or acquire Covered Data from commercial data brokers to circumvent warrant requirements or build warrantless surveillance databases. (*Cf. Fourth Amendment Is Not For Sale Act*, H.R. 4639 / S. 4006, 118th Cong.).

(b) First Amendment Guardrails Against Government Coercion.—

1. **No Censorship Mandates.**—The Federal Government shall not compel, pressure, or incentivize any private AI system developer or deployer to suppress, steer, filter, or censor constitutionally protected speech or lawful political expression within an AI model's training data or inference output. (*See National Institute of Family and Life Advocates v. Becerra*, 585 U.S. 755 (2018); *Murthy v. Missouri*, 603 U.S. ____ (2024)).
2. **User Preference Autonomy.**—Individuals retain the right under the First Amendment to deploy, modify, or interact with open-source or custom-configured AI models reflecting their own political, religious, or ideological views, provided such models do not facilitate federal criminal activity under Title 18, United States Code.

SEC. 4. CONSUMER DATA OWNERSHIP, MINIMIZATION, & CONSENT ARCHITECTURE.

(a) Data Minimization Mandate.—

1. **Collection Limits.**—Covered entities shall collect, retain, or process only the minimum amount of Covered Data strictly necessary to deliver a specific, explicit product or service requested by the consumer. (*Cf. FTC Act Section 5, 15 U.S.C. 45; American Data Privacy and Protection Act, H.R. 8152, 117th Cong.*).
2. **Prohibition on Training-by-Default.**—No developer or deployer shall utilize a consumer's private communications, personal photos, document uploads, or proprietary inputs to train commercial or foundational AI models without obtaining express, unbundled, opt-in consent.

(b) Consumer Rights Architecture.—

1. **Right to Opt-Out & Erasure.**—Consumers retain the absolute right to opt out of data collection and demand the prompt, complete deletion of their Covered Data from active inference pipelines and future training datasets. (*Cf. Cal. Civ. Code § 1798.105*).
2. **Protection Against Unauthorized Digital Replicas.**—It shall be unlawful to synthesize or deploy an individual's digital likeness, voice, or biometric profile to create a synthetic replica without prior, written consent. (*Cf. NO FAKES Act, S. 4875, 118th Cong.; 17 U.S.C. 101 et seq.*). Unauthorized commercial exploitation shall constitute direct infringement subject to statutory damages under Section 7 of this Act.

SEC. 5. HIGH-IMPACT & HIGH-PERFORMANCE AI CLASSIFICATIONS.

(a) Requirements for High-Impact AI Deployers.—

Deployers of High-Impact AI systems shall:

1. Conduct annual pre-deployment impact assessments evaluating algorithmic bias, safety vulnerabilities, and data integrity. (*Cf. National Institute of Standards and Technology (NIST) AI Risk Management Framework 1.0, Special Publication 1270*).
2. Maintain **Meaningful Human Oversight** mechanisms that ensure qualified human personnel retain the authority to review and override automated decisions in healthcare, lending, employment, and law enforcement. (*Cf. EEOC Select Task Force Guidance on AI, 42 U.S.C. 2000e-2*).

(b) Safety Protocols for High-Performance AI Developers.—

Developers of High-Performance AI systems ($>10^{26}$ FLOPs) shall:

1. Implement independent adversarial testing ("Red-Teaming") to assess risks relating to chemical, biological, radiological, or nuclear (CBRN) threat generation or cyber-attack acceleration. (*Cf. 50 U.S.C. 4301 et seq.; E.O. 14110*).
2. Maintain rigorous cybersecurity key management standards (*compliant with NIST FIPS 140-3*) to safeguard model weights against exfiltration by foreign adversaries under the Export Control Reform Act (*50 U.S.C. 4801 et seq.*).

SEC. 6. TRANSPARENCY, WATERMARKING, & RIGHT TO EXPLANATION.

(a) Synthetic Content Identification.—

1. **Cryptographic Watermarking.**—Developers of generative AI models producing visual, audio, or multi-modal synthetic media shall embed imperceptible, cryptographically verifiable watermarks into generated outputs. (*Cf. C2PA Coalition Standards; 15 U.S.C. 45*).
2. **User Disclosures.**—Platforms serving AI-generated media that reasonably resembles real human beings or actual events must display clear, conspicuous user-facing disclosures identifying the content's synthetic origin.

(b) Right to Explanation.—

1. In any case where an individual is subjected to an adverse outcome influenced by a High-Impact AI system (including loan denials under 15 U.S.C. 1691(d), employment rejections under 42 U.S.C. 2000e-2, or benefit cutoffs), the deployer shall provide a written, plain-language explanation of the primary variables, decision logic, and data points used to arrive at the decision within 30 days.

SEC. 7. CORPORATE ACCOUNTABILITY, CIVIL LIABILITY, & ENFORCEMENT.

(a) Duty of Care & Liability Rules.—

1. **Standard of Care.**—AI system developers and deployers owe a statutory duty of care under federal common law to design, test, and maintain systems to prevent foreseeable severe financial, physical, or constitutional injuries.
2. **Downstream Modification Exemption.**—An upstream developer of an open-source or general-purpose AI model shall not be liable for damages resulting from a downstream third party's unauthorized alteration, un-censoring, or intentional illegal misuse of the model, provided the original model complied with federal safety standards upon release. (*Cf. 47 U.S.C. 230(c)(1) principle adaptation*).

(b) Enforcement Structure.—

1. **Federal Trade Commission Authority.**—The Federal Trade Commission (FTC) shall enforce compliance with this Act under Section 5 of the Federal Trade Commission Act (*15 U.S.C. 45*) regarding unfair or deceptive acts or practices.
2. **Private Right of Action.**—Any individual whose statutory privacy, likeness, or Fourth Amendment rights under this Act are directly violated may bring a civil action in an appropriate United States district court (*pursuant to 28 U.S.C. 1331*) for actual damages or statutory damages up to \$10,000 per violation, plus reasonable attorney fees. (*Cf. 18 U.S.C. 2710; 47 U.S.C. 227*).

SEC. 8. REGULATORY AGILITY & SUNSET CLAUSES.

(a) Dynamic Compute & Metric Audits.—

The Federal Trade Commission, in consultation with the Director of the National Institute of Standards and Technology (NIST) (*pursuant to 15 U.S.C. 272*), shall review and adjust technical metrics (including the 10^{26} FLOPs training threshold) every 24 months to account for advancements in hardware performance and algorithmic efficiency.

(b) Technical Sunset.—

The regulatory requirements under Sections 5 and 6 shall expire 5 years after the date of enactment pursuant to formal congressional review under the Congressional Review Act (*5 U.S.C. 801 et seq.*), unless explicitly reauthorized by Congress following a formal audit of market conditions and technical developments.

SEC. 9. NATIONAL PREEMPTION & RESERVED STATE AUTHORITIES.

(a) National Standard.—This Act preempts state laws or local ordinances to the extent they establish conflicting commercial AI deployment registries, algorithmic disclosures, or technical

standards for interstate commerce under Article I, Section 8, Clause 3 of the United States Constitution.

(b) Preserved State Authorities.—Nothing in this Act shall be construed to diminish or preempt state constitutional privacy rights, general state consumer protection statutes (*e.g.*, *Cal. Civ. Code § 1798.100 et seq.*; *N.Y. Gen. Bus. Law § 349*), local police powers, or state common law tort liabilities. (*See Wyeth v. Levine*, 555 U.S. 555 (2009)).

References:

Image generated using Google Gemini in response to the prompt: 'Generate an image that captures the American spirit of this Bill. Google. (2026). *Gemini* (Aug 19 version) [Large language model]. <https://gemini.google.com>