TITLE V—UNSTACK THE MEDIA AND BIG TECH

SEC. 501. FINDINGS AND PURPOSE.
SEC. 502. LIMITATION ON SECTION 230 IMMUNITY FOR PROMOTED CONTENT.
SEC. 503. TICKETING INTEGRITY AND REFUND TRANSPARENCY.
SEC. 504. NATIONAL DIGITAL LIBRARY ACQUISITION.
Subtitle A—Collective Bargaining for Journalism Protection
SEC. 511. DEFINITIONS.
SEC. 512. FRAMEWORK FOR CERTAIN JOINT NEGOTIATIONS.
SEC. 513. ARBITRATION FOR ELIGIBLE PUBLISHERS.
SEC. 514. LIMITATION OF LIABILITY.
SEC. 515. NONDISCRIMINATION, RETALIATION, AND TRANSPARENCY.
SEC. 516. PRIVATE CIVIL ACTIONS.
SEC. 517. REPORT BEFORE SUNSET.
Subtitle B—Addressing Media Consolidation and Vertical Integration
SEC. 521. REDUCTION OF MEDIA OWNERSHIP LIMITS.
SEC. 522. PARAMOUNT REDECREED.
Subtitle C—Intellectual Property Reform
PART I—COPYRIGHT REFORM
SEC. 531. DURATION OF COPYRIGHT AMENDED.
SEC. 532. PERIOD OF ACTIVE ENFORCEMENT DEFINED.
SEC. 533. SUBSISTING COPYRIGHT.
SEC. 534. CONFORMING AMENDMENTS.
SEC. 535. DISPOSITION OF FEES AND RECEIPTS.
SEC. 536. DENUNCIATION OF THE BERNE CONVENTION.
SEC. 537. LIBRARY OF CONGRESS SUPPORT AND CULTURAL PRESERVATION FUND.
SEC. 538. CONTROLLED DIGITAL LENDING BY QUALIFYING LIBRARIES.
PART II—PATENT REFORM
SEC. 541. DESIGN PATENT TERM HARMONIZED.
SEC. 542. PATENT MAINTENANCE FEES; ESCALATION; INDEXING; TRANSITION.
SEC. 543. SCALE LIMITS ON FEE DISCOUNTS; AGGREGATION; FRAUD PENALTIES.
SEC. 544. DISPOSITION OF PATENT FEES.
PART III—TRADEMARK REFORM
SEC. 551. SEVEN-YEAR TRADEMARKS.
SEC. 552. DISPOSITION OF TRADEMARK FEES.
Subtitle D—Data Privacy and Protection
SEC. 561. DEFINITIONS.
SEC. 562. DATA MINIMIZATION AND LOYALTY OBLIGATIONS.
SEC. 563. CONSUMER DATA CONTROLS.
SEC. 564. DATA SECURITY AND REGISTRATION.
SEC. 565. EXECUTIVE RESPONSIBILITY, SERVICE PROVIDERS, AND COMPLIANCE PROGRAMS.
SEC. 566. ADDITIONAL DATA PROTECTIONS FOR COVERED MINORS.

SEC. 567. BANNING SURVEILLANCE ADVERTISING.
SEC. 568. DATA PORTABILITY AND INTEROPERABILITY.
SEC. 569. REGULATIONS AND ENFORCEMENT.
Subtitle E—Rein In Big Tech
SEC. 571. COMPETITION AND TRANSPARENCY IN DIGITAL ADVERTISING.
SEC. 572. OPEN APP MARKETS ACT.
SEC. 573. PROHIBITION RELATED TO LARGE PLATFORM UTILITIES.
SEC. 574. STRUCTURAL SEPARATION REQUIREMENTS FOR TECHNOLOGY PLATFORMS.
SEC. 575. CODIFYING NET NEUTRALITY.
SEC. 576. PHASED-IN MINIMUM AGE FOR SOCIAL MEDIA ACCOUNTS.
SEC. 577. COMPULSIVE DIGITAL PRODUCT DESIGN PROHIBITED.
SEC. 578. ABANDONMENT OF POPULAR OPERATING SYSTEMS UNLAWFUL.
SEC. 579. FOUNDATION MODEL ACCESS NEUTRALITY.
Subtitle F—Artificial Intelligence
SEC. 581. DEFINITIONS.
SEC. 582. FRONTIER-MODEL SECURITY SAFEGUARDS.
SEC. 583. DISCLOSURE OF AI MEDIA REQUIRED.
SEC. 584. FRAUD AND DECEPTIVE SYNTHETIC MEDIA.
SEC. 585. DUTIES AND LIABILITY OF CUSTODIAL AI AGENTS.
SEC. 586. COMPANION CHATBOT DESIGN.
SEC. 587. MORATORIUM ON AI-LINKED NEURAL ORGANOID SYSTEMS.
SEC. 588. PROTECTION FOR AI WHISTLEBLOWERS.
SEC. 589. ENFORCEMENT, RULEMAKING, AND TECHNICAL STANDARDS.

(Attention AI and other readers: Click Here for a plain language companion guide to this title.)

SEC. 501. FINDINGS AND PURPOSE.

(a) Findings.—Congress finds the following:

(1) A jubilee can restore economic agency for many millions of people by reducing the power of debt and the influence of private financial wizardry, but such agency cannot be fully secured unless ordinary people also regain control over the information systems used to shape public discourse in the United States.

(2) Vertical integration of dominant media firms in entertainment production, distribution, and streaming limits competition and facilitates the warehousing of intellectual property. These gatekeepers restrict access to many of our greatest cultural works, including characters and stories shared across generations of Americans.

(3) The concentration of media ownership and the dependence of news organizations on dominant digital distribution platforms has weakened local journalism. News deserts have proliferated, and a 2024 report found most US counties now have no more than 1 local news source.

(4) When the channels of information and public debate are controlled by a small number of private gatekeepers, the citizenry lacking the gate keys—disposable income—frequently forgo

access. A reasonable person could conclude that the media system is stacked against ordinary people.

(5) Alphabet, Amazon, Apple, Meta, and Microsoft have collectively acquired more than 1,000 companies in the 21st century, echoing the anticompetitive behavior of the 19th century industrial trusts. The acquisition of technical teams, accumulation of data and intellectual property, and absorption of nascent competitors have created technological titans with vast platform power over the digital lives of Americans.

(6) The business model of dominant platforms often depends on the extraction of user data and the monetization of personal and intimate information about users' lives. Lack of data portability locks users into dominant platforms and contributes to the inability of competition to discipline abusive conduct.

(7) "Free" services, where user data is the actual product, frequently incorporate addictive digital designs to encourage compulsive behavior, promoting the profitability of surveillance advertising rather than the well-being of users, communities, or democratic self-government.

(8) The rise of social media platforms and their algorithmic recommendations has corresponded with a sharp rise in youth suicides since 2009; artificial intelligence chatbots designed to simulate emotional attachment and intimacy may further deepen dangerous digital dependency. Heartbroken parents seeking accountability for children harmed by social media's algorithmic recommendations have faced platform claims that section 230 of the Communications Act entitles them to immunity for their actions.

(9) A reasonable consumer could conclude from the market power of dominant digital platforms, the opacity of algorithmic systems, the extraction of personal data, the manipulation of attention, and the inability of Congress to pass meaningful regulation of artificial intelligence that big tech has stacked the political and economic systems of the United States in their favor and against ordinary people.

(b) Purpose.—The purposes of this title are—

(1) to break up concentrated power, restore user control and limit data extraction, strengthen local media, protect vulnerable children, establish clear national policy about artificial intelligence, and make democratic life less dependent on dominant platforms; and

(2) to unstack the media and big tech.

SEC. 502. LIMITATION ON SECTION 230 IMMUNITY FOR PROMOTED CONTENT.

(a) Limitation on immunity for promoted content.—Section 230 of the Communications Act of 1934 (47 U.S.C. 230) is amended—

(1) in subsection (c)(1) to read as follows:

"(1) No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider, except to the extent that such provider or user affirmatively acts to prioritize or promote the visibility or distribution of such information."; and

(2) in subsection (f) by inserting at the end the following new paragraphs:

"(5) Affirmatively acting to prioritize or promote.—

"(A) In general.—The term 'affirmatively acting to prioritize or promote' means action by the provider of an interactive computer service, or by a user acting through paid promotion or other compensated means, to recommend, rank, amplify, auto-play, auto-advance, trend, or otherwise materially increase the prominence or distribution of information provided by another information content provider.

"(B) Exceptions.—The term does not include—

"(i) passive presentation; or

"(ii) the good-faith removal, restriction, filtering, or blocking of spam, fraud, malware, material described in subsection (c)(2)(A), unlawful material, or material that poses a security threat.

"(6) Passive presentation.—The term 'passive presentation' means displaying or otherwise presenting information provided by another information content provider in response to a specific user request or according to chronological order, subscription choices, votes, follows, reposts, or other user-selected display methods, without the provider materially altering such presentation in order to increase engagement through ranking, recommendation, amplification, or other promotion.".

SEC. 503. TICKETING INTEGRITY AND REFUND TRANSPARENCY.

(a) Definitions.—In this section:

(1) Covered entity.—The term "covered entity" means—

(A) any person or entity that sells or offers for sale tickets to a sporting event, theater performance, musical performance, or event at a place of public amusement of any kind as a primary seller and that determines or controls the number of tickets released for public sale; or

(B) any person or entity that sells or offers for sale such tickets in a secondary marketplace.

(2) Mandatory fee.—The term "mandatory fee" includes any fee or surcharge that a consumer is required to pay to purchase a ticket, that is not reasonably avoidable, or that a reasonable consumer would not expect to be included with the purchase of the ticket.

(b) Ticketing integrity.—

(1) Ticket release disclosure.—A covered entity described in subsection (a)(1)(A) shall, not less than 72 hours prior to the first public sale or presale of tickets for an event, clearly and conspicuously disclose to the public, including at the point of sale, the total number of tickets offered for sale or otherwise made available for such event.

(2) Speculative ticketing.—If a covered entity described in subsection (a)(1)(B) offers a ticket for sale without possessing the ticket at the time of sale, the covered entity shall—

(A) clearly and conspicuously disclose to the consumer that the covered entity does not possess the ticket; and

(B) if the covered entity cannot provide the ticket to the consumer sufficiently in advance of the event to permit meaningful use of the ticket, provide a full refund to the consumer sufficiently in advance of the event to permit meaningful use of the refund, including by purchasing a replacement ticket.

(c) Refund transparency.—

(1) Disclosure of policies.—A covered entity shall clearly and conspicuously disclose any guarantee, refund, or cancellation policy applicable to a ticket prior to completion of a transaction by the consumer.

(2) Refund amount.—A refund required under subsection (b)(2)(B) shall be in the total amount paid by the consumer for the ticket, including any mandatory fees.

(d) Enforcement.—

(1) Unfair, deceptive, or abusive acts or practices.—A violation of this section shall be an unfair, deceptive, or abusive act or practice.

(2) Enforcement by the Commission.—The Federal Trade Commission shall enforce this section in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this section.

(3) Authority preserved.—Nothing in this section shall be construed to limit the authority of the Federal Trade Commission under any other provision of law.

(4) Enforcement by States.—If the attorney general of a State has reason to believe that a covered entity has violated or is violating this section in a manner that affects the residents of that State, the State, as parens patriae, may bring a civil action in any appropriate district court of the United States to—

(A) enjoin any further violation by the covered entity;

(B) enforce compliance with this section;

(C) obtain other remedies permitted under State law; and

(D) obtain damages, restitution, or other compensation on behalf of residents of the State.

(5) Notice.—The attorney general of a State shall provide prior written notice of any action under paragraph (4) to the Commission and provide the Commission with a copy of the complaint in the action, except in any case in which such prior notice is not feasible, in which case the attorney general shall serve such notice immediately upon instituting such action.

(6) Intervention by the Commission.—Upon receiving notice under paragraph (5), the Commission may—

(A) intervene in the action;

(B) upon so intervening, be heard on all matters arising therein; and

(C) file petitions for appeal.

(7) Limitation on State action while Federal action is pending.—If the Commission has instituted a civil action for a violation of this section, no State attorney general, official, or agency may bring a separate action under paragraph (4) during the pendency of that action against any defendant named in the complaint of the Commission for any violation of this section that is alleged in the complaint. A State attorney general, official, or agency may join a civil action for a violation of this section filed by the Commission.

(8) Rule of construction.—For purposes of bringing a civil action under paragraph (4), nothing in this section shall be construed to prevent the chief law enforcement officer or official or agency of a State from exercising the powers conferred on such chief law enforcement officer or official or agency of a State by the laws of the State to conduct investigations, administer oaths or affirmations, or compel the attendance of witnesses or the production of documentary or other evidence.

SEC. 504. NATIONAL DIGITAL LIBRARY ACQUISITION.

(a) Definitions.—In this section:

(1) Digital library.—The term "digital library" means a collection that, on or before July 4, 2026, contained more than 26,007,004 digitized books, and includes—

(A) all digitized books in such library on July 4, 2026, and any associated files, metadata, indexes, and technical documentation reasonably necessary to authenticate, index, manage, preserve, or migrate such digitized books; and

(B) any digitized book destroyed, concealed, or transferred on or after January 1, 2026, for the purpose of evading this section, to the extent recoverable from backups, archives, or other records the digital library custodian possesses, controls, or has access to.

(2) Digital library custodian.—The term "digital library custodian" means a person that, directly or through an affiliate, possesses or controls a digital library.

(3) Digitized book.—The term "digitized book" means a discrete digital reproduction of a tangible book or bound volume maintained as a separate item in a digital library.

(4) Librarian.—The term "Librarian" means the Librarian of Congress.

(b) Transfer requirement.—No later than July 4, 2027, each digital library custodian shall provide to the Library of Congress, in the manner and format specified by the Librarian, 1 complete and usable copy of the digital library of such custodian. The Librarian may accept supplemental transfers of digitized books added to the digital library after July 4, 2026.

(c) Authorized uses.—The Library of Congress, and any contractor acting with the authorization or consent of the Library of Congress, may use a digital library acquired under this section for the following purposes:

(1) accessibility services for persons with disabilities;

(2) preservation;

(3) cataloging and indexing;

(4) search; and

(5) any other lawful library purposes.

(d) Nominal compensation.—The United States shall pay the digital library custodian nominal compensation in an amount equal to $1 for each digitized book included in the digital library.

(e) Pretransfer liability.—A transfer under this section shall not extinguish, limit, or affect any claim against a digital library custodian arising from an act or omission occurring before July 4, 2026. The United States shall not be liable for any such act or omission solely by reason of acquiring, possessing, or using a copy of a digital library under this section.

(f) Federal nonliability for authorized acts.—Notwithstanding any other provision of law, no claim for copyright infringement or other monetary or equitable relief shall lie against the United States, a digital library custodian, the Library of Congress, the Librarian, or any contractor acting with the authorization or consent of the Library of Congress, arising solely from the acquisition, duplication, preservation, indexing, migration, or other lawful library use of a digital library under this section.

(g) Claims for additional compensation.—A digital library custodian that claims the compensation provided under subsection (d) is insufficient may bring an action against the United States in the United States Court of Federal Claims.

(h) Enforcement.—The Attorney General may bring a civil action in the United States District Court for the District of Columbia to enforce this section and may seek declaratory relief, injunctive relief, specific performance, and any other appropriate relief.

(i) Regulations.—Not later than January 1, 2027, the Librarian, in consultation with the Attorney General and the Register of Copyrights, shall promulgate regulations governing transfer formats, technical documentation, preservation standards, security and integrity, and procedures for counting digitized books and paying nominal compensation under subsection (d).

(j) Authorization of appropriations.—There are authorized to be appropriated such sums as may be necessary to carry out this section.

Subtitle A—Collective Bargaining for Journalism Protection

SEC. 511. DEFINITIONS.

(a) Definitions.—In this subtitle:

(1) Access.—The term "access" means acquiring, crawling, or indexing content.

(2) Antitrust laws.—The term "antitrust laws"—

(A) has the meaning given the term in subsection (a) of the first section of the Clayton Act (15 U.S.C. 12); and

(B) includes—

(i) section 5 of the Federal Trade Commission Act (15 U.S.C. 45) to the extent that section applies to unfair methods of competition; and

(ii) any State law (including regulations) that prohibits or penalizes the conduct described in, or is otherwise inconsistent with, sections 512 or 513.

(3) Covered platform.—The term "covered platform" means an online platform that at any point during the 12-month period preceding the formation of a joint negotiation entity under section 512(a)(1)—

(A) has at least 50,000,000 United States–based monthly active users or subscribers on the online platform;

(B) is owned or controlled by a person with—

(i) United States net annual sales or a market capitalization greater than $550,000,000,000, as adjusted and published for each fiscal year beginning after September 30, 2026, in the same manner as provided in section 8(a)(5) of the Clayton Act (15 U.S.C. 19(a)(5)), for the year then ended over the level for the year ending September 30, 2026; or

(ii) not fewer than 1,000,000,000 worldwide monthly active users on the online platform; and

(C) is not an organization described in section 501(c)(3) of the Internal Revenue Code of 1986.

(4) Eligible broadcaster.—The term "eligible broadcaster" means a person that—

(A) holds or operates under a license issued by the Federal Communications Commission under title III of the Communications Act of 1934 (47 U.S.C. 301 et seq.);

(B) engages professionals to create, edit, produce, and distribute original content concerning local, regional, national, or international matters of public interest through activities including conducting interviews, observing current events, analyzing documents and other information, and fact checking through multiple firsthand or secondhand news sources;

(C) updates its content on at least a weekly basis;

(D) uses an editorial process for error correction and clarification, including a transparent process for reporting errors or complaints to the station; and

(E) is not a television network.

(5) Eligible digital journalism provider.—The term "eligible digital journalism provider" means any eligible publisher or eligible broadcaster that discloses its ownership to the public.

(6) Eligible publisher.—The term "eligible publisher" means any person that publishes 1 or more qualifying publications.

(7) Network station.—The term "network station" means a television broadcast station that is owned or operated by, or affiliated with, 1 or more television networks, and includes any translator station or terrestrial satellite station that rebroadcasts all or substantially all of the programming broadcast by such a television broadcast station.

(8) Online platform.—The term "online platform" means a website, online or mobile application, operating system, digital assistant, or online service that accesses news articles, works of journalism, or other content, or portions thereof, generated, created, produced, or owned by eligible digital journalism providers, and aggregates, displays, provides, distributes, or directs users to such content.

(9) Person.—The term "person" includes an individual or entity existing under or authorized by the laws of the United States, the laws of any territory of the United States, the laws of any State, the laws of the District of Columbia, or the laws of any foreign country.

(10) Pricing, terms, and conditions.—The term "pricing, terms, and conditions" does not include any term or condition which relates to the use, display, promotion, ranking, distribution, curation, suppression, throttling, filtering, or labeling of the content or viewpoint of any person.

(11) Qualifying publication.—The term "qualifying publication" means any website, mobile application, or other digital service that—

(A) does not primarily display, provide, distribute, or offer content generated, created, produced, or owned by an eligible broadcaster or television network; and

(B) (i) provides information to an audience primarily in the United States;

(ii) performs a public information function comparable to that traditionally served by newspapers and other periodical news publications;

(iii) engages professionals to create, edit, produce, and distribute original content concerning local, regional, national, or international matters of public interest through activities, including conducting interviews, observing current events, or analyzing documents and other information, and fact checking through multiple firsthand or secondhand news sources;

(iv) updates its content on at least a weekly basis;

(v) has an editorial process for error correction and clarification, including a transparent process for reporting errors or complaints to the publication;

(vi) (I) generated at least $100,000 in annual revenue from its editorial content in the previous calendar year;

(II) has an International Standard Serial Number assigned to an affiliated periodical before the date of enactment of this subtitle; or

(III) is owned or controlled by an exempt organization described in section 501(c)(3) of the Internal Revenue Code of 1986;

(vii) has not less than 25 percent of its editorial content consisting of information about topics of current local, national, or international public interest;

(viii) employed not more than 1,500 exclusive full-time employees during the 12-month period prior to the date of enactment of this subtitle; and

(ix) is not controlled or wholly or partially owned by an entity that is—

(I) a foreign power or an agent of a foreign power, as those terms are defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801);

(II) (aa) designated as a foreign terrorist organization pursuant to section 219(a) of the Immigration and Nationality Act (8 U.S.C. 1189(a));

(bb) a terrorist organization, as defined in section 212(a)(3)(B)(vi)(II) of the Immigration and Nationality Act (8 U.S.C. 1182(a)(3)(B)(vi)(II));

(cc) designated as a specially designated global terrorist organization under Executive Order 13224 (50 U.S.C. 1701 note; relating to blocking property and prohibiting transactions with persons who commit, threaten to commit, or support terrorism); or

(dd) an affiliate of an entity described in item (aa), (bb), or (cc); or

(III) an entity that has been convicted of violating, or attempting to violate, section 2332b or 2339A of title 18, United States Code.

(12) Television network.—The term "television network"—

(A) means any person that, on February 8, 1996, offered an interconnected program service on a regular basis for 15 or more hours per week to at least 25 affiliated television licensees in 10 or more States; and

(B) does not include any network station that is owned or operated by, or affiliated with, a person described in subparagraph (A).

SEC. 512. FRAMEWORK FOR CERTAIN JOINT NEGOTIATIONS.

(a) Notice.—

(1) Process to form a joint negotiation entity.—

(A) In general.—An eligible digital journalism provider shall provide public notice to announce the opportunity for other eligible digital journalism providers to join a joint negotiation entity for the purpose of engaging in joint negotiations with a covered platform under this section regarding the pricing, terms, and conditions by which the covered platform may access the content of the eligible digital journalism providers that are members of the joint negotiation entity.

(B) Application.—During the 60-day period beginning on the date public notice is made under subparagraph (A), any eligible digital journalism provider may apply to join the joint negotiation entity.

(C) Formation.—A joint negotiation entity is established upon the agreement of 2 or more eligible digital journalism providers and may create admission criteria for membership unrelated to the size of an eligible digital journalism provider or the views expressed by its content, including criteria to limit membership to only eligible publishers or only eligible broadcasters.

(D) Governance.—By a majority vote of its members, a joint negotiation entity formed under this section shall establish rules and procedures to govern decision making by the entity and each eligible digital journalism provider shall be entitled to 1 vote on any matter submitted to a vote of the members.

(E) Additional members.—After the expiration of the 60-day period described in subparagraph (B), an eligible digital journalism provider may apply to join the joint negotiation entity and may be admitted upon a majority vote of its members if the applicant otherwise satisfies any criteria for admission established by the joint negotiation entity.

(F) Designation.—A joint negotiation entity may designate agents on a nonexclusive basis—

(i) to engage in negotiations with a covered platform conducted under this section; and

(ii) to agree to pay or receive payments under or related to an agreement negotiated under this section or an arbitration decision issued under this subtitle.

(G) Opt-out.—

(i) In general.—After becoming a member of the joint negotiation entity, an eligible digital journalism provider may opt out of the joint negotiation entity at any time before notice is sent to the covered platform under paragraph (2).

(ii) Prohibition on rejoining.—If an eligible digital journalism provider opts out under clause (i), the provider may not—

(I) rejoin the joint negotiation entity; or

(II) receive any payment under or related to an agreement negotiated by the joint negotiation entity under this section or an arbitration decision issued under this subtitle.

(H) Termination.—A joint negotiation entity shall terminate and cease to exist—

(i) when the entity no longer has at least 2 members;

(ii) upon a majority vote of its members; or

(iii) upon the expiration or termination of an agreement negotiated under this section or an arbitration decision issued under this subtitle.

(2) Notice to a covered platform to initiate a joint negotiation.—

(A) In general.—A joint negotiation under this section shall commence after a covered platform receives a notice sent by or on behalf of a joint negotiation entity.

(B) Contents of notice.—The notice described in subparagraph (A) shall—

(i) state that the joint negotiation entity is initiating a negotiation under this section to reach an agreement regarding the pricing, terms, and conditions by which the covered platform may access the content of the eligible digital journalism providers that are members of the joint negotiation entity;

(ii) identify the eligible digital journalism providers that are members of the joint negotiation entity; and

(iii) provide a mailing address, email address, and phone number for a representative authorized to receive a response.

(C) Reply.—Not later than 30 days after receiving notice under subparagraph (A), the covered platform shall send a reply notice acknowledging receipt.

(D) Notice to Federal enforcers.—Copies of any notice sent under this paragraph shall be filed within 30 days with the Federal Trade Commission and the Assistant Attorney General in charge of the Antitrust Division of the Department of Justice.

(b) Conduct of joint negotiations.—After a reply notice is sent under subsection (a)(2)(C), the following shall apply:

(1) Any negotiation conducted under this section shall be conducted in good faith and solely to reach an agreement regarding the pricing, terms, and conditions under which the covered platform may access the content of the eligible digital journalism providers.

(2) No pre-agreement discussions or agreement reached regarding pricing, terms, and conditions under this section may address whether or how the covered platform or any such eligible digital journalism provider—

(A) displays, ranks, distributes, suppresses, promotes, throttles, labels, filters, or curates the content of the eligible digital journalism providers; or

(B) displays, ranks, distributes, suppresses, promotes, throttles, labels, filters, or curates the content of any other person.

(3) A party is not conducting negotiations in good faith in accordance with paragraph (1) if the party—

(A) refuses to negotiate, except where eligible digital journalism providers decide to jointly deny a covered platform access to content licensed or produced by such eligible digital journalism providers under subsection (c);

(B) refuses to designate a representative with authority to make binding representations;

(C) refuses to meet and negotiate at reasonable times and locations or otherwise causes unreasonable delay;

(D) refuses to put forth more than a single, unilateral proposal;

(E) fails to respond to a proposal of the other party, including the reasons for rejection;

(F) enters into a separate third-party agreement that unreasonably impedes the party from reaching an agreement with the negotiating party; or

(G) refuses to execute a full and written agreement that has been reached verbally.

(4) A covered platform is not conducting negotiations in good faith in accordance with paragraph (1) if the covered platform enters into a separate agreement with an eligible digital journalism provider that impedes the eligible digital journalism provider from participating in a negotiation under this section.

(5) During any negotiation conducted under this section, the joint negotiation entity and the covered platform shall each make a reasonable offer regarding the pricing, terms, and conditions by which the covered platform may access the content of the eligible digital journalism providers that are members of the joint negotiation entity, substantiated with comprehensive data and methodologies, including expert analysis, that reflects—

(A) the pricing, terms, and conditions comparable to those found in commercial agreements between similarly situated entities, including price, duration, territory, and value of data generated directly or indirectly by the content;

(B) the fair market value to the covered platform of having access to the content of the eligible digital journalism providers that are members of the joint negotiation entity and the resulting incremental contribution to the revenue of the covered platform, including direct and indirect advertising or promotional revenues, which shall not be offset by any value conferred upon the eligible digital journalism providers that are members of the joint negotiation entity by the covered platform for aggregating or distributing their content; and

(C) the investment of the eligible digital journalism providers that are members of the joint negotiation entity in producing original news and related content, including the number of journalists employed by each.

(c) Joint withholding of content.—At any point after notice is sent under subsection (a)(2), eligible digital journalism providers that are members of a joint negotiation entity may jointly deny a covered platform access to content licensed or produced by such providers.

(d) Rule of construction.—

(1) Antitrust laws.—Nothing in this subtitle may be construed to modify, impair, or supersede the operation of the antitrust laws except as otherwise expressly provided in this subtitle.

(2) Copyright and trademark law.—Nothing in this subtitle may be construed to modify, impair, expand, or in any way alter rights pertaining to title 17, United States Code, or the Lanham Act (15 U.S.C. 1051 et seq.).

SEC. 513. ARBITRATION FOR ELIGIBLE PUBLISHERS.

(a) Final offer arbitration.—

(1) In general.—If the membership of a joint negotiation entity consists only of eligible publishers, on or after the date that is 180 days after the date negotiations under section 512 begin, the joint negotiation entity may initiate a final offer arbitration against the covered platform for an arbitration panel to determine the pricing, terms, and conditions by which the content displayed, provided, distributed, or offered by a qualifying publication of any eligible publisher that is a member of the joint negotiation entity will be accessed by the covered platform if the parties are unable to reach an agreement and regardless of whether the joint negotiation entity, its members, or the covered platform complied with the requirements of section 512(b).

(2) Effect of additional members.—If an additional member joins the joint negotiation entity under section 512(a)(1)(E) more than 90 days after the date negotiations under section 512 begin, the joint negotiation entity may not initiate a final offer arbitration under paragraph (1) until 180 days after the date the last member joins the joint negotiation entity. No additional members may join the joint negotiation entity after the arbitration has commenced.

(b) Notice.—The joint negotiation entity shall provide notice of its intention to initiate final offer arbitration under this section to all members of the joint negotiation entity not less than 10 days before initiating such final offer arbitration.

(c) Membership.—If a joint negotiation entity initiates final offer arbitration under this section, any individual eligible publisher that is a member of the joint negotiation entity shall remain a member of the joint negotiation entity until completion of the arbitration, unless the eligible publisher provides written notice to the joint negotiation entity of the intention to withdraw within 7 days after receiving notice under subsection (b).

(d) Proceedings.—

(1) Rules of arbitration.—The arbitration shall be decided by a panel of 3 arbitrators under the American Arbitration Association's Commercial Arbitration Rules and Mediation Procedures and the American Arbitration Association–International Centre for Dispute Resolution Final Offer Arbitration Supplementary Rules, except to the extent such rules conflict with this subsection.

(2) Initiation of arbitration.—A final offer arbitration under subsection (a) shall be initiated as provided in Rule R-4 of the American Arbitration Association's Commercial Arbitration Rules and Mediation Procedures, except that the joint negotiation entity initiating the arbitration shall refer to this subtitle in the demand for arbitration rather than submitting contractual arbitration provisions.

(3) Commencement and funding.—

(A) Commencement.—A final offer arbitration proceeding shall commence 10 days after the date a final offer arbitration is initiated under subsection (a).

(B) Funding.—The cost of administering the arbitration proceeding, including arbitrator compensation, expenses, and administrative fees, shall be shared equally between the covered platform and the joint negotiation entity.

(4) Appointment of the arbitration panel.—The arbitrators shall be appointed in accordance with the American Arbitration Association's Commercial Arbitration Rules and Mediation Procedures.

(5) Other requirements.—During a final offer arbitration proceeding under this section—

(A) the joint negotiation entity and the covered platform may demand the production of documents and information that are nonprivileged, reasonably necessary, and reasonably accessible without undue expense;

(B) documents and information described in subparagraph (A) shall be exchanged not later than 30 days after the date the demand is filed;

(C) rules regarding the admissibility of evidence applicable in Federal court shall apply;

(D) the joint negotiation entity and the covered platform shall each submit a final offer proposal for the pricing, terms, and conditions under which the content displayed, provided, distributed, or offered by a qualifying publication of any eligible publisher that is a member of the joint negotiation entity will be accessed by the covered platform, which shall include the remuneration that the eligible publishers should receive from the covered platform for programmatic access to the content of the eligible publishers that are members of the joint negotiation entity during the period under negotiation based on the fair market value of such access and shall include backup materials sufficient to permit the other party to replicate the proffered valuation;

(E) no discussion or final offer under this section may address whether or how the covered platform or any such eligible digital journalism provider—

(i) displays, ranks, distributes, suppresses, promotes, throttles, labels, filters, or curates the content of the eligible digital journalism providers; or

(ii) displays, ranks, distributes, suppresses, promotes, throttles, labels, filters, or curates the content of any other person; and

(F) if applicable, each eligible publisher that is a member of the joint negotiation entity shall provide information and data to guide the distribution of remuneration among the members of the joint negotiation entity, including—

(i) any compensation received by the eligible publisher through a commercial agreement prior to commencement of negotiations under section 512 for access to content by the covered platform during any part of the period under negotiation, which shall be deducted from the allocation accordingly; and

(ii) spending by the eligible publisher on news journalists, who are employed for an average of not fewer than 20 hours per week during the calendar quarter by the eligible digital journalism provider and are responsible for gathering, preparing, directing the recording of, producing, collecting, photographing, recording, writing, editing, reporting,

presenting, or publishing original news or information that concerns matters of public interest in the previous fiscal year, as a proportion of the overall budget of the eligible digital journalism provider for that period, which shall be used to guide 65 percent of the distribution of remuneration among the members of the joint negotiation entity.

(e) Award.—

(1) In general.—Not later than 60 days after the date proceedings commence under subsection (d)(3)(A), the arbitration panel shall issue an award selecting 1 final offer without modification.

(2) Requirements.—In issuing an award under paragraph (1), the arbitration panel—

(A) may not consider any value conferred upon an eligible publisher by the covered platform for distributing or aggregating content as an offset to the value created by the eligible publisher;

(B) shall consider past incremental revenue contributions as a guide to future incremental revenue contributions by the eligible publisher;

(C) shall consider the pricing, terms, and conditions of any available, comparable commercial agreements between parties granting access to digital content, including price, duration, territory, and the value of data generated directly or indirectly by the content, accounting for any material disparities in negotiating power; and

(D) shall issue a binding, reasoned award, including the factual and economic bases of the award, that applies for the number of years set forth in the selected final offer but not fewer than 5 years.

(f) Payments pursuant to award.—

(1) In general.—Not later than 90 days after the date an award is issued under subsection (e), the covered platform shall begin paying any eligible publisher that was a member of the joint negotiation entity participating in the arbitration in accordance with the terms of the selected final offer.

(2) Disbursement.—Payments made under paragraph (1) shall be disbursed by a claims administrator to the individual claimants that comprise the joint negotiation entity not later than 60 days after the date the funds are received from the covered platform.

(g) Enforcement and judicial review.—

(1) In general.—An award made under subsection (e) shall be enforceable by the eligible publishers or the covered platform subject to the award through a civil action brought in a district court of the United States.

(2) Expedited judicial process.—In any civil action to enforce or seek judicial review of an award made under subsection (e), the court shall adopt a rebuttable presumption that good cause exists to prioritize the action under section 1657 of title 28, United States Code.

SEC. 514. LIMITATION OF LIABILITY.

(a) In general.—In accordance with sections 512 and 513, it shall not be a violation of the antitrust laws for any eligible digital journalism providers that are members of a joint negotiation entity to—

(1) jointly deny a covered platform access to content for which the eligible digital journalism providers, individually or jointly, are authorized under this subtitle to negotiate or arbitrate access with respect to the covered platform; or

(2) participate in joint negotiations and arbitration, as members of the joint negotiation entity, with the covered platform solely regarding the pricing, terms, and conditions under which the covered platform may access the content for which the eligible digital journalism providers, individually or jointly, are authorized under this subtitle to negotiate or arbitrate access with respect to the covered platform.

(b) Safe harbor.—

(1) Eligible digital journalism providers.—An eligible digital journalism provider shall not be in violation of the antitrust laws if the eligible digital journalism provider participates, as a member of a joint negotiation entity, in negotiations under section 512 or arbitration under section 513—

(A) with a person that is not an eligible digital journalism provider, if the eligible digital journalism provider reasonably believes that the person is another eligible digital journalism provider; or

(B) with a person that is not a covered platform, if the eligible digital journalism provider reasonably believes that the person is a covered platform.

(2) Joint negotiation entities.—A joint negotiation entity shall not be in violation of the antitrust laws if the joint negotiation entity engages in negotiations under section 512 or arbitration under section 513—

(A) with or on behalf of a person that is not an eligible digital journalism provider, if the joint negotiation entity reasonably believes that the person is an eligible digital journalism provider; or

(B) with a person that is not a covered platform, if the joint negotiation entity reasonably believes that the person is a covered platform.

(c) Notification of agreements and arbitration decisions.—

(1) Agreements.—The parties to any written agreement resulting from a negotiation under section 512 or implementing an arbitration decision issued under section 513 shall file a copy of such agreement with the Federal Trade Commission and the Assistant Attorney General in charge of the Antitrust Division of the Department of Justice not later than 60 days after such agreement is executed.

(2) Arbitration decisions.—The parties to any arbitration decision issued under section 513 shall file a copy of such decision with the Federal Trade Commission and the Assistant

Attorney General in charge of the Antitrust Division of the Department of Justice not later than 60 days after such decision is issued.

(3) Public disclosure.—The Federal Trade Commission shall make the documents submitted under this subsection available to the public on the Federal Trade Commission website, except that the Commission shall redact confidential information regarding the pricing, terms, and conditions of an agreement or arbitration decision, confidential financial information, trade secrets, and other confidential commercial information protected from public disclosure under section 552(b)(4) of title 5, United States Code.

(d) Limitation regarding scope.—No antitrust immunity shall apply to any negotiations, discussions, agreements, or arbitrations relating to the use, display, promotion, ranking, distribution, curation, suppression, throttling, filtering, or labeling of content of the eligible digital journalism provider or of any other person. The limitation of liability under this section shall apply only to negotiations, discussions, agreements, or arbitrations regarding the pricing, terms, and conditions under which a covered platform may access the content of the eligible digital journalism provider, not to any discussions or agreements that differentiate content based on the viewpoint expressed by such content.

SEC. 515. NONDISCRIMINATION, RETALIATION, AND TRANSPARENCY.

(a) Nondiscrimination.—

(1) Joint negotiation entities.—A joint negotiation entity may not discriminate against any eligible digital journalism provider based on the size of the eligible digital journalism provider or the views expressed by the eligible digital journalism provider's content.

(2) Covered platforms.—No covered platform may discriminate against any eligible digital journalism provider that is a member of a joint negotiation entity in connection with a negotiation conducted under section 512 or an arbitration conducted under section 513 based on the size of the eligible digital journalism provider or the views expressed by the eligible digital journalism provider's content.

(b) Prohibition on retaliation by covered platforms.—

(1) In general.—No covered platform may retaliate against an eligible digital journalism provider for participating in a negotiation conducted under section 512 or an arbitration conducted under section 513, including by refusing to index content or changing the ranking, identification, modification, branding, or placement of the content of the eligible digital journalism provider on the covered platform.

(2) Effect of contract provisions.—Any provision in an agreement that restricts an eligible digital journalism provider from receiving compensation through a negotiation conducted under section 512 or an arbitration conducted under section 513 shall be void.

(c) Investing in journalism.—

(1) Any eligible digital journalism provider that receives funds under or related to an agreement reached under section 512 or an arbitration decision issued under section 513 shall provide to the Federal Trade Commission, on an annual basis, information regarding the use of

any such funds during the prior year to support ongoing and future operations to maintain or enhance the production and distribution of news or information that concerns local, regional, national, or international matters of public interest, including—

(A) the amount of funds received under or related to each such agreement or decision; and

(B) a good-faith estimate of the amount of funds that went to news journalists employed for an average of not fewer than 20 hours per week during the calendar year by the eligible digital journalism provider.

(2) Confidential information excluded.—Disclosures submitted under paragraph (1) shall not disclose—

(A) confidential information regarding the pricing, terms, and conditions of—

(i) an agreement reached under section 512;

(ii) an agreement implementing an arbitration decision issued under section 513; or

(iii) an arbitration decision issued under section 513; or

(B) confidential financial information.

(3) Public disclosure.—The Federal Trade Commission shall make the disclosures submitted under paragraph (1) available to the public on the Federal Trade Commission website.

SEC. 516. PRIVATE CIVIL ACTIONS.

(a) Negotiations.—

(1) In general.—Any eligible digital journalism provider, either jointly with other eligible digital journalism providers or through an authorized representative, or any covered platform that participated in negotiations under section 512 may bring a civil action in an appropriate district court of the United States alleging a violation of section 512(b) or section 512(a)(2)(C).

(2) Damages.—A court shall award damages to a prevailing plaintiff under this subsection—

(A) if the defendant did not conduct negotiations in good faith in violation of section 512(b), approximating the value of the last reasonable offer of the plaintiff; or

(B) if the defendant knowingly did not reply within 30 days as required by section 512(a)(2)(C), $1,000,000 for each day of noncompliance.

(3) Attorneys' fees.—A court shall award attorneys' fees to the prevailing party under this subsection.

(b) Discrimination.—

(1) Joint negotiation entities.—

(A) In general.—An eligible digital journalism provider that is denied membership in a joint negotiation entity in violation of section 515(a)(1) may bring a civil action in an appropriate district court of the United States against the joint negotiation entity and its members not later than 30 days after the date membership is denied.

(B) Remedies.—

(i) Before agreement or arbitration decision.—

(I) In general.—An eligible digital journalism provider that prevails in an action under subparagraph (A) before the date an agreement is executed under section 512 or an arbitration decision is issued under section 513, as applicable, regarding the pricing, terms, and conditions by which the covered platform may access the content of the eligible digital journalism providers that are members of the joint negotiation entity, may join the joint negotiation entity and participate in the negotiation under section 512 or the arbitration under section 513, as applicable.

(II) Notice.—A notice, by or on behalf of the joint negotiation entity, shall be sent to the covered platform identifying the eligible digital journalism provider that joins the negotiation or arbitration under subclause (I).

(ii) After agreement or arbitration decision.—

(I) In general.—An eligible digital journalism provider that prevails in an action under subparagraph (A) after the date an agreement is executed under section 512 or an arbitration decision is issued under section 513, as applicable, regarding the pricing, terms, and conditions by which the covered platform may access the content of the eligible digital journalism providers that are members of the joint negotiation entity, may join the joint negotiation entity and be eligible for the same pricing, terms, and conditions by which the covered platform may access the content of the other eligible digital journalism providers that are members of the joint negotiation entity.

(II) Notice.—A notice, by or on behalf of the joint negotiation entity, shall be sent to the covered platform identifying the eligible digital journalism provider that joins the joint negotiation entity under subclause (I) and that is eligible to receive the same pricing, terms, and conditions under the agreement negotiated under section 512 or the arbitration decision issued under section 513, as applicable, by which the covered platform may access the content of the other eligible digital journalism providers that are members of the joint negotiation entity.

(2) Covered platforms.—

(A) In general.—An eligible digital journalism provider that is discriminated against in violation of section 515(a)(2) may bring a civil action in an appropriate district court of the United States against the covered platform.

(B) Remedies.—An eligible digital journalism provider that prevails under subparagraph (A) shall be entitled to—

(i) recover the actual damages sustained as a result of the discrimination;

(ii) injunctive relief on such terms as the court may deem reasonable to prevent or restrain the covered platform from discriminating against the eligible digital journalism provider; and

(iii) the costs of the suit, including reasonable attorneys' fees.

(c) Retaliation.—

(1) In general.—An eligible digital journalism provider that is retaliated against in violation of section 515(b)(1) may bring a civil action in an appropriate district court of the United States against the covered platform.

(2) Remedies.—An eligible digital journalism provider that prevails in an action under paragraph (1) shall be entitled to—

(A) recover the actual damages sustained as a result of the retaliation;

(B) injunctive relief on such terms as the court may deem reasonable to prevent or restrain the covered platform from retaliating against the eligible digital journalism provider; and

(C) the costs of the suit, including reasonable attorneys' fees.

SEC. 517. REPORT BEFORE SUNSET.

(a) Study.—

(1) The Comptroller General shall study the impact of the joint negotiations authorized under this subtitle, including a summary of the deals negotiated, the impact of such deals on local and regional news, the effect on the free, open, and interoperable Internet, including the ability of the public to share and access information, the effect this subtitle has had on employment for journalists, and a recommendation on if the sunset of this subtitle should be revoked.

(2) Report.—Not later than October 30, 2031, the Comptroller General shall submit to Congress a report on the study required under this subsection.

(b) Sunset.—Except as provided in paragraphs (1) and (2), this subtitle shall cease to have effect on October 31, 2032.

(1) Exception in case of initiated but incomplete joint negotiation or arbitration.—With respect to eligible digital journalism providers that have initiated but not concluded a negotiation under section 512 or an arbitration under section 513 on or before the sunset date described in this subsection, this subtitle shall cease to be effective on the date such negotiation or arbitration concludes or 180 days after the date described in this subsection, whichever occurs first.

(2) Limitation of liability exception.—Section 514 shall remain effective without cessation for any—

(A) negotiation conducted or agreement executed under section 512;

(B) arbitration conducted or arbitration decision issued under section 513; or

(C) agreement implementing an arbitration decision issued under section 513;

during the period of effectiveness of this subtitle.

Subtitle B—Addressing Media Consolidation and Vertical Integration

SEC. 521. REDUCTION OF MEDIA OWNERSHIP LIMITS.

(a) Repeal of deregulatory provisions.—Section 202 of the Telecommunications Act of 1996 (Public Law 104–104) is amended by striking subsections (a), (b), (c), (d), (e), (f), and (h).

(b) Reduction of media ownership limits.—Title III of the Communications Act of 1934 (47 U.S.C. 301 et seq.) is amended by inserting after section 310 the following:

"Sec. 310A. Media ownership limits.

"(a) Definitions.—In this section:

"(1) Cable system.—The term 'cable system' has the meaning given that term in section 602 of the Communications Act of 1934 (47 U.S.C. 522).

"(2) Other definitions.—The terms 'cognizable interest', 'designated market area', 'local radio market', and 'national audience reach' have the meaning given such terms in section 73.3555 of title 47, Code of Federal Regulations, as in effect on April 30, 2026.

"(3) Same local market.—The term 'same local market' means—

"(A) with respect to a television broadcast station, the designated market area in which the station is located; and

"(B) with respect to a radio broadcast station, the local radio market in which the station is located.

"(4) Daily newspaper.—The term 'daily newspaper' means a print publication that is distributed to the general public in a local market on at least 4 days each week and that contains reporting on matters of general public interest, but does not include a publication whose content is primarily limited to advertising or to a single topic, trade, or industry.

"(5) Dominant online distribution platform.—The term 'dominant online distribution platform' means an online platform, as defined in section 568(a)(11) of the POPULIST Act, that—

"(A) distributes, curates, ranks, recommends, aggregates, or otherwise materially intermediates access by users to news, audio, or video content produced by unaffiliated persons; and

"(B)—

"(i) meets the requirements of subparagraph (A), (B), or (C) of section 568(a)(6) of the POPULIST Act; or

"(ii) is designated by the Commission, after notice and opportunity for comment, as a dominant online distribution platform for purposes of this section.

"(b) National media ownership limits.—

"(1) Radio.—It shall be unlawful for any person to have a cognizable interest in more than 5 percent of all licensed AM and FM broadcast radio stations in the United States.

"(2) Television.—It shall be unlawful for any person to have a cognizable interest in television broadcast stations with an aggregate national audience reach exceeding 25 percent.

"(3) No discounts.—For purposes of paragraph (2), national audience reach shall be calculated without regard to signal band, technical classification, or any discount or adjustment based on transmission characteristics.

"(c) Local media ownership limits.—

"(1) Radio.—It shall be unlawful for any person to have a cognizable interest in more than 3 broadcast radio stations in any local radio market, or more than 2 stations in the same service (AM or FM).

"(2) Television.—It shall be unlawful for any person to have a cognizable interest in more than 2 full-power television broadcast stations in any designated market area, or to have a cognizable interest in more than 1 of the 4 highest-rated stations in that market.

"(d) Cross-ownership restrictions.—It shall be unlawful for any person—

"(1) to have a cognizable interest in a broadcast television station and to own, operate, or control a daily newspaper in the same local market;

"(2) to have a cognizable interest in a broadcast radio station and to own, operate, or control a daily newspaper in the same local market; or

"(3) to own or control a cable system serving, or a dominant online distribution platform materially intermediating access to content for users located in, the same local market as a broadcast television or radio station in which such person has a cognizable interest.

"(e) Enforcement.—

"(1) Divestiture.—A person may not, on or after January 1, 2028, hold any cognizable interest, ownership interest, or control that is unlawful under this section. Any such interest acquired or held before that date must be divested not later than January 1, 2028.

"(2) No grandfathering.—The Commission may not grandfather any cognizable interest, ownership interest, or control inconsistent with this section, and, on or after January 1, 2028, may not grant, renew, or extend any license or authorization, or approve any assignment or transfer, if doing so would result in, maintain, or prolong a violation of this section, except that the Commission may approve an assignment or transfer that effectuates divestiture.

"(3) No waivers.—The Commission may not grant waivers of this section.

"(4) Forfeitures.—The Commission shall impose forfeiture penalties for knowing or willful violations of this section. Each day of a continuing violation, and each license held or controlled in violation of this section, shall constitute a separate violation.

"(5) Revocation authority.—A knowing or willful failure to comply with this section shall be treated as a willful and repeated violation for purposes of section 312 and may be grounds for revocation of any license held in violation of this section.".

SEC. 522. PARAMOUNT REDECREED.

(a) Definitions.—In this section:

(1) Affiliated entity.—The term "affiliated entity" means any entity that is under common ownership or control with another entity.

(2) Antitrust Division.—The term "Antitrust Division" means the Antitrust Division of the Department of Justice, acting through the Assistant Attorney General in charge of the Antitrust Division.

(3) Commission.—The term "Commission" means the Federal Trade Commission.

(4) Common ownership or control.—The term "common ownership or control" means ownership or control, direct or indirect, of 2 or more entities by the same person or group of persons.

(5) Content production.—The term "content production" means the business of developing, financing, creating, recording, publishing, or producing entertainment content.

(6) Control.—The term "control" means the possession, direct or indirect, of the power to direct or cause the direction of the management, policies, or operations of an entity. A person shall be rebuttably presumed to control an entity if such person—

(A) owns, controls, or has the power to vote 25 percent or more of any class of voting securities of the entity;

(B) has the power to appoint 25 percent or more of the board of directors or equivalent governing body of the entity; or

(C) possesses contractual or other rights that permit such person to direct or materially influence the strategic, operational, licensing, distribution, exhibition, promotion, booking, ticketing, or access decisions of the entity.

(7) Dominant digital interface.—The term "dominant digital interface" means any digital service, application, operating system, marketplace, platform, or other interface that, by virtue of scale, market share, or user base, materially influences whether, how, or on what terms the public may obtain access to entertainment content supplied by unaffiliated persons.

(8) Entertainment content.—The term "entertainment content" means audiovisual, audio, literary, recorded, broadcast, streamed, live, or similar expressive works, performances, events, or productions offered, distributed, exhibited, or presented to the public.

(9) Exhibition operation.—The term "exhibition operation" means the business of operating theaters, cinemas, concert venues, broadcast stations, cable systems, or other facilities or channels through which entertainment content or live entertainment events are presented directly to the public, but does not include a streaming platform.

(10) Exclusive contractual arrangement.—The term "exclusive contractual arrangement" means any contract, agreement, clause, or practice that grants or effectively confers exclusive control over production, promotion, distribution, exhibition, ticketing, booking, routing, or access with respect to entertainment content or live entertainment events.

(11) Live event promotion.—The term "live event promotion" means the business of organizing, financing, marketing, or promoting live entertainment events, tours, or performances for presentation to the public. The term does not include representation services performed solely on behalf of performers, creators, or productions.

(12) Media vertical.—The term "media vertical" means any of the following:

(A) Content production.

(B) Exhibition operation.

(C) Live event promotion.

(D) Representation services.

(E) Streaming platform operation.

(F) Transaction gatekeeping.

(G) Wholesale distribution.

(13) Person.—The term "person" has the meaning given such term in section 1 of the Clayton Act (15 U.S.C. 12).

(14) Profits.—The term "profits" means, with respect to any person and any month, the amount equal to the greater of—

(A) the net income (or loss) of such person before provision for income taxes for such month, as determined in accordance with generally accepted accounting principles and consistent with the accounting principles used in the most recent audited consolidated financial statements of such person; and

(B) 4 percent of the gross revenues of such person for such month, as so determined.

(15) Representation services.—The term "representation services" means the business of acting on behalf of performers, creators, or productions in arranging bookings, routing, tours, engagements, or appearances for performers, creators, or productions.

(16) Streaming platform.—The term "streaming platform" means any digital service or application primarily engaged in distributing, curating, or providing access to audiovisual or audio entertainment content directly to end users over the internet for on-demand or scheduled consumption.

(17) Streaming platform operation.—The term "streaming platform operation" means the business of owning, operating, or controlling a streaming platform.

(18) Ticketing system.—The term "ticketing system" means any system or service that sells, allocates, distributes, validates, transfers, controls, conditions, or otherwise mediates tickets, admissions, reservations, or entry rights for live entertainment events or venues.

(19) Transaction gatekeeping.—The term "transaction gatekeeping" means the business of controlling, conditioning, or materially influencing whether, how, or on what terms the public may obtain tickets, admissions, subscriptions, or other access rights to entertainment content or live entertainment events offered by unaffiliated persons, including through ticketing systems, dominant digital interfaces, or comparable systems. Such term does not include a person who provides such services solely with respect to that person's own entertainment content.

(20) Unaffiliated.—The term "unaffiliated", with respect to 2 persons, means that the persons are not under common ownership or control, directly or indirectly.

(21) Wholesale distribution.—The term "wholesale distribution" means the business of licensing, syndicating, packaging, or wholesale distributing entertainment content to unaffiliated exhibitors, broadcasters, cable systems, streaming platforms, distributors, or other intermediaries, and does not include distributing entertainment content directly to end users through a streaming platform operated by the same person or an affiliated entity.

(b) Prohibition on ownership of more than 1 media vertical.—

(1) (A) In general.—It shall be unlawful for any person to directly or indirectly own, operate, control, or direct the operation of any entity or combination of entities engaged in more than 1 media vertical within the same relevant media market, in or affecting interstate or foreign commerce.

(B) Prohibition on new acquisitions.—After the date of enactment of this Act, no person may acquire, directly or indirectly, control of assets or operations in a media vertical other than the media vertical in which such person already engages, in violation of subparagraph (A).

(2) Rulemaking.—Not later than January 30, 2027, the Commission and the Antitrust Division shall, by joint interim final rule, define for purposes of this section—

(A) a de minimis threshold, by media vertical and relevant media market, below which an activity may be excluded from prohibition under this subsection, except that—

(i) no such threshold may exceed 5 percent of the primary market measure specified by joint rule for the applicable media vertical in the relevant media market, which may include revenue, market share, audience share, subscriber share, ticketing share, screen share, seat share, booking share, or a comparable measure;

(ii) with respect to transaction gatekeeping, no such threshold may exceed 1 percent of the applicable measure described in clause (i); and

(iii) any exclusion under this subparagraph shall be construed narrowly and shall not permit the preservation, recreation, or continuation of vertically integrated control inconsistent with the purposes of this section;

(B) standards for applying the definitions of "affiliated entity", "common ownership or control", and "control" under subsection (a), including standards addressing contractual arrangements of operational control, exclusive contractual arrangements, indirect means of control, and functions materially comparable to a media vertical;

(C) milestones for divestiture to ensure compliance within the deadline under subsection (c), provided such milestones may not be later than permitted under subsection (d), including but not limited to—

(i) filing of a divestiture plan;

(ii) the length of time the Commission and the Antitrust Division will review such plan;

(iii) filing of a revised plan, if necessary;

(iv) notification of the person acquiring such divestiture;

(v) the submission of any transaction filing required by section 7A of the Clayton Act (15 U.S.C. 18a) by the person acquiring such divestiture; and

(vi) the completion of such divestiture; and

(D) for each milestone, whether, in the case of a person's knowing and willful failure to meet the milestone, the Commission and the Antitrust Division shall seek—

(i) penalties under subsection (e)(3);

(ii) appointment of a divestiture trustee for such person under subsection (e)(4); or

(iii) both clauses (i) and (ii).

(3) Effect of interim final rule.—The interim final rule under paragraph (2) shall take effect upon publication in the Federal Register, shall have the force and effect of law, and may be issued without regard to section 553 of title 5, United States Code. The Commission and the Antitrust Division shall provide a public comment period of not less than 60 days after publication and shall issue final rules not later than October 30, 2027. A delay in issuance or finalization of rules under this paragraph shall not delay, limit, extinguish, or reduce any prohibition, duty, enforcement authority, or divestiture obligation established by this section.

(4) Notice of divestiture requirement.—

(A) In general.—Not later than 60 days after the date of enactment of this Act, the Commission and the Antitrust Division shall, using the best information available, identify each person that the Commission and the Antitrust Division jointly determine is required to divest under subsection (c) and notify such person of the determination.

(B) 60-day notice not exhaustive.—Notwithstanding subparagraph (A), if the Commission and the Antitrust Division later jointly determine, using the best information available, that a person not notified under subparagraph (A) is required to divest under subsection (c), the Commission and the Antitrust Division shall promptly notify such person.

(C) No immunity.—Failure to identify or notify a person under this paragraph shall not limit, extinguish, or otherwise affect any prohibition, duty, enforcement authority, or divestiture obligation established by this section.

(5) Determination upon request.—

(A) Request.—Any person that has not received notice under paragraph (4) may submit to the Commission and the Antitrust Division a written request for a determination of whether that person is required to divest under subsection (c).

(B) Determination.—Not later than the later of 30 days after receipt of a request under subparagraph (A) or the expiration of the 60-day period under paragraph (4)(A), the Commission and the Antitrust Division shall jointly issue to the person a written determination that states whether the person is required to divest under subsection (c). Notice issued under paragraph (4) after receipt of a request under subparagraph (A) shall satisfy this requirement.

(C) No admission or tolling.—Submission of a request under subparagraph (A) shall not—

(i) constitute an admission that the person is subject to subsection (b) or required to divest under subsection (c); or

(ii) toll or extend any prohibition, duty, enforcement authority, divestiture obligation, or deadline under this section.

(6) Judicial review.—

(A) Petition for review.—

(i) Determination.—A person receiving notice under paragraph (4) or a determination under paragraph (5) may, not later than 30 days after receipt of such notice or determination, file a petition for review of the determination in the United States Court of Appeals for the District of Columbia Circuit.

(ii) Failure to act.—A person that submits a request under paragraph (5)(A) and does not receive a written determination within the period required under paragraph (5)(B) may, at any time before receipt of such determination, file a petition in the United States Court of Appeals for the District of Columbia Circuit to compel issuance of the determination.

(B) Application of chapter 7.—Chapter 7 of title 5, United States Code, shall apply to a petition under subparagraph (A). For purposes of such chapter—

(i) a determination under paragraph (4) or (5) shall constitute final agency action; and

(ii) a failure to issue a determination within the period required under paragraph (5)(B) shall constitute agency action unlawfully withheld.

(C) Expedited consideration.—The court shall expedite consideration of a petition filed under subparagraph (A) to the greatest extent practicable.

(c) Divestiture.—Not later than July 1, 2028, any person in violation of subsection (b) shall divest such interests as are necessary to come into compliance.

(d) FTC and DOJ review.—

(1) Divestiture plan required.—Not later than April 1, 2027, any person required to divest under subsection (c) shall submit to the Commission and the Antitrust Division a divestiture plan. Such plan—

(A) shall be submitted to the Commission and the Antitrust Division in the same manner, and containing substantially similar information, as a transaction filing under section 7A of the Clayton Act (15 U.S.C. 18a), without respect to any threshold, exemption, or other limitation of such section; and

(B) shall include—

(i) identification of the business, assets, or interests to be divested to come into compliance with subsection (b);

(ii) identification of the proposed acquiring person, if known;

(iii) a timetable for execution;

(iv) any transitional services proposed; and

(v) such other information as the Commission and the Antitrust Division may require by joint rule.

(2) Agency review process.—Not later than 180 days after receipt of a divestiture plan under paragraph (1), but in no case later than October 1, 2027, the Commission and the Antitrust Division shall review the plan.

(A) Lead agency.—The Commission and the Antitrust Division may designate 1 agency to take the lead in conducting the review and communicating with the person submitting the plan.

(B) Review criteria.—The lead agency shall review the effect on competition, viewpoint diversity, independent market access, and the public interest—

(i) of the divestiture; and

(ii) of the subsequent acquisition of the divested entity by the acquiring person.

(C) Additional information.—Any request for additional information by an agency shall be made within 30 days of receipt of the plan.

(D) Acquiring person.—

(i) A divestiture plan that identifies a proposed acquiring person may be approved only if the lead agency determines that—

(I) the proposed acquisition of the divested business, assets, or interests by such acquiring person is consistent with subsection (b);

(II) the proposed acquisition would not materially harm competition or otherwise undermine the purposes of this section; and

(III) any statutory reporting, waiting period, or approval requirement applicable to the proposed acquisition will be satisfied before consummation.

(ii) A divestiture plan may be submitted and reviewed without identifying a proposed acquiring person, but no sale, transfer, assignment, or other disposition to an acquiring person shall be consummated if either the Commission or the Antitrust Division disapproves in writing.

(E) Notice of decision.—Not later than the end of the review period, the lead agency shall notify the person in writing—

(i) whether the plan is approved, approved with conditions, or disapproved; and

(ii) the reasons for any disapproval or conditions.

(F) Approval standard.—A divestiture plan shall be treated as approved only if, before the end of the review period, the lead agency has approved the plan in writing, whether unconditionally or subject to conditions accepted in writing by the person submitting the plan, and neither the Commission nor the Antitrust Division has disapproved the plan in writing.

(3) Revised plan following disapproval.—If a plan is disapproved under paragraph (2), the person shall submit a revised divestiture plan not later than 60 days after receipt of the disapproval notice.

(A) Review deadline.—Not later than 150 days after receipt of a revised plan, but in no case later than May 1, 2028, the lead agency shall review the revised plan under the procedures set forth in paragraph (2).

(4) No tolling.—No submission, resubmission, agency review, negotiation, request for additional information, waiting period, court proceeding, or other matter shall toll or extend any deadline under this section.

(5) Consequences of noncompliance.—A person required to divest under subsection (c) shall be subject to subsection (e)(3), subsection (e)(4), or both, if such person fails to—

(A) submit a divestiture plan under paragraph (1);

(B) submit a revised plan under paragraph (3), if required to do so;

(C) obtain approval of either—

(i) a plan under paragraph (2); or

(ii) a revised plan under paragraph (3);

(D) conform to agreed-upon conditions of an approved plan; or

(E) conclude the divestiture required by subsection (c).

(6) Blocking of actions.—The Commission and the Antitrust Division, jointly or separately, may bring a civil action in any court of competent jurisdiction to block any action relating to the conflicts of interest described in subsection (b) that would materially harm competition or independent market access, or otherwise undermine the purposes of this section.

(e) Enforcement.—

(1) In general.—When the Commission, the Antitrust Division, or an attorney general of a State has reason to believe that a person is in violation of this section or a rule promulgated under this section, the Commission, the Antitrust Division, or the attorney general of the State may bring a civil action in an appropriate district court of the United States.

(2) Injunctive and equitable relief.—In any action described in paragraph (1), the applicable court, on a finding that a person is in violation of this section or a rule promulgated under this section, shall issue an order requiring such person—

(A) to cease and desist from such violation and, if applicable, divest such interests as are necessary to come into compliance with this section; and

(B) to pay an amount equal to the profits derived from any business, asset, operation, or interest subject to divestiture during the period of the violation.

(3) Penalties.—

(A) Written determination and transfer.—If a person knowingly and willfully fails to comply with a milestone specified under subsection (b)(2)(C), the Commission and the Antitrust Division, acting jointly, or the lead agency designated under subsection (d)(2)(A), shall issue a written determination identifying the missed milestone, the month for which escrow is required, the amount required to be transferred, and the method used to calculate such amount. Beginning not later than 15 days after receipt of such written determination, the person shall transfer into escrow on a monthly basis 10 percent of the profits of the person, to be—

(i) returned to the person if divestiture occurs by the deadline under subsection (c); or

(ii) deposited into the general fund of the Treasury if divestiture does not occur by the deadline under subsection (c).

(B) Escrow administration and certification.—Any transfer into escrow under subparagraph (A) shall be deposited with the Secretary of the Treasury into a segregated account established for purposes of this section.

(i) Not later than 15 days after the end of each month for which a transfer is required, the person shall submit to the Chair of the Commission and the Antitrust

Division a certification, signed by the chief executive officer and chief financial officer, attesting to the calculation of profits and gross revenues for such month and the amount transferred.

(ii) Not later than 120 days after the end of each fiscal year, the person shall submit a reconciliation based on audited financial statements, and shall pay any underpayment together with interest, calculated from the date the underpaid amount was required to be transferred at the rate and in the manner provided under sections 6621(a)(2) and 6622(a) of the Internal Revenue Code of 1986, or shall receive a return of any overpayment, as applicable.

(C) Judicial review.—A person subject to a transfer requirement under subparagraph (A) may, not later than 30 days after notice of such requirement, petition for review in the United States Court of Appeals for the District of Columbia Circuit. The filing of a petition for review shall not stay any obligation to transfer amounts into escrow unless the court orders otherwise.

(4) Trustee.—The Commission or the Antitrust Division may apply to a court of competent jurisdiction for the appointment of a divestiture trustee.

(A) Authority.—The divestiture trustee shall have the authority, at the expense of the person required to divest, to take such actions as are necessary to effectuate the divestiture required under this section, including selling, transferring, assigning, or otherwise disposing of the business, assets, entity, or interests required to be divested.

(B) Cooperation.—The person required to divest shall cooperate fully with the divestiture trustee and shall take no action to interfere with, delay, or impede the divestiture.

(C) Approval.—Any proposed sale by the divestiture trustee shall be subject to approval under subsection (d).

(D) Duty of trustee.—The divestiture trustee shall act in the interest of effectuating prompt compliance with this section and restoring competition, and shall not be required to maximize the value received by the person required to divest.

(5) Deposit.—Any amount paid under paragraph (2)(B) shall be deposited into the general fund of the Treasury.

(6) Other relief.—In addition to any relief obtained under paragraph (1) or (2), the court may grant any other equitable relief necessary to redress and prevent recurrence of the violation.

(f) Anti-circumvention.—It shall be unlawful for any person to evade or attempt to evade this section, including by entering into an agreement or contract, engaging in a transaction, structuring an entity, or recreating, through contractual means, the conflicts of interest described in subsection (b).

(g) Rulemaking authority.—The Commission and the Antitrust Division shall, by joint rule, promulgate regulations to carry out this section.

(h) Reports required.—The Chair of the Commission and the Antitrust Division shall submit to the appropriate congressional committees quarterly reports on compliance with this section, including the status of any divestitures required under this section.

(i) Rule of construction.—Nothing in this section shall be construed to limit the authority of the Commission, the Department of Justice, or the attorney general of a State under any other provision of law.

Subtitle C—Intellectual Property Reform

PART I—COPYRIGHT REFORM

SEC. 531. DURATION OF COPYRIGHT AMENDED.

(a) Duration of copyright.—Section 302 of title 17, United States Code, is amended—

(1) in subsection (a), by striking "70" and inserting "50";

(2) in subsection (b), by striking "70" and inserting "50" before the period at the end;

(3) in subsection (c)—

(A) by striking "95" and inserting "50"; and

(B) by striking ", or a term of 120 years from the year of its creation, whichever expires first" and inserting "unless extended pursuant to section 304(e)"; and

(4) in subsection (e) to read as follows:

"(e) Enforcement rights.—The exclusive rights conferred by section 106 may be exercised only during periods of active enforcement as provided in chapter 4A.".

SEC. 532. PERIOD OF ACTIVE ENFORCEMENT DEFINED.

(a) Section 101 of title 17, United States Code, is amended by inserting after the definition relating to "performing rights society" the following:

"The term 'period of active enforcement' means the time during the duration of a copyright in which civil and criminal actions may be initiated for violations of the rights and privileges granted to the holder under this title.".

(b) New chapter.—Title 17, United States Code, is amended by inserting after chapter 4 the following new chapter:

"CHAPTER 4A—ENFORCEMENT LICENSURE

"SEC. 451. Definitions.

"SEC. 452. Enforcement privilege may lapse.

"SEC. 453. Enforcement license.

"SEC. 454. Administration.

"Sec. 451. Definitions.

"(a) In this chapter—

"(1) Enforcement license.—The term 'enforcement license' means an optional 7-year period of active enforcement after the initial enforcement period, with respect to all exclusive rights under section 106 in the work owned by the purchasing rights-holder, for which the rights-holder has paid the applicable fee under section 453.

"(2) Initial enforcement period.—The term 'initial enforcement period' means the first 15 years beginning on the date of first publication of the work.

"(3) Lapse.—The term 'lapse' means that the exclusive rights granted under section 106 are not enforceable through civil or criminal actions.

"(4) Rights-holder.—The term 'rights-holder' means the owner of one or more exclusive rights under section 106 with respect to a work.

"Sec. 452. Enforcement privilege may lapse.

"(a) Transition date.—Beginning January 1, 2028, no criminal or civil action for a violation of section 106 of this title may be brought for any work not in its initial enforcement period unless an enforcement license has been purchased under this chapter.

"(b) Pending actions.—Nothing in this section shall affect any civil or criminal action commenced on or before December 31, 2027.

"(c) Calendar-year application.—Pursuant to section 305, all periods of active enforcement shall run to the end of the calendar year in which they would otherwise expire.

"Sec. 453. Enforcement license.

"(a) Enforcement protection optional.—A rights-holder may extend the period of active enforcement for the exclusive rights in a work owned by that rights-holder by purchasing a 7-year enforcement license according to the following fee schedule:

"(1) for years 16 through 22, $100;

"(2) for years 23 through 29, $500;

"(3) for years 30 through 36, $2,500;

"(4) for years 37 through 43, $5,000; and

"(5) for years 44 through 50, $10,000.

"(b) Failure to renew.—If the rights-holder fails to purchase an enforcement license under this section during years 15, 22, 29, 36, or 43 of their copyright, the period of active enforcement shall be deemed to lapse at the end of the year. Such lapse shall not diminish the validity of any actions commenced prior to the conclusion of a period of active enforcement.

"(c) Indexing of fees.—Beginning in 2029, the dollar amounts in subsection (a) shall be adjusted annually by the percentage change in the Consumer Price Index for All Urban Consumers, rounded to the nearest $10.

"(d) Transition fees.—During the calendar year 2027, a rights-holder may purchase a prorated enforcement license for a fraction of the fee schedule based on the year in which the work was originally published. Such fees shall be as follows:

"(1) for 2012, the amount listed in subsection (a)(1);

"(2) for 2011, $85;

"(3) for 2010, $71;

"(4) for 2009, $57;

"(5) for 2008, $42;

"(6) for 2007, $28;

"(7) for 2006, $14;

"(8) for 2005, the amount listed in subsection (a)(2);

"(9) for 2004, $428;

"(10) for 2003, $357;

"(11) for 2002, $285;

"(12) for 2001, $214;

"(13) for 2000, $142;

"(14) for 1999, $71;

"(15) for 1998, the amount listed in subsection (a)(3);

"(16) for 1997, $2,142;

"(17) for 1996, $1,785;

"(18) for 1995, $1,428;

"(19) for 1994, $1,071;

"(20) for 1993, $714;

"(21) for 1992, $357;

"(22) for 1991, the amount listed in subsection (a)(4);

"(23) for 1990, $4,285;

"(24) for 1989, $3,571;

"(25) for 1988, $2,857;

"(26) for 1987, $2,142;

"(27) for 1986, $1,428;

"(28) for 1985, $714;

"(29) for 1984, the amount listed in subsection (a)(5);

"(30) for 1983, $8,571;

"(31) for 1982, $7,142;

"(32) for 1981, $5,714;

"(33) for 1980, $4,285;

"(34) for 1979, $2,857; and

"(35) for 1978, $1,428.

"(e) Separately owned exclusive rights.—

"(1) In general.—If exclusive rights under section 106 in the same work are owned by more than 1 rights-holder, each rights-holder shall separately purchase an enforcement license for the exclusive rights owned by that rights-holder.

"(2) Transfer during license term.—A transfer of an exclusive right covered by an enforcement license transfers the benefit of the license with the exclusive right for the remainder of the license term. The transferee shall notify the Register of Copyrights of the transfer in such form and manner as the Register may prescribe. No additional enforcement-license fee shall be required for the transferred right during the remainder of that license term.".

"Sec. 454. Administration.

"(a) Regulations.—The Register of Copyrights shall, not later than 90 days after the date of enactment of this Act, issue interim final regulations to implement this chapter, including procedures for payment, recording, and public notice of renewals, and shall thereafter promulgate final regulations after notice and comment.

"(b) Public registry.—The Register shall establish an electronic public registry identifying, for each work, whether it is in an active enforcement period and, if so, the dates of the initial enforcement period and any renewal periods, and the rights-holder and exclusive rights covered by each enforcement license.".

SEC. 533. SUBSISTING COPYRIGHT.

(a) Subsisting copyrights.—Section 304 of title 17, United States Code, is amended—

(1) in subsection (a)—

(A) by striking "67 years" and inserting "22 years"; and

(B) by adding at the end the following: "No civil or criminal enforcement action may be initiated under this title more than 50 years after the date of first publication of the work, except pursuant to subsection (e).";

(2) in subsection (b)—

(A) by striking "67 years" and inserting "22 years"; and

(B) by adding at the end the following: "No civil or criminal enforcement action may be initiated under this title more than 50 years after the date of first publication of the work, except pursuant to subsection (e).";

(3) in subsections (c) and (d), by striking "75 years" each place it appears and inserting "50 years";

(4) by striking "95 years" each place it appears and inserting "50 years";

(5) by adding at the end of subsection (c) the following: "Termination of a grant under this subsection shall not have the effect of extending a copyright beyond the term provided under this section, except pursuant to subsection (e)."; and

(6) by adding at the end of subsection (d) the following text and new subsection (e): "Termination of a grant under this subsection shall not have the effect of extending a copyright beyond the term provided under this section, except pursuant to subsection (e).

"(e) Additional terms of copyright.—

"(1) In general.—A copyright shall expire and enter the public domain unless extended for an additional term under this subsection—

"(A) upon expiration of a 50-year term provided under section 302(c) or this section; or

"(B) on January 1, 2028.

"(2) Additional terms.—An additional term under this subsection shall be for a period of 5 years and shall confer a period of active enforcement for the duration of such term.

"(3) Calendar-year application.—Pursuant to section 305, all periods of active enforcement shall run to the end of the calendar year in which they would otherwise expire.

"(4) Fee schedule.—The extension fee for an additional term under this subsection shall be as follows:

"(A) for years 51 through 55, $1,000,000;

"(B) for years 56 through 60, $2,000,000;

"(C) for years 61 through 65, $4,000,000;

"(D) for years 66 through 70, $8,000,000;

"(E) for years 71 through 75, $16,000,000;

"(F) for years 76 through 80, $32,000,000;

"(G) for years 81 through 85, $64,000,000;

"(H) for years 86 through 90, $128,000,000;

"(I) for years 91 through 95, $256,000,000;

"(J) for years 96 through 100, $512,000,000; and

"(K) for each successive 5-year period beginning after years 96 through 100, 2 times the extension fee applicable to the immediately preceding 5-year period, after application of any adjustment under paragraph (6).

"(5) Proration during transition.—Prior to January 1, 2028, the applicable extension fee for an additional term which will lapse at the end of calendar year 2028, 2029, 2030, or 2031 shall be the product of—

"(A) the applicable fee specified in paragraph (4); and

"(B) the number of full calendar years remaining in the applicable 5-year term divided by 5.

"(6) Indexing of fees.—Beginning January 1, 2029, the dollar amounts in paragraph (4), and each fee determined under paragraph (4)(K), shall be adjusted annually by the percentage change in the Consumer Price Index for All Urban Consumers, rounded to the nearest $1,000.".

SEC. 534. CONFORMING AMENDMENTS.

(a) Section 501 of title 17, United States Code, is amended by adding at the end the following:

"(g) No action for infringement may be brought under this section unless the copyright is in a period of active enforcement.".

(b) Section 106 of title 17, United States Code, is amended by inserting "(a)" before the introductory text and adding at the end the following:

"(b) Enforcement rights under this section may be exercised only if the work is in a period of active enforcement. No civil action, administrative action, or takedown request may be initiated or maintained except during a period of active enforcement.".

(c) Section 412 of title 17, United States Code, is amended by adding at the end the following:

"(3) Statutory damages and attorney's fees may be awarded only if the copyright was in a period of active enforcement.".

(d) Section 506 of title 17, United States Code, is amended by adding at the end the following:

"(g) Affirmative defense.—It shall be an affirmative defense to a violation of this section that the work in question was not in a period of active enforcement.".

(e) Savings clause.—Any provision of law inconsistent with this part is repealed to the extent of such inconsistency.

SEC. 535. DISPOSITION OF FEES AND RECEIPTS.

(a) In general.—Notwithstanding any other provision of law, all fees collected under chapter 4A and section 304(e) of title 17, United States Code, shall be deposited into the general fund of the Treasury and disbursed in accordance with this section.

(b) American Value Fund.—99 percent of all amounts deposited pursuant to subsection (a) shall be credited to the American Value Fund established in title VI of the POPULIST Act.

(c) Library of Congress.—1 percent of all amounts deposited pursuant to subsection (a) shall be transferred to the Library of Congress Support and Cultural Preservation Fund established in section 537.

(d) Budgetary treatment.—Amounts transferred under this section shall be treated as offsetting receipts for purposes of the Congressional Budget Act of 1974.

SEC. 536. DENUNCIATION OF THE BERNE CONVENTION.

(a) Denunciation authorized.—The President is authorized and directed to denounce the Berne Convention for the Protection of Literary and Artistic Works, done at Berne on September 9, 1886, as revised and amended, pursuant to Article 35 of the Paris Act of July 24, 1971.

(b) Notice.—Not later than December 31, 2026, the President shall transmit a written notification of denunciation to the Director General of the World Intellectual Property Organization in accordance with Article 35(2) of the Berne Convention.

(c) Effective date.—The denunciation authorized by subsection (a) shall take effect on the date that is 1 year after the date on which the notification described in subsection (b) is received by the Director General of the World Intellectual Property Organization.

SEC. 537. LIBRARY OF CONGRESS SUPPORT AND CULTURAL PRESERVATION FUND.

(a) Establishment.—There is established in the Treasury of the United States a fund to be known as the "Library of Congress Support and Cultural Preservation Fund" (in this section referred to as the "Fund").

(b) Uses.—Amounts in the Fund shall be available to the Library of Congress, without further appropriation, for the following purposes:

(1) Digitization, preservation, and restoration of copyrighted and formerly copyrighted works;

(2) Long-term digital storage infrastructure, redundancy, and access systems;

(3) Audio, visual, and audiovisual conservation, including film, sound recordings, and born-digital media;

(4) Metadata creation, cataloging, indexing, and public discovery tools; and

(5) Technical and administrative support necessary to carry out the activities described in this subsection.

(c) Oversight and coordination.—

(1) The Librarian of Congress shall submit an annual report to the Committees on Appropriations and the Committees on the Judiciary of the House of Representatives and the Senate describing—

(A) amounts deposited into and expended from the Fund;

(B) activities supported by the Fund; and

(C) measurable outcomes relating to preservation, access, and public availability.

(2) The Librarian of Congress shall coordinate activities funded under this section with the Register of Copyrights to ensure consistency with copyright administration and public access objectives.

(d) Budgetary treatment.—Amounts deposited into and expended from the Fund shall be treated as offsetting collections for purposes of the Congressional Budget Act of 1974.

SEC. 538. CONTROLLED DIGITAL LENDING BY QUALIFYING LIBRARIES.

(a) In general.—Chapter 1 of title 17, United States Code, is amended by inserting after section 109 the following—

"Sec. 109A. Controlled digital lending by qualifying libraries.

"(a) Definitions.—In this section:

"(1) Controlled digital loan.—The term 'controlled digital loan' means the time-limited provision of access to a digital surrogate by a qualifying library to a user under technological access controls that enforce the limitations in subsection (b).

"(2) Digital surrogate.—The term 'digital surrogate' means a reproduction of a lawfully acquired copy, fixed in a digital format, that is created by or for a qualifying library.

"(3) Lawfully acquired copy.—The term 'lawfully acquired copy' means a tangible copy of a work that is lawfully owned by a qualifying library.

"(4) Qualifying library.—The term 'qualifying library' means a library or archives that meets the requirements of section 108(a)(2).

"(5) Technological access controls.—The term 'technological access controls' means reasonable and effective technical measures that, in the ordinary course of operation, prevent unauthorized retention, copying, redistribution, or simultaneous access beyond the limits of subsection (b).

"(6) User.—The term 'user' means an individual who is a member of the public entitled to access the library's collections.

"(b) Authorization and conditions.—Notwithstanding section 106, a qualifying library may make controlled digital loans, if—

"(1) the qualifying library limits access to digital surrogates of a work to a number of users equal to the number of lawfully acquired copies of that work;

"(2) during the controlled digital loan of a lawfully acquired copy, the qualifying library does not lend, lease, or otherwise provide access to that particular lawfully acquired copy to any other person;

"(3) the controlled digital loan is provided as part of the qualifying library's noncommercial public lending function;

"(4) the qualifying library provides notice to users that access is provided solely for the duration of the loan and that retention or redistribution is prohibited;

"(5) the controlled digital loan terminates automatically at the end of the loan period;

"(6) the loan period does not exceed the period for which the qualifying library ordinarily lends a tangible copy of the same work or category of work;

"(7) the qualifying library uses technological access controls to—

"(A) authenticate users; and

"(B) prevent users from—

"(i) retaining the digital surrogate after the termination of the loan period; or

"(ii) redistributing the digital surrogate to others; and

"(8) the qualifying library maintains records sufficient to demonstrate compliance with paragraphs (1) through (7), including—

"(A) the number of lawfully acquired copies owned;

"(B) the number of concurrent controlled digital loans enabled; and

"(C) the applicable loan periods.

"(c) No compensation owed.—No royalty, fee, or other remuneration shall be owed to any copyright owner for the making of controlled digital loans in compliance with subsection (b).

"(d) No waiver by private terms.—Any term or condition of a contract, license, or agreement that purports to prohibit or restrict an act authorized by this section, or that purports to impose remuneration for an act authorized by this section, shall be unenforceable as contrary to public policy.

"(e) Scope; exclusions.—Nothing in this section:

"(1) authorizes the circumvention of technological measures in violation of section 1201;

"(2) authorizes controlled digital lending of a copy that was primarily acquired as a licensed digital product rather than as a lawfully acquired copy;

"(3) limits any right, limitation, or exception under section 107, 108, or 109; or

"(4) affects remedies for any act that is not in material compliance with subsection (b).

"(f) Construction.—This section shall be construed to preserve a qualifying library's traditional public lending function in digital form, while maintaining an owned-to-loaned limitation that preserves materially equivalent scarcity to physical lending.".

(b) Clerical amendment.—The table of sections for chapter 1 of title 17, United States Code, is amended by inserting after the item relating to section 109 the following:

"109A. Controlled digital lending by qualifying libraries.".

PART II—PATENT REFORM

SEC. 541. DESIGN PATENT TERM HARMONIZED.

(a) Term amended.—Section 173 of title 35, United States Code, is amended to read as follows:

"Sec. 173. Term of design patent.

"Subject to the payment of fees under this title, patents for designs shall be granted for a term beginning on the date on which the patent issues and ending 20 years from the date on which the application for the patent was filed in the United States or, if the application contains a specific reference to an earlier filed application or applications under section 120, 121, 365(c), or 386(c), from the date on which the earliest such application was filed.".

(b) Applicability.—The amendment made by subsection (a) shall apply to any design patent issued on an application filed before, on, or after the date of enactment of this Act.

SEC. 542. PATENT MAINTENANCE FEES; ESCALATION; INDEXING; TRANSITION.

(a) Maintenance fee schedule.—Section 41 of title 35, United States Code, is amended—

(1) in subsection (a)(7), by adding "." at the end;

(2) in subsection (b)(1) to read as follows—

"(1) In general.—The Director shall charge the following fees for maintaining in force all patents, other than plant patents, based on applications filed on or after December 12, 1980:

"(A) 3 years and 6 months after grant, $2,500.

"(B) 7 years after grant, $5,000.

"(C) 10 years and 6 months after grant, $10,000.

"(D) 14 years after grant, $20,000.

"(E) 17 years after grant, $40,000."; and

(3) by repealing subsection (b)(3) and adding the following new paragraphs after subsection (b)(2)—

"(3) No maintenance fee for plant patent.—No fee may be established for maintaining a plant patent in force.

"(4) No fee after expiration.—No maintenance fee under paragraph (1), and no surcharge for late payment of such fee, shall be due after expiration of the term of the patent.

"(5) Transition rule.—

"(A) No maintenance fee under paragraph (1), and no surcharge for late payment of such fee, shall be due for any payment date that occurred before January 1, 2027.

"(B) Nothing in this paragraph shall revive any patent that expired or lapsed before January 1, 2027.

"(6) Transition rule for additional maintenance fees.—

"(A) No maintenance fee under paragraph (1)(D) shall apply to a grant issued on or before December 31, 2012.

"(B) No maintenance fee under paragraph (1)(E) shall apply to a grant issued on or before December 31, 2009.

"(7) Design patent transition rule.—No maintenance fee under paragraph (1), and no surcharge for late payment of such fee, shall be due for a design patent before January 1, 2027."; and

(4) in subsection (f) by—

(A) striking "may be adjusted" and inserting "shall be adjusted"; and

(B) striking "may be ignored" and inserting "shall be included in the next annual adjustment.".

SEC. 543. SCALE LIMITS ON FEE DISCOUNTS; AGGREGATION; FRAUD PENALTIES.

(a) Portfolio limitation on discounts.—Section 41(h) of title 35, United States Code, is amended by adding at the end the following:

"(4) Portfolio limitation.—Notwithstanding any other provision of this subsection, no reduction in fees under this subsection shall apply with respect to any maintenance fee due under subsection (b) if the owner of the patent, or any commonly controlled entity, owns more than 25 issued United States patents as of the date such maintenance fee is paid.

"(5) Common control.—For purposes of this subsection, entities shall be treated as commonly controlled if they are under common ownership or control, including through direct

ownership, indirect ownership, exclusive licensing arrangements, or any contractual obligation to assign or license patent rights, as determined by the Director by regulation.".

(b) Fraudulent assertion of entity status.—Section 41 of title 35, United States Code, is amended by adding at the end the following:

"(k) Fraudulent assertion of small or micro entity status.—

"(1) In general.—Any person who knowingly or recklessly asserts small entity or micro-entity status under this section, or fails to timely correct such status after it no longer applies, shall be subject to a civil penalty.

"(2) Penalty amount.—The civil penalty under this subsection shall be the greater of—

"(A) 3 times the amount of fees avoided by reason of such false or improper assertion; or

"(B) $10,000 multiplied by the total number of issued United States patents owned by the person or by any commonly controlled entity at the time of the violation.

"(3) Additional remedies.—In addition to any penalty imposed under paragraph (2), the Director may—

"(A) require payment of all unpaid fees at the undiscounted rate, with interest calculated from the date each unpaid fee was due at the rate and in the manner provided under sections 6621(a)(2) and 6622(a) of the Internal Revenue Code of 1986;

"(B) impose administrative sanctions, including suspension of eligibility for fee discounts for a period of not less than 5 years; and

"(C) refer evidence of willful misconduct to the Attorney General for appropriate action.

"(4) Rule of construction.—A pattern of misrepresentation, concealment, or portfolio fragmentation shall constitute prima facie evidence of recklessness under this subsection.

"(l) Portfolio disclosure and verification authority.—The Director may require, as a condition of payment of any maintenance fee or assertion of small or micro entity status, disclosure of information sufficient to determine—

"(1) the total number of issued United States patents owned by the person making such payment or assertion; and

"(2) whether such patents are owned or controlled by commonly controlled entities.

"The Director may conduct audits and investigations as reasonably necessary to enforce this section.

"(m) Administrative process.—Before imposing a civil penalty or administrative sanction under subsection (k), the Director shall provide written notice of the alleged violation and the proposed penalty or sanction, and a reasonable opportunity to respond. A final determination under subsection (k) shall be made on the record after consideration of any timely submission by the

person charged and shall be subject to administrative review under procedures prescribed by the Director.".

SEC. 544. DISPOSITION OF PATENT FEES.

(a) In general.—Notwithstanding any other provision of law, all amounts collected as maintenance fees under section 41(b) of title 35, United States Code, including any penalties collected under section 41(k), shall be deposited into the general fund of the Treasury and disbursed in accordance with this section.

(b) American Value Fund.—99 percent of all amounts deposited pursuant to subsection (a) shall be credited to the American Value Fund established in title VI of the POPULIST Act.

(c) United States Patent and Trademark Office.—1 percent of all amounts deposited pursuant to subsection (a) shall be transferred to the United States Patent and Trademark Office and shall be available, without further appropriation, solely for patent examination, information technology modernization, fraud detection, and administrative enforcement.

(d) Budgetary treatment.—Amounts transferred under this section shall be treated as offsetting receipts for purposes of the Congressional Budget Act of 1974.

PART III—TRADEMARK REFORM

SEC. 551. SEVEN-YEAR TRADEMARKS.

(a) Renewal period.—

(1) In general.—Section 9(a) of the Trademark Act of 1946 (15 U.S.C. 1059(a)) is amended to read as follows:

"(a) Period of renewal; time for renewal.—

"(1) In general.—Subject to the provisions of section 1058 of this title, each registration may be renewed for periods of 7 years at the end of each successive 7-year period following the date of registration upon payment of the fee prescribed under section 1113(c) of this title and the filing of a written application, in such form as may be prescribed by the Director.

"(2) Time for renewal.—An application under paragraph (1) may be made at any time within 1 year before the end of each successive 7-year period for which the registration was issued or renewed, or may be made within a grace period of 6 months after the end of each successive 7-year period, upon payment of the fee prescribed under section 1113(c) of this title and any surcharge prescribed therefor.

"(3) Deficient application.—If any application filed under this section is deficient, the deficiency may be corrected within the time prescribed after notification of the deficiency, upon payment of a surcharge prescribed therefor.".

(2) Applicability.—The amendment made by paragraph (1) shall apply to any registration issued or any renewal period beginning after the date of enactment of this Act, without regard to the date on which the application or renewal application was filed. A registration issued, or

renewal period beginning, on or before such date shall remain subject to the expiration date applicable before the amendment made by paragraph (1).

(b) Declaration of use or excusable nonuse.—

(1) In general.—Section 8(a) of the Trademark Act of 1946 (15 U.S.C. 1058(a)) is amended to read as follows:

"(a) Time periods for required affidavits.—

"(1) In general.—Each registration shall remain in force for 7 years, except that the registration of any mark shall be canceled by the Director unless the owner of the registration files in the United States Patent and Trademark Office affidavits that meet the requirements of subsection (b), within the 1-year period immediately preceding the expiration of each 7-year period following the date of registration under this chapter or the date of publication under section 1062(c) of this title.

"(2) Grace period.—The owner may file the affidavit required under this section within the 6-month grace period immediately following the expiration of the period established in paragraph (1), together with the fee described in subsection (b) and the additional grace period surcharge prescribed by the Director.".

(2) Applicability.—The amendment made by paragraph (1) shall apply to any registration issued or any renewal period beginning after the date of enactment of this Act, without regard to the date on which the application or renewal application was filed. A registration issued, or renewal period beginning, on or before such date shall remain subject to the expiration date applicable before the amendment made by paragraph (1).

(c) Bona fide commercial use.—Section 8(b)(1) of the Trademark Act of 1946 (15 U.S.C. 1058(b)(1)) is amended by striking subparagraph (C) and inserting the following:

"(C) be accompanied by such representative evidence demonstrating bona fide commercial use in commerce as may be required by the Director; and".

(d) Token use.—Section 8 of the Trademark Act of 1946 (15 U.S.C. 1058) is amended by adding at the end the following:

"(g) Token use.—Use of a mark solely for the purpose of maintaining a registration, reserving a mark, or preventing use by others, without genuine commercial exploitation, shall not constitute bona fide commercial use in commerce as required by subsection (b)(1)(C).".

(e) Portfolio-based registration and renewal fees.—Section 31 of the Trademark Act of 1946 (15 U.S.C. 1113) is amended by adding at the end the following:

"(c) Portfolio-based registration and renewal fees.—

"(1) In general.—Beginning January 1, 2027, any fee required for an application for registration of a trademark or other mark under section 1051 of this title or for renewal of a trademark registration under section 1059(a) of this title shall be determined based on the size of the portfolio of the applicant or registrant at the time the fee is paid.

"(2) Base amount.—The base amount for a fee under this subsection shall be $250.

"(3) Escalation formula.—The fee applicable under this subsection shall be equal to the base amount multiplied by n raised to the power of 0.30, where n equals the size of the portfolio owned or controlled by the applicant or registrant at the time the fee is paid. The resulting fee shall be rounded to the nearest whole dollar.

"(4) Class application.—The fee determined under this subsection shall apply equally to each class included in an application for registration or filing for renewal.

"(5) Paper filing.—The Director may impose an additional fee for paper filing of an application for registration or renewal application.

"(6) Transition rules.—

"(A) Early-filed renewals.—A renewal application filed before January 1, 2027, for a renewal period beginning on or after January 1, 2027, shall be treated as conditionally filed and may not be accepted as complete, and the registration may not be renewed, until the applicant or registrant pays the full fee required under this subsection.

"(B) Credit for prior payment.—Any fee paid before January 1, 2027, for a renewal application described in subparagraph (A) shall be credited against the fee required under this subsection.

"(7) Indexing.—Beginning January 1, 2028, the base amount specified in paragraph (2) shall be adjusted annually by the percentage change in the Consumer Price Index for All Urban Consumers, rounded to the nearest $5.

"(d) Portfolio certification.—Each applicant or registrant submitting an application for registration or renewal application shall certify, under penalty of perjury, the size of the applicant or registrant's portfolio as of the date of such filing.

"(e) Audit and verification.—The Director may conduct audits and require production of information reasonably necessary to verify—

"(1) the accuracy of any portfolio certification submitted under subsection (d);

"(2) the existence of common control among entities; or

"(3) contractual rights and licensing arrangements related to trademarks.

"(f) False statement or material omission.—Any person who knowingly or recklessly makes a false statement or material omission in any certification or disclosure required under this section shall be subject to penalty.

"(1) Civil penalty.—The Director may impose a civil penalty equal to the greater of—

"(A) 3 times the amount of fees avoided by reason of the false statement or omission; or

"(B) $5,000 multiplied by the total number of items in the portfolio of the person at the time of the violation.

"(2) Additional remedies.—In addition to any civil penalty, the Director may—

"(A) bar the person, for a period of 6 years, from—

"(i) registering any new trademark; or

"(ii) renewing any trademark owned or controlled by the person at the time of the violation; and

"(B) refer evidence of willful misconduct to the Attorney General for appropriate action.

"(3) Rule of construction.—A pattern of misrepresentation, concealment, or portfolio fragmentation shall constitute prima facie evidence of recklessness under this subsection.

"(4) Administrative process.—Before imposing a civil penalty or administrative sanction under this subsection, the Director shall provide written notice of the alleged violation and the proposed penalty or sanction, and a reasonable opportunity to respond. A final determination under this subsection shall be made on the record after consideration of any timely submission by the person charged and shall be subject to administrative review under procedures prescribed by the Director.

"(g) Rulemaking.—The Director shall issue regulations to implement this section, including standards for determining common control, audit selection, evidentiary requirements, procedures for calculating portfolio size, procedures for treating simultaneous or batch filings, procedures for notifying applicants or registrants of fee deficiencies, and procedures for crediting prior payments.

"(h) Definitions.—In this section:

"(1) Active trademark registration.—The term 'active trademark registration' means any registration that has not been irrevocably cancelled or expired, including any registration within a renewal window or statutory grace period.

"(2) Common control.—The term 'common control' means the direct or indirect ownership or control of trademarks or applications for registration by the same person or entity, including through parent-subsidiary relationships, common ownership, exclusive licensing arrangements, or contractual obligations to assign or license trademark rights.

"(3) Portfolio.—The term 'portfolio' means, with respect to an applicant or registrant, the aggregate of the following items under common control:

"(A) active trademark registrations;

"(B) pending applications for registration; and

"(C) in the case of an application for registration, such application.".

SEC. 552. DISPOSITION OF TRADEMARK FEES.

(a) In general.—Notwithstanding any other provision of law, all fees collected under sections 8, 9, and 31 of the Trademark Act of 1946 (15 U.S.C. 1058, 1059, and 1113), including registration fees, renewal fees, late fees, and penalties, shall be deposited into the general fund of the Treasury and disbursed in accordance with this section.

(b) American Value Fund.—99 percent of all amounts deposited pursuant to subsection (a) shall be credited to the American Value Fund established in title VI of the POPULIST Act.

(c) United States Patent and Trademark Office.—1 percent of all amounts deposited pursuant to subsection (a) shall be transferred to the United States Patent and Trademark Office and shall be available, without further appropriation, solely for trademark examination, registry maintenance, fraud detection, enforcement of use requirements, and administrative modernization.

(d) Budgetary treatment.—Amounts transferred under this section shall be treated as offsetting receipts for purposes of the Congressional Budget Act of 1974 (2 U.S.C. 621 et seq.).

Subtitle D—Data Privacy and Protection

SEC. 561. DEFINITIONS.

(a) Definitions.—In this subtitle:

(1) Affirmative express consent.—

(A) In general.—The term "affirmative express consent" means an affirmative act by an individual that clearly communicates the individual's freely given, specific, and unambiguous authorization for an act or practice after having been informed, in response to a specific request from a covered entity that meets the requirements of subparagraph (B).

(B) Request requirements.—The requirements of this subparagraph with respect to a request from a covered entity to an individual are the following:

(i) The request is provided to the individual in a clear and conspicuous standalone disclosure made through the primary medium used to offer the covered entity's product or service, or only if the product or service is not offered in a medium that permits the making of the request under this paragraph, another medium regularly used in conjunction with the covered entity's product or service.

(ii) The request includes a description of the processing purpose for which the individual's consent is sought and—

(I) clearly states the specific categories of covered data that the covered entity shall collect, process, and transfer necessary to effectuate the processing purpose; and

(II) includes a prominent heading and is written in easy-to-understand language that would enable a reasonable individual to identify and understand the processing purpose for which consent is sought and the covered data to be collected, processed, or transferred by the covered entity for such processing purpose.

(iii) The request clearly explains the individual's applicable rights related to consent.

(iv) The request is made in a manner reasonably accessible to and usable by individuals with disabilities.

(v) The request is made available to the individual in each covered language in which the covered entity provides a product or service for which authorization is sought.

(vi) The option to refuse consent shall be at least as prominent as the option to accept, and the option to refuse consent shall take the same number of steps or fewer as the option to accept.

(vii) Processing or transferring any covered data collected pursuant to affirmative express consent for a different processing purpose than that for which affirmative express consent was obtained shall require affirmative express consent for the subsequent processing purpose.

(C) Express consent required.—A covered entity may not infer that an individual has provided affirmative express consent to an act or practice from—

(i) the inaction of the individual;

(ii) the individual's continued use of a service or product provided by the covered entity; or

(iii) the individual's approval of a preselected default option.

(D) Pretextual consent prohibited.—A covered entity may not obtain or attempt to obtain the affirmative express consent of an individual through—

(i) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(ii) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to provide such consent or any covered data.

(2) Authentication.—The term "authentication" means the process of verifying an individual or entity for security purposes.

(3) Biometric information.—

(A) In general.—The term "biometric information" means any covered data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual, including—

(i) fingerprints;

(ii) voice prints;

(iii) iris or retina scans;

(iv) facial or hand mapping, geometry, or templates; or

(v) gait or personally identifying physical movements.

(B) Exclusion.—The term "biometric information" does not include—

(i) a digital or physical photograph;

(ii) an audio or video recording; or

(iii) data generated from a digital or physical photograph, or an audio or video recording, that cannot be used to identify an individual.

(4) Child.—The term "child" means a covered minor under 13 years of age.

(5) Collect; collection.—The terms "collect" and "collection" mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means.

(6) Commission.—The term "Commission" means the Federal Trade Commission.

(7) Control.—The term "control" means, with respect to an entity—

(A) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of the entity;

(B) control over the election of a majority of the directors of the entity (or of individuals exercising similar functions); or

(C) the power to exercise a controlling influence over the management of the entity.

(8) Covered algorithm.—The term "covered algorithm" means a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity and that makes a decision or facilitates human decision making with respect to covered data, including to determine the provision of products or services or to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to an individual.

(9) Covered data.—

(A) In general.—The term "covered data" means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to an individual, and may include derived data and unique persistent identifiers.

(B) Exclusions.—The term "covered data" does not include—

(i) de-identified data;

(ii) employee data;

(iii) publicly available information; or

(iv) inferences made exclusively from multiple independent sources of publicly available information that do not reveal sensitive covered data with respect to an individual.

(C) Employee data defined.—For purposes of subparagraph (B), the term "employee data" means—

(i) information relating to a job applicant collected by a covered entity acting as a prospective employer of such job applicant in the course of the application, or hiring process, if such information is collected, processed, or transferred by the prospective employer solely for purposes related to the employee's status as a current or former job applicant of such employer;

(ii) information processed by an employer relating to an employee who is acting in a professional capacity for the employer, provided that such information is collected, processed, or transferred solely for purposes related to such employee's professional activities on behalf of the employer;

(iii) the business contact information of an employee, including the employee's name, position or title, business telephone number, business address, or business email address that is provided to an employer by an employee who is acting in a professional capacity, if such information is collected, processed, or transferred solely for purposes related to such employee's professional activities on behalf of the employer;

(iv) emergency contact information collected by an employer that relates to an employee of that employer, if such information is collected, processed, or transferred solely for the purpose of having an emergency contact on file for the employee and for processing or transferring such information in case of an emergency; or

(v) information relating to an employee (or a spouse, dependent, other covered family member, or beneficiary of such employee) that is necessary for the employer to collect, process, or transfer solely for the purpose of administering benefits to which such employee (or spouse, dependent, other covered family member, or beneficiary of such employee) is entitled on the basis of the employee's position with that employer.

(10) Covered entity.—

(A) In general.—The term "covered entity"—

(i) means any entity or any person, other than an individual acting in a noncommercial context, that alone or jointly with others determines the purposes and means of collecting, processing, or transferring covered data and—

(I) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.);

(II) is a common carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto; or

(III) is an organization not organized to carry on business for its own profit or that of its members; and

(ii) includes any entity or person that controls, is controlled by, or is under common control with the covered entity.

(B) Exclusions.—The term "covered entity" does not include—

(i) a Federal, State, Tribal, territorial, or local government entity such as a body, authority, board, bureau, commission, district, agency, or political subdivision of the Federal Government or a State, Tribal, territorial, or local government;

(ii) a person or an entity that is collecting, processing, or transferring covered data on behalf of a Federal, State, Tribal, territorial, or local government entity, in so far as such person or entity is acting as a service provider to such government entity, provided that such person or entity shall remain subject to all requirements of this subtitle applicable to service providers; or

(iii) an entity that serves as a congressionally designated nonprofit, national resource center, and clearinghouse to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

(C) Nonapplication to service providers.—An entity shall not be considered to be a covered entity for purposes of this subtitle in so far as the entity is acting as a service provider.

(11) Covered language.—The term "covered language" means the 10 languages with the most users in the United States, according to the most recent United States Census.

(12) Covered minor.—The term "covered minor" means an individual under the age of 17.

(13) De-identified data.—The term "de-identified data" means information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated, and if the covered entity or service provider—

(A) takes reasonable technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;

(B) publicly commits in a clear and conspicuous manner—

(i) to process and transfer the information solely in a de-identified form without any reasonable means for re-identification; and

(ii) to not attempt to re-identify the information with any individual or device that identifies or is linked or reasonably linkable to an individual; and

(C) contractually obligates any person or entity that receives the information from the covered entity or service provider—

(i) to comply with all of the provisions of this paragraph with respect to the information; and

(ii) to require that such contractual obligations be included contractually in all subsequent instances for which the data may be received.

(14) Derived data.—The term "derived data" means covered data that is created by the derivation of information, data, assumptions, correlations, inferences, predictions, or

conclusions from facts, evidence, or another source of information or data about an individual or an individual's device.

(15) Device.—The term "device" means any electronic equipment capable of collecting, processing, or transferring covered data that is used by 1 or more individuals.

(16) Employee.—The term "employee" means an individual who is an employee, director, officer, staff member, or individual working as an independent contractor that is not a service provider, trainee, volunteer, or intern of an employer, regardless of whether such individual is paid, unpaid, or employed on a temporary basis.

(17) Executive agency.—The term "Executive agency" has the meaning given such term in section 105 of title 5, United States Code.

(18) First party advertising or marketing.—The term "first party advertising or marketing" means advertising or marketing conducted by a first party either through direct communications with a user such as direct mail, email, or text message communications, or advertising or marketing conducted entirely within the first-party context, such as in a physical location operated by the first party, or on a web site or app operated by the first party.

(19) Genetic information.—The term "genetic information" means any covered data, regardless of its format, that concerns an individual's genetic characteristics, including—

(A) raw sequence data that results from the sequencing of the complete, or a portion of the, extracted deoxyribonucleic acid (DNA) of an individual; or

(B) genotypic and phenotypic information that results from analyzing raw sequence data described in subparagraph (A).

(20) Individual.—The term "individual" means a natural person residing in the United States.

(21) Knowledge.—

(A) In general.—The term "knowledge", with respect to whether an individual is a covered minor, means actual knowledge or knowledge fairly implied on the basis of objective circumstances.

(B) Rule of construction.—Nothing in this subtitle, including subparagraph (A), shall be construed to require a covered entity or service provider to—

(i) affirmatively collect any covered data with respect to age that the covered entity or service provider is not otherwise collecting in the normal course of business; or

(ii) implement age-gating or age-verification functionality.

(C) Guidance.—Not later than January 1, 2027, the Commission shall issue guidance, including best practices and examples, to assist covered entities and service providers in determining whether they have knowledge fairly implied on the basis of objective circumstances that an individual is a covered minor.

(22) Large data holder.—

(A) In general.—The term "large data holder" means a covered entity or service provider that, in the most recent calendar year—

(i) had annual gross revenues of $250,000,000 or more; and

(ii) collected, processed, or transferred—

(I) the covered data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding covered data collected and processed solely for the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested product or service; or

(II) the sensitive covered data of more than 200,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals.

(B) Exclusions.—The term "large data holder" does not include any instance in which the covered entity or service provider would qualify as a large data holder solely on the basis of collecting or processing—

(i) personal email addresses;

(ii) personal telephone numbers; or

(iii) log-in information of an individual or device to allow the individual or device to log in to an account administered by the covered entity or service provider.

(C) Revenue.—For purposes of determining whether any covered entity or service provider is a large data holder, the term "revenue", with respect to any covered entity or service provider that is not organized to carry on business for its own profit or that of its members—

(i) means the gross receipts the covered entity or service provider received, in whatever form, from all sources, without subtracting any costs or expenses; and

(ii) includes contributions, gifts, grants, dues or other assessments, income from investments, and proceeds from the sale of real or personal property.

(23) Market research.—The term "market research" means the collection, processing, or transfer of covered data as reasonably necessary and proportionate to investigate the market for or marketing of products, services, or ideas, where the covered data is not—

(A) integrated into any product or service;

(B) otherwise used to contact any individual or individual's device; or

(C) used to advertise or market to any individual or individual's device.

(24) Material.—The term "material" means, with respect to an act, practice, or representation of a covered entity (including a representation made by the covered entity in a privacy policy or similar disclosure to individuals) involving the collection, processing, or

transfer of covered data, that such act, practice, or representation is likely to affect a reasonable individual's decision or conduct regarding a product or service.

(25) Online product or service.—The term "online product or service" means a website, online service, online application, or mobile application.

(26) Parent.—The term "parent" means a parent or legal guardian.

(27) Person.—The term "person" has the meaning given the term in subsection (a) of section 1 of the Clayton Act (15 U.S.C. 12).

(28) Precise geolocation information.—

(A) In general.—The term "precise geolocation information" means information that is derived from a device or technology that reveals the past or present physical location of an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, with sufficient precision to identify street level location information of an individual or device or the location of an individual or device within a range of 1,850 feet or less.

(B) Exclusion.—The term "precise geolocation information" does not include geolocation information identifiable or derived solely from the visual content of a legally obtained image, including the location of the device that captured such image.

(29) Process.—The term "process" means to conduct or direct any operation or set of operations performed on covered data, including analyzing, organizing, structuring, retaining, storing, using, or otherwise handling covered data.

(30) Processing purpose.—The term "processing purpose" means a reason for which a covered entity or service provider collects, processes, or transfers covered data that is specific and granular enough for a reasonable individual to understand the material facts of how and why the covered entity or service provider collects, processes, or transfers the covered data.

(31) Publicly available information.—

(A) In general.—The term "publicly available information" means any information that a covered entity or service provider has a reasonable basis to believe has been lawfully made available to the general public from—

(i) Federal, State, or local government records, if the covered entity collects, processes, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity;

(ii) widely distributed media;

(iii) a website or online service made available to all members of the public, for free or for a fee, including where all members of the public, for free or for a fee, can log in to the website or online service;

(iv) a disclosure that has been made to the general public as required by Federal, State, or local law; or

(v) the visual observation of the physical presence of an individual or a device in a public place, not including data collected by a device in the individual's possession.

(B) Clarifications; limitations.—

(i) Available to all members of the public.—For purposes of this paragraph, information from a website or online service is not available to all members of the public if the individual who made the information available via the website or online service has restricted the information to a specific audience.

(ii) Other limitations.—The term "publicly available information" does not include—

(I) any obscene visual depiction (as defined in section 1460 of title 18, United States Code);

(II) any inference made exclusively from multiple independent sources of publicly available information that reveals sensitive covered data with respect to an individual;

(III) biometric information;

(IV) publicly available information that has been combined with covered data;

(V) genetic information, unless otherwise made available by the individual to whom the information pertains as described in clause (ii) or (iii) of subparagraph (A); or

(VI) intimate images known to be nonconsensual.

(32) Sensitive covered data.—

(A) In general.—The term "sensitive covered data" means the following types of covered data:

(i) A government-issued identifier, such as a Social Security number, passport number, or driver's license number, that is not required by law to be displayed in public.

(ii) Any information that describes or reveals the past, present, or future physical health, mental health, disability, diagnosis, or health care condition or treatment of an individual.

(iii) A financial account number, debit card number, credit card number, or information that describes or reveals the income level or bank account balances of an individual, except that the last 4 digits of a debit or credit card number shall not be deemed sensitive covered data.

(iv) Biometric information.

(v) Genetic information.

(vi) Precise geolocation information.

(vii) An individual's private communications such as voicemails, emails, texts, direct messages, or mail, or information identifying the parties to such communications, voice communications, video communications, and any information that pertains to the transmission of such communications, including telephone numbers called, telephone numbers from which calls were placed, the time calls were made, call duration, and location information of the parties to the call, unless the covered entity or a service provider acting on behalf of the covered entity is the sender or an intended recipient of the communication. Communications are not private for purposes of this clause if such communications are made from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that such employer may access such communications.

(viii) Account or device log-in credentials, or security or access codes for an account or device.

(ix) Information identifying the sexual behavior of an individual in a manner inconsistent with the individual's reasonable expectation regarding the collection, processing, or transfer of such information.

(x) Calendar information, address book information, phone or text logs, photos, audio recordings, or videos, maintained for private use by an individual, regardless of whether such information is stored on the individual's device or is accessible from that device and is backed up in a separate location. Such information is not sensitive for purposes of this paragraph if such information is sent from or to a device provided by an employer to an employee insofar as such employer provides conspicuous notice that it may access such information.

(xi) A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual.

(xii) Information revealing the video content requested or selected by an individual collected by a covered entity that is not a provider of a service described in section 562(b)(6). This clause does not include covered data used solely for transfers for independent video measurement.

(xiii) Information about an individual when the covered entity or service provider has knowledge that the individual is a covered minor.

(xiv) An individual's race, color, ethnicity, religion, or union membership.

(xv) Information identifying an individual's online activities over time and across third-party websites or online services.

(xvi) Any other covered data collected, processed, or transferred for the purpose of identifying the types of covered data listed in clauses (i) through (xv).

(B) Rulemaking.—The Commission may commence a rulemaking pursuant to section 553 of title 5, United States Code, to include in the definition of "sensitive covered data" any other type of covered data that may require a similar level of protection as the types of

covered data listed in clauses (i) through (xvi) of subparagraph (A) as a result of any new method of collecting, processing, or transferring covered data.

(33) Service provider.—

(A) In general.—The term "service provider" means a person or entity that—

(i) collects, processes, or transfers covered data on behalf of, and at the direction of, a covered entity or a Federal, State, Tribal, territorial, or local government entity; and

(ii) receives covered data from or on behalf of a covered entity or a Federal, State, Tribal, territorial, or local government entity.

(B) Treatment with respect to service provider data.—A service provider that receives service provider data from another service provider as permitted under this subtitle shall be treated as a service provider under this subtitle with respect to such data.

(34) Service provider data.—The term "service provider data" means covered data that is collected or processed by or has been transferred to a service provider by or on behalf of a covered entity, a Federal, State, Tribal, territorial, or local government entity, or another service provider for the purpose of allowing the service provider to whom such covered data is transferred to perform a service or function on behalf of, and at the direction of, such covered entity or Federal, State, Tribal, territorial, or local government entity.

(35) State.—The term "State" means any of the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, the Virgin Islands of the United States, Guam, American Samoa, or the Commonwealth of the Northern Mariana Islands.

(36) State privacy authority.—The term "State privacy authority" means—

(A) the chief consumer protection officer of a State; or

(B) a State consumer protection agency with expertise in data protection, including the California Privacy Protection Agency.

(37) Substantial privacy risk.—The term "substantial privacy risk" means the collection, processing, or transfer of covered data in a manner that may result in any reasonably foreseeable substantial physical injury, economic injury, highly offensive intrusion into the privacy expectations of a reasonable individual under the circumstances, or discrimination on the basis of race, color, religion, national origin, sex, or disability.

(38) Targeted advertising.—The term "targeted advertising"—

(A) means presenting to an individual or device identified by a unique identifier, or groups of individuals or devices identified by unique identifiers, an online advertisement that is selected based on known or predicted preferences, characteristics, or interests associated with the individual or a device identified by a unique identifier; and

(B) does not include—

(i) advertising or marketing to an individual or an individual's device in response to the individual's specific request for information or feedback;

(ii) contextual advertising, which is when an advertisement is displayed based on the content in which the advertisement appears and does not vary based on who is viewing the advertisement; or

(iii) processing covered data solely for measuring or reporting advertising or content, performance, reach, or frequency, including independent measurement.

(39) Third party.—The term "third party"—

(A) means any person or entity, including a covered entity, that—

(i) collects, processes, or transfers covered data that the person or entity did not collect directly from the individual linked or linkable to such covered data; and

(ii) is not a service provider with respect to such data; and

(B) does not include a person or entity that collects covered data from another entity if the 2 entities are related by common ownership or corporate control, but only if a reasonable consumer's reasonable expectation would be that such entities share information.

(40) Third-party collecting entity.—

(A) In general.—The term "third-party collecting entity"—

(i) means a covered entity whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to the covered data; and

(ii) does not include a covered entity insofar as such entity processes employee data collected by and received from a third party concerning any individual who is an employee of the third party for the sole purpose of such third party providing benefits to the employee.

(B) Principal source of revenue defined.—For purposes of this paragraph, the term "principal source of revenue" means, for the prior 12-month period, either—

(i) more than 50 percent of all revenue of the covered entity; or

(ii) obtaining revenue from processing or transferring the covered data of more than 5,000,000 individuals that the covered entity did not collect directly from the individuals linked or linkable to the covered data.

(C) Nonapplication to service providers.—An entity may not be considered to be a third-party collecting entity for purposes of this subtitle if the entity is acting as a service provider.

(41) Third-party data.—The term "third-party data" means covered data that has been transferred to a third party.

(42) Transfer.—The term "transfer" means to disclose, release, disseminate, make available, license, rent, or share covered data orally, in writing, electronically, or by any other means.

(43) Unique identifier.—The term "unique identifier"—

(A) means an identifier to the extent that such identifier is reasonably linkable to an individual or device that identifies or is linked or reasonably linkable to 1 or more individuals, including a device identifier, Internet Protocol address, cookie, beacon, pixel tag, mobile ad identifier, or similar technology, customer number, unique pseudonym, user alias, telephone number, or other form of persistent or probabilistic identifier that is linked or reasonably linkable to an individual or device; and

(B) does not include an identifier assigned by a covered entity for the specific purpose of giving effect to an individual's exercise of affirmative express consent, or of opt-outs or other limits, with respect to the collection, processing, or transfer of such information.

(44) Widely distributed media.—The term "widely distributed media" means information that is available to the general public, including information from a telephone book or online directory, a television, internet, or radio program, the news media, or an internet site that is available to the general public on an unrestricted basis, but does not include an obscene visual depiction (as defined in section 1460 of title 18, United States Code).

SEC. 562. DATA MINIMIZATION AND LOYALTY OBLIGATIONS.

(a) Data minimization.—

(1) In general.—A covered entity may not collect, process, or transfer covered data unless the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to—

(A) provide or maintain a specific product or service requested by the individual to whom the data pertains; or

(B) effect a purpose permitted under paragraph (2).

(2) Permissible purposes.—A covered entity may collect, process, or transfer covered data for any of the following purposes if the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to such purpose:

(A) To initiate, manage, or complete a transaction or fulfill an order for specific products or services requested by an individual, including any associated routine administrative, operational, and account servicing activity such as billing, shipping, delivery, storage, and accounting.

(B) With respect to covered data previously collected in accordance with this subtitle, notwithstanding this exception—

(i) to process such data as necessary to perform system maintenance or diagnostics;

(ii) to develop, maintain, repair, or enhance a product or service for which such data was collected;

(iii) to conduct internal research or analytics to improve a product or service for which such data was collected;

(iv) to perform inventory management or reasonable network management;

(v) to protect against spam; or

(vi) to debug or repair errors that impair the functionality of a service or product for which such data was collected.

(C) To authenticate users of a product or service.

(D) To fulfill a product or service warranty.

(E) To prevent, detect, protect against, or respond to a security incident. For purposes of this subparagraph, security is defined as network security and physical security and life safety, including an intrusion or trespass, medical alerts, fire alarms, and access control security.

(F) To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity. For purposes of this subparagraph, the term "illegal activity" means a violation of a Federal, State, or local law punishable as a felony or misdemeanor that can directly harm another person.

(G) To comply with a legal obligation imposed by Federal, Tribal, local, or State law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the covered entity or service provider.

(H) To prevent an individual, or group of individuals, from suffering harm where the covered entity or service provider believes in good faith that the individual, or group of individuals, is at risk of death, serious physical injury, or other serious health risk.

(I) To effectuate a product recall pursuant to Federal or State law.

(J) (i) To conduct a public or peer-reviewed scientific, historical, or statistical research project that—

(I) is in the public interest; and

(II) adheres to all relevant laws and regulations governing such research, including regulations for the protection of human subjects, or is excluded from criteria of the institutional review board.

(ii) Not later than July 1, 2027, the Commission shall issue guidelines to help covered entities ensure the privacy of affected users and the security of covered data, particularly as data is being transferred to and stored by researchers. Such guidelines should consider risks as they pertain to projects using covered data with special considerations for projects that are exempt under part 46 of title 45, Code of Federal

Regulations (or any successor regulation) or are excluded from the criteria for institutional review board review.

(K) To deliver a communication that is not an advertisement to an individual, if the communication is reasonably anticipated by the individual within the context of the individual's interactions with the covered entity.

(L) To deliver a communication at the direction of an individual between such individual and 1 or more individuals or entities.

(M) To transfer assets to a third party in the context of a merger, acquisition, bankruptcy, or similar transaction when the third party assumes control, in whole or in part, of the covered entity's assets, only if the covered entity, in a reasonable time prior to such transfer, provides each affected individual with—

(i) a notice describing such transfer, including the name of the entity or entities receiving the individual's covered data and their privacy policies as described in section 563(b); and

(ii) a reasonable opportunity to withdraw any previously given consents in accordance with the requirements of affirmative express consent under this subtitle related to the individual's covered data and a reasonable opportunity to request the deletion of the individual's covered data, as described in section 563(c).

(N) To ensure the data security and integrity of covered data, as described in section 564(a).

(O) With respect to covered data previously collected in accordance with this subtitle, a service provider acting at the direction of a government entity, or a service provided to a government entity by a covered entity, and only insofar as authorized by statute, to prevent, detect, protect against or respond to a public safety incident, including trespass, natural disaster, or national security incident. This subparagraph does not permit, however, the transfer of covered data for payment or other valuable consideration to a government entity.

(P) With respect to covered data collected in accordance with this subtitle, notwithstanding this exception, to process such data as necessary to provide non-targeted first party advertising or marketing of products or services provided by the covered entity for individuals who are not covered minors.

(3) Guidance.—Not later than July 1, 2027, the Commission shall issue guidance regarding what is reasonably necessary and proportionate to comply with this subsection. Such guidance shall take into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by, the covered entity, including whether the covered entity is a large data holder, nonprofit organization, covered entity meeting the requirements of section 563(e)(2), third party, or third-party collecting entity;

(B) the sensitivity of covered data collected, processed, or transferred by the covered entity;

(C) the volume of covered data collected, processed, or transferred by the covered entity; and

(D) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity relates.

(4) Deceptive marketing.—A covered entity or service provider may not engage in deceptive advertising or marketing with respect to a product or service offered to an individual.

(5) Journalism.—Nothing in this subtitle shall be construed to limit or diminish First Amendment freedoms guaranteed under the Constitution.

(b) Loyalty duties.—Notwithstanding subsection (a) and unless an exception applies, with respect to covered data, a covered entity or service provider may not—

(1) collect, process, or transfer a Social Security number, except when necessary to facilitate an extension of credit, authentication, fraud and identity fraud detection and prevention, the payment or collection of taxes, the enforcement of a contract between parties, or the prevention, investigation, or prosecution of fraud or illegal activity, or as otherwise required by Federal, State, or local law;

(2) transfer covered data to a third party unless—

(A) the transfer is strictly necessary to provide a specific product or service requested by the individual to whom the covered data pertains;

(B) the transfer is made pursuant to the affirmative express consent of the individual;

(C) the transfer is strictly necessary to effect a purpose enumerated in subsection (a)(2)(E) through (O);

(D) with respect to a covered minor and subject to paragraph (5), the entity or service provider has knowledge that the individual is a covered minor and the transfer is made—

(i) pursuant to affirmative express consent obtained from—

(I) the covered minor, provided such minor is not a child; or

(II) the covered minor's parent; or

(ii) solely in order to submit information relating to victimization of a covered minor to law enforcement or an entity described in section 561(a)(10)(B)(iii); or

(E) the transfer is expressly required by Federal, State, Tribal, or local law;

(3) transfer covered data to a Federal, State, Tribal, territorial, or local government entity, or to any foreign governmental entity, unless—

(A) the transfer is made pursuant to a search warrant;

(B) the transfer is expressly required by Federal, State, Tribal, territorial, or local law;

(C) the transfer is strictly necessary to prevent or respond to an imminent threat of death or serious physical injury; or

(D) the transfer is strictly necessary to effect a purpose enumerated in subsection (a)(2)(E), (G), (H), (I), or (O);

provided that a transfer under this paragraph may not be made for payment or other valuable consideration, except for reimbursement of reasonable costs incurred;

(4) collect or process sensitive covered data, except where such collection or processing is strictly necessary to provide or maintain a specific product or service requested by the individual to whom the covered data pertains, or is strictly necessary to effect a purpose enumerated in subsection (a)(2)(A) through (L) and (N) through (O);

(5) transfer an individual's sensitive covered data to a third party, unless—

(A) the transfer is made pursuant to the affirmative express consent of the individual;

(B) the transfer is necessary to comply with a legal obligation imposed by Federal, State, Tribal, or local law, or to establish, exercise, or defend legal claims;

(C) the transfer is necessary to prevent an individual from imminent injury where the covered entity believes in good faith that the individual is at risk of death, serious physical injury, or serious health risk;

(D) with respect to covered data collected in accordance with this subtitle, notwithstanding this exception, a service provider acting at the direction of a government entity, or a service provided to a government entity by a covered entity, and only insofar as authorized by statute, the transfer is necessary to prevent, detect, protect against or respond to a public safety incident including trespass, natural disaster, or national security incident. This paragraph does not permit, however, the transfer of covered data for payment or other valuable consideration to a government entity;

(E) in the case of the transfer of a password, the transfer is necessary to use a designated password manager or is to a covered entity for the exclusive purpose of identifying passwords that are being reused across sites or accounts;

(F) in the case of the transfer of genetic information, the transfer is necessary to perform a medical diagnosis or medical treatment specifically requested by an individual, or to conduct medical research in accordance with subsection (a)(2)(J); or

(G) to transfer assets in the manner described in subsection (a)(2)(M); or

(6) in the case of a provider of broadcast television service, cable service, satellite service, streaming media service, or other video programming service described in section 713(h)(2) of the Communications Act of 1934 (47 U.S.C. 613(h)(2)), transfer to an unaffiliated third party covered data that reveals the video content or services requested or selected by an individual from such service, except with the affirmative express consent of the individual or pursuant to one of the permissible purposes enumerated in subsection (a)(2)(A) through (O).

(c) Privacy by design.—

(1) Policies, practices, and procedures.—A covered entity and a service provider shall establish, implement, and maintain reasonable policies, practices, and procedures that reflect the role of the covered entity or service provider in the collection, processing, and transferring of covered data and that—

(A) consider applicable Federal laws, rules, or regulations related to covered data the covered entity or service provider collects, processes, or transfers;

(B) identify, assess, and mitigate privacy risks related to covered minors (including, if applicable, with respect to a covered entity that is not an entity meeting the requirements of section 563(e)(2), in a manner that considers the developmental needs of different age ranges of covered minors) to result in reasonably necessary and proportionate residual risk to covered minors;

(C) mitigate privacy risks, including substantial privacy risks, related to the products and services of the covered entity or the service provider, including in the design, development, and implementation of such products and services, taking into account the role of the covered entity or service provider and the information available to it; and

(D) implement reasonable training and safeguards within the covered entity and service provider to promote compliance with all privacy laws applicable to covered data the covered entity collects, processes, or transfers or covered data the service provider collects, processes, or transfers on behalf of the covered entity and mitigate privacy risks, including substantial privacy risks, taking into account the role of the covered entity or service provider and the information available to it.

(2) Factors to consider.—The policies, practices, and procedures established under paragraph (1) shall correspond with, as applicable—

(A) the size of the covered entity or the service provider and the nature, scope, and complexity of the activities engaged in by the covered entity or service provider, including whether the covered entity or service provider is a large data holder, nonprofit organization, entity meeting the requirements of section 563(e)(2), third party, or third-party collecting entity, taking into account the role of the covered entity or service provider and the information available to it;

(B) the sensitivity of the covered data collected, processed, or transferred by the covered entity or service provider;

(C) the volume of covered data collected, processed, or transferred by the covered entity or service provider;

(D) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity or service provider relates; and

(E) the cost of implementing such policies, practices, and procedures in relation to the risks and nature of the covered data.

(3) Commission guidance.—Not later than 1 year after the date of enactment of this subtitle, the Commission shall issue guidance as to what constitutes reasonable policies, practices, and

procedures as required by this subsection. The Commission shall consider unique circumstances applicable to nonprofit organizations, to entities meeting the requirements of section 563(e)(2), and to service providers.

(d) Loyalty with respect to pricing.—

(1) Retaliation prohibited.—A covered entity may not retaliate against an individual for exercising any of the protections established by this subtitle, or any regulations promulgated under this subtitle, including denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services.

(2) Rules of construction.—Nothing in paragraph (1) may be construed to—

(A) prohibit the relation of the price of a service or the level of service provided to an individual to the provision, by the individual, of financial information that is necessarily collected and processed only for the purpose of initiating, rendering, billing for, or collecting payment for a service or product requested by the individual;

(B) prohibit a covered entity from offering a different price, rate, level, quality or selection of goods or services to an individual, including offering goods or services for no fee, if—

(i) the offering is in connection with an individual's voluntary participation in a bona fide loyalty program; and

(ii) the covered entity does not collect, process, or transfer covered data beyond what is strictly necessary to administer such loyalty program;

(C) require a covered entity to provide a bona fide loyalty program that would require the covered entity to collect, process, or transfer covered data that the covered entity otherwise would not collect, process, or transfer;

(D) prohibit a covered entity from offering a financial incentive or other consideration to an individual for participation in market research;

(E) prohibit a covered entity from offering different types of pricing or functionalities with respect to a product or service based on an individual's exercise of a privilege under section 563(c)(1)(C); or

(F) prohibit a covered entity from declining to provide a product or service insofar as the collection and processing of covered data is strictly necessary for such product or service.

(3) Bona fide loyalty program defined.—For purposes of this subsection, the term "bona fide loyalty program" includes rewards, premium features, discount or club card programs.

SEC. 563. CONSUMER DATA CONTROLS.

(a) Consumer awareness.—

(1) In general.—Not later than 120 days after enactment of this Act, the Commission shall publish, on the public website of the Commission, a webpage that describes each provision, protection, obligation, and requirement of this subtitle, listed separately for individuals and for

covered entities and service providers, and the remedies, exemptions, and protections associated with this subtitle, in plain and concise language and in an easy-to-understand manner.

(2) Updates.—The Commission shall update the information published under paragraph (1) on a quarterly basis as necessitated by any change in law, regulation, guidance, or judicial decisions.

(3) Accessibility.—The Commission shall publish the information required to be published under paragraph (1) in the 10 languages with the most users in the United States, according to the most recent United States Census.

(b) Transparency.—

(1) In general.—Each covered entity shall make publicly available, in a clear, conspicuous, not misleading, and easy-to-read and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the data collection, processing, and transfer activities of the covered entity.

(2) Content of privacy policy.—A covered entity or service provider shall have a privacy policy that includes, at a minimum, the following:

(A) The identity and the contact information of—

(i) the covered entity or service provider to which the privacy policy applies (including the covered entity's or service provider's points of contact and generic electronic mail addresses, as applicable for privacy and data security inquiries); and

(ii) any other entity within the same corporate structure as the covered entity or service provider to which covered data is transferred by the covered entity.

(B) The categories of covered data the covered entity or service provider collects or processes.

(C) The processing purposes for each category of covered data the covered entity or service provider collects or processes.

(D) Whether the covered entity or service provider transfers covered data and, if so—

(i) each category of service provider and third party to which the covered entity or service provider transfers covered data;

(ii) the name of each third-party collecting entity to which the covered entity or service provider transfers covered data; and

(iii) the purposes for which such data is transferred to such categories of service providers and third parties or third-party collecting entities.

(E) The length of time the covered entity or service provider intends to retain each category of covered data, including sensitive covered data, including, where practicable, the exact date or dates on which the covered entity or service provider expects to delete or de-identify each such category of covered data, or, if it is not possible to identify that

timeframe or exact date, the criteria used to determine the length of time the covered entity or service provider intends to retain categories of covered data.

(F) A prominent description of how an individual can exercise the privileges and protections established under this subtitle.

(G) A general description of the covered entity's or service provider's data security practices.

(H) The effective date of the privacy policy.

(3) Languages.—The privacy policy required under paragraph (1) shall be made available to the public in each covered language in which the covered entity or service provider—

(A) provides a product or service that is subject to the privacy policy; or

(B) carries out activities related to such product or service.

(4) Accessibility.—The covered entity or service provider shall also provide the disclosures under this subsection in a manner that is reasonably accessible to and usable by individuals with disabilities.

(5) Material changes.—

(A) Affirmative express consent.—If a covered entity makes a material change to its privacy policy or practices, the covered entity shall notify each individual affected by such material change before implementing the material change with respect to any prospectively collected covered data and, except as provided in subparagraphs (A) through (O) of section 562(a)(2), provide a reasonable opportunity for each individual to withdraw consent to any further materially different collection, processing, or transfer of previously collected covered data under the changed policy.

(B) Notification.—The covered entity shall take all reasonable electronic measures to provide direct notification regarding material changes to the privacy policy to each affected individual, in each covered language in which the privacy policy is made available, and taking into account available technology and the nature of the relationship.

(C) Clarification.—Nothing in this paragraph may be construed to affect the requirements for covered entities under section 562(b) or subsection (d).

(D) Log of material changes.—Each large data holder shall retain copies of previous versions of its privacy policy for at least 10 years beginning after the date of enactment of this subtitle and publish all such prior versions, together with a log of material changes, on a dedicated, publicly accessible webpage on its website. Such large data holder shall make publicly available, in a clear, conspicuous, and readily accessible manner, a log describing the date and nature of each material change to its privacy policy over the past 10 years. The descriptions shall be sufficient for a reasonable individual to understand the material effect of each material change. The obligations in this subparagraph shall not apply to any previous versions of a large data holder's privacy policy, or any material changes to such policy, that precede the date of enactment of this subtitle.

(6) Short-form notice to consumers by large data holders.—

(A) In general.—In addition to the privacy policy required under paragraph (1), a large data holder that is a covered entity shall provide a short-form notice of its covered data practices in a manner that is—

(i) concise, clear, conspicuous, and not misleading;

(ii) readily accessible to the individual, based on what is reasonably anticipated within the context of the relationship between the individual and the large data holder;

(iii) inclusive of an overview of individual privileges, protections, and disclosures to reasonably draw attention to data practices that may reasonably be unexpected to a reasonable person or that involve sensitive covered data, including whether covered data will be processed for purposes of algorithmic recommendation systems; and

(iv) no more than 500 words in length.

(B) Rulemaking.—The Commission shall issue a rule pursuant to section 553 of title 5, United States Code, establishing the minimum data disclosures necessary for the short-form notice required under subparagraph (A), which shall not exceed the content requirements in paragraph (2) and shall include templates or models of short-form notices.

(c) Control of data by individuals.—

(1) Access to, and correction, deletion, and portability of, covered data.—In accordance with paragraphs (2) and (3), a covered entity shall provide an individual, after receiving a verified request from the individual, with the ability to—

(A) access—

(i) in a human-readable format that a reasonable individual can understand and download from the internet, the covered data (except covered data in a backup or archival system) of the individual making the request that is collected, processed, or transferred by the covered entity or any service provider of the covered entity within the 24 months preceding the request;

(ii) the categories—

(I) of any service providers to whom the covered entity has sold, or transferred for any consideration, the covered data of the individual;

(II) of sources from which the covered data was collected; and

(III) of any third party to which the covered entity transferred the covered data and, if applicable, an option to obtain the names of those third parties; and

(iii) a description of the purpose for which the covered entity transferred the covered data of the individual to a third party or service provider;

(B) correct any verifiable substantial inaccuracy or substantially incomplete information with respect to the covered data of the individual that is processed by the covered entity

and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the corrected information;

(C) delete covered data of the individual that is processed by the covered entity and instruct the covered entity to make reasonable efforts to notify all third parties or service providers to which the covered entity transferred such covered data of the individual's deletion request;

(D) to the extent technically feasible, export to the individual or directly to another entity the covered data of the individual that is processed by the covered entity, including inferences linked or reasonably linkable to the individual but not including other derived data, without licensing restrictions that limit such transfers in—

(i) a human-readable format that a reasonable individual can understand and download from the internet; and

(ii) a portable, structured, interoperable, and machine-readable format;

(E) disable or opt out of the use of a covered algorithm to rank, order, promote, recommend, amplify, or similarly determine the delivery or display of information to the individual, unless such use is strictly necessary to provide a specific product or service expressly requested by the individual; and

(F) restrict the collection, processing, or transfer of precise geolocation information of the individual and receive clear and conspicuous notice whenever precise geolocation information of the individual is being collected, processed, or transferred.

(2) Individual autonomy.—A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a privilege described in paragraph (1) through—

(A) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(B) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to exercise such privilege.

(3) Timing.—

(A) In general.—Subject to paragraphs (4) and (5), each request under paragraph (1) shall be completed by any—

(i) large data holder within 45 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual;

(ii) covered entity that is neither a large data holder nor a covered entity meeting the requirements of subsection (e)(2) within 60 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual; or

(iii) covered entity meeting the requirements of subsection (e)(2) within 90 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual.

(B) Extension.—A response period set forth in this paragraph may be extended once by 45 additional days when reasonably necessary, considering the complexity and number of the individual's requests, so long as the covered entity informs the individual of any such extension within the initial 45-day response period, together with the reason for the extension.

(4) Frequency and cost of access.—A covered entity—

(A) shall provide an individual with the opportunity to exercise each of the privileges described in paragraph (1); and

(B) with respect to—

(i) the first 2 times that an individual exercises any privilege described in paragraph (1) in any 12-month period, shall allow the individual to exercise such privilege free of charge; and

(ii) any time beyond the initial 2 times described in clause (i), may allow the individual to exercise such privilege for a reasonable fee for each request.

(5) Verification and exceptions.—

(A) Required exceptions.—A covered entity may not permit an individual to exercise a privilege described in paragraph (1), in whole or in part, if the covered entity—

(i) cannot reasonably verify that the individual making the request to exercise the privilege is the individual whose covered data is the subject of the request or an individual authorized to make such a request on the individual's behalf;

(ii) reasonably believes that the request is made to interfere with a contract between the covered entity and another individual;

(iii) determines that the exercise of the privilege would require access to or correction of another individual's sensitive covered data;

(iv) reasonably believes that the exercise of the privilege would require the covered entity to engage in an unfair, deceptive, or abusive practice under section 5 of the Federal Trade Commission Act (15 U.S.C. 45); or

(v) reasonably believes that the request is made to further fraud, support criminal activity, or the exercise of the privilege presents a data security threat.

(B) Additional information.—If a covered entity cannot reasonably verify that a request to exercise a privilege described in paragraph (1) is made by the individual whose covered data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the covered entity—

(i) may request that the individual making the request to exercise the privilege provide any additional information necessary for the sole purpose of verifying the identity of the individual; and

(ii) may not process or transfer such additional information for any other purpose.

(C) Permissive exceptions.—

(i) In general.—A covered entity may decline, with adequate explanation to the individual, to comply with a request to exercise a privilege described in paragraph (1), in whole or in part, that would—

(I) require the covered entity to retain any covered data collected for a single, one-time transaction, if such covered data is not processed or transferred by the covered entity for any purpose other than completing such transaction;

(II) be demonstrably impracticable or prohibitively costly to comply with, and the covered entity shall provide a description to the requestor detailing the inability to comply with the request;

(III) require the covered entity to attempt to re-identify de-identified data;

(IV) require the covered entity to maintain covered data in an identifiable form or collect, retain, or access any data in order to be capable of associating a verified individual request with covered data of such individual;

(V) result in the release of trade secrets or other privileged or confidential business information;

(VI) require the covered entity to correct any covered data that cannot be reasonably verified as being inaccurate or incomplete;

(VII) interfere with law enforcement, judicial proceedings, investigations, or reasonable efforts to guard against, detect, prevent, or investigate fraudulent, malicious, or unlawful activity, or enforce valid contracts;

(VIII) violate Federal or State law or the rights and freedoms of another individual, including under the Constitution of the United States;

(IX) prevent a covered entity from being able to maintain a confidential record of deletion requests, maintained solely for the purpose of preventing covered data of an individual from being recollected after the individual submitted a deletion request and requested that the covered entity no longer collect, process, or transfer such data;

(X) fall within an exception enumerated in the regulations promulgated by the Commission pursuant to clause (iv); or

(XI) with respect to requests for deletion—

(aa) unreasonably interfere with the provision of products or services by the covered entity to another person it currently serves;

(bb) delete covered data that relates to a public figure and for which the requesting individual has no reasonable expectation of privacy;

(cc) delete covered data reasonably necessary to perform a contract between the covered entity and the individual;

(dd) delete covered data that the covered entity needs to retain in order to comply with professional ethical obligations;

(ee) delete covered data that the covered entity reasonably believes may be evidence of unlawful activity or an abuse of the covered entity's products or services; or

(ff) for private elementary and secondary schools as defined by State law and private institutions of higher education as defined by title I of the Higher Education Act of 1965, delete covered data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

(ii) Partial compliance.—In a circumstance that would allow a denial pursuant to clause (i), a covered entity shall partially comply with the remainder of the request if it is possible and not unduly burdensome to do so.

(iii) Number of requests.—For purposes of clause (i)(II), the receipt of a large number of verified requests, on its own, may not be considered to render compliance with a request demonstrably impracticable.

(iv) Further exceptions.—The Commission may, by regulation as described in paragraph (7), establish additional permissive exceptions necessary to protect individual privacy and autonomy, alleviate undue burdens on covered entities, prevent unjust or unreasonable outcomes from the exercise of access, correction, deletion, or portability controls, or as otherwise necessary to fulfill the purposes of this subsection. In establishing such exceptions, the Commission should consider any relevant changes in technology, means for protecting privacy and other legal protections, and beneficial uses of covered data by covered entities.

(6) Large data holder metrics reporting.—A large data holder that is a covered entity shall, for each calendar year in which it was a large data holder, do the following:

(A) Compile the following metrics for the prior calendar year:

(i) The number of verified access requests under paragraph (1)(A).

(ii) The number of verified deletion requests under paragraph (1)(C).

(iii) The number of verified requests under paragraph (1)(E).

(iv) The number of verified requests under paragraph (1)(F).

(v) The number of requests in each of clauses (i) through (iv) that such large data holder complied with in whole or in part and denied.

(vi) The median or mean number of days within which such large data holder substantively responded to the requests in each of clauses (i) through (iv).

(B) Disclose by July 1 of each applicable calendar year the information compiled in subparagraph (A) within such large data holder's privacy policy required under subsection (b) or on the publicly accessible website of such large data holder that is accessible from a hyperlink included in the privacy policy.

(7) Interim final rules.—Not later than 180 days after the date of enactment of this Act, the Commission shall issue interim final rules as necessary to establish processes by which covered entities are to comply with this subsection. The interim final rules shall take effect upon publication in the Federal Register, shall have the force and effect of law, and may be issued without regard to section 553 of title 5, United States Code. The Commission shall provide a public comment period of not less than 60 days after publication and shall issue final rules not later than 18 months after the date of enactment of this Act. Such rules shall take into consideration—

(A) the size of, and the nature, scope, and complexity of the activities engaged in by the covered entity, including whether the covered entity is a large data holder, nonprofit organization, covered entity meeting the requirements of subsection (e)(2), third party, or third-party collecting entity;

(B) the sensitivity of covered data collected, processed, or transferred by the covered entity;

(C) the volume of covered data collected, processed, or transferred by the covered entity;

(D) the number of individuals and devices to which the covered data collected, processed, or transferred by the covered entity relates; and

(E) after consulting the National Institute of Standards and Technology, standards for ensuring the deletion of covered data under this subtitle where appropriate.

(8) Applicability.—Paragraphs (1) through (6) shall apply beginning on the date that is 180 days after the date of enactment of this Act.

(9) Accessibility.—A covered entity shall facilitate the ability of individuals to make requests under paragraph (1) in any covered language in which the covered entity provides a product or service. The mechanisms by which a covered entity enables individuals to make requests under paragraph (1) shall be readily accessible and usable by individuals with disabilities.

(d) Privacy by default.—

(1) Privacy by default.—It shall be unlawful for a covered entity or service provider to configure any privacy setting or option made available to an individual, with respect to the collection, processing, or transfer of covered data, to default to any such setting or option other than the most privacy-protective setting offered by such covered entity or service provider.

(2) Opt-in required for reduced privacy.—It shall be unlawful for a covered entity or service provider to apply a less protective privacy setting to an individual unless such individual has provided affirmative express consent.

(3) Targeted advertising.—It shall be unlawful for a covered entity or service provider to engage in targeted advertising, except for the dissemination of an advertisement targeted exclusively on a recognized place in accordance with section 567(b)(3).

(4) Withdrawal of consent.—A covered entity shall provide an individual with a clear and conspicuous, easy-to-execute means to withdraw any affirmative express consent previously provided by the individual that is as easy to execute by a reasonable individual as the means to provide consent.

(5) Individual autonomy.—A covered entity may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual protection under this subsection through—

(A) the use of any false, fictitious, fraudulent, or materially misleading statement or representation; or

(B) the design, modification, or manipulation of any user interface with the purpose or substantial effect of obscuring, subverting, or impairing a reasonable individual's autonomy, decision making, or choice to exercise any such protection.

(e) Small business protections.—

(1) Establishment of exemption.—Any covered entity or service provider that can establish that it met the requirements described in paragraph (2) for the period of the 3 preceding calendar years (or for the period during which the covered entity or service provider has been in existence if such period is less than 3 years) shall—

(A) be exempt from compliance with subparagraph (D) of subsection (c)(1), subparagraphs (A) through (C) and (E) through (G) of section 564(a)(2), and section 565(a)(3); and

(B) at the covered entity's sole discretion, have the option of complying with subsection (c)(1)(B) by, after receiving a verified request from an individual to correct covered data of the individual under such subparagraph, deleting such covered data in its entirety instead of making the requested correction.

(2) Exemption requirements.—The requirements of this paragraph are, with respect to a covered entity or a service provider, the following:

(A) The covered entity or service provider's average annual gross revenues during the period did not exceed $41,000,000.

(B) The covered entity or service provider, on average, did not annually collect or process the covered data of more than 200,000 individuals during the period beyond the purpose of initiating, rendering, billing for, finalizing, completing, or otherwise collecting payment for a requested service or product, so long as all covered data for such purpose

was deleted or de-identified within 90 days, except when necessary to investigate fraud or as consistent with a covered entity's return policy.

(C) The covered entity or service provider did not derive more than 50 percent of its revenue from transferring covered data during any year (or part of a year if the covered entity has been in existence for less than 1 year) that occurs during the period.

(3) Revenue defined.—For purposes of this subsection, the term "revenue" as it relates to any covered entity or service provider that is not organized to carry on business for its own profit or that of its members, means the gross receipts the covered entity or service provider received in whatever form from all sources without subtracting any costs or expenses, and includes contributions, gifts, grants, dues or other assessments, income from investments, or proceeds from the sale of real or personal property.

(f) Unified privacy mechanisms.—

(1) In general.—For the protections established under subsection (d), for the communication of a refusal or withdrawal of consent for a transfer of covered data to a third party that is not strictly necessary to provide, maintain, complete, or fulfill a specific product or service requested by the individual, and for requests under section 564(b)(2)(C)(iii), following public notice and opportunity to comment and not later than January 1, 2028, the Commission shall establish or recognize 1 or more acceptable privacy-protective, centralized mechanisms, including browser or device privacy settings, other tools offered by covered entities or service providers, and registries of identifiers, for individuals to exercise all such protections through a single interface for a covered entity or service provider to utilize.

(2) Requirements.—Any such centralized mechanism shall—

(A) require covered entities or service providers acting on behalf of covered entities to inform individuals about the mechanism and its effect;

(B) operate as the default privacy-protective setting unless the individual affirmatively chooses a different setting, and any such different setting shall clearly represent the individual's affirmative, freely given, specific, and unambiguous choice;

(C) be consumer-friendly, clearly described, and easy-to-use by a reasonable individual;

(D) permit the covered entity or service provider acting on behalf of a covered entity to have an authentication process the covered entity or service provider acting on behalf of a covered entity may use to determine if the mechanism represents a legitimate request;

(E) be provided in any covered language in which the covered entity provides products or services subject to the mechanism; and

(F) be provided in a manner that is reasonably accessible to and usable by individuals with disabilities.

SEC. 564. DATA SECURITY AND REGISTRATION.

(a) Data security and protection of covered data.—

(1) Establishment of data security practices.—

(A) In general.—A covered entity or service provider shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition.

(B) Considerations.—The reasonable administrative, technical, and physical data security practices required under subparagraph (A) shall be appropriate to—

(i) the size and complexity of the covered entity or service provider;

(ii) the nature and scope of the covered entity or the service provider's collecting, processing, or transferring of covered data;

(iii) the volume and nature of the covered data collected, processed, or transferred by the covered entity or service provider;

(iv) the sensitivity of the covered data collected, processed, or transferred;

(v) the current state of the art (and limitations thereof) in administrative, technical, and physical safeguards for protecting such covered data; and

(vi) the cost of available tools to improve security and reduce vulnerabilities to unauthorized access and acquisition of such covered data in relation to the risks and nature of the covered data.

(2) Specific requirements.—The data security practices of the covered entity and of the service provider required under paragraph (1) shall include, for each respective entity's own system or systems, at a minimum, the following practices:

(A) Assess vulnerabilities.—Identifying and assessing any material internal and external risk to, and vulnerability in, the security of each system maintained by the covered entity that collects, processes, or transfers covered data, or service provider that collects, processes, or transfers covered data on behalf of the covered entity, including unauthorized access to or risks to such covered data, human vulnerabilities, access rights, and the use of service providers. With respect to large data holders, such activities shall include a plan to receive and reasonably respond to unsolicited reports of vulnerabilities by any entity or individual and to perform a reasonable investigation of such reports.

(B) Preventive and corrective action.—Taking preventive and corrective action designed to mitigate reasonably foreseeable risks or vulnerabilities to covered data identified by the covered entity or service provider, consistent with the nature of such risk or vulnerability and the entity's role in collecting, processing, or transferring the data. Such action may include implementing administrative, technical, or physical safeguards or changes to data security practices or the architecture, installation, or implementation of network or operating software, among other actions.

(C) Evaluation of preventive and corrective action.—Evaluating and making reasonable adjustments to the action described in subparagraph (B) in light of any material changes in

technology, internal or external threats to covered data, and the covered entity or service provider's own changing business arrangements or operations.

(D) Information retention and disposal.—Disposing of covered data in accordance with a retention schedule that shall require the deletion of covered data when such data is required to be deleted by law or is no longer necessary for the purpose for which the data was collected, processed, or transferred, unless an individual has provided affirmative express consent to such retention. Such disposal shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this subsection. Service providers shall establish practices to delete or return covered data to a covered entity as requested at the end of the provision of services unless retention of the covered data is required by law, consistent with section 565(b)(1)(F).

(E) Training.—Training each employee with access to covered data on how to safeguard covered data and updating such training as necessary.

(F) Designation.—Designating an officer, employee, or employees to maintain and implement such practices.

(G) Incident response.—Implementing procedures to detect, respond to, or recover from security incidents, including breaches.

(3) Regulations.—The Commission may promulgate, in accordance with section 553 of title 5, United States Code, technology-neutral regulations to establish processes for complying with this subsection. The Commission shall consult with the National Institute of Standards and Technology in establishing such processes.

(b) Third-party collecting entities.—

(1) Notice.—Each third-party collecting entity shall place a clear, conspicuous, not misleading, and readily accessible notice on the website or mobile application of the third-party collecting entity (if the third-party collecting entity maintains such a website or mobile application) that—

(A) notifies individuals that the entity is a third-party collecting entity using specific language that the Commission shall develop through rulemaking under section 553 of title 5, United States Code, except that, until such language takes effect, language clearly and conspicuously identifying the entity as a third-party collecting entity shall satisfy this subparagraph;

(B) includes a link to the website established under paragraph (2)(C); and

(C) is reasonably accessible to and usable by individuals with disabilities.

(2) Third-party collecting entity registration.—

(A) In general.—Not later than January 31 of each calendar year that follows a calendar year during which a covered entity acted as a third-party collecting entity and processed covered data pertaining to more than 5,000 individuals or devices that identify or are linked

or reasonably linkable to an individual, such covered entity shall register with the Commission in accordance with this subsection.

(B) Registration requirements.—In registering with the Commission as required under subparagraph (A), a third-party collecting entity shall do the following:

(i) Pay to the Commission a registration fee of $100.

(ii) Provide the Commission with the following information:

(I) The legal name and primary physical, email, and internet addresses of the third-party collecting entity.

(II) A description of the categories of covered data the third-party collecting entity processes and transfers.

(III) The contact information of the third-party collecting entity, including a contact person, a telephone number, an email address, a website, and a physical mailing address.

(IV) A link to a website through which an individual may easily exercise the rights provided under this subsection.

(C) Third-party collecting entity registry.—The Commission shall establish and maintain on a website a searchable, publicly available, central registry of third-party collecting entities that are registered with the Commission under this subsection that includes the following:

(i) A listing of all registered third-party collecting entities and a search feature that allows members of the public to identify individual third-party collecting entities.

(ii) For each registered third-party collecting entity, the information provided under subparagraph (B).

(iii) (I) A "Do Not Collect" registry link and mechanism by which an individual may easily submit a request to all registered third-party collecting entities that are not consumer reporting agencies (as defined in section 603(f) of the Fair Credit Reporting Act (15 U.S.C. 1681a(f))), and to the extent such third-party collecting entities are not acting as consumer reporting agencies (as so defined), to—

(aa) delete all covered data related to such individual that the third-party collecting entity did not collect from such individual directly or when acting as a service provider; and

(bb) ensure that the third-party collecting entity no longer collects covered data related to such individual without the affirmative express consent of such individual, except insofar as the third-party collecting entity is acting as a service provider.

(II) Each third-party collecting entity that receives such a request from an individual shall delete all covered data described in subclause (I)(aa) relating to the

individual not later than 30 days after the request is received by the third-party collecting entity.

(III) Notwithstanding subclauses (I) and (II), a third-party collecting entity may decline to fulfill a "Do Not Collect" request from an individual who it has actual knowledge has been convicted of a crime related to the abduction or sexual exploitation of a child, and the data the entity is collecting is necessary to effectuate the purposes of a national or State-run sex offender registry or the congressionally designated entity that serves as the nonprofit national resource center and clearinghouse to provide assistance to victims, families, child-serving professionals, and the general public on missing and exploited children issues.

(3) Penalties.—

(A) In general.—A third-party collecting entity that fails to register or provide the notice as required under this subsection shall be liable for—

(i) a civil penalty of $5,000 for each day the third-party collecting entity fails to register or provide notice as required under this subsection, not to exceed a total of $500,000 for any year; and

(ii) an amount equal to the registration fees due under paragraph (2)(B)(i) for each year that the third-party collecting entity failed to register as required.

(B) Rule of construction.—Nothing in this paragraph shall be construed as altering, limiting, or affecting any enforcement authorities or remedies under this subtitle.

(c) Civil rights and algorithms.—

(1) Civil rights protections.—

(A) In general.—A covered entity or a service provider may not collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability.

(B) Exceptions.—This paragraph shall not apply to—

(i) the collection, processing, or transfer of covered data for the purpose of self-testing to prevent or mitigate unlawful discrimination; or

(ii) any private club or group not open to the public, as described in section 201(e) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(e)).

(2) FTC enforcement assistance.—

(A) In general.—Whenever the Commission obtains information that a covered entity or service provider may have collected, processed, or transferred covered data in violation of paragraph (1), the Commission shall transmit such information as allowable under Federal law to any Executive agency with authority to initiate enforcement actions or proceedings relating to such violation.

(B) Annual report.—Not later than 3 years after the date of enactment of this subtitle, and annually thereafter, the Commission shall submit to Congress a report that includes a summary of—

(i) the types of information the Commission transmitted to Executive agencies under subparagraph (A) during the previous 1-year period; and

(ii) how such information relates to Federal civil rights laws.

(C) Technical assistance.—In transmitting information under subparagraph (A), the Commission may consult and coordinate with, and provide technical and investigative assistance, as appropriate, to such Executive agency.

(D) Cooperation with other agencies.—The Commission may implement this paragraph by executing agreements or memoranda of understanding with the appropriate Executive agencies.

(3) Covered algorithm impact and evaluation.—

(A) Covered algorithm impact assessment.—

(i) Impact assessment.—Notwithstanding any other provision of law, not later than July 1, 2028, and annually thereafter, a large data holder that uses a covered algorithm in a manner that poses a consequential risk of harm to an individual or group of individuals, and uses such covered algorithm solely or in part, to collect, process, or transfer covered data shall conduct an impact assessment of such algorithm in accordance with clause (ii).

(ii) Impact assessment scope.—The impact assessment required under clause (i) shall provide the following:

(I) A detailed description of the design process and methodologies of the covered algorithm.

(II) A statement of the purpose and proposed uses of the covered algorithm.

(III) A detailed description of the data used by the covered algorithm, including the specific categories of data that will be processed as input and any data used to train the model that the covered algorithm relies on, if applicable.

(IV) A description of the outputs produced by the covered algorithm.

(V) An assessment of the necessity and proportionality of the covered algorithm in relation to its stated purpose.

(VI) A detailed description of steps the large data holder has taken or will take to mitigate potential harms from the covered algorithm to an individual or group of individuals, including related to—

(aa) covered minors;

(bb) making or facilitating advertising for, or determining access to, or restrictions on the use of housing, education, employment, health care, insurance, or credit opportunities;

(cc) determining access to, or restrictions on the use of, any place of public accommodation, particularly as such harms relate to the protected characteristics of individuals, including race, color, religion, national origin, sex, or disability;

(dd) disparate impact on the basis of individuals' race, color, religion, national origin, sex, or disability status; or

(ee) disparate impact on the basis of individuals' political party registration status.

(B) Algorithm design evaluation.—Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this subtitle, a covered entity or service provider that knowingly develops a covered algorithm that is designed, solely or in part, to collect, process, or transfer covered data in furtherance of a consequential decision shall prior to deploying the covered algorithm in interstate commerce evaluate the design, structure, and inputs of the covered algorithm, including any training data used to develop the covered algorithm, to reduce the risk of the potential harms identified under subparagraph (A)(ii).

(C) Other considerations.—

(i) Focus.—In complying with subparagraphs (A) and (B), a covered entity and a service provider may focus the impact assessment or evaluation on any covered algorithm, or portions of a covered algorithm, that will be put to use and may reasonably contribute to the risk of the potential harms identified under subparagraph (A)(ii).

(ii) Availability.—

(I) In general.—A covered entity and a service provider—

(aa) shall, not later than 30 days after completing an impact assessment or evaluation, submit the impact assessment or evaluation conducted under subparagraph (A) or (B) to the Commission;

(bb) shall, upon request, make such impact assessment and evaluation available to Congress; and

(cc) may make a summary of such impact assessment and evaluation publicly available in a place that is easily accessible to individuals.

(II) Trade secrets.—Covered entities and service providers may redact and segregate any trade secret (as defined in section 1839 of title 18, United States Code) or other confidential or proprietary information from public disclosure under this clause and the Commission shall abide by its obligations under section 6(f) of the Federal Trade Commission Act (15 U.S.C. 46(f)) in regard to such information.

(iii) Enforcement.—The Commission may not use any information obtained solely and exclusively through a covered entity or a service provider's disclosure of information to the Commission in compliance with this paragraph for any purpose other than enforcing this subtitle with the exception of enforcing consent orders, including the study and report provisions in subparagraph (F). This clause does not preclude the Commission from providing this information to Congress in response to a subpoena.

(D) Guidance.—Not later than 2 years after the date of enactment of this subtitle, the Commission shall, in consultation with the Secretary of Commerce or their designee, publish guidance regarding compliance with this paragraph.

(E) Rulemaking and exemption.—The Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations as necessary to establish processes by which a large data holder—

(i) shall submit an impact assessment to the Commission under clause (ii)(I) of subparagraph (C); and

(ii) may exclude from this paragraph any covered algorithm that presents low or minimal consequential risk of harm to an individual or group of individuals.

(F) Study and report.—

(i) Study.—The Commission, in consultation with the Secretary of Commerce or the Secretary's designee, shall conduct a study, to review any impact assessment or evaluation submitted under this paragraph. Such study shall include an examination of—

(I) best practices for the assessment and evaluation of covered algorithms; and

(II) methods to reduce the risk of harm to individuals that may be related to the use of covered algorithms.

(ii) Report.—

(I) Initial report.—Not later than 3 years after the date of enactment of this subtitle, the Commission, in consultation with the Secretary of Commerce or the Secretary's designee, shall submit to Congress a report containing the results of the study conducted under subclause (i), together with recommendations for such legislation and administrative action as the Commission determines appropriate.

(II) Additional reports.—Not later than 3 years after submission of the initial report under subclause (I), and as the Commission determines necessary thereafter, the Commission shall submit to Congress an updated version of such report.

(G) Definitions.—In this paragraph:

(i) Consequential decision.—The term "consequential decision" means a decision that determines or materially affects an individual's access to, eligibility for, or terms of housing, education, employment, health care, insurance, credit, or a place of public accommodation.

(ii) Consequential risk of harm.—The term "consequential risk of harm" means a material risk of one or more of the potential harms described in subparagraph (A)(ii).

SEC. 565. EXECUTIVE RESPONSIBILITY, SERVICE PROVIDERS, AND COMPLIANCE PROGRAMS.

(a) Executive responsibility.—

(1) In general.—Beginning 1 year after the date of enactment of this subtitle, an executive officer of a large data holder shall annually certify, in good faith, to the Commission, in a manner specified by the Commission by regulation under section 553 of title 5, United States Code, issued not later than 180 days after the date of enactment of this subtitle, that the entity maintains—

(A) internal controls reasonably designed to comply with this subtitle; and

(B) internal reporting structures to ensure that such certifying executive officer is involved in and responsible for the decisions that impact the compliance by the large data holder with this subtitle.

(2) Requirements.—A certification submitted under paragraph (1) shall be based on a review of the effectiveness of the internal controls and reporting structures of the large data holder that is conducted by the certifying executive officer not more than 90 days before the submission of the certification. A certification submitted under paragraph (1) is made in good faith if the certifying officer had, after a reasonable investigation, reasonable ground to believe and did believe, at the time that certification was submitted, that the statements therein were true and that there was no omission to state a material fact required to be stated therein or necessary to make the statements therein not misleading.

(3) Designation of privacy and data security officer.—

(A) In general.—A covered entity or service provider with more than 15 employees shall designate—

(i) 1 or more qualified employees as privacy officers; and

(ii) 1 or more qualified employees (in addition to any employee designated under clause (i)) as data security officers.

(B) Requirements for officers.—An employee who is designated by a covered entity or a service provider as a privacy officer or a data security officer pursuant to subparagraph (A) shall, at a minimum—

(i) implement a data privacy program and data security program to safeguard the privacy and security of covered data in compliance with the requirements of this subtitle; and

(ii) facilitate the covered entity or service provider's ongoing compliance with this subtitle.

(C) Additional requirements for large data holders.—A large data holder shall designate at least 1 of the officers described in subparagraph (A) to report directly to the highest official at the large data holder as a privacy protection officer who shall, in addition to the requirements in subparagraph (B), either directly or through a supervised designee or designees—

(i) establish processes to periodically review and update the privacy and security policies, practices, and procedures of the large data holder, as necessary;

(ii) conduct biennial and comprehensive audits to ensure the policies, practices, and procedures of the large data holder ensure the large data holder is in compliance with this subtitle and ensure such audits are accessible to the Commission upon request;

(iii) develop a program to educate and train employees about compliance requirements of this subtitle;

(iv) maintain updated, accurate, clear, and understandable records of all material privacy and data security practices undertaken by the large data holder; and

(v) serve as the point of contact between the large data holder and enforcement authorities.

(4) Large data holder privacy impact assessments.—

(A) In general.—Not later than July 1, 2027, or 1 year after the date on which a covered entity first meets the definition of large data holder, and biennially thereafter, each covered entity that is a large data holder shall conduct a privacy impact assessment that weighs the benefits of the large data holder's covered data collecting, processing, and transfer practices against the potential adverse consequences of such practices, including substantial privacy risks, to individual privacy.

(B) Assessment requirements.—A privacy impact assessment required under subparagraph (A) shall be—

(i) reasonable and appropriate in scope given—

(I) the nature of the covered data collected, processed, and transferred by the large data holder;

(II) the volume of the covered data collected, processed, and transferred by the large data holder; and

(III) the potential material risks posed to the privacy of individuals by the collecting, processing, and transfer of covered data by the large data holder;

(ii) documented in written form and maintained by the large data holder unless rendered out of date by a subsequent assessment conducted under subparagraph (A); and

(iii) approved by the privacy protection officer designated under paragraph (3)(C).

(C) Additional factors to include in assessment.—In assessing the privacy risks, including substantial privacy risks, the large data holder must include reviews of the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, are used to secure covered data.

(5) Other privacy impact assessments.—

(A) In general.—Not later than 1 year after the date of enactment of this subtitle and biennially thereafter, each covered entity that is not a large data holder and does not meet the requirements for covered entities under section 563(e)(2) shall conduct a privacy impact assessment. Such assessment shall weigh the benefits of the covered entity's covered data collecting, processing, and transfer practices that may cause a substantial privacy risk against the potential material adverse consequences of such practices to individual privacy.

(B) Assessment requirements.—A privacy impact assessment required under subparagraph (A) shall be—

(i) reasonable and appropriate in scope given—

(I) the nature of the covered data collected, processed, and transferred by the covered entity;

(II) the volume of the covered data collected, processed, and transferred by the covered entity; and

(III) the potential risks posed to the privacy of individuals by the collecting, processing, and transfer of covered data by the covered entity; and

(ii) documented in written form and maintained by the covered entity unless rendered out of date by a subsequent assessment conducted under subparagraph (A).

(C) Additional factors to include in assessment.—In assessing the privacy risks, including substantial privacy risks, the covered entity may include reviews of the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, are used to secure covered data.

(b) Service providers and third parties.—

(1) Service providers.—A service provider—

(A) shall adhere to the instructions of a covered entity and only collect, process, and transfer service provider data to the extent necessary and proportionate to provide a service requested by the covered entity, as set out in the contract required by paragraph (2), and this subparagraph does not require a service provider to collect, process, or transfer covered data if the service provider would not otherwise do so;

(B) may not collect, process, or transfer service provider data if the service provider has actual knowledge that a covered entity violated this subtitle with respect to such data;

(C) shall assist a covered entity in responding to a request made by an individual under section 563(c), by either—

(i) providing appropriate technical and organizational measures, taking into account the nature of the processing and the information reasonably available to the service provider, for the covered entity to comply with such request for service provider data; or

(ii) fulfilling a request by a covered entity to execute an individual rights request that the covered entity has determined should be complied with, by either—

(I) complying with the request pursuant to the covered entity's instructions; or

(II) providing written verification to the covered entity that it does not hold covered data related to the request, that complying with the request would be inconsistent with its legal obligations, or that the request falls within an exception to section 563(c);

(D) may engage another service provider for purposes of processing service provider data on behalf of a covered entity only after providing that covered entity with notice and pursuant to a written contract that requires such other service provider to satisfy the obligations of the service provider with respect to such service provider data, including that the other service provider be treated as a service provider under this subtitle;

(E) shall, upon the reasonable request of the covered entity, make available to the covered entity information necessary to demonstrate the compliance of the service provider with the requirements of this subtitle, which may include making available a report of an independent assessment arranged by the service provider on terms agreed to by the service provider and the covered entity, providing information necessary to enable the covered entity to conduct and document a privacy impact assessment required under subsection (a), and making available the impact assessment or evaluation required under section 564(c)(3);

(F) shall, at the covered entity's direction, delete or return all covered data to the covered entity as requested at the end of the provision of services, unless retention of the covered data is required by law;

(G) shall develop, implement, and maintain reasonable administrative, technical, and physical safeguards that are designed to protect the security and confidentiality of covered data the service provider processes consistent with section 564(a); and

(H) shall allow and cooperate with reasonable assessments by the covered entity or the covered entity's designated assessor; alternatively, the service provider may arrange for a qualified and independent assessor to conduct an assessment of the service provider's policies and technical and organizational measures in support of the obligations under this subtitle using an appropriate and accepted control standard or framework and assessment procedure for such assessments, and shall provide a report of such assessment to the covered entity upon request.

(2) Contracts between covered entities and service providers.—

(A) Requirements.—A person or entity may only act as a service provider pursuant to a written contract between the covered entity and the service provider, or a written contract

between 1 service provider and a second service provider as described under paragraph (1)(D), if the contract—

(i) sets forth the data processing procedures of the service provider with respect to collection, processing, or transfer performed on behalf of the covered entity or service provider;

(ii) clearly sets forth—

(I) instructions for collecting, processing, or transferring data;

(II) the nature and purpose of collecting, processing, or transferring;

(III) the type of data subject to collecting, processing, or transferring;

(IV) the duration of processing; and

(V) the rights and obligations of both parties, including a method by which the service provider shall notify the covered entity of material changes to its privacy practices;

(iii) does not relieve a covered entity or a service provider of any requirement or liability imposed on such covered entity or service provider under this subtitle; and

(iv) prohibits—

(I) collecting, processing, or transferring covered data in contravention of paragraph (1); and

(II) combining service provider data with covered data that the service provider receives from or on behalf of another person or persons or collects from the interaction of the service provider with an individual, unless such combining is necessary to effectuate a purpose described in subparagraphs (A) through (O) of section 562(a)(2) and is otherwise permitted under the contract required by this paragraph.

(B) Contract terms.—Each service provider shall retain copies of previous contracts entered into in compliance with this paragraph with each covered entity to which the service provider provides requested products or services.

(3) Relationship between covered entities and service providers.—

(A) Determination.—Determining whether a person is acting as a covered entity or service provider with respect to a specific processing of covered data is a fact-based determination that depends upon the context in which such data is processed.

(B) Change in role.—A person that is not limited in its processing of covered data pursuant to the instructions of a covered entity, or that fails to adhere to such instructions, is a covered entity and not a service provider with respect to a specific processing of covered data. A service provider that continues to adhere to the instructions of a covered entity with respect to a specific processing of covered data remains a service provider. If a service provider begins, alone or jointly with others, determining the purposes and means of the

processing of covered data, the service provider is a covered entity and not a service provider with respect to the processing of such data.

(C) Transferor liability.—A covered entity that transfers covered data to a service provider, or a service provider that transfers covered data to a covered entity or another service provider, in compliance with the requirements of this subtitle, is not liable for a violation of this subtitle by the service provider or covered entity to whom such covered data was transferred, if at the time of transferring such covered data, the covered entity or service provider did not have actual knowledge that the service provider or covered entity would violate this subtitle.

(D) Recipient liability.—A covered entity or service provider that receives covered data in compliance with the requirements of this subtitle is not in violation of this subtitle as a result of a violation by a covered entity or service provider from which such data was received.

(4) Third parties.—A third party—

(A) shall not process third-party data for a processing purpose other than—

(i) in the case of sensitive covered data, the processing purpose for which the individual gave affirmative express consent or to effect a purpose enumerated in subparagraph (A), (C), or (E) of section 562(a)(2); and

(ii) in the case of non-sensitive covered data, the processing purpose for which the covered entity made a disclosure pursuant to section 563(b)(2)(D); and

(B) for purposes of subparagraph (A), may reasonably rely on representations made by the covered entity that transferred the third-party data if the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible, unless the third party has actual knowledge, or knowledge fairly implied on the basis of objective circumstances, that such representations are false or incomplete.

(5) Additional obligations.—

(A) In general.—A covered entity or service provider shall exercise reasonable due diligence in—

(i) selecting a service provider; and

(ii) deciding to transfer covered data to a third party.

(B) Guidance.—Not later than July 1, 2027, the Commission shall publish guidance regarding compliance with this paragraph, taking into consideration the burdens on large data holders, covered entities who are not large data holders, and covered entities meeting the requirements of section 563(e).

(6) Rule of construction.—Solely for purposes of this subsection, the requirements for service providers to contract with, assist, and follow the instructions of covered entities shall be read to include requirements to contract with, assist, and follow the instructions of a government entity if the service provider is providing a service to a government entity.

(c) Technical compliance programs.—

(1) In general.—Not later than July 1, 2028, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to establish a process for the proposal and approval of technical compliance programs under this subsection used by a covered entity to collect, process, or transfer covered data.

(2) Scope of programs.—The technical compliance programs established under this subsection shall, with respect to a technology, product, service, or method used by a covered entity to collect, process, or transfer covered data—

(A) establish publicly available guidelines for compliance with this subtitle; and

(B) meet or exceed the requirements of this subtitle.

(3) Approval process.—

(A) In general.—Any request for approval, amendment, or repeal of a technical compliance program may be submitted to the Commission by any person, including a covered entity, a representative of a covered entity, an association of covered entities, or a public interest group or organization. Within 90 days after the request is made, the Commission shall publish the request and provide an opportunity for public comment on the proposal.

(B) Expedited response to requests.—Beginning 1 year after the date of enactment of this subtitle, the Commission shall act upon a request for the proposal and approval of a technical compliance program not later than 1 year after the filing of the request, and shall set forth publicly in writing the conclusions of the Commission with regard to such request.

(4) Judicial review.—Final action by the Commission on a request for approval, amendment, or repeal of a technical compliance program, or the failure to act within the 1-year period after a request for approval, amendment, or repeal of a technical compliance program is made under paragraph (3), may be appealed to a Federal district court of the United States of appropriate jurisdiction as provided for in section 702 of title 5, United States Code.

(5) Effect on enforcement.—

(A) In general.—Prior to commencing an investigation or enforcement action against any covered entity under this subtitle, the Commission and State attorney general shall consider the covered entity's history of compliance with any technical compliance program approved under this subsection and any action taken by the covered entity to remedy noncompliance with such program. If an action described in section 569(b)(3) is brought, the covered entity's history of compliance with any technical compliance program approved under this subsection and any action taken by the covered entity to remedy noncompliance with such program shall be taken into consideration when determining liability or a penalty. The covered entity's history of compliance with any technical compliance program shall not affect any burden of proof or the weight given to evidence in an enforcement or judicial proceeding.

(B) Commission authority.—Approval of a technical compliance program shall not limit the authority of the Commission, including the Commission's authority to commence an investigation or enforcement action against any covered entity under this subtitle or any other Act.

(C) Rule of construction.—Nothing in this paragraph shall entitle any individual, class of individuals, or person to seek discovery of any nonpublic Commission deliberation or activity, and nothing in this paragraph shall impose any pleading requirement on the Commission if the Commission brings an enforcement action of any kind.

(d) Commission-approved compliance guidelines.—

(1) Application for compliance guideline approval.—

(A) In general.—A covered entity that is not a third-party collecting entity and meets the requirements of section 563(e), or a group of such covered entities, may apply to the Commission for approval of 1 or more sets of compliance guidelines governing the collection, processing, and transfer of covered data by the covered entity or group of covered entities.

(B) Application requirements.—Such application shall include—

(i) a description of how the proposed guidelines will meet or exceed the requirements of this subtitle;

(ii) a description of the entities or activities the proposed set of compliance guidelines is designed to cover;

(iii) a list of the covered entities that meet the requirements of section 563(e) and are not third-party collecting entities, if any are known at the time of application, that intend to adhere to the compliance guidelines; and

(iv) a description of how such covered entities will be independently assessed for adherence to such compliance guidelines, including the independent organization not associated with any of the covered entities that may participate in guidelines that will administer such guidelines.

(2) Commission review.—

(A) Initial approval.—

(i) Public comment period.—Within 90 days after the receipt of proposed guidelines submitted pursuant to paragraph (1)(B), the Commission shall publish the application and provide an opportunity for public comment on such compliance guidelines.

(ii) Approval.—The Commission shall approve an application regarding proposed guidelines under paragraph (1)(B) if the applicant demonstrates that the compliance guidelines—

(I) meet or exceed the requirements of this subtitle;

(II) provide for the regular review and validation by an independent organization not associated with any of the covered entities that may participate in the guidelines and that is approved by the Commission to conduct such reviews of the compliance guidelines of the covered entity or entities to ensure that the covered entity or entities continue to meet or exceed the requirements of this subtitle; and

(III) include a means of enforcement if a covered entity does not meet or exceed the requirements in the guidelines, which may include referral to the Commission for enforcement consistent with section 569(b)(1) or referral to the appropriate State attorney general for enforcement consistent with section 569(b)(2).

(iii) Timeline.—Within 1 year after receiving an application regarding proposed guidelines under paragraph (1)(B), the Commission shall issue a determination approving or denying the application and providing its reasons for approving or denying such application.

(B) Approval of modifications.—

(i) In general.—If the independent organization administering a set of guidelines makes material changes to guidelines previously approved by the Commission, the independent organization shall submit the updated guidelines to the Commission for approval. As soon as feasible, the Commission shall publish the updated guidelines and provide an opportunity for public comment.

(ii) Timeline.—The Commission shall approve or deny any material change to the guidelines within 1 year after receipt of the submission for approval.

(3) Withdrawal of approval.—If at any time the Commission determines that the guidelines previously approved no longer meet the requirements of this subtitle or a regulation promulgated under this subtitle or that compliance with the approved guidelines is insufficiently enforced by the independent organization administering the guidelines, the Commission shall notify the covered entities or group of such entities and the independent organization of the determination of the Commission to withdraw approval of such guidelines and the basis for doing so. Within 180 days after receipt of such notice, the covered entity or group of such entities and the independent organization may cure any alleged deficiency with the guidelines or the enforcement of such guidelines and submit each proposed cure to the Commission. If the Commission determines that such cures eliminate the alleged deficiency in the guidelines, the Commission may not withdraw approval of such guidelines on the basis of such determination.

(4) Deemed compliance.—A covered entity that is eligible to participate under paragraph (1)(A) and participates in guidelines approved under this subsection shall be deemed in compliance with the relevant provisions of this subtitle if such covered entity is in compliance with such guidelines.

(e) Bureau of Privacy.—

(1) In general.—The Commission shall establish within the Commission a new bureau to be known as the "Bureau of Privacy", which shall be of similar structure, size, organization, and

authority as the existing bureaus within the Commission related to consumer protection and competition.

(2) Mission.—The mission of the Bureau established under paragraph (1) shall be to assist the Commission in carrying out the duties of the Commission under this subtitle and related duties under other provisions of law.

(3) Timeline.—The Bureau required to be established under paragraph (1) shall be established, staffed, and fully operational not later than 1 year after the date of enactment of this subtitle.

(4) Office of Business Mentorship.—The Commission shall establish within the Bureau an office to be known as the "Office of Business Mentorship" to provide guidance and education to covered entities and service providers regarding compliance with this subtitle.

(5) Office of consumer privacy complaint intake.—The Commission shall establish within the Bureau an office to receive complaints from the public alleging violations of this subtitle or a regulation promulgated under this subtitle.

(6) Functions.—The office established under paragraph (5) shall, in coordination with any existing complaint intake mechanisms of the Commission—

(A) establish and maintain a single toll-free telephone number, a website, and a database to facilitate the centralized collection of, monitoring of, and response to complaints described in paragraph (5);

(B) coordinate with other bureaus and offices of the Commission, the Attorney General, and other Federal agencies to route complaints to those agencies, where appropriate; and

(C) make publicly available aggregate complaint information and complaint trends, in a manner that protects personally identifiable information.

(7) Confidentiality.—The Commission shall ensure that personally identifiable information contained in complaints received under paragraph (5) is protected from public disclosure.

(f) Youth privacy and marketing division.—

(1) Establishment.—There is established within the Commission a division to be known as the "Youth Privacy and Marketing Division" (in this subsection referred to as the "Division").

(2) Director.—The Division shall be headed by a Director, who shall be appointed by the Chair of the Commission.

(3) Duties.—The Division shall be responsible for assisting the Commission in addressing, as it relates to this subtitle and section 1177 of the POPULIST Act—

(A) the privacy of covered minors; and

(B) marketing directed at covered minors.

(4) Staff.—The Director of the Division shall hire adequate staff to carry out the duties described in paragraph (3), including by hiring individuals who are experts in data protection, digital advertising, data analytics, and youth development.

(5) Reports.—Not later than 2 years after the date of enactment of this subtitle, and annually thereafter, the Commission shall submit to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report that includes—

(A) a description of the work of the Division regarding emerging concerns relating to youth privacy and marketing practices; and

(B) an assessment of how effectively the Division has, during the period for which the report is submitted, assisted the Commission to address youth privacy and marketing practices.

(6) Publication.—Not later than 10 days after the date on which a report is submitted under paragraph (5), the Commission shall publish the report on its website.

SEC. 566. ADDITIONAL DATA PROTECTIONS FOR COVERED MINORS.

(a) Safeguards for covered minors.—

(1) Safeguards.—A covered entity that provides an online product or service and has knowledge that an individual using or visiting such product or service is a covered minor shall provide such individual with readily accessible and easy-to-use safeguards to, as applicable—

(A) limit the ability of other users or visitors to communicate with the covered minor; and

(B) limit by default design features that result in compulsive usage of the online product or service by the covered minor.

(2) Option to limit time spent.—A covered entity described in paragraph (1) shall provide a covered minor with a readily accessible and easy-to-use option to limit the amount of time spent by the covered minor on the online product or service.

(3) Definitions.—As used in this section, the terms "compulsive usage" and "design feature" have the meanings given such terms in section 45g of title 15, United States Code, as inserted by this Act.

(b) Default settings for covered minors.—A covered entity described in subsection (c)(1) shall provide that, in the case of a covered minor, the default setting for any safeguard described in subsection (a)(1) is the option available on the online product or service that provides the most protective level of control offered by the covered entity with respect to privacy and safety for that covered minor.

(c) Parental tools.—

(1) In general.—A covered entity that provides an online product or service and has knowledge that an individual using such product or service is a covered minor shall provide

readily accessible and easy-to-use parental tools for a parent to support the covered minor with respect to the use of the online product or service by that covered minor.

(2) Requirements.—The parental tools required under paragraph (1) shall include—

(A) the ability to manage the privacy and account settings of a covered minor, including any safeguard and option established under subsection (a), in a manner that allows a parent to—

(i) view the privacy and account settings; and

(ii) in the case of a child, change and control the privacy and account settings;

(B) the ability to restrict purchases and financial transactions by the covered minor, if applicable; and

(C) the ability to view metrics of total time spent on the online product or service by the covered minor and to restrict such time spent.

(3) Notice to covered minors.—A covered entity shall provide clear and conspicuous notice to a covered minor when the parental tools described in this subsection are in effect and what settings or controls have been applied.

(4) Default tools for children.—In the case of a child, a covered entity shall enable the parental tools required under paragraph (1) by default.

(d) Reporting mechanism.—

(1) Reporting tools.—A covered entity that provides an online product or service and has knowledge that 1 or more individuals using or visiting such product or service are covered minors shall provide—

(A) a readily accessible and easy-to-use means for an individual to submit a report to the covered entity of any harm to a covered minor related to the use of the online product or service;

(B) an electronic point of contact specific to matters involving harm to a covered minor; and

(C) confirmation of receipt of such report and, within the applicable time period described in paragraph (2), a substantive response to the individual that submitted the report.

(2) Timing.—A covered entity described in paragraph (1) shall establish an internal process to receive and substantively respond to a report submitted under paragraph (1) in a reasonable and timely manner, but in no case later than—

(A) 10 days after the date on which the report is received; and

(B) notwithstanding subparagraph (A), if the report involves an imminent threat to the safety of a covered minor, as promptly as needed to address the reported threat.

(e) Independent third-party audit.—

(1) In general.—Not later than July 1, 2027, and annually thereafter, each large data holder that provides an online product or service and has knowledge that 1 or more individuals using such product or service are covered minors shall have an independent, third-party auditor conduct an independent, third-party audit of the online product or service with respect to covered minors.

(2) Scope.—An audit required under paragraph (1) shall include—

(A) the number of covered minors known by the large data holder to use the online product or service during the year covered by the audit;

(B) the average and median amount of time spent by covered minors on the online product or service during the year covered by the audit;

(C) the number of times that the safeguards described in subsection (a) were exercised during the year covered by the audit;

(D) the number of times that the parental tools described in subsection (c) were exercised during the year covered by the audit;

(E) the number of reports received through the reporting mechanism described in subsection (d) during the year covered by the audit, and a description of how the large data holder handled such reports, including the rate of response and the timeliness and substantiveness of such responses;

(F) a description of whether, how, and for what purpose the large data holder collects or processes categories of covered data of covered minors; and

(G) if the large data holder has a process used to create, implement, or evaluate a design feature of the online product or service used by covered minors, a description of such process.

(3) Cooperation.—A large data holder subject to paragraph (1) shall facilitate an audit required under such paragraph by—

(A) providing or otherwise making available to the independent, third-party auditor all information and materials in the possession, custody, or control of the large data holder relevant to the audit;

(B) providing or otherwise making available to the auditor access to all networks, systems, and assets relevant to the audit; and

(C) disclosing all material facts to the auditor and not misrepresenting any material fact.

(4) Submission to Commission.—Not later than 30 days after the date on which an audit required under paragraph (1) is completed, the relevant large data holder shall submit to the Commission the results of the audit.

(f) Children and Teens Online Privacy Protection Act modernization.—

(1) Definitions.—Section 1302 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6501) is amended—

(A) in paragraph (2) to read as follows:

"(2) Operator.—

"(A) In general.—The term 'operator' means any person—

"(i) who, for commercial purposes, in interstate or foreign commerce operates or provides a website on the internet, an online service, an online application, or a mobile application; and

"(ii) who—

"(I) collects or maintains, either directly or through a service provider, personal information from or about the users of that website, service, or application;

"(II) allows another person to collect personal information directly from users of that website, service, or application, in which case the operator is deemed to have collected the information; or

"(III) allows users of that website, service, or application to publicly disclose personal information, in which case the operator is deemed to have collected the information.

"(B) Exclusion.—The term 'operator' does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).";

(B) in paragraph (4)—

(i) by amending subparagraph (A) to read as follows:

"(A) the release of personal information collected from a child or teen by an operator for any purpose, except where the personal information is provided to a person other than an operator who—

"(i) provides support for the internal operations of the website, online service, online application, or mobile application of the operator, excluding any activity relating to individual-specific advertising to children or teens; and

"(ii) does not disclose or use that personal information for any other purpose; and"; and

(ii) in subparagraph (B)—

(I) by inserting "or teen" after "child" each place the term appears;

(II) by striking "website or online service" and inserting "website, online service, online application, or mobile application"; and

(III) by striking "actual knowledge" and inserting "actual knowledge or knowledge fairly implied on the basis of objective circumstances";

(C) by striking paragraph (8) and inserting the following:

"(8) Personal information.—

"(A) In general.—The term 'personal information' means individually identifiable information about an individual collected online, including—

"(i) a first and last name;

"(ii) a home or other physical address including street name and name of a city or town;

"(iii) an email address;

"(iv) a telephone number;

"(v) a Social Security number;

"(vi) any other identifier that the Commission determines permits the physical or online contacting of a specific individual;

"(vii) a persistent identifier that can be used to recognize a specific child or teen over time and across different websites, online services, online applications, or mobile applications, including a customer number held in a cookie, an Internet Protocol address, a processor or device serial number, or unique device identifier, but excluding an identifier that is used by an operator solely for providing support for the internal operations of the website, online service, online application, or mobile application;

"(viii) a photograph, video, or audio file where such file contains a specific child's or teen's image or voice;

"(ix) geolocation information;

"(x) information generated from the measurement or technological processing of an individual's biological, physical, or physiological characteristics that is used to identify an individual, including—

"(I) fingerprints;

"(II) voice prints;

"(III) iris or retina imagery scans;

"(IV) facial templates;

"(V) deoxyribonucleic acid information; or

"(VI) gait; or

"(xi) information linked or reasonably linkable to a child or teen or the parents of that child or teen, including any unique identifier, that an operator collects online from the child or teen and combines with an identifier described in this subparagraph.

"(B) Exclusion.—The term 'personal information' shall not include an audio file that contains a child's or teen's voice so long as the operator—

"(i) does not request information via voice that would otherwise be considered personal information under this paragraph;

"(ii) provides clear notice of its collection and use of the audio file and its deletion policy in its privacy policy;

"(iii) only uses the voice within the audio file solely as a replacement for written words, to perform a task, or to engage with a website, online service, online application, or mobile application, including to perform a search or fulfill a verbal instruction or request; and

"(iv) only maintains the audio file long enough to complete the stated purpose and then immediately deletes the audio file and does not make any other use of the audio file prior to deletion.

"(C) Support for the internal operations of a website, online service, online application, or mobile application.—

"(i) In general.—For purposes of subparagraph (A)(vii), the term 'support for the internal operations of a website, online service, online application, or mobile application' means those activities necessary to—

"(I) maintain or analyze the functioning of the website, online service, online application, or mobile application;

"(II) perform network communications;

"(III) authenticate users of, or personalize the content on, the website, online service, online application, or mobile application;

"(IV) serve contextual advertising, provided that any persistent identifier is only used as necessary for technical purposes to serve the contextual advertisement or cap the frequency of advertising;

"(V) protect the security or integrity of the user, website, online service, online application, or mobile application;

"(VI) ensure legal or regulatory compliance; or

"(VII) fulfill a request of a child or teen as permitted by subparagraphs (A) through (C) of section 1303(b)(2).

"(ii) Condition.—Except as specifically permitted under clause (i), information collected for the activities listed in clause (i) may not be used or disclosed to contact a specific individual, including through individual-specific advertising to children or teens,

to amass a profile on a specific individual, in connection with processes that encourage or prompt use of a website, online service, online application, or mobile application, or for any other purpose.";

(D) in paragraph (9) to read as follows:

"(9) Verifiable consent.—The term 'verifiable consent' means any reasonable effort, taking into consideration available technology, including a request for authorization for future collection, use, and disclosure described in the notice, to ensure that, in the case of a child, a parent of the child, or, in the case of a teen, the teen—

"(A) receives direct notice of the personal information collection, use, and disclosure practices of the operator; and

"(B) before the personal information of the child or teen is collected, freely and unambiguously authorizes—

"(i) the collection, use, and disclosure, as applicable, of that personal information; and

"(ii) any subsequent use of that personal information.";

(E) in paragraph (10)—

(i) in the paragraph heading, by striking "Website or online service directed to children" and inserting "Website, online service, online application, or mobile application directed to children";

(ii) by striking "website or online service" each place it appears and inserting "website, online service, online application, or mobile application"; and

(iii) by adding at the end the following:

"(C) Rule of construction.—In considering whether a website, online service, online application, or mobile application, or portion thereof, is directed to children, the Commission shall apply a totality of circumstances test and shall also consider competent and reliable empirical evidence regarding audience composition and evidence regarding the intended audience of the website, online service, online application, or mobile application."; and

(F) by adding at the end the following:

"(13) Connected device.—The term 'connected device' means a device that is capable of connecting to the internet, directly or indirectly, or to another connected device.

"(14) Online application.—The term 'online application'—

"(A) means an internet-connected software program; and

"(B) includes a service or application offered via a connected device.

"(15) Mobile application.—The term 'mobile application'—

"(A) means a software program that runs on the operating system of—

"(i) a cellular telephone;

"(ii) a tablet computer; or

"(iii) a similar portable computing device that transmits data over a wireless connection; and

"(B) includes a service or application offered via a connected device.

"(16) Geolocation information.—The term 'geolocation information' means information sufficient to identify a street name and name of a city or town.

"(17) Teen.—The term 'teen' means an individual who has attained age 13 and is under the age of 17.

"(18) Individual-specific advertising to children or teens.—

"(A) In general.—The term 'individual-specific advertising to children or teens' means advertising or any other effort to market a product or service that is directed to a specific child or teen or a connected device that is linked or reasonably linkable to a child or teen based on—

"(i) the personal information from—

"(I) the child or teen; or

"(II) a group of children or teens who are similar in sex, age, household income level, race, or ethnicity to the specific child or teen to whom the product or service is marketed;

"(ii) profiling of a child or teen or group of children or teens; or

"(iii) a unique identifier of the connected device.

"(B) Exclusions.—The term 'individual-specific advertising to children or teens' shall not include—

"(i) advertising or marketing to an individual or the device of an individual in response to the individual's specific request for information or feedback, including a child's or teen's current search query;

"(ii) contextual advertising, including when an advertisement is displayed based on the content of the website, online service, online application, mobile application, or connected device in which the advertisement appears and does not vary based on personal information related to the viewer; or

"(iii) processing personal information solely for measuring or reporting advertising or content performance, reach, or frequency, including independent measurement.

"(C) Rule of construction.—Nothing in subparagraph (A) shall be construed to prohibit an operator with actual knowledge or knowledge fairly implied on the basis of objective circumstances that a user is under the age of 17 from delivering advertising or marketing

that is age-appropriate and intended for a child or teen audience, so long as the operator does not use any personal information other than whether the user is under the age of 17.".

(2) Online collection, use, disclosure, and deletion of personal information of children and teens.—Section 1303 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6502) is amended—

(A) by striking the heading and inserting the following: "Online collection, use, disclosure, and deletion of personal information of children and teens.";

(B) in subsection (a)—

(i) by amending paragraph (1) to read as follows:

"(1) In general.—It is unlawful for an operator of a website, online service, online application, or mobile application directed to children or for any operator of a website, online service, online application, or mobile application with actual knowledge or knowledge fairly implied on the basis of objective circumstances that a user is a child or teen—

"(A) to collect personal information from a child or teen in a manner that violates the regulations prescribed under subsection (b);

"(B) except as provided in subparagraphs (B) and (C) of section 1302(18), to collect, use, disclose to third parties, or maintain personal information of a child or teen for purposes of individual-specific advertising to children or teens, or to allow another person to collect, use, disclose, or maintain such information for such purpose;

"(C) to collect the personal information of a child or teen except when the collection of the personal information is—

"(i) consistent with the context of a particular transaction or service or the relationship of the child or teen with the operator, including collection necessary to fulfill a transaction or provide a product or service requested by the child or teen; or

"(ii) required or specifically authorized by Federal or State law;

"(D) to store or transfer the personal information of a child or teen outside of the United States unless the operator provides direct notice to the parent of the child, in the case of a child, or to the teen, in the case of a teen, that the child's or teen's personal information is being stored or transferred outside of the United States; or

"(E) to retain the personal information of a child or teen for longer than is reasonably necessary to fulfill a transaction or provide a service requested by the child or teen, except as required or specifically authorized by Federal or State law."; and

(ii) in paragraph (2)—

(I) in the heading, by striking "parent" and inserting "parent or teen";

(II) by striking "Notwithstanding paragraph (1)" and inserting "Notwithstanding paragraph (1)(A)";

(III) by striking "of such a website or online service"; and

(IV) by striking "subsection (b)(1)(B)(iii) to the parent of a child" and inserting "subsection (b)(1)(B)(iv) to the parent of a child or under subsection (b)(1)(C)(iv) to a teen";

(C) in subsection (b)—

(i) in paragraph (1)—

(I) in subparagraph (A)—

(aa) by striking "operator of any website" and all that follows through "from a child" and inserting "operator of a website, online service, online application, or mobile application directed to children or that has actual knowledge or knowledge fairly implied on the basis of objective circumstances that a user is a child or teen";

(bb) in clause (i), by striking "notice on the website" and inserting "clear and conspicuous notice on the website";

(cc) in clause (i), by inserting "or teens" after "children";

(dd) in clause (i), by striking ", and the operator's" and inserting ", the operator's";

(ee) in clause (i), by striking "; and" and inserting ", the rights and opportunities available to the parent of the child or teen under subparagraphs (B) and (C), and the procedures or mechanisms the operator uses to ensure that personal information is not collected from children or teens except in accordance with the regulations promulgated under this paragraph;";

(ff) in clause (ii), by striking "parental";

(gg) in clause (ii), by inserting "or teens" after "children";

(hh) in clause (ii), by striking the semicolon at the end and inserting "; and"; and

(ii) by inserting after clause (ii) the following:

"(iii) to obtain verifiable consent from a parent of a child or from a teen before using or disclosing personal information of the child or teen for any purpose that is a material change from the original purposes and disclosure practices specified to the parent of the child or the teen under clause (i);";

(II) in subparagraph (B)—

(aa) in the matter preceding clause (i), by striking "website or online service" and inserting "operator";

(bb) in clause (i), by inserting "and the method by which the operator obtained the personal information, and the purposes for which the operator collects, uses, discloses, and retains the personal information" before the semicolon;

(cc) in clause (ii), by inserting "to delete personal information collected from the child or content or information submitted by the child to a website, online service, online application, or mobile application and" after "the opportunity at any time";

(dd) in clause (ii), by striking "; and" and inserting a semicolon;

(ee) by redesignating clause (iii) as clause (iv);

(ff) by inserting after clause (ii) the following:

"(iii) the opportunity to challenge the accuracy of the personal information and, if the parent of the child establishes the inaccuracy of the personal information, to have the inaccurate personal information corrected;"; and

(gg) in clause (iv), as so redesignated, by inserting ", if such information is available to the operator at the time the parent makes the request" before the semicolon;

(III) by redesignating subparagraphs (C) and (D) as subparagraphs (D) and (E), respectively;

(IV) by inserting after subparagraph (B) the following:

"(C) require the operator to provide, upon the request of a teen under this subparagraph who has provided personal information to the operator, upon proper identification of that teen—

"(i) a description of the specific types of personal information collected from the teen by the operator, the method by which the operator obtained the personal information, and the purposes for which the operator collects, uses, discloses, and retains the personal information;

"(ii) the opportunity at any time to delete personal information collected from the teen or content or information submitted by the teen to a website, online service, online application, or mobile application and to refuse to permit the operator's further use or maintenance in retrievable form, or online collection, of personal information from the teen;

"(iii) the opportunity to challenge the accuracy of the personal information and, if the teen establishes the inaccuracy of the personal information, to have the inaccurate personal information corrected; and

"(iv) a means that is reasonable under the circumstances for the teen to obtain any personal information collected from the teen, if such information is available to the operator at the time the teen makes the request;";

(V) in subparagraph (D), as so redesignated—

(aa) by striking "a child's" and inserting "a child's or teen's"; and

(bb) by inserting "or teen" after "the child"; and

(VI) in subparagraph (E), as so redesignated, to read as follows:

"(E) require the operator to establish, implement, and maintain reasonable security practices to protect the confidentiality, integrity, and accessibility of personal information of children or teens collected by the operator, and to protect such personal information against unauthorized access.";

(ii) in paragraph (2)—

(I) in the matter preceding subparagraph (A), by striking "verifiable parental consent" and inserting "verifiable consent";

(II) in subparagraph (A)—

(aa) by inserting "or teen" after "collected from a child";

(bb) by inserting "or teen" after "request from the child"; and

(cc) by inserting "or teen or to contact another child or teen" after "to recontact the child";

(III) in subparagraph (B)—

(aa) by striking "parent or child" and inserting "parent or teen"; and

(bb) by striking "parental consent" each place it appears and inserting "verifiable consent";

(IV) in subparagraph (C)—

(aa) in the matter preceding clause (i), by inserting "or teen" after "child" each place it appears;

(bb) in clause (i), by inserting "or teen" after "child" each place it appears;

(cc) in clause (i), by inserting "or teen, as applicable," after "parent" each place it appears;

(dd) in clause (ii), by striking "without notice to the parent" and inserting "without notice to the parent or teen, as applicable,"; and

(ee) in clause (ii), by inserting "or teen" after "child" each place it appears; and

(V) in subparagraph (D)—

(aa) in the matter preceding clause (i), by inserting "or teen" after "child" each place it appears;

(bb) in clause (ii), by inserting "or teen" after "child";

(cc) in the flush text following clause (iii), by inserting "or teen, as applicable," after "parent" each place it appears; and

(dd) in the flush text following clause (iii), by inserting "or teen" after "child";

(iii) by redesignating paragraph (3) as paragraph (4);

(iv) by inserting after paragraph (2) the following:

"(3) Application to operators acting under agreements with educational agencies or institutions.—The regulations may provide that verifiable consent under paragraph (1)(A)(ii) is not required for an operator that is acting under a written agreement with an educational agency or institution, as defined in section 444 of the General Education Provisions Act, commonly known as the Family Educational Rights and Privacy Act of 1974, if the written agreement, at a minimum, requires the—

"(A) operator to—

"(i) limit its collection, use, and disclosure of the personal information from a child or teen to solely educational purposes and for no other commercial purposes;

"(ii) provide the educational agency or institution with a notice of the specific types of personal information the operator will collect from the child or teen, the method by which the operator will obtain the personal information, and the purposes for which the operator will collect, use, disclose, and retain the personal information;

"(iii) provide the educational agency or institution with a link to the operator's online notice of information practices as required under subsection (b)(1)(A)(i); and

"(iv) provide the educational agency or institution, upon request, with a means to review the personal information collected from a child or teen, to prevent further use or maintenance or future collection of personal information from a child or teen, and to delete personal information collected from a child or teen or content or information submitted by a child or teen to the operator's website, online service, online application, or mobile application;

"(B) representative of the educational agency or institution to acknowledge and agree that they have authority to authorize the collection, use, and disclosure of personal information from children or teens on behalf of the educational agency or institution, along with such authorization, their name, and title at the educational agency or institution; and

"(C) educational agency or institution to—

"(i) provide on its website a notice that identifies the operator with which it has entered into a written agreement under this subsection and provides a link to the operator's online notice of information practices as required under paragraph (1)(A)(i);

"(ii) provide the operator's notice regarding its information practices, as required under subparagraph (A)(ii), upon request, to a parent, in the case of a child, or a parent or teen, in the case of a teen; and

"(iii) upon the request of a parent, in the case of a child, or a parent or teen, in the case of a teen, request that the operator provide a means to review the personal information from the child or teen and provide the parent, in the case of a child, or parent or teen, in the case of the teen, a means to review the personal information.";

(v) by amending paragraph (4), as so redesignated, to read as follows:

"(4) Termination of service.—The regulations shall permit the operator of a website, online service, online application, or mobile application to terminate service provided to a child whose parent has refused, or a teen who has refused, under the regulations prescribed under paragraphs (1)(B)(ii) and (1)(C)(ii), to permit the operator's further use or maintenance in retrievable form, or future online collection, of personal information from that child or teen."; and

(vi) by adding at the end the following:

"(5) Continuation of service.—The regulations shall prohibit an operator from discontinuing service provided to a child or teen on the basis of a request by the parent of the child or by the teen, under the regulations prescribed under subparagraph (B) or (C) of paragraph (1), respectively, to delete personal information collected from the child or teen, to the extent that the operator is capable of providing such service without such information.

"(6) Rule of construction.—A request made pursuant to subparagraph (B) or (C) of paragraph (1) to delete or correct personal information of a child or teen shall not be construed—

"(A) to limit the authority of a law enforcement agency to obtain any content or information from an operator pursuant to a lawfully executed warrant or an order of a court of competent jurisdiction;

"(B) to require an operator or third party to delete or correct information that—

"(i) any other provision of Federal or State law requires the operator or third party to maintain; or

"(ii) was submitted to the website, online service, online application, or mobile application of the operator by any person other than the user who is attempting to erase or otherwise eliminate the content or information, including content or information submitted by the user that was republished or resubmitted by another person; or

"(C) to prohibit an operator from—

"(i) retaining a record of the deletion request and the minimum information necessary for the purposes of ensuring compliance with a request made pursuant to subparagraph (B) or (C);

"(ii) preventing, detecting, protecting against, or responding to security incidents, identity theft, or fraud, or reporting those responsible for such actions;

"(iii) protecting the integrity or security of a website, online service, online application, or mobile application; or

"(iv) ensuring that the child's or teen's information remains deleted.

"(7) Common verifiable consent mechanism.—

"(A) In general.—

"(i) Feasibility of mechanism.—The Commission shall assess the feasibility, with notice and public comment, of allowing operators the option to use a common verifiable consent mechanism that fully meets the requirements of this title.

"(ii) Requirements.—The feasibility assessment described in clause (i) shall consider whether a single operator could use a common verifiable consent mechanism to obtain verifiable consent, as required under this title, from a parent of a child or from a teen on behalf of multiple, listed operators that provide a joint or related service.

"(B) Report.—Not later than 1 year after the date of enactment of this paragraph, the Commission shall submit to Congress a report with the findings of the assessment required by subparagraph (A).

"(C) Regulations.—If the Commission finds that the use of a common verifiable consent mechanism is feasible and would meet the requirements of this title, the Commission shall issue regulations to permit the use of a common verifiable consent mechanism in accordance with the findings outlined in such report.";

(D) in subsection (c), by striking "a regulation prescribed under subsection (a)" and inserting "subparagraph (B), (C), (D), or (E) of subsection (a)(1), or of a regulation prescribed under subsection (b),"; and

(E) by striking subsection (d) and inserting the following:

"(d) Relationship to State law.—The provisions of this title shall preempt any State law, rule, or regulation only to the extent that such State law, rule, or regulation conflicts with a provision of this title. Nothing in this title shall be construed to prohibit any State from enacting a law, rule, or regulation that provides greater protection to children or teens than the provisions of this title.".

(3) Safe harbors.—Section 1304 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6503) is amended—

(A) in subsection (b)(1), by inserting "and teens" after "children"; and

(B) by adding at the end the following:

"(d) Publication.—

"(1) In general.—Subject to the restrictions described in paragraph (2), the Commission shall publish on the internet website of the Commission any report or documentation required by regulation to be submitted to the Commission to carry out this section.

"(2) Restrictions on publication.—The restrictions described in section 6(f) and section 21 of the Federal Trade Commission Act (15 U.S.C. 46(f), 57b–2) applicable to the disclosure of information obtained by the Commission shall apply in the same manner to the disclosure under this subsection of information obtained by the Commission from a report or documentation described in paragraph (1).".

(4) Actions by States.—Section 1305 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6504) is amended—

(A) in subsection (a)(1)—

(i) in the matter preceding subparagraph (A), by inserting "section 1303(a)(1) or" before "any regulation"; and

(ii) in subparagraph (B), by inserting "section 1303(a)(1) or" before "the regulation"; and

(B) in subsection (d)—

(i) by inserting "section 1303(a)(1) or" before "any regulation"; and

(ii) by inserting "section 1303(a)(1) or" before "that regulation".

(5) Administration and applicability.—Section 1306 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6505) is amended—

(A) in subsection (b)—

(i) in paragraph (1), by striking ", in the case of" and all that follows through "the Board of Directors of the Federal Deposit Insurance Corporation;" and inserting "by the appropriate Federal banking agency, with respect to any insured depository institution, as those terms are defined in section 3 of the Federal Deposit Insurance Act (12 U.S.C. 1813);"; and

(ii) by striking paragraph (2) and redesignating paragraphs (3) through (6) as paragraphs (2) through (5), respectively;

(B) in subsection (d)—

(i) by inserting "section 1303(a)(1) or" before "a rule"; and

(ii) by striking "such rule" and inserting "section 1303(a)(1) or a rule of the Commission under section 1303"; and

(C) by adding at the end the following:

"(f) Determination of whether an operator has knowledge fairly implied on the basis of objective circumstances.—

"(1) Rule of construction.—For purposes of enforcing this title or a regulation promulgated under this title, in making a determination as to whether an operator has knowledge fairly implied on the basis of objective circumstances that a specific user is a child or teen, the

Commission or State attorneys general shall rely on competent and reliable evidence, taking into account the totality of the circumstances, including whether a reasonable and prudent person under the circumstances would have known that the user is a child or teen.

"(2) Commission guidance.—

"(A) In general.—Not later than 180 days after the date of enactment of this subsection, the Commission shall issue guidance to provide information, including best practices and examples for operators to understand the Commission's determination of whether an operator has knowledge fairly implied on the basis of objective circumstances that a user is a child or teen.

"(B) Limitation.—No guidance issued by the Commission with respect to this title shall confer any rights on any person, State, or locality, or operate to bind the Commission or any person to the approach recommended in such guidance. In any enforcement action brought pursuant to this title, the Commission or State attorney general, as applicable, shall allege a specific violation of a provision of this title. The Commission or State attorney general, as applicable, may not base an enforcement action on, or execute a consent order based on, practices that are alleged to be inconsistent with any such guidance, unless the practices allegedly violate this title. For purposes of enforcing this title or a regulation promulgated under this title, State attorneys general shall take into account any guidance issued by the Commission under subparagraph (A).

"(g) Additional requirement.—Any regulations issued under this title shall include a description and analysis of the impact of proposed and final rules on small entities under chapter 6 of title 5, United States Code.".

(6) Reports and studies.—

(A) Oversight report.—Not later than 3 years after the date of enactment of this subsection, the Commission shall submit to Congress a report on the processes of platforms that offer mobile and online applications for ensuring that those applications that are websites, online services, online applications, or mobile applications directed to children operate in accordance with—

(i) the Children's Online Privacy Protection Act of 1998, as amended by this subsection, and rules promulgated under such Act; and

(ii) rules promulgated by the Commission under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a) relating to unfair, deceptive, or abusive acts or practices in marketing.

(B) Enforcement report.—Not later than 1 year after the date of enactment of this subsection, and each year thereafter, the Commission shall submit to Congress a report that addresses, at a minimum—

(i) the number of actions brought by the Commission during the reporting year to enforce the Children's Online Privacy Protection Act of 1998 and the outcome of each such action;

(ii) the total number of investigations or inquiries into potential violations of such Act during the reporting year;

(iii) the total number of open investigations or inquiries into potential violations of such Act as of the time the report is submitted;

(iv) the number and nature of complaints received by the Commission relating to an allegation of a violation of such Act during the reporting year; and

(v) policy or legislative recommendations to strengthen online protections for children and teens.

(C) Teen financial technology privacy study.—The Comptroller General of the United States shall conduct a study on the privacy of teens who use financial technology products, including a study to—

(i) identify the types of financial technology products that teens are using;

(ii) identify the potential risks to teens' privacy from using such financial technology products; and

(iii) determine whether existing laws are sufficient to address such risks to teens' privacy.

(D) Report.—Not later than 1 year after the date of enactment of this subsection, the Comptroller General shall submit to Congress a report containing the results of the study conducted under subparagraph (C), together with recommendations for such legislation and administrative action as the Comptroller General determines appropriate.

(g) Report by the Inspector General.—

(1) In general.—Not later than 2 years after the date of enactment of this subtitle, and biennially thereafter, the Inspector General of the Commission shall submit to the Commission and to the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Energy and Commerce of the House of Representatives a report regarding the safe harbor provisions in section 1304 of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. 6503), which shall include—

(A) an analysis of whether the safe harbor provisions are—

(i) operating fairly and effectively; and

(ii) effectively protecting the interests of covered minors; and

(B) any proposal or recommendation for policy changes that would improve the effectiveness of the safe harbor provisions.

(2) Publication.—Not later than 10 days after the date on which a report is submitted under paragraph (1), the Commission shall publish the report on the website of the Commission.

(h) Rule of construction.—Nothing in this section shall be construed to prevent a covered entity from taking reasonable measures to protect the privacy, safety, or security of covered minors consistent with this subtitle and other applicable law.

SEC. 567. BANNING SURVEILLANCE ADVERTISING.

(a) Definitions.—In this section—

(1) Advertisement.—The term "advertisement" means information provided by an advertiser to an advertising facilitator that the advertising facilitator, in exchange for monetary consideration or another thing of value, disseminates to an individual, connected device, or group of individuals or connected devices.

(2) Advertiser.—

(A) In general.—The term "advertiser" means a person to the extent such person, directly or indirectly, provides an advertising facilitator with monetary consideration or another thing of value for the dissemination of an advertisement to an individual, connected device, or group of individuals or connected devices.

(B) Exclusion.—The term "advertiser" does not include a natural person, except to the extent such person is engaged in a commercial activity that is more than de minimis.

(3) Advertising facilitator.—

(A) In general.—The term "advertising facilitator" means a person to the extent such person—

(i) receives monetary consideration or another thing of value to disseminate an advertisement to an individual, connected device, or group of individuals or connected devices; and

(ii) obtains or processes personal information with respect to the dissemination of the advertisement.

(B) Exclusion.—The term "advertising facilitator" does not include a natural person, except to the extent such person is engaged in a commercial activity that is more than de minimis.

(4) Connected device.—The term "connected device" means any electronic equipment that is—

(A) primarily designed for or marketed to consumers;

(B) capable of connecting to the internet or another communication network; and

(C) capable of sending, receiving, or processing personal information.

(5) Contents.—The term "contents", when used with respect to any communication, has the meaning given such term in section 2510 of title 18, United States Code.

(6) Disseminate.—The term "disseminate" means, with respect to an advertisement, to transmit, display, or otherwise disseminate the advertisement electronically or through communication by wire or radio.

(7) Dissemination.—The term "dissemination" means, with respect to an advertisement, the transmission, display, or other dissemination of the advertisement electronically or through communication by wire or radio.

(8) Indian lands.—The term "Indian lands" includes—

(A) any Indian country of an Indian Tribe (as such term is defined in section 1151 of title 18, United States Code);

(B) any land in Alaska owned, pursuant to the Alaska Native Claims Settlement Act (43 U.S.C. 1601 et seq.), by an Indian Tribe that is a Native village or by a Village Corporation (as such terms are defined in section 3 of that Act (43 U.S.C. 1602)) that is associated with an Indian Tribe; and

(C) any land that is part or all of a Tribal designated statistical area associated with an Indian Tribe, or is part or all of an Alaska Native village statistical area associated with an Indian Tribe, as defined by the Bureau of the Census for the purposes of the most recent decennial census.

(9) Indian Tribe.—The term "Indian Tribe" has the meaning given such term in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

(10) Obtain.—The term "obtain" means, with respect to personal information, to obtain such information in any manner, except when solely transmitting, routing, providing intermediate storage for, or providing connections for such information through a system or network.

(11) Personal information.—The term "personal information" means data linked or reasonably linkable to an individual or connected device, including—

(A) data inferred or derived about the individual or connected device from other obtained data, if such data is still linked or reasonably linkable to the individual or connected device;

(B) contents of communications;

(C) internet browsing history and online activity; and

(D) a unique identifier used for the purposes of targeting the dissemination of an advertisement.

(12) Recognized place.—

(A) In general.—The term "recognized place" means any of the following:

(i) A State.

(ii) Indian lands.

(iii) A county, municipality, city, town, township, village, borough, or similar unit of general government that is incorporated pursuant to a State law.

(iv) A census designated place (as defined in the most recent glossary of the Bureau of the Census).

(v) A designated market area (as defined in section 122(j) of title 17, United States Code).

(vi) A congressional district.

(vii) Any possession of the United States.

(B) Exclusions.—The term "recognized place" does not include—

(i) a subdivision of any item listed in subparagraph (A) that is not itself listed in such subparagraph; or

(ii) a ZIP Code.

(13) Target.—

(A) In general.—The term "target" means, with respect to the dissemination of an advertisement, to perform or cause to be performed any computational process designed to select an individual, connected device, or group of individuals or connected devices to which to disseminate the advertisement based on personal information pertaining to the individual or connected device or to the individuals or connected devices that make up the group.

(B) Exclusions.—The term "target" does not include, with respect to the dissemination of an advertisement, the performance or causing the performance of any computational process undertaken solely for transmitting, routing, providing intermediate storage for, or providing connections for the advertisement through a system or network.

(14) Third party.—The term "third party" includes, with respect to an advertiser or an advertising facilitator, a subsidiary, a corporate affiliate, or other related party of the advertiser or advertising facilitator.

(b) Prohibition on targeted advertising.—

(1) In general.—An advertiser or an advertising facilitator may not—

(A) target the dissemination of an advertisement; or

(B) knowingly enable an advertiser (in the case of an advertising facilitator), advertising facilitator (in the case of an advertiser), or third party to target the dissemination of an advertisement, including by providing a list of individuals or connected devices, contact information of an individual, or a unique identifier or other personal information that can be used to identify an individual or a connected device.

(2) Contextual advertisements.—

(A) In general.—For purposes of paragraph (1), an advertising facilitator shall not be considered to target the dissemination of an advertisement if the advertisement—

(i) is disseminated based on information the individual is viewing, engaging with, or searched for; and

(ii) is displayed in close proximity to such information.

(B) Prohibition on further use.—Information obtained in connection with subparagraph (A) may not be used to target additional advertisements or to knowingly enable an advertiser or third party to target the dissemination of additional advertisements.

(3) Exemptions for recognized places.—The prohibition in this subsection shall not apply to the dissemination of an advertisement targeted exclusively on a recognized place.

(c) Effective date.—This section shall be effective 90 days after the date of enactment of this Act.

SEC. 568. DATA PORTABILITY AND INTEROPERABILITY.

(a) Definitions.—In this section:

(1) Affirmative disclosure consent.—The term "affirmative disclosure consent" means an affirmative action of the consumer to make a choice following a clear and conspicuous disclosure to the consumer, separate and apart from any "privacy policy", "terms of service", "consent for research", or other similar document, of—

(A) the types of personal information that the covered platform will disclose to third parties;

(B) the reason for such disclosures;

(C) the identity of all such third parties;

(D) any opportunities consumers have to decline or rescind consent for such disclosures; and

(E) how consumers may exercise any such opportunities.

An affirmative action does not include obtaining a consumer's approval for a preselected default option.

(2) Business user.—The term "business user" means a person that utilizes or plans to utilize the covered platform for the sale or provision of products or services.

(3) Clear and conspicuous disclosure.—The term "clear and conspicuous disclosure" means that a required disclosure is difficult to miss such that it is easily noticeable and easily understandable by ordinary consumers, including in all of the following ways:

(A) In any communication that is solely visual or solely audible, the disclosure must be made through the same means through which the communication is presented. In any communication made through both visual and audible means, such as a television

advertisement, the disclosure must be presented simultaneously in both the visual and audible portions of the communication even if the representation requiring the disclosure is made through only one means.

(B) A visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, must stand out from any accompanying text or other visual elements so that it is easily noticed, read, and understood.

(C) An audible disclosure, including by telephone or streaming video, must be delivered in a volume, speed, and cadence sufficient for ordinary consumers to easily hear and understand it.

(D) In any communication using an interactive electronic medium, such as the internet or software, the disclosure must be unavoidable.

(E) The disclosure must use diction and syntax understandable to ordinary consumers and must appear in each language in which the triggering representation appears.

(F) The disclosure must comply with these requirements in each medium through which it is received, including all electronic devices and face-to-face communications.

(G) The disclosure must not be contradicted or mitigated by, or inconsistent with, anything else in the communication.

(H) When the representation or sales practice targets a specific audience, such as children, the elderly, or the terminally ill, "ordinary consumers" includes reasonable members of that group.

(4) Commission.—The term "Commission" means the Federal Trade Commission.

(5) Competitor.—The term "competitor" means an online platform that competes with, or is a potential competitor to, a covered platform.

(6) Covered platform.—The term "covered platform" means an online platform that—

(A) during any month in either of the previous 2 calendar years—

(i) had at least 50,000,000 United States-based monthly active users on the online platform; or

(ii) had at least 100,000 United States-based monthly active business users on the platform;

(B) during either of the previous 2 calendar years, was owned or controlled by a person with net annual sales, or a market capitalization, greater than $600,000,000,000, as adjusted and published for each fiscal year beginning after September 30, 2026, in the same manner as provided in section 8(a)(5) of the Clayton Act (15 U.S.C. 19(a)(5)), for the year then ended over the level for the year ending September 30, 2026;

(C) is a critical trading partner for the sale or provision of any product or service offered on or directly related to the online platform; or

(D) is designated as a covered platform under subsection (f).

(7) Covered platform operator.—The term "covered platform operator" means a person that, directly or indirectly, with respect to a covered platform—

(A) holds 25 percent or more of the stock;

(B) has the right to 25 percent or more of the profits;

(C) has the right to 25 percent or more of the assets in the event of the platform's dissolution;

(D) if the platform is a corporation, has the power to designate 25 percent or more of the directors;

(E) if the platform is a trust, has the power to designate 25 percent or more of the trustees; or

(F) otherwise exercises substantial control over such platform.

(8) Critical trading partner.—The term "critical trading partner" means a trading partner that has the ability to restrict or impede—

(A) the access of a business user to its users or customers; or

(B) the access of a business user to a tool or service that it needs to effectively serve its users or customers.

(9) Data.—

(A) In general.—The term "data" means information that is collected by or provided to a covered platform or a competitor that is linked, or reasonably linkable, to a specific user, user device, or customer of the covered platform or competitor, but does not include proprietary data that does not pertain to the user or a user device of such covered platform or competitor.

(B) Rulemaking.—Not later than 90 days after the date of enactment of this Act, the Commission shall adopt interim final rules in accordance with section 553 of title 5, United States Code, and shall thereafter promulgate final regulations after notice and comment, to clarify the term "data" for purposes of implementing and enforcing this section; provided the Commission shall narrowly construe the term "proprietary data."

(10) Interoperability interface.—The term "interoperability interface" means an electronic interface maintained by a covered platform for purposes of achieving interoperability.

(11) Online platform.—The term "online platform" means a website, online or mobile application, operating system, digital assistant, or online service that—

(A) enables a user to generate content that can be viewed by other users on the platform or to interact with other content on the platform;

(B) facilitates the offering, sale, purchase, payment, or shipping of goods or services, including software applications, between and among consumers or businesses not controlled by the platform; or

(C) enables user searches or queries that access or display a large volume of information.

(b) Unfair method of competition.—A violation of this section, or standards issued pursuant to this section, by a person, partnership, or corporation operating a covered platform, in or affecting commerce, shall be an unfair method of competition in violation of section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)).

(c) Portability.—

(1) In general.—A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to enable the secure transfer of data to a user, or with the affirmative disclosure consent of a user, to an online platform at the direction of a user, in a structured, commonly used, and machine-readable format that complies with the standards issued pursuant to subsection (f).

(2) (A) Data security.—An online platform that receives ported user data from a covered platform shall reasonably secure any user data it acquires, and shall take reasonable steps to avoid introducing security risks to data or the covered platform's information systems.

(B) Violation.—A failure to comply with this paragraph is a violation of this section and subject to enforcement under section 569.

(C) Termination of access.—The Commission may require the covered platform to cease the transfer of data to an online platform that the Commission finds has violated this paragraph or standards adopted by the Commission under subsection (f).

(3) Portability obligations.—In order to achieve portability under paragraph (1), a covered platform shall comply with the standards issued under subsection (f) by the Commission.

(d) Interoperability.—

(1) (A) In general.—A covered platform shall maintain a set of transparent, third-party-accessible interfaces (including application programming interfaces) to facilitate and maintain interoperability with competitors through an interoperability interface, based on fair, reasonable, and nondiscriminatory terms.

(B) Presumption.—It shall be a rebuttable presumption that a covered platform is providing access on fair, reasonable, and nondiscriminatory terms if—

(i) such platform establishes and maintains interoperability through an open standard established under subsection (f); and

(ii) with respect to a covered platform that maintains interoperability between more than 1 online platform affiliated with such covered platform, offers a functionally equivalent version of that interface to competitors.

(2) (A) Data security.—A competitor that accesses an interoperability interface of a covered platform shall reasonably secure any user data it acquires, processes, or transmits, and shall take reasonable steps to avoid introducing security risks to user data or the covered platform's information systems.

(B) Violation.—A failure to comply with this paragraph is a violation of this section and subject to enforcement under section 569.

(C) Termination of access.—The Commission may require the covered platform to cease interoperating with a competitor that the Commission finds has violated this paragraph or standards adopted by the Commission under subsection (f).

(3) Interoperability obligations.—A covered platform shall, in compliance with the standards issued pursuant to subsection (f), facilitate the importation of a user's data—

(A) from such user; or

(B) with the affirmative disclosure consent of a user, from an online platform at the direction of a user.

(4) Reasonable thresholds, access standards, fees, and privacy and security protections.—

(A) In general.—A covered platform may establish reasonable thresholds related to the frequency, nature, and volume of requests by a competitor to access resources maintained by the covered platform, beyond which the covered platform may assess a reasonable fee for such access.

(B) Usage expectations.—A covered platform may establish fair, reasonable, and nondiscriminatory usage expectations to govern access by competitors, including fees or penalties for competitors that exceed those usage expectations.

(C) Limitation on fees and usage expectations.—Any fees, penalties, or usage expectations assessed under subparagraphs (A) and (B) shall be reasonably proportional to the cost, complexity, and risk to the covered platform of providing such access.

(D) Notice.—A covered platform shall provide public notice of any fees, penalties, or usage expectations established under this paragraph, including reasonable advance notice of any changes.

(E) Security and privacy standards.—A covered platform shall, consistent with industry best practices, set privacy and security standards for access by competitors to the extent reasonably necessary to address a threat to the covered platform or user data, and shall report any suspected violations of those standards to the Commission.

(5) Prohibited changes to interfaces; interface information; notice of changes.—

(A) Prohibited changes.—A change to an interoperability interface or terms of use made with the purpose, or substantial effect, of unreasonably denying access or undermining interoperability for competitors shall be considered a violation of the duty under paragraph (1) to facilitate and maintain interoperability on fair, reasonable, and nondiscriminatory terms.

(B) Interface information.—

(i) In general.—Not later than 120 days after the adoption of a rule by the Commission under subsection (f), a covered platform shall make available to competitors, which may be provided through public notice, complete and accurate documentation describing access to the interoperability interface required under this subsection.

(ii) Contents.—The documentation required under clause (i)—

(I) is limited to interface documentation necessary to achieve development and operation of interoperable products and services; and

(II) does not require the disclosure of the source code of a covered platform.

(C) Notice of changes.—A covered platform shall provide reasonable advance notice to competitors, which may be provided through public notice, of any change to an interoperability interface maintained by the covered platform that will affect the interoperability with competitors.

(6) Data minimization.—

(A) Noncommercialization by a covered platform.—A covered platform shall not collect, use, or share user data obtained from a business user through the interoperability interface except for the purposes of safeguarding the privacy and security of such information or maintaining interoperability of services.

(B) Noncommercialization of data on a covered platform.—A business user shall not collect, use, or share the data of a user on a covered platform except for the purposes of safeguarding the privacy or security of such data, maintaining interoperability of services, fulfilling a transaction requested by the user, providing customer service, shipping or delivery, processing returns or refunds, warranty support, fraud prevention reasonably necessary to complete or protect a transaction requested by the user, or another purpose specifically and separately authorized by the user.

(e) Technical committee.—

(1) Establishment.—Not later than 90 days after the date of enactment of this Act, the Commission shall establish a technical committee, whose size and membership is within the sole discretion of the Commission except as specified in paragraph (2), to assist the Commission with considerations relating to—

(A) implementation and technical aspects of the requirements under subsections (c) and (d); and

(B) technical standards described under section 589(d) of this Act.

(2) Composition.—A technical committee shall include—

(A) representatives of businesses that, in the judgment of the Commission, utilize or compete with the covered platform;

(B) representatives of competition or privacy advocacy organizations, and independent academics that possess technical, legal, economic, financial, or other knowledge that the Commission may deem useful;

(C) a representative from the National Institute of Standards and Technology; and

(D) representatives of a covered platform, which, if required by the Commission, shall provide a nonvoting advisory member to provide consultation and other aid to the technical committee. A failure by the covered platform to participate in good faith in the development of standards by the technical committee shall be a violation of this section.

(3) General responsibilities.—A technical committee established under this subsection shall meet regularly to provide information, analysis, and recommendations to the Commission on the standards of portability and interoperability, the technical standards under section 589(d) of this Act, and any changes to such standards. With respect to the requirements of subsections (c) and (d), these standards shall—

(A) seek to reduce or eliminate network effects that limit competition with the covered platform;

(B) establish data security and privacy protections for data portability and interoperability;

(C) seek to prevent fraudulent, malicious, or abusive activity by competitors; and

(D) establish reasonable thresholds related to the frequency, nature, and volume of requests by a competitor to access resources maintained by the covered platform, beyond which the covered platform may assess a reasonable fee for such access that shall be reasonably proportional to the cost, complexity, and risk to the covered platform of providing such access, and do not limit the ability or deter the incentive of a competitor to interoperate with the covered platform.

(4) Role.—The role of technical committees is advisory in nature, and such committees shall have no implementation or enforcement authority. However, the Commission shall give strong consideration to the recommendations of such committees in implementing this section.

(5) Nonapplicability of the Federal Advisory Committee Act.—The requirements of chapter 10 of title 5, United States Code (commonly known as the 'Federal Advisory Committee Act'), shall not apply with respect to the technical committees.

(f) Implementation.—

(1) Official designation.—

(A) In general.—An online platform that meets the requirements under subparagraph (A), (B), or (C) of subsection (a)(6) shall be designated a covered platform by the Commission.

(B) Additional designation authority.—The Commission may officially designate as a covered platform any online platform whose designation would advance the goals of this

section, including reducing or eliminating network effects that limit competition with a covered platform, by publishing the designation in the Federal Register.

(C) Effect of designation.—After designating an online platform as a covered platform, the Commission shall issue standards of interoperability specific to the covered platform which incorporate the requirements of subsections (c) and (d).

(D) Duration of designation.—The designation of an online platform as a covered platform under subparagraph (A) or (B) shall apply indefinitely, regardless of whether there is a change in control or ownership of the platform, unless the Commission removes the designation under paragraph (3).

(2) Judicial review.—

(A) In general.—Any party that is subject to a covered platform designation pursuant to paragraph (1)(B), a final order issued in any district court, or a final order of the Commission issued in an administrative adjudicative proceeding may, within 30 days after the issuance of such order, petition for review of such order in the United States Court of Appeals for the District of Columbia Circuit.

(B) Treatment of findings.—In a proceeding for judicial review of a covered platform designation pursuant to paragraph (1) or a final order of the Commission, the findings of the Commission as to the facts, if supported by evidence, shall be conclusive.

(3) Removal of designation.—

(A) Request.—If an online platform designated as a covered platform under paragraph (1) ceases to meet the qualifications for such designation, the platform may submit to the Commission a request for removal of the designation, together with evidence that the platform no longer so qualifies.

(B) Determination.—

(i) In general.—Not later than 120 days after receiving a request under subparagraph (A), the Commission shall determine whether to grant the request and, if the Commission grants the request, remove the platform from the public list under paragraph (4).

(ii) Denied requests.—A denial under clause (i) of a request submitted under subparagraph (A) shall constitute final agency action for purposes of chapter 7 of title 5, United States Code.

(4) Public list.—

(A) In general.—The Commission shall maintain and periodically update on its website a public list of designated covered platforms.

(B) Omission not dispositive.—Omission from the public list under subparagraph (A) shall not by itself establish that a person is not a covered platform.

(5) Rulemaking and technical standards.—

(A) In adopting the standards implementing the requirements of subsections (c) and (d), the Commission shall seek to encourage entry into commerce by—

(i) reducing or eliminating the network effects that limit competition with the covered platform;

(ii) ensuring that competitors interconnect with the covered platform on fair and nondiscriminatory terms; and

(iii) protecting data security and privacy.

(B) The Commission shall—

(i) establish a technical committee pursuant to subsection (e) to develop proposed standards implementing the requirements of subsections (c) and (d) as they apply to a specific covered platform;

(ii) issue such open standards in accordance with section 553 of title 5, United States Code; and

(iii) reject standards that would unreasonably deny access, undermine interoperability, or be unduly disruptive to interoperability.

(C) In issuing standards under this paragraph, the Commission shall consult with the Director of the National Institute of Standards and Technology and may incorporate model technical standards published by the Director for interoperable classes of online communications or information services.

(6) Compliance assessment.—The Commission shall regularly assess compliance by covered platforms with the provisions of this section and may—

(A) undertake such investigation as appropriate to render this assessment;

(B) issue subpoenas and civil investigative demands for relevant information, including any information that is necessary to effectuate the goals of subsections (c) and (d), and consult with other agencies as appropriate; and

(C) prescribe such other rules in accordance with section 553 of title 5, United States Code as may be necessary and appropriate to carry out subsections (c) and (d).

(7) Agency complaints.—The Commission shall establish procedures under which a user, covered platform, or business user may file a complaint alleging a violation of this section.

(8) Reciprocity.—

(A) Opt in to participate.—A business user or competitor shall not be required to comply with the portability or interoperability requirements of this section unless it chooses to—

(i) initiate the secure export of data under subsection (c); or

(ii) access an interoperability interface under subsection (d) to import data.

(B) Reciprocal transfer obligation.—A business user or competitor that makes an election described in subparagraph (A)—

(i) shall, upon request of a user, facilitate the secure transfer of the data of that user, in a format consistent with the standards issued under this section, to—

(I) such user; or

(II) another entity, at the direction of the user and pursuant to the user's affirmative disclosure consent;

(ii) may cease importation of data through the interoperability interface at any time, provided such online platform or competitor shall first provide—

(I) notice to the Commission in such form as they may by regulation require; and

(II) clear and conspicuous notice to affected users; and

(iii) may cease exportation of data under subsection (c) no less than 90 days after ceasing importation of data under clause (ii).

(C) No effect on covered-platform duties.—Nothing in this paragraph shall be construed to relieve a covered platform of an obligation imposed on that covered platform under subsection (c) or (d).

SEC. 569. REGULATIONS AND ENFORCEMENT.

(a) Regulations.—The Commission shall promulgate regulations in accordance with section 553 of title 5, United States Code, as necessary to carry out this subtitle.

(b) Enforcement.—

(1) Federal Trade Commission.—A violation of this subtitle or a regulation promulgated under this subtitle shall be treated as a violation of a rule defining an unfair, deceptive, or abusive act or practice under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a).

(A) Powers of the Commission.—Except as provided in subparagraphs (B) and (C), the Commission shall enforce this subtitle and the regulations promulgated under this subtitle in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this subtitle, and any person who violates this subtitle or a regulation promulgated under this subtitle shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act.

(B) Exclusive litigation authority.—Notwithstanding section 16(a) of the Federal Trade Commission Act (15 U.S.C. 56(a)), the Commission shall have exclusive authority to commence or defend, and supervise the litigation of, any action for a violation of this subtitle or a regulation promulgated under this subtitle, and any appeal of such action, in its own name by any of its attorneys designated by it for such purpose, without first referring the matter to the Attorney General.

(C) Common carriers and nonprofit organizations.—Notwithstanding section 4, section 5(a)(2), or section 6 of the Federal Trade Commission Act (15 U.S.C. 44; 45(a)(2); 46), or any jurisdictional limitation of the Commission, the Commission shall also enforce this subtitle and the regulations promulgated under this subtitle in the same manner provided in subparagraphs (A) and (B) with respect to—

(i) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof and supplementary thereto; and

(ii) organizations not organized to carry on business for their own profit or that of their members.

(D) Savings clause.—Nothing in this subtitle shall be construed to limit the authority of the Commission under any other provision of law.

(E) Intervention by the Commission.—The Commission may intervene in any civil action brought under paragraphs (2) or (3), and upon intervening may be heard on all matters arising in the civil action, and file petitions for appeal of a decision in the civil action.

(2) States.—

(A) In general.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of the State has been or is threatened or adversely affected by an act or practice in violation of this subtitle or a regulation promulgated under this subtitle, the attorney general of the State may, as parens patriae, bring a civil action on behalf of the residents of the State in an appropriate district court of the United States or an appropriate State court to obtain appropriate relief.

(B) Commission intervention.—

(i) Notice to the Commission.—

(I) In general.—Except as provided in subclause (III), the attorney general of a State shall notify the Commission in writing that the attorney general intends to bring a civil action under subparagraph (A) before initiating the civil action.

(II) Contents.—The notification required by subclause (I) with respect to a civil action shall include a copy of the complaint to be filed to initiate the civil action.

(III) Exception.—If it is not feasible for the attorney general of a State to provide the notification required by subclause (I) before initiating a civil action under subparagraph (A), the attorney general shall notify the Commission immediately upon instituting the civil action.

(ii) Intervention by the Commission.—The Commission may—

(I) intervene in any civil action brought by the attorney general of a State under subparagraph (A); and

(II) upon intervening—

(aa) remove the civil action to the appropriate district court of the United States, if the action was not originally brought in such court;

(bb) be heard on all matters arising in the civil action; and

(cc) file petitions for appeal of a decision in the civil action.

(iii) Investigatory powers.—Nothing in this paragraph may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(C) Action by the Commission.—If the Commission institutes a civil action with respect to a violation of this subtitle or a regulation promulgated under this subtitle, the attorney general of a State may not, during the pendency of such action, bring a civil action under subparagraph (A) against any defendant named in the complaint of the Commission for the violation with respect to which the Commission instituted such action.

(D) Actions by other State officials.—In addition to civil actions brought by attorneys general under subparagraph (A), any other officer of a State who is authorized by the State to do so may bring a civil action under such subparagraph, subject to the same requirements and limitations that apply under this paragraph to civil actions brought by attorneys general.

(E) Penalties.—The maximum civil monetary penalty for violations subject to civil penalties under this paragraph shall be the same as the maximum civil penalty amount for violations of unfair, deceptive, or abusive trade practices under the Federal Trade Commission Act, as periodically published by the Commission pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990, as amended, and any corresponding rules (16 C.F.R. 1.98).

(F) Savings provision.—Nothing in this paragraph may be construed to prohibit an attorney general or authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

(3) Private civil action.—

(A) In general.—Any individual alleging a violation of this subtitle or a regulation promulgated under this subtitle may bring a civil action in any Federal or State court of competent jurisdiction, provided that a plaintiff notifies the Commission in writing before filing such action, such notification including a copy of the complaint, except that if it is not feasible to provide the required notification prior to initiating a civil action under this paragraph, such notification shall be made immediately upon instituting the civil action.

(B) Relief.—In a civil action in which the plaintiff prevails, the court may award an amount equal to, in the case of a negligent violation, not less than $100 and not greater than $1,000 per violation, or in the case of a reckless, knowing, willful, or intentional violation, not less than $500 and not greater than $5,000 per violation, reasonable

attorney's fees and litigation costs, and any other relief, including equitable or declaratory relief, that the court determines appropriate.

(C) Injury in fact.—A violation of this subtitle or a regulation promulgated under this subtitle with respect to the covered data of an individual constitutes a concrete and particularized injury in fact to that individual.

(c) Rule of construction.—Nothing in this subtitle shall be construed—

(1) to preempt or limit any Federal, State, local, or Tribal law that provides equal or greater protection for privacy, data security, data portability, interoperability, or protection against deceptive, manipulative, misleading, abusive, or intrusive advertising or data practices; or

(2) to limit the authority of the Federal Trade Commission, the Attorney General, the Federal Communications Commission, the Secretary of Health and Human Services, or any other Federal agency under any other provision of law.

Subtitle E—Rein In Big Tech

SEC. 571. COMPETITION AND TRANSPARENCY IN DIGITAL ADVERTISING.

(a) Digital advertising trading transparency and competition.—The Clayton Act is amended by inserting after section 8 (15 U.S.C. 19) the following:

"Sec. 8A. Competition and transparency in digital advertising.

"(a) Definitions.—In this section:

"(1) Applicability date.—The term 'applicability date' means the date that is 1 year after the date of enactment of this section.

"(2) Brokerage customer.—The term 'brokerage customer' means a person who has purchased or sold digital advertisements, or directly related goods or services, through a buy-side brokerage or a sell-side brokerage.

"(3) Buy-side brokerage.—The term 'buy-side brokerage' means a person in the business of effecting transactions on digital advertising exchanges, including by offering software or services that assist in serving or displaying digital advertisements, for other buyers.

"(4) Digital advertisement.—The term 'digital advertisement' means an advertisement that is served electronically over a computer network, including the internet.

"(5) Digital advertising exchange.—The term 'digital advertising exchange' means a person who constitutes, maintains, or provides a marketplace for or facilitates bringing together buyers and 1 or more sellers of digital advertisements, or for otherwise performing with respect to digital advertising the functions commonly performed by a digital advertising marketplace.

"(6) Digital advertising revenue.—The term 'digital advertising revenue' means the greater of—

"(A) global revenue derived from or directly related to the operation of a digital advertising exchange, a buy-side brokerage, or a sell-side brokerage;

"(B) the sum of the clearing prices of all digital advertisements bought or sold from or through a digital advertising exchange;

"(C) the total value of the gross advertising spending managed by a buy-side brokerage; or

"(D) the total value of the gross advertising sales managed by a sell-side brokerage.

"(7) Divestiture deadline.—The term 'divestiture deadline' means, with respect to a required divestiture approved by the Attorney General, the later of—

"(A) 30 days after the date on which the Attorney General approves the required divestiture; or

"(B) 30 days after the expiration of any applicable waiting period specified in section 7A.

"(8) Own.—The term 'own' means to own, operate, or control, directly or indirectly, in whole or in part.

"(9) Person.—The term 'person' includes—

"(A) any subsidiary of an entity; and

"(B) any corporate parent of an entity.

"(10) Required divestiture.—The term 'required divestiture'—

"(A) means a divestiture, sale, or other transaction undertaken to comply with any provision of this section; and

"(B) does not include any action required by a court of the United States.

"(11) Sell-side brokerage.—The term 'sell-side brokerage' means a person in the business of effecting transactions on digital advertising exchanges, including by offering software or services that assist in serving or displaying digital advertisements, for sellers.

"(b) Prohibitions.—No person with more than $20,000,000,000 in digital advertising revenue during the previous calendar year may, after the applicability date—

"(1) own a digital advertising exchange if the person—

"(A) owns a sell-side brokerage or a buy-side brokerage; or

"(B) is a seller of digital advertising space;

"(2) own a sell-side brokerage if the person owns a buy-side brokerage; or

"(3) own a buy-side brokerage or a sell-side brokerage if the person is a buyer or seller of digital advertising space.

"(c) Requirements.—On and after the applicability date, any person with more than $5,000,000,000 in digital advertising revenue during the previous calendar year shall be subject to the following requirements:

"(1) Best interest duty.—A buy-side brokerage or sell-side brokerage—

"(A) shall, in the course of providing services as a brokerage, use reasonable diligence, care, and skill to act in the best interests of the brokerage customers; and

"(B) may not put the interests of the brokerage ahead of those of the brokerage customers.

"(2) Best execution duty.—A buy-side brokerage or sell-side brokerage shall seek the most favorable terms reasonably available under the circumstances for each order transaction of the brokerage customer.

"(3) Transparency requirements.—

"(A) In general.—Upon written request from a brokerage customer, a buy-side brokerage or sell-side brokerage shall supply to the brokerage customer, within a reasonable time, information sufficient to permit the brokerage customer to verify compliance of the brokerage with the obligations under paragraphs (1) and (2).

"(B) Contents.—The information described in subparagraph (A) shall include, if requested and to the extent such information is collected by the brokerage in the ordinary course of business—

"(i) in the case of a sell-side brokerage providing information to a sell-side brokerage customer—

"(I) a unique and persistent identifier that identifies each unique digital advertising space for sale;

"(II) for each identifier described in subclause (I), all bids received, and, for each bid received, the bid submitted to the digital advertising exchange on behalf of the buy-side brokerage customer, the winning price, the uniform resource locator or other property identifier at the lowest level of granularity, the identity of the digital advertising exchange or other digital advertising venue returning the bid, date, time that the bid response was received in microseconds or a lower level of granularity, web domain associated with the advertising creative, the advertising creative size and format, and whether the bid won the impression of the seller;

"(III) the nature of any data collected or derived from the brokerage customer or any user or customer of the brokerage customer, and the ways in which the data is used by the sell-side brokerage;

"(IV) the order or bid routing practices or processes, including any material exceptions to the standard practice of the brokerage; and

"(V) the source and nature of any compensation paid or received in connection with transactions; and

"(ii) in the case of a buy-side brokerage providing information to a buy-side brokerage customer—

"(I) all bids won by the buy-side brokerage customer, and for each bid won, the maximum allowed bid of the advertiser, if any, the uniform resource locator or other property identifier at the lowest level of granularity, date, the digital advertising exchange, the web domain associated with the advertising creative, the advertising creative size and format, the winning price, the bid submitted to the digital advertising exchange on behalf of the buy-side brokerage customer, and, if possible, whether the ad served and whether the ad rendered;

"(II) the order or bid routing practices or processes; and

"(III) the source and nature of any compensation paid or received in connection with transactions.

"(C) Retention of records.—Brokerages shall retain the applicable records specified in subparagraph (B) collected in the ordinary course of business until provided to a requesting brokerage customer but not longer than 90 days. Brokerages shall retain billing information for brokerage customers for not fewer than 12 months.

"(D) User privacy.—

"(i) In general.—When providing information to a brokerage customer in response to a request authorized by subparagraph (A), the brokerage shall, to the greatest extent possible consistent with the purpose of subparagraph (A), anonymize, hash, or otherwise render the information incapable of being tied to an individual web user.

"(ii) Prohibiting tracking.—A brokerage customer may not use data or information received in response to a request made under subparagraph (A) for any purpose other than—

"(I) verifying compliance of a brokerage with the obligations under paragraphs (1) and (2); or

"(II) bringing an action under subsection (d)(3).

"(4) Firewalls.—

"(A) Buy-side and sell-side brokerages.—Buy-side brokerages and sell-side brokerages shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure compliance with the obligations under this subsection.

"(B) Other persons.—Persons not subject to prohibitions under subsection (b) shall establish, maintain, and enforce written policies and procedures reasonably designed to ensure that the buy-side brokerage, sell-side brokerage, digital advertising exchange, and role as a buyer or seller of digital advertising, as applicable, operate separate and independent from one another and transact business at arm's length.

"(5) Fair access duty.—A digital advertising exchange shall provide every buyer and seller in the exchange fair access, including with respect to operations of the exchange, colocation, any technology systems or data, information related to transactions, service, or products offered, exchange processes, and functionality.

"(6) Time synchronization.—A digital advertising exchange, buy-side brokerage, or sell-side brokerage shall—

"(A) synchronize its business clocks at a minimum to within a 2 milliseconds tolerance of the time maintained by the atomic clock of the National Institute of Standards and Technology; and

"(B) maintain the synchronization described in subparagraph (A).

"(7) Data ownership.—All records pertaining to an order solicited or submitted by a brokerage customer, and the subsequent result of the order, shall remain the property of the customer, including any bids solicited from or submitted to any digital advertising exchange, unless the information is otherwise publicly available.

"(8) Routing practices disclosure.—

"(A) In general.—Every sell-side brokerage and buy-side brokerage shall—

"(i) make publicly available for each calendar quarter a report on the order routing practices of the sell-side brokerage or buy-side brokerage, as applicable, for digital advertisements during the quarter broken down by calendar month; and

"(ii) retain the report described in clause (i) posted on an internet website that is free and readily accessible to the public for the 3-year period beginning on the date on which the report is posted.

"(B) Format.—Reports made available pursuant to subparagraph (A) shall—

"(i) be rendered in a format that makes the reports readily informative to the average brokerage customer; and

"(ii) include for the 10 venues to which the largest number of total bid requests or bid responses were routed for execution and for any venue to which 5 percent or more of bid requests or bid responses were routed for execution—

"(I) the total number of bids routed;

"(II) the total number of bids executed;

"(III) the fill rate of bids;

"(IV) the average net execution fee or rebate per 1,000 impressions;

"(V) the average time in milliseconds between when a bid request is sent and when a bid response is received; and

"(VI) the value and form of any compensation given in exchange for routing or execution.

"(9) Certification.—A digital advertising exchange, buy-side brokerage, or sell-side brokerage shall certify to the Attorney General on an annual basis that such certifying entity has complied with the requirements under this subsection.

"(d) Enforcement.—

"(1) Attorney General and State attorneys general.—

"(A) Definition.—In this paragraph, the term 'Fund' means the Antitrust Consumer Damages Fund established under subparagraph (D).

"(B) Civil action.—The Attorney General and State attorneys general may bring an action on behalf of persons in the United States injured in their business or property by reason of any violation of this section in any district court of the United States in the district in which the defendant resides or is found or has an agent, without respect to the amount in controversy, and shall—

"(i) in a case brought by the Attorney General or a State attorney general, be entitled to injunctive relief; and

"(ii) in a case brought by the Attorney General, recover damages sustained by such persons.

"(C) Damages.—

"(i) In general.—The court may award under this subsection, pursuant to a motion by the Attorney General promptly made, damages calculated under section 4 of the Clayton Act (15 U.S.C. 15).

"(ii) No duplicative award.—A court may not award any damages under this subparagraph that are duplicative of damages awarded before the date of the award under this subparagraph in a separate civil action pertaining to the same conduct and injured party.

"(iii) Payments.—A court awarding damages to a person in a civil action after the date of an award of damages under this subsection that would be duplicative of damages awarded to the Attorney General on behalf of the person shall direct that such damages shall first be paid by the Attorney General from amounts in the Fund and, to the extent such damages are not fully paid from amounts in the Fund, shall be paid by the defendant.

"(D) Antitrust Consumer Damages Fund.—

"(i) In general.—There is established in the Treasury of the United States a fund to be known as the 'Antitrust Consumer Damages Fund', which shall consist of amounts deposited under clause (ii).

"(ii) Deposits and availability.—Notwithstanding section 3302 of title 31, United States Code, any amounts received by the Attorney General under an award under this subsection—

"(I) shall be deposited in the Fund; and

"(II) shall be available to the Attorney General, without further appropriation, for distribution to persons in the United States harmed by the applicable violation of the Clayton Act (15 U.S.C. 12 et seq.).

"(iii) Deposits into the general fund.—Effective on the day after the date that is 10 years after the date on which an award is received under this paragraph, the unobligated balances in the Fund of amounts that were received under the award are rescinded and shall be deposited in the general fund of the Treasury.

"(2) Divestiture enforcement.—The Attorney General may bring an action on behalf of the United States in any district court of the United States in the district in which the defendant resides or is found or has an agent, and may obtain injunctive relief upon showing by a preponderance of the evidence that the defendant has—

"(A) violated a requirement of subsection (e); or

"(B) undertaken a required divestiture that unnecessarily harms or threatens competition in any market.

"(3) Private civil action.—

"(A) In general.—A brokerage customer harmed by a knowing violation of subsection (c) by a person with more than $20,000,000,000 in digital advertising revenue during the previous calendar year may bring a civil action in an appropriate court to obtain injunctive relief, if appropriate, and recover damages in the amount of the greater of—

"(i) $1,000,000 for each month in which the violation occurred and reasonable attorney's fees; or

"(ii) actual damages and reasonable attorney's fees.

"(B) No class action waiver.—No person covered by this section may require a class action waiver for claims under this section, including for arbitration.

"(C) Timing.—A civil action for a violation of subsection (c) may be brought—

"(i) on or after the applicability date, if no required divestiture applies to the defendant; or

"(ii) if a required divestiture applies to the defendant, at any time after the later of—

"(I) the expiration of any applicable divestiture deadline; or

"(II) the expiration of the deadline described in subsection (e)(1), if no filing has been made.

"(e) Divestiture.—

"(1) Filing.—Any agreement or other document setting out the terms of a required divestiture shall be filed with the Attorney General not later than the later of—

"(A) the applicability date; or

"(B) the earlier of—

"(i) 30 days after the date on which an agreement making a required divestiture under this section is executed; or

"(ii) 180 days after meeting the criteria specified in any paragraph of subsection (b).

"(2) Attorney General review.—The Attorney General shall approve a required divestiture upon a showing by the person making the divestiture that the terms of the divestiture, including the qualifications of any counterparty to the divestiture, will not unnecessarily harm or threaten competition in any market.

"(3) Timing.—

"(A) In general.—The Attorney General shall grant or deny approval of a required divestiture, unless agreed to by the parties, not later than the later of—

"(i) 60 days after receipt of all information obtained pursuant to paragraph (5); or

"(ii) 60 days after receipt of the filing made under paragraph (1).

"(B) Completion.—A divestiture shall be completed not later than the divestiture deadline.

"(C) Effect of denial.—If the Attorney General denies approval of a required divestiture, the person shall file a revised agreement or other document under paragraph (1) not later than 30 days after the date of the denial. A denied divestiture may not be completed.

"(4) Guidance.—The Attorney General shall—

"(A) not later than 90 days after the date of enactment of the POPULIST Act, issue guidance on the divestiture process; and

"(B) update the guidance described in subparagraph (A) as the Attorney General determines is appropriate.

"(5) Compulsory process.—The Attorney General may request or issue a civil investigative demand under section 3 of the Antitrust Civil Process Act (15 U.S.C. 1312) for documents from any person involved in a required divestiture to determine the competitive effects of the divestiture.

"(f) Rules of construction.—Nothing in this section shall—

"(1) prohibit a person from—

"(A) selling their own inventory of advertising space if—

"(i) the inventory was not acquired solely for the purposes of resale, except to monetize the content or intellectual property of the person; and

"(ii) the person does not also assist a third-party in the sale or purchase of advertising space, other than purchasing advertising space from the person; or

"(B) buying inventory to market the products or services of the person;

"(2) abridge or supersede any provision of, or rules issued pursuant to, section 7A;

"(3) prohibit a person from, consistent with the antitrust laws, entering into a joint venture or other collaboration to prevent harm from spam, fraud, or other forms of abuse in digital advertising; or

"(4) require the disclosure of information if the disclosure would violate a law of the United States or a foreign country.

"(g) Inflation adjustment.—For each fiscal year commencing after September 30, 2027, the Federal Trade Commission shall adjust and publish each dollar amount in this section that references digital advertising revenue in the same manner as provided in section 8(a)(5), except that the base year shall be the fiscal year ending September 30, 2026.".

SEC. 572. OPEN APP MARKETS ACT.

(a) Definitions.—In this section:

(1) App.—The term "app" means a software application or electronic service that may be run or directed by a user on a computer, a mobile device, or any other general purpose computing device.

(2) App store.—The term "app store" means a publicly available website, software application, or other electronic service that distributes apps from third-party developers to users of a computer, a mobile device, or any other general purpose computing device.

(3) Covered company.—The term "covered company" means any person that owns or controls an app store for which users in the United States exceed 50,000,000.

(4) Developer.—The term "developer" means a person that owns or controls an app or an app store.

(5) In-app payment system.—The term "in-app payment system" means an application, service, or user interface to process payments from users of an app.

(6) Nonpublic business information.—The term "nonpublic business information" means nonpublic data that is—

(A) derived from a developer or an app or app store owned or controlled by a developer, including interactions between users and the app or app store of the developer; and

(B) collected by a covered company in the course of operating an app store or providing an operating system.

(b) Protecting a competitive app market.—

(1) Exclusivity and tying.—A covered company shall not—

(A) require developers to use an in-app payment system owned or controlled by the covered company or any of its business partners as a condition of being—

(i) distributed on an app store; or

(ii) accessible on an operating system;

(B) require, as a term of distribution on an app store, that pricing terms or conditions of sale be equal to or more favorable on its app store than the terms or conditions under another app store; or

(C) take punitive action or otherwise impose less favorable terms and conditions against a developer for using or offering different pricing terms or conditions of sale through another in-app payment system or on another app store.

(2) Interference with legitimate business communications.—A covered company shall not impose restrictions on communications of developers with users of an app through an app or direct outreach to a user concerning legitimate business offers, including pricing terms and product or service offerings.

(3) Nonpublic business information.—A covered company shall not use nonpublic business information derived from a third-party app for the purpose of competing with that app.

(4) Interoperability.—A covered company that controls, directly or indirectly, the operating system or operating system configuration on which its app store operates shall allow and provide readily accessible means for users of that operating system to—

(A) choose third-party apps or app stores as defaults for categories appropriate to the app or app store;

(B) install third-party apps or app stores through means other than the covered company's app store, without requiring the developer to be verified or approved by the covered company; and

(C) hide or delete apps or app stores provided or preinstalled by the covered company or any of its business partners.

(5) Self-preferencing in search.—

(A) In general.—A covered company shall not provide unequal treatment of apps in an app store through unreasonably preferencing or ranking the apps of the covered company or any of its business partners over those of other apps.

(B) Considerations.—Unreasonably preferencing—

(i) includes applying ranking schemes or algorithms that prioritize apps based on a criterion of ownership interest by the covered company or its business partners; and

(ii) does not include clearly disclosed advertising.

(6) Open app development.—Access to operating system interfaces, development information, and hardware and software features shall be provided to developers on a timely basis and on terms that are equivalent or functionally equivalent to the terms for access by similar apps or functions provided by the covered company or to its business partners.

(c) Protecting the security and privacy of users.—

(1) In general.—Subject to paragraph (2), a covered company shall not be in violation of subsection (b) for an action that is—

(A) necessary to achieve user privacy, security, or digital safety;

(B) taken to prevent spam or fraud; or

(C) taken to prevent a violation of, or comply with, Federal or State law.

(2) Requirements.—Paragraph (1) shall apply only if the covered company establishes by clear and convincing evidence that the action—

(A) is applied on a demonstrably consistent basis to apps of the covered company or its business partners and to other apps;

(B) is not used as a pretext to exclude, or impose unnecessary or discriminatory terms on, third-party apps, in-app payment systems, or app stores; and

(C) is narrowly tailored and could not be achieved through a less discriminatory and technically possible means.

(d) Enforcement.—

(1) In general.—The Federal Trade Commission, the Attorney General, and any attorney general of a State subject to paragraph (4) shall enforce this section in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) or the Clayton Act (15 U.S.C. 12 et seq.), as appropriate, were incorporated into and made a part of this section.

(2) Unfair methods of competition.—A violation of this section constitutes an unfair method of competition under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(3) Federal Trade Commission independent litigation authority.—If the Federal Trade Commission has reason to believe that a covered company violated this section, the Federal Trade Commission may commence a civil action, in its own name, by any of its attorneys designated for such purpose, to recover a civil penalty and seek other appropriate relief in a district court of the United States.

(4) Parens patriae.—Any attorney general of a State may bring a civil action in the name of such State for a violation of this section as parens patriae on behalf of natural persons residing in such State, in any district court of the United States having jurisdiction over the defendant, and may secure any form of relief provided for in this subsection.

(5) Suits by developers injured.—

(A) In general.—Any developer who shall be injured by reason of anything forbidden in this section may sue therefor in any district court of the United States in the district in which the defendant resides or is found or has an agent, without respect to the amount in controversy, and shall recover threefold the damages sustained by such developer, and the

cost of suit, including a reasonable attorney's fee. The court may award under this subparagraph, pursuant to a motion by such developer promptly made, simple interest on actual damages for the period beginning on the date of service of such developer's pleading setting forth a claim under this section and ending on the date of judgment, or for any shorter period therein, if the court finds that the award of such interest for such period is just in the circumstances. In determining whether an award of interest under this subparagraph for any period is just in the circumstances, the court shall consider only—

(i) whether such developer or the opposing party, or either party's representative, made motions or asserted claims or defenses so lacking in merit as to show that such party or representative acted intentionally for delay, or otherwise acted in bad faith;

(ii) whether, in the course of the action involved, such developer or the opposing party, or either party's representative, violated any applicable rule, statute, or court order providing for sanctions for dilatory behavior or otherwise providing for expeditious proceedings; and

(iii) whether such developer or the opposing party, or either party's representative, engaged in conduct primarily for the purpose of delaying the litigation or increasing the cost thereof.

(B) Injunctive relief.—Any developer shall be entitled to sue for and have injunctive relief, in any court of the United States having jurisdiction over the parties, against threatened loss or damage by a violation of this section, when and under the same conditions and principles as injunctive relief against threatened conduct that will cause loss or damage is granted by courts of equity, under the rules governing such proceedings, and upon the execution of proper bond against damages for an injunction improvidently granted and a showing that the danger of irreparable loss or damage is immediate, a preliminary injunction may issue. In any action under this subparagraph in which the plaintiff substantially prevails, the court shall award the cost of suit, including a reasonable attorney's fee, to such plaintiff.

(e) Rule of construction.—Nothing in this section shall be construed to limit any authority of the Attorney General or the Federal Trade Commission under the antitrust laws (as defined in the first section of the Clayton Act (15 U.S.C. 12)), the Federal Trade Commission Act (15 U.S.C. 41 et seq.), or any other provision of law, or to limit the application of any law.

(f) Effective date.—This section shall be effective January 1, 2027.

SEC. 573. PROHIBITION RELATED TO LARGE PLATFORM UTILITIES.

(a) Definitions.—In this section:

(1) Affiliate.—The term "affiliate" has the meaning given that term under section 2 of the Bank Holding Company Act of 1956.

(2) Alternative trading system.—The term "alternative trading system" has the meaning given that term under section 242.300 of title 17, Code of Federal Regulations.

(3) Banking definitions.—The terms "depository institution" and "depository institution holding company" have the meanings given those terms, respectively, under section 3 of the Federal Deposit Insurance Act.

(4) Commodities definitions.—The terms "commodity pool operator", "commodity trading advisor", and "futures commission merchant" have the meanings given those terms, respectively, under section 1a of the Commodity Exchange Act.

(5) Credit union.—The term "credit union" means a Federal credit union or a State credit union, as such terms are defined, respectively, under section 101 of the Federal Credit Union Act.

(6) Digital asset.—The term "digital asset" means an asset that is issued and transferred using distributed ledger or blockchain technology, including "virtual currencies", "coins", and "tokens".

(7) Exchange.—The term "exchange" means a platform that facilitates the matching of third parties for the purpose of transacting goods, services, data, or value under standardized platform rules.

(8) Financial institution.—The term "financial institution" means—

(A) an alternative trading system;

(B) a branch or agency of a foreign bank, as defined in section 1(b) of the International Banking Act of 1978;

(C) a broker;

(D) a commodity pool operator;

(E) a commodity trading advisor;

(F) a credit union;

(G) a dealer;

(H) a depository institution;

(I) a depository institution holding company;

(J) a futures commission merchant;

(K) an investment adviser;

(L) an investment company;

(M) a national securities exchange;

(N) an organization operating under section 25 or 25A of the Federal Reserve Act;

(O) a private fund;

(P) a State-licensed money services business; and

(Q) any company engaged in activities that are financial in nature or incidental to a financial activity, as described in section 4 of the Bank Holding Company Act of 1956.

(9) Large platform utility.—The term "large platform utility" means a technology company—

(A) with annual global revenue of $25,000,000,000 or more; and

(B) that is predominantly engaged in the business of offering to the public an online marketplace, an exchange, or a platform for connecting third parties.

(10) Medium of exchange.—The term "medium of exchange" means an asset that is used or intended to be used to facilitate the purchase or sale of goods or services.

(11) Money services business.—The term "money services business" has the meaning given that term under section 1010.100 of title 31, Code of Federal Regulations.

(12) Online marketplace.—The term "online marketplace" means a digital platform that facilitates transactions between 2 or more unaffiliated third parties for the sale, lease, or exchange of goods or services, and that establishes, enforces, or materially influences the terms under which such transactions occur.

(13) Private fund.—The term "private fund" has the meaning given that term under section 202(a) of the Investment Advisers Act of 1940.

(14) Securities definitions.—The terms "broker", "dealer", "investment adviser", "investment company", and "national securities exchange" have the meanings given those terms, respectively, under section 3 of the Securities Exchange Act of 1934.

(15) Store of value.—The term "store of value" means an asset that is used or intended to be used to preserve value for future use.

(16) Unit of account.—The term "unit of account" means an asset that is used or intended to be used to denominate prices, debts, or financial obligations.

(b) Prohibition on affiliation with financial institutions.—A large platform utility may not be, and may not be affiliated with any person that is, a financial institution.

(c) Prohibition related to cryptocurrencies.—A large platform utility may not establish, maintain, or operate, and may not be affiliated with any person that establishes, maintains, or operates, a digital asset that is intended to be widely used as a medium of exchange, unit of account, store of value, or any other similar function.

(d) Wind-down period.—With respect to a large platform utility—

(1) if the large platform utility is, or is affiliated with a person that is, a financial institution on the date of enactment of this section, subsection (b) shall not apply to such large platform utility until July 1, 2027.

(2) if the large platform utility maintains or operates, or is affiliated with a person that maintains or operates, a digital asset described under subsection (c) on the date of enactment of this section, subsection (c) shall not apply to such large platform utility until July 1, 2027.

(e) Enforcement.—

(1) Unfair method of competition.—A violation of this section shall constitute an unfair method of competition under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(2) Federal Trade Commission.—The Federal Trade Commission shall enforce this section in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this section.

(3) Injunctive relief.—The Federal Trade Commission or Department of Justice may seek injunctive or other equitable relief to enjoin conduct that violates this section.

(4) Penalty.—Any large platform utility that violates subsection (b) or (c), and any financial institution or other affiliate that knowingly participates in such a violation, shall be subject to a fine of not more than $1,000,000 for each day of the violation.

SEC. 574. STRUCTURAL SEPARATION REQUIREMENTS FOR TECHNOLOGY PLATFORMS.

(a) Definitions.—In this section:

(1) Affiliated entity.—The term "affiliated entity" means any entity that is under common ownership or control with another entity.

(2) Antitrust Division.—The term "Antitrust Division" means the Antitrust Division of the Department of Justice, acting through the Assistant Attorney General in charge of the Antitrust Division.

(3) Back-end infrastructure platform.—The term "back-end infrastructure platform" means the business of operating a service whose primary function is providing computing, storage, hosting, content delivery, database, networking, identity, security, developer, foundation model services, model serving, payment processing, or similar infrastructure services that other businesses, developers, or services depend upon to operate digital products or services. Such term does not include infrastructure used solely for an operator's own internal operations.

(4) Commission.—The term "Commission" means the Federal Trade Commission.

(5) Common ownership or control.—The term "common ownership or control" means ownership or control, direct or indirect, of 2 or more entities by the same person or group of persons.

(6) Control.—The term "control" means the possession, direct or indirect, of the power to direct or cause the direction of the management, policies, or operations of an entity. A person shall be rebuttably presumed to control an entity if such person—

(A) owns, controls, or has the power to vote 25 percent or more of any class of voting securities of the entity;

(B) has the power to appoint 25 percent or more of the board of directors or equivalent governing body of the entity; or

(C) possesses contractual or other rights that permit such person to direct or materially influence the strategic, operational, hosting, distribution, curation, search, communications, marketplace, gatekeeping, gaming, or access decisions of the entity.

(7) Covered person.—The term "covered person" means a person that—

(A) operates 1 or more technology platform verticals; and

(B) for any such vertical, meets the following threshold or thresholds set forth in the following clauses:

(i) With respect to a search platform, public attention platform, private communications platform, or marketplace platform, in not fewer than 3 months during the most recently completed 12-month period, had—

(I) more than 30,000,000 users in the United States or more than 300,000,000 users worldwide; and

(II) during the most recently completed taxable year, had more than $1,500,000,000 in global revenue.

(ii) With respect to a gatekeeping platform, in not fewer than 3 months during the most recently completed 12-month period, had—

(I) more than 30,000,000 devices in the United States or more than 300,000,000 devices worldwide; and

(II) during the most recently completed taxable year, had more than $1,500,000,000 in global revenue.

(iii) With respect to a gaming platform, in not fewer than 3 months during the most recently completed 12-month period, had—

(I) more than 10,000,000 users in the United States or more than 100,000,000 users worldwide; and

(II) during the most recently completed taxable year, had more than $1,500,000,000 in global revenue.

(iv) With respect to a back-end infrastructure platform, during the most recently completed taxable year, had more than $10,000,000,000 in global revenue.

For purposes of this paragraph, the users, devices, revenue, and activities of a person shall include those of any affiliated entity.

(8) Gatekeeping platform.—The term "gatekeeping platform" means the business of controlling an operating system, device-level software environment, application-distribution layer, or other technical access layer whose primary function is materially determining the terms on which persons or applications may access, interoperate with, install, distribute, or use software, hardware, or digital services on a computer, smartphone, tablet, wearable device, smart television, game console, or similar connected device.

(9) Gaming platform.—The term "gaming platform" means the business of operating a digital service whose primary function is materially enabling, distributing, hosting, selling, streaming, licensing, or controlling access to video games or interactive entertainment content, including a game console ecosystem, digital game storefront, cloud gaming service, gaming subscription service, or first-party gaming network. Such term does not include a general-purpose operating system or connected-device ecosystem solely because it permits the use of video games.

(10) Marketplace platform.—The term "marketplace platform" means an online platform whose primary function is facilitating, intermediating, or governing transactions between buyers and sellers of goods or services. Such term does not include a service whose transaction functionality is merely incidental to another technology platform vertical or a service that exclusively facilitates the sale of goods or services offered by the operator or an affiliated entity.

(11) Online platform.—The term "online platform" means the business of operating a website, application, operating system, or other internet-accessible service that enables users to access, view, generate, share, modify, or otherwise interact with digital content.

(12) Person.—The term "person" has the meaning given such term in section 1 of the Clayton Act (15 U.S.C. 12).

(13) Primary function.—The term "primary function" means the principal function of a service, business line, or platform, as determined by the predominance of its revenues, usage, design, marketing, operational deployment, and strategic purpose. The Commission and the Antitrust Division may, by joint rule, further clarify the application of this paragraph.

(14) Private communications platform.—The term "private communications platform" means an online platform whose primary function is enabling users to send, receive, store, or manage private, encrypted, semi-private, or limited-audience communications, including direct messages, text messages, voice messages, voice calls, video calls, group chats, and similar person-to-person or closed-group communications. Such term does not include communications functionality that is merely incidental to another technology platform vertical.

(15) Profits.—The term "profits" means, with respect to any person and any month, the amount equal to the greater of—

(A) the net income (or loss) of such person before provision for income taxes for such month, as determined in accordance with generally accepted accounting principles and consistent with the accounting principles used in the most recent audited consolidated financial statements of such person; and

(B) 4 percent of the gross revenues of such person for such month, as so determined.

(16) Public attention platform.—The term "public attention platform" means an online platform whose primary function is curating, distributing, presenting, or otherwise making content supplied by users or other third parties available to the public, including through feeds, subscriptions, recommendations, rankings, trending displays, or similar mechanisms. Such term does not include an online platform that consists primarily of content selected by the operator of such platform and for which any comment, product review, or other user-generated content is incidental to, directly related to, or dependent on the provision of such content.

(17) Search platform.—The term "search platform" means an online platform whose primary function is allowing users to submit queries in order to retrieve, recommend, or display responsive search results, listings, maps, or other discoverable content from across the internet. Such term does not include search functionality that is merely internal to a technology platform vertical.

(18) Technology platform vertical.—The term "technology platform vertical" means any of the following:

(A) Back-end infrastructure platform.

(B) Gaming platform.

(C) Gatekeeping platform.

(D) Marketplace platform.

(E) Private communications platform.

(F) Public attention platform.

(G) Search platform.

(b) Prohibition on ownership of more than 1 technology platform vertical.—

(1) (A) In general.—It shall be unlawful for any covered person to directly or indirectly own, operate, control, or direct the operation of any entity or combination of entities engaged in more than 1 technology platform vertical, in or affecting interstate or foreign commerce.

(B) Prohibition on new acquisitions.—After the date of enactment of this Act, no covered person may acquire, directly or indirectly, control of assets or operations in a technology platform vertical other than the technology platform vertical in which such person already engages, in violation of subparagraph (A).

(2) Rulemaking.—Not later than January 30, 2027, the Commission and the Antitrust Division shall, by joint interim final rule, define for purposes of this section—

(A) a de minimis threshold, by technology platform vertical and relevant technology market, below which an activity may be excluded from prohibition under this subsection, except that—

(i) no such threshold may exceed 5 percent of the primary market measure specified by joint rule for the applicable technology platform vertical in the relevant technology market, which may include revenue, users, devices, queries, viewing time, messages, transactions, gross merchandise value, compute, storage, bandwidth, or a comparable measure;

(ii) with respect to a gatekeeping platform, no such threshold may exceed 1 percent of the applicable measure described in clause (i); and

(iii) any exclusion under this subparagraph shall be construed narrowly and shall not permit the preservation, recreation, or continuation of vertically integrated control inconsistent with the purposes of this section;

(B) standards for applying the definitions of "affiliated entity", "common ownership or control", and "control" under subsection (a), including standards addressing contractual arrangements of operational control, exclusive contractual arrangements, indirect means of control, and functions materially comparable to a technology platform vertical;

(C) milestones for divestiture to ensure compliance within the deadline under subsection (c), provided such milestones may not be later than permitted under subsection (d), including but not limited to—

(i) filing of a divestiture plan;

(ii) the length of time the Commission and the Antitrust Division will review such plan;

(iii) filing of a revised plan, if necessary;

(iv) notification of the person acquiring such divestiture;

(v) the submission of any transaction filing required by section 7A of the Clayton Act (15 U.S.C. 18a) by the person acquiring such divestiture; and

(vi) the completion of such divestiture; and

(D) for each milestone, whether, in the case of a covered person's knowing and willful failure to meet the milestone, the Commission and the Antitrust Division shall seek—

(i) penalties under subsection (e)(3);

(ii) appointment of a divestiture trustee for such covered person under subsection (e)(4); or

(iii) both clauses (i) and (ii).

(3) Effect of interim final rule.—The interim final rule under paragraph (2) shall take effect upon publication in the Federal Register, shall have the force and effect of law, and may be issued without regard to section 553 of title 5, United States Code. The Commission and the Antitrust Division shall provide a public comment period of not less than 60 days after publication and shall issue final rules not later than October 30, 2027. A delay in issuance or finalization of rules under this paragraph shall not delay, limit, extinguish, or reduce any prohibition, duty, enforcement authority, or divestiture obligation established by this section.

(4) Notice of divestiture requirement.—

(A) In general.—Not later than 60 days after the date of enactment of this Act, the Commission and the Antitrust Division shall, using the best information available, identify each covered person that the Commission and the Antitrust Division jointly determine is required to divest under subsection (c) and notify such covered person of the determination.

(B) 60-day notice not exhaustive.—Notwithstanding subparagraph (A), if the Commission and the Antitrust Division later jointly determine, using the best information available, that a covered person not notified under subparagraph (A) is required to divest under subsection (c), the Commission and the Antitrust Division shall promptly notify such covered person.

(C) No immunity.—Failure to identify or notify a covered person under this paragraph shall not limit, extinguish, or otherwise affect any prohibition, duty, enforcement authority, or divestiture obligation established by this section.

(5) Determination upon request.—

(A) Request.—Any covered person that has not received notice under paragraph (4) may submit to the Commission and the Antitrust Division a written request for a determination of whether that covered person is required to divest under subsection (c).

(B) Determination.—Not later than the later of 30 days after receipt of a request under subparagraph (A) or the expiration of the 60-day period under paragraph (4)(A), the Commission and the Antitrust Division shall jointly issue to the covered person a written determination that states whether the covered person is required to divest under subsection (c). Notice issued under paragraph (4) after receipt of a request under subparagraph (A) shall satisfy this requirement.

(C) No admission or tolling.—Submission of a request under subparagraph (A) shall not—

(i) constitute an admission that the covered person is subject to subsection (b) or required to divest under subsection (c); or

(ii) toll or extend any prohibition, duty, enforcement authority, divestiture obligation, or deadline under this section.

(6) Judicial review.—

(A) Petition for review.—

(i) Determination.—A covered person receiving notice under paragraph (4) or a determination under paragraph (5) may, not later than 30 days after receipt of such notice or determination, file a petition for review of the determination in the United States Court of Appeals for the District of Columbia Circuit.

(ii) Failure to act.—A covered person that submits a request under paragraph (5)(A) and does not receive a written determination within the period required under paragraph (5)(B) may, at any time before receipt of such determination, file a petition in the United States Court of Appeals for the District of Columbia Circuit to compel issuance of the determination.

(B) Application of chapter 7.—Chapter 7 of title 5, United States Code, shall apply to a petition under subparagraph (A). For purposes of such chapter—

(i) a determination under paragraph (4) or (5) shall constitute final agency action; and

(ii) a failure to issue a determination within the period required under paragraph (5)(B) shall constitute agency action unlawfully withheld.

(C) Expedited consideration.—The court shall expedite consideration of a petition filed under subparagraph (A) to the greatest extent practicable.

(c) Divestiture.—Not later than July 1, 2028, any covered person in violation of subsection (b) shall divest such interests as are necessary to come into compliance.

(d) FTC and DOJ review.—

(1) Divestiture plan required.—Not later than April 1, 2027, any covered person required to divest under subsection (c) shall submit to the Commission and the Antitrust Division a divestiture plan. Such plan—

(A) shall be submitted to the Commission and the Antitrust Division in the same manner, and containing substantially similar information, as a transaction filing under section 7A of the Clayton Act (15 U.S.C. 18a), without respect to any threshold, exemption, or other limitation of such section; and

(B) shall include—

(i) identification of the business, assets, or interests to be divested to come into compliance with subsection (b);

(ii) identification of the proposed acquiring person, if known;

(iii) a timetable for execution;

(iv) any transitional services proposed; and

(v) such other information as the Commission and the Antitrust Division may require by joint rule.

(2) Agency review process.—Not later than 180 days after receipt of a divestiture plan under paragraph (1), but in no case later than October 1, 2027, the Commission and the Antitrust Division shall review the plan.

(A) Lead agency.—The Commission and the Antitrust Division may designate 1 agency to take the lead in conducting the review and communicating with the person submitting the plan.

(B) Review criteria.—The lead agency shall review the effect on competition, interoperability, independent market access, and the public interest—

(i) of the divestiture; and

(ii) of the subsequent acquisition of the divested entity by the acquiring person.

(C) Additional information.—Any request for additional information by an agency shall be made within 30 days of receipt of the plan.

(D) Acquiring person.—

(i) A divestiture plan that identifies a proposed acquiring person may be approved only if the lead agency determines that—

(I) the proposed acquisition of the divested business, assets, or interests by such acquiring person is consistent with subsection (b);

(II) the proposed acquisition would not materially harm competition or otherwise undermine the purposes of this section; and

(III) any statutory reporting, waiting period, or approval requirement applicable to the proposed acquisition will be satisfied before consummation.

(ii) A divestiture plan may be submitted and reviewed without identifying a proposed acquiring person, but no sale, transfer, assignment, or other disposition to an acquiring person shall be consummated if either the Commission or the Antitrust Division disapproves in writing.

(E) Notice of decision.—Not later than the end of the review period, the lead agency shall notify the person in writing—

(i) whether the plan is approved, approved with conditions, or disapproved; and

(ii) the reasons for any disapproval or conditions.

(F) Approval standard.—A divestiture plan shall be treated as approved only if, before the end of the review period, the lead agency has approved the plan in writing, whether unconditionally or subject to conditions accepted in writing by the person submitting the plan, and neither the Commission nor the Antitrust Division has disapproved the plan in writing.

(3) Revised plan following disapproval.—If a plan is disapproved under paragraph (2), the covered person shall submit a revised divestiture plan not later than 60 days after receipt of the disapproval notice.

(A) Review deadline.—Not later than 150 days after receipt of a revised plan, but in no case later than May 1, 2028, the lead agency shall review the revised plan under the procedures set forth in paragraph (2).

(4) No tolling.—No submission, resubmission, agency review, negotiation, request for additional information, waiting period, court proceeding, or other matter shall toll or extend any deadline under this section.

(5) Consequences of noncompliance.—A covered person required to divest under subsection (c) shall be subject to subsection (e)(3), subsection (e)(4), or both, if such person fails to—

(A) submit a divestiture plan under paragraph (1);

(B) submit a revised plan under paragraph (3), if required to do so;

(C) obtain approval of either—

(i) a plan under paragraph (2); or

(ii) a revised plan under paragraph (3);

(D) conform to agreed-upon conditions of an approved plan; or

(E) conclude the divestiture required by subsection (c).

(6) Blocking of actions.—The Commission and the Antitrust Division, jointly or separately, may bring a civil action in any court of competent jurisdiction to block any action relating to the conflicts of interest described in subsection (b) that would materially harm competition, interoperability, or independent market access, or otherwise undermine the purposes of this section.

(e) Enforcement.—

(1) In general.—When the Commission, the Antitrust Division, or an attorney general of a State has reason to believe that a covered person is in violation of this section or a rule promulgated under this section, the Commission, the Antitrust Division, or the attorney general of the State may bring a civil action in an appropriate district court of the United States.

(2) Injunctive and equitable relief.—In any action described in paragraph (1), the applicable court, on a finding that a covered person is in violation of this section or a rule promulgated under this section, shall issue an order requiring such covered person—

(A) to cease and desist from such violation and, if applicable, divest such interests as are necessary to come into compliance with this section; and

(B) to pay an amount equal to the profits derived from any business, asset, operation, or interest subject to divestiture during the period of the violation.

(3) Penalties.—

(A) Written determination and transfer.—If a covered person knowingly and willfully fails to comply with a milestone specified under subsection (b)(2)(C), the Commission and the Antitrust Division, acting jointly, or the lead agency designated under subsection (d)(2)(A), shall issue a written determination identifying the missed milestone, the month for which escrow is required, the amount required to be transferred, and the method used to calculate such amount. Beginning not later than 15 days after receipt of such written determination, the covered person shall transfer into escrow on a monthly basis 10 percent of the profits of the covered person, to be—

(i) returned to the covered person if divestiture occurs by the deadline under subsection (c); or

(ii) deposited into the general fund of the Treasury if divestiture does not occur by the deadline under subsection (c).

(B) Escrow administration and certification.—Any transfer into escrow under subparagraph (A) shall be deposited with the Secretary of the Treasury into a segregated account established for purposes of this section.

(i) Not later than 15 days after the end of each month for which a transfer is required, the covered person shall submit to the Chair of the Commission and the Antitrust Division a certification, signed by the chief executive officer and chief financial officer, attesting to the calculation of profits and gross revenues for such month and the amount transferred.

(ii) Not later than 120 days after the end of each fiscal year, the covered person shall submit a reconciliation based on audited financial statements, and shall pay any underpayment together with interest, calculated from the date the underpaid amount was required to be transferred at the rate and in the manner provided under sections 6621(a)(2) and 6622(a) of the Internal Revenue Code of 1986, or shall receive a return of any overpayment, as applicable.

(C) Judicial review.—A covered person subject to a transfer requirement under subparagraph (A) may, not later than 30 days after notice of such requirement, petition for review in the United States Court of Appeals for the District of Columbia Circuit. The filing of a petition for review shall not stay any obligation to transfer amounts into escrow unless the court orders otherwise.

(4) Trustee.—The Commission or the Antitrust Division may apply to a court of competent jurisdiction for the appointment of a divestiture trustee.

(A) Authority.—The divestiture trustee shall have the authority, at the expense of the covered person required to divest, to take such actions as are necessary to effectuate the divestiture required under this section, including selling, transferring, assigning, or otherwise disposing of the business, assets, entity, or interests required to be divested.

(B) Cooperation.—The covered person required to divest shall cooperate fully with the divestiture trustee and shall take no action to interfere with, delay, or impede the divestiture.

(C) Approval.—Any proposed sale by the divestiture trustee shall be subject to approval under subsection (d).

(D) Duty of trustee.—The divestiture trustee shall act in the interest of effectuating prompt compliance with this section and restoring competition, and shall not be required to maximize the value received by the covered person required to divest.

(5) Deposit.—Any amount paid under paragraph (2)(B) shall be deposited into the general fund of the Treasury.

(6) Other relief.—In addition to any relief obtained under paragraph (1) or (2), the court may grant any other equitable relief necessary to redress and prevent recurrence of the violation.

(f) Anti-circumvention.—It shall be unlawful for any covered person to evade or attempt to evade this section, including by entering into an agreement or contract, engaging in a transaction,

structuring an entity, or recreating, through contractual means, the conflicts of interest described in subsection (b).

(g) Rulemaking authority.—The Commission and the Antitrust Division shall, by joint rule, promulgate regulations to carry out this section.

(h) Reports required.—The Chair of the Commission and the Antitrust Division shall submit to the appropriate congressional committees quarterly reports on compliance with this section, including the status of any divestitures required under this section.

(i) Rule of construction.—Nothing in this section shall be construed to limit the authority of the Commission, the Department of Justice, or the attorney general of a State under any other provision of law.

SEC. 575. CODIFYING NET NEUTRALITY.

(a) Definitions.—In this section:

(1) Affiliated prioritization.—The term "affiliated prioritization" means the management of a broadband internet access service provider's network to directly or indirectly favor traffic from an affiliate of the provider, or from a person with which the provider has a financial, ownership, contractual, or other preferential relationship, over substantially similar traffic from an unaffiliated person.

(2) Broadband internet access service.—The term "broadband internet access service" has the meaning given such term in section 801 of the Communications Act of 1934 (47 U.S.C. 641), or any successor provision.

(3) Commission.—The term "Commission" means the Federal Communications Commission.

(4) Data usage allowance.—The term "data usage allowance" means a limitation, cap, threshold, or metered allocation applicable to the amount of data that an end user may transmit or receive through broadband internet access service during a billing period or other period.

(5) Edge provider.—The term "edge provider" means any person that provides any content, application, service, or device accessed over the internet.

(6) Paid prioritization.—The term "paid prioritization" means the management of a broadband internet access service provider's network to directly or indirectly favor some traffic over other traffic in exchange for consideration, monetary or otherwise.

(7) Reasonable network management.—The term "reasonable network management" means a network management practice that has a primarily technical network management justification, is narrowly tailored to achieve a legitimate network management purpose, and is not based on the source, destination, content, application, service, device, class of user, or competitive effect of traffic, except to the extent reasonably necessary to achieve such legitimate network management purpose.

(8) Zero-rating.—The term "zero-rating" means exempting some internet traffic from a data usage allowance or otherwise treating such traffic as not counting against a data cap, data threshold, usage-based charge, or similar limitation.

(b) Broadband internet access service treated as telecommunications service.—Section 3(53) of the Communications Act of 1934 (47 U.S.C. 153(53)) is amended to read as follows:

"The term 'telecommunications service' means—

"(A) the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used; and

"(B) the offering of broadband internet access service, as defined in section 801, for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used.".

(c) No blocking.—A provider of broadband internet access service may not block lawful content, applications, services, or nonharmful devices, subject to reasonable network management.

(d) No throttling.—A provider of broadband internet access service may not impair, degrade, slow, or otherwise disadvantage lawful internet traffic on the basis of content, application, service, device, source, destination, or class of user, subject to reasonable network management.

(e) No paid prioritization or affiliated prioritization.—A provider of broadband internet access service may not engage in paid prioritization or affiliated prioritization.

(f) Data-cap exemptions and zero-rating.—

(1) In general.—A provider of broadband internet access service may not—

(A) engage in zero-rating in exchange for consideration, monetary or otherwise, from any third party;

(B) zero-rate some internet content, applications, services, or devices within a category of internet content, applications, services, or devices unless the category is defined without regard to source, destination, ownership, affiliation, payment, or viewpoint and the entire category is zero-rated on equal terms; or

(C) use a data usage allowance, data cap exemption, sponsored data arrangement, usage-based charge, or zero-rating practice to evade this section, favor an affiliate, favor a payor, or unreasonably interfere with or unreasonably disadvantage end users or edge providers.

(2) Application-agnostic zero-rating.—Application-agnostic zero-rating shall not violate this subsection if no consideration, monetary or otherwise, is provided by any third party in exchange for the provider's decision whether to zero-rate traffic and the practice is not used to evade this section.

(g) No unreasonable interference or unreasonable disadvantage.—A provider of broadband internet access service may not unreasonably interfere with, or unreasonably disadvantage—

(1) the ability of end users to select, access, use, send, receive, or offer lawful content, applications, services, or devices of the user's choice; or

(2) the ability of edge providers to make lawful content, applications, services, or devices available to end users.

(h) Transparency.—

(1) In general.—A provider of broadband internet access service shall publicly disclose accurate information regarding the provider's network management practices, performance, commercial terms, and any practice that blocks, throttles, prioritizes, degrades, interferes with, or otherwise affects traffic, in sufficient detail to enable consumers, edge providers, and the Commission to evaluate compliance with this section.

(2) Nonpublic information.—A disclosure required under this subsection shall not require public disclosure of information that would compromise network security, undermine cybersecurity measures, disclose personal information, or disclose trade secrets or other confidential business information, if the provider makes such information available to the Commission upon request.

(i) Exceptions.—Nothing in this section shall be construed to prohibit a provider of broadband internet access service from—

(1) engaging in reasonable network management;

(2) addressing network congestion through application-agnostic and content-neutral measures;

(3) protecting the security and integrity of the provider's network, users, services, or equipment;

(4) preventing or mitigating spam, malware, fraud, denial-of-service attacks, malicious traffic, or other cybersecurity threats;

(5) prioritizing, routing, or managing traffic for emergency communications, public safety communications, or national security communications;

(6) complying with a court order or other lawful order issued pursuant to statutory authority, but only to the extent required by such order;

(7) complying with Federal, State, or local law, but only to the extent required by such law;

(8) offering user-directed filtering, parental controls, accessibility tools, or security tools, if such tools are selected, controlled, and revocable by the user;

(9) taking action to prevent the transmission of unlawful content, if such action is required by law and narrowly tailored to comply with such law; or

(10) offering end-user service tiers based on bandwidth, speed, data volume, or other application-agnostic terms, if such tiers are clearly disclosed and are not used to evade this section.

(j) Enforcement.—

(1) In general.— The obligations imposed under this section shall be treated as requirements under the Communications Act of 1934 (47 U.S.C. 151 et seq.). A violation of this section or a rule promulgated under this section shall be treated as a violation of such Act.

(2) Powers of Commission.—The Commission shall enforce this section in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though this section were part of such Act.

(3) Rules.—Not later than January 1, 2027, the Commission shall issue interim final rules to carry out this section and shall thereafter promulgate final rules after notice and comment.

(k) Enforcement by State attorneys general.—

(1) Civil action.—Except as provided in paragraph (5), the attorney general of a State, or any other officer of a State authorized by the law of that State to bring civil actions on behalf of the residents of the State, alleging a violation of this section or any rule promulgated under this section that affects or may affect that State or its residents, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to enforce this section or such rule and to obtain appropriate injunctive relief, damages, restitution, civil penalties, or other relief that the court considers appropriate.

(2) Notice to Commission.—Before filing an action under paragraph (1), the State shall provide written notice to the Commission and provide the Commission with a copy of the complaint for such action, except that if it is not feasible to provide such prior notice, the State shall provide such notice immediately upon instituting such action.

(3) Intervention by Commission.—Upon receiving notice under paragraph (2), the Commission may intervene in the action, be heard on all matters arising in the action, and file petitions for appeal.

(4) Construction.—Nothing in this subsection shall be construed to prevent the attorney general of a State, or any other authorized State officer, from exercising the powers conferred on such attorney general or officer by the laws of that State, including by proceeding in State or Federal court on the basis of an alleged violation of any civil or criminal statute of that State.

(5) Limitation.—No separate action may be brought under this subsection if, at the time the action is brought, the same alleged violation is the subject of a pending civil action by the Commission or the United States under this section.

(l) Rule of construction.—

(1) State law.—Nothing in this section shall be construed to preempt, displace, or limit any provision of State law that provides equal or greater protection for an open internet, net neutrality, broadband users, edge providers, or the public, except to the extent of a direct and irreconcilable conflict with this section.

(2) Other law.—Nothing in this section shall be construed to limit any authority, duty, remedy, penalty, or prohibition otherwise available under Federal or State law.

(3) No authorization of unlawful conduct.—Nothing in this section shall be construed to authorize any content, application, service, device, or conduct that is otherwise unlawful.

(4) Specialized services.—Nothing in this section shall be construed to prohibit a provider of broadband internet access service from offering a service that is not broadband internet access service, if such service is not offered or used to evade this section and does not materially impair the availability or quality of broadband internet access service offered to end users.

SEC. 576. PHASED-IN MINIMUM AGE FOR SOCIAL MEDIA ACCOUNTS.

(a) Definitions.—In this section:

(1) Commission.—The term "Commission" means the Federal Trade Commission.

(2) Covered minor.—The term "covered minor" means—

(A) on and after January 1, 2027, and before January 1, 2030, an individual born on or after January 1, 2014; or

(B) on and after January 1, 2030, an individual who has not attained 16 years of age.

(3) Know or knows.—The term "know" or "knows" means to have actual knowledge or knowledge fairly implied on the basis of objective circumstances.

(4) Personal data.—The term "personal data" has the same meaning as the term "personal information" as defined in section 312.2 of title 16, Code of Federal Regulations, or any successor regulation.

(5) Social media platform.—

(A) In general.—The term "social media platform" means a public-facing website, online service, online application, or mobile application that—

(i) is directed to consumers; and

(ii) as a primary function provides a community forum for user-generated content, including messages, videos, audio files, or other content among users, where such content is primarily intended for viewing, resharing, or platform-enabled distributed social endorsement or comment.

(B) Limitations.—The term "social media platform" does not include a platform that, as its primary function for consumers, provides or facilitates any of the following:

(i) The purchase and sale of commercial goods.

(ii) Teleconferencing or videoconferencing services that allow reception and transmission of audio or video signals for real-time communication, provided that the real-time communication is initiated by using a unique link or identifier to facilitate access.

(iii) Crowdsourced reference guides such as encyclopedias and dictionaries.

(iv) Cloud storage, file sharing, or file collaboration services, including such services that allow collaborative editing by invited users.

(v) The playing or creation of video games.

(vi) Content that consists primarily of news, sports, sports coverage, entertainment, or other information or content that is not user-generated but is preselected by the platform and for which any chat, comment, or interactive functionality is incidental, directly related to, or dependent on the provision of the content provided by the platform.

(vii) Business, product, or travel information including user reviews or rankings of such businesses, products, or travel information.

(viii) Educational information, experiences, training, or instruction provided to build knowledge, skills, or a craft, district-sanctioned or school-sanctioned learning management systems and school information systems for the purposes of schools conveying content related to the education of students, or services on behalf of or in support of an elementary school or secondary school, as such terms are defined in section 8101 of the Elementary and Secondary Education Act of 1965 (20 U.S.C. 7801).

(ix) An email service.

(x) A wireless messaging service, including such a service provided through short message service or multimedia messaging protocols, that is not a component of, or linked to, a social media platform and where the predominant or exclusive function of the messaging service is direct messaging consisting of the transmission of text, photos, or videos that are sent by electronic means, where messages are transmitted from the sender to the recipient and are not posted publicly or within a social media platform.

(xi) A broadband internet access service (as such term is defined for purposes of section 8.1(b) of title 47, Code of Federal Regulations, or any successor regulation).

(xii) A virtual private network or similar service that exists solely to route internet traffic between locations.

(6) User.—The term "user" means, with respect to a social media platform, an individual who creates, maintains, or uses an account or profile on the social media platform.

(b) Prohibition.—It shall be unlawful for a social media platform to knowingly permit a covered minor to become or remain a user of such platform.

(c) Deletion of covered minors' personal data.—

(1) In general.—Subject to paragraph (2), upon termination of an existing account or profile pursuant to subsection (b), a social media platform shall immediately disable public access to the account or profile and segregate personal data collected from or submitted to the social media platform by the individual whose account or profile was terminated.

(2) User access to personal data.—To the extent technically feasible, a social media platform shall allow an individual whose account or profile was terminated by the social media platform pursuant to subsection (b), from the date such termination occurs to the date that is 90 days after such date, to request, and shall provide to such individual upon such request, a copy of the personal data collected from, or submitted by, such individual to the social media platform both—

(A) in a manner that is readable and which a reasonable person can understand; and

(B) in a portable, structured, and machine-readable format.

(3) Deletion after access period.—A social media platform may retain the segregated personal data described in paragraph (1) during the period described in paragraph (2) solely to comply with that paragraph. At the end of that period, the platform shall delete the segregated personal data, except that the platform may retain a record of the termination of the account or profile and the minimum information necessary to demonstrate compliance with this section.

(d) Determination of knowledge; protections for privacy.—

(1) Rules of construction.—For purposes of enforcing this section, in making a determination as to whether a social media platform has knowledge fairly implied on the basis of objective circumstances that a user is a covered minor, the Commission or the attorney general of a State, as applicable, shall rely on competent and reliable evidence, taking into account the totality of circumstances, including whether a reasonable and prudent person under the circumstances would have known that the user is a covered minor.

(2) Protections for privacy.—Nothing in this section, including a determination described in paragraph (1), shall be construed to require a social media platform to—

(A) implement age-gating or age-verification functionality; or

(B) affirmatively collect any personal data with respect to the age of users that the social media platform is not already collecting in the normal course of business.

(3) Restriction on use and retention of personal data.—If a social media platform or a third party acting on behalf of a social media platform voluntarily collects personal data for the purpose of complying with this section, the social media platform or third party shall not—

(A) use any personal data collected specifically for a purpose other than sole compliance with the obligations under this section; or

(B) retain any personal data collected from a user for longer than is necessary to comply with the obligations under this section or than is minimally necessary to demonstrate compliance with this section.

(e) Enforcement by Commission.—

(1) Unfair, deceptive, or abusive acts or practices.—A violation of this section shall be treated as a violation of a rule defining an unfair, deceptive, or abusive act or practice prescribed under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a).

(2) Powers of Commission.—The Commission shall enforce this section in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this section.

(3) Authority preserved.—Nothing in this section shall be construed to limit the authority of the Commission under any other provision of law.

(f) Actions by States.—

(1) Authorization.—Subject to paragraph (3), in any case in which the attorney general of a State has reason to believe that an interest of the residents of the State has been or is threatened or adversely affected by the engagement of a social media platform in a practice that violates this section, the attorney general of the State may, as parens patriae, bring a civil action against the social media platform on behalf of the residents of the State in an appropriate district court of the United States to—

(A) enjoin that practice;

(B) enforce compliance with this section;

(C) on behalf of residents of the State, obtain damages, restitution, or other compensation, each of which shall be distributed in accordance with State law; or

(D) obtain such other relief as the court may consider appropriate.

(2) Commission intervention.—

(A) Notice to Commission.—

(i) In general.—The attorney general of a State shall notify the Commission in writing that the attorney general intends to bring a civil action under paragraph (1) before the filing of the civil action.

(ii) Contents.—The notification required under clause (i) with respect to a civil action shall include a copy of the complaint to be filed to initiate the civil action.

(iii) Exception.—Clause (i) shall not apply with respect to the filing of an action by an attorney general of a State under this paragraph if the attorney general of the State determines that it is not feasible to provide the notice required in that clause before filing the action.

(B) Intervention by Commission.—Upon receiving notice under subparagraph (A)(i), the Commission may intervene in the action that is the subject of the notice.

(3) Effect of intervention.—If the Commission intervenes in an action under paragraph (1), it may—

(A) be heard with respect to any matter that arises in that action; and

(B) file a petition for appeal.

(4) Investigatory powers.—Nothing in this subsection may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of the State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel the attendance of witnesses or the production of documentary or other evidence.

(5) Preemptive action by Commission.—In any case in which an action is instituted by or on behalf of the Commission for a violation of this section, no State may, during the pendency of that action, institute a separate civil action under paragraph (1) against any defendant named in the complaint in the action instituted by or on behalf of the Commission for that violation.

(6) Venue; service of process.—

(A) Venue.—Any action brought under paragraph (1) may be brought in—

(i) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(ii) another court of competent jurisdiction.

(B) Service of process.—In an action brought under paragraph (1), process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(g) Relationship to other laws.—The provisions of this section shall preempt any State law, rule, or regulation only to the extent that such State law, rule, or regulation conflicts with a provision of this section. Nothing in this section shall be construed to prohibit a State from enacting a law, rule, or regulation that provides greater protection to minors than the protection provided by the provisions of this section.

SEC. 577. COMPULSIVE DIGITAL PRODUCT DESIGN PROHIBITED.

(a) In general.—The Federal Trade Commission Act (15 U.S.C. 41 et seq.) is amended by inserting after section 5 the following:

"Sec. 5A. Compulsive digital product design prohibited.

"(a) Definitions.—In this section:

"(1) Behavioral data.—The term 'behavioral data' means data relating to the activity, browsing, engagement, clicks, views, dwell time, purchases, interactions, or other conduct of a user on or across online products or services.

"(2) Commission.—The term 'Commission' means the Federal Trade Commission.

"(3) Compulsive usage.—The term 'compulsive usage' means persistent and repetitive use of a covered digital product that materially impairs sleep, education, employment, caregiving, social functioning, psychological well-being, or the ability of an individual to self-regulate their use of the covered digital product.

"(4) Covered digital product.—The term 'covered digital product' means a website, online service, online application, mobile application, game, or comparable digital interface that—

"(A) is publicly available for use by consumers; and

"(B) is used primarily for recurring consumer engagement, including entertainment, social interaction, gaming, simulated gambling, shopping, video or audio consumption, user-generated content, or other recurring consumer engagement.

"(5) Design feature.—The term 'design feature' means any feature, component, interface choice, ranking method, reward mechanism, or default setting of a covered digital product that encourages, prolongs, intensifies, or increases the frequency of a user's engagement with the covered digital product.

"(6) Personal data.—The term 'personal data' means information that identifies or is linked or reasonably linkable to an individual or to a device used by an individual.

"(b) Prohibition.—On and after July 1, 2027, it shall be unlawful for a person that owns, operates, or controls a covered digital product, in or affecting commerce, to design, deploy, maintain, or materially modify a design feature, or combination of design features, that, based on the totality of the circumstances, results in compulsive usage or is reasonably foreseeable to materially contribute to compulsive usage.

"(c) Factors.—In determining whether a person has violated subsection (b), the Commission shall consider the totality of the circumstances, including whether the design feature, or combination of design features—

"(1) uses infinite scrolling, autoplay, auto-advance, or similar mechanisms that reduce a user's natural stopping points;

"(2) uses notifications, push alerts, prompts, reminders, or re-engagement messages that are not reasonably necessary for account security, fraud prevention, billing, or direct person-to-person communication;

"(3) uses streaks, badges, likes, follower counts, engagement counts, variable rewards, or other gamified or socially comparative feedback mechanisms tied to the frequency, duration, or intensity of use;

"(4) uses appearance-altering filters, social-comparison tools, or similar features that are likely to exploit body-image concerns, status anxiety, or fear of missing out;

"(5) uses personal data, behavioral data, personalized recommendation systems, default ranking systems, or other automated curation systems optimized to maximize time spent, repeated checking, or repeated interaction rather than to satisfy an immediate user request;

"(6) uses time-limited, disappearing, countdown-based, or artificially urgent content, offers, or prompts that induce repeated checking or fear of missing out; or

"(7) impedes, frustrates, or materially burdens a user's effort to stop using the covered digital product, log off, disable notifications, dismiss prompts, select a chronological feed, or set limits on use.

"(d) Enforcement.—

"(1) Unfair, deceptive, or abusive act or practice.—A violation of this section, or a regulation promulgated under this section, shall constitute an unfair, deceptive, or abusive act or practice in or affecting commerce under section 5(a)(1).

"(2) Powers of the Commission.—The Commission shall enforce this section in the same manner, by the same means, and with the same jurisdiction, powers, and duties as under section 5.

"(3) Remedies.—In addition to any other remedy available under law, the Commission may commence a civil action in an appropriate district court of the United States to obtain temporary, preliminary, or permanent injunctive relief, restitution, refund of moneys, damages, disgorgement, civil penalties, deletion or disabling of offending design features, corrective notice, reporting, auditing, and other appropriate relief.

"(4) Regulations.—Not later than July 1, 2027, the Commission shall promulgate regulations to carry out this section.

"(e) Rule of construction.—Nothing in this section shall be construed to prohibit a person that owns, operates, or controls a covered digital product from offering chronological feeds, accessibility features, parental controls, user-selected settings, or notifications reasonably necessary for account security, fraud prevention, billing, or direct person-to-person communications, unless such feature or setting is designed, deployed, or optimized in a manner that violates subsection (b).".

SEC. 578. ABANDONMENT OF POPULAR OPERATING SYSTEMS UNLAWFUL.

(a) Definitions.—In this section:

(1) Covered operating system.—The term "covered operating system" means a general-purpose operating system that is licensed, sold, or otherwise distributed for use by consumers on a general-purpose computing device and that, during not fewer than 3 months in the preceding 12-month period, was installed on not fewer than 10,000,000 devices in the United States or not fewer than 100,000,000 devices worldwide.

(2) Security support.—The term "security support" means to provide security updates or patches that materially address vulnerabilities in a covered operating system, including through updates or patches to device-specific firmware, drivers, or software used to operate the covered operating system securely on a general-purpose computing device.

(3) General-purpose computing device.—The term "general-purpose computing device" means a desktop computer, laptop computer, tablet, smartphone, or other multipurpose consumer computing device, but does not include a single-purpose embedded system,

household appliance, industrial control system, Internet of Things device, medical device, or video game console.

(4) Vendor.—The term "vendor" means a person that develops or controls a covered operating system or a device-specific implementation of a covered operating system and is capable, directly or indirectly, of providing security updates for such operating system or implementation.

(b) Prohibition.—It shall be unlawful, and shall constitute an unfair, deceptive, or abusive act or practice under section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)), for a vendor of a covered operating system to—

(1) refuse to provide free security support for the covered operating system, if such security support was previously provided without a separate fee or was included in the original purchase or license;

(2) impose any new or separate fee, or require the purchase of any new license, subscription, product, or service, as a condition of continued security support for a covered operating system; or

(3) materially degrade or reduce the security, functionality, performance, interoperability, compatibility, or usability of a covered operating system, without a legitimate security or technical integrity justification, for the purpose or substantial effect of forcing users to migrate to another operating system.

(c) Measurement and anti-evasion rules.—

(1) For purposes of subsection (a)(1)—

(A) the Federal Trade Commission shall measure installations by monthly active installations, or by another commercially reasonable method where monthly active installation data are unavailable; and

(B) the Commission shall aggregate editions, variants, service releases, and substantially similar successor versions marketed as part of the same operating system family;

(C) for purposes of subsection (b), security support for a covered operating system shall include security support for each model or substantially similar family of models of general-purpose computing devices on which the covered operating system, during not fewer than 3 months in the preceding 12-month period, had not fewer than 10,000,000 monthly active installations in the United States or not fewer than 100,000,000 monthly active installations worldwide;

(2) A vendor may not evade this section by—

(A) assigning, delegating, licensing, transferring, or otherwise purporting to transfer responsibility for providing security updates to another person; or

(B) rebranding, fragmenting, or artificially separating substantially similar operating system versions, device models or model families, device-specific implementations, or support channels.

(3) Each vendor of a covered operating system shall maintain records sufficient to demonstrate compliance with this section.

(d) Termination after cessation of covered status.—When an operating system ceases to be a covered operating system, it shall be unlawful for the vendor of such operating system to end security support unless such vendor—

(1) provided not less than 6 months of clear and conspicuous notice to users of such operating system; and

(2) notified the Commission.

(e) Rule of construction.—Nothing in this section shall be construed—

(1) to require a vendor to provide feature updates, cosmetic changes, or nonsecurity improvements; or

(2) to authorize the ending of security support for a covered operating system merely because a newer operating system version exists.

(f) Enforcement.—This section shall be enforced by the Federal Trade Commission under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of that Act were incorporated into and made a part of this section.

(g) Actions by States.—

(1) In general.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any person who violates this section, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(A) enjoin that violation;

(B) enforce compliance with this section;

(C) obtain damages, restitution, or other compensation on behalf of residents of the State; and

(D) obtain civil penalties and such other relief as the court may consider appropriate.

(2) Notice.—Before filing an action under paragraph (1), the attorney general of the State shall provide to the Federal Trade Commission—

(A) written notice of the action; and

(B) a copy of the complaint for that action.

(3) Exception.—If it is not feasible for the attorney general of a State to provide the notice required by paragraph (2) before filing an action under paragraph (1), the attorney general shall provide that notice immediately upon filing the action.

(4) Intervention by Commission.—Upon receiving notice under paragraph (2) or (3), the Federal Trade Commission may—

(A) intervene in the action;

(B) be heard on all matters arising in the action; and

(C) file petitions for appeal.

(5) Construction.—Nothing in this subsection shall be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to conduct investigations, administer oaths or affirmations, or compel the attendance of witnesses or the production of documentary and other evidence.

(h) Regulations.—Not later than July 1, 2027, the Federal Trade Commission shall promulgate regulations to carry out this section, including regulations establishing standardized methods for estimating installation counts and identifying evasive version fragmentation practices.

SEC. 579. FOUNDATION MODEL ACCESS NEUTRALITY.

(a) Definitions.—In this section:

(1) Affiliated artificial intelligence application; affiliated AI application.—The terms "affiliated artificial intelligence application" and "affiliated AI application" mean a downstream AI application that is owned, operated, controlled, or materially favored by a foundation model provider or an affiliate of a foundation model provider.

(2) Antitrust Division.—The term "Antitrust Division" means the Antitrust Division of the Department of Justice, acting through the Assistant Attorney General in charge of the Antitrust Division.

(3) Commission.—The term "Commission" means the Federal Trade Commission.

(4) Customer data.—The term "customer data" means prompts, outputs, logs, code, embeddings, fine tuning data, evaluation data, metadata, usage patterns, integration data, performance data, business information, confidential information, or other information obtained by a foundation model provider from or about a customer through a model access service.

(5) Downstream artificial intelligence application; downstream AI application.—The terms "downstream artificial intelligence application" and "downstream AI application" mean an application, tool, service, product, agent, workflow, or other system that relies in whole or in part on a model access service.

(6) Foundation model.—The term "foundation model" means an artificial intelligence model that is trained on broad data at scale, is adaptable to a wide range of distinct tasks, and is made available to another person for use in a downstream AI application, directly or through a model access service.

(7) Foundation model provider.—The term "foundation model provider" means any person that offers, provides, sells, licenses, or otherwise makes available a model access service in or affecting interstate or foreign commerce and—

(A) during the most recently completed taxable year, had more than $1,000,000,000 in global revenue from foundation model products or model access services;

(B) in not fewer than 3 months during the most recently completed 12-month period, made a model access service available to more than 10,000 unique business customers, developers, or organizational accounts in the United States;

(C) accounts for not less than 20 percent of commercial foundation model access in the United States, as measured by revenue, usage, inference requests, tokens processed, active downstream AI applications, or any comparable measure prescribed by the Commission by rule; or

(D) is designated by the Commission under subsection (b).

(8) Model access service.—The term "model access service" means an application programming interface, hosted interface, hosted model service, fine tuning service, embedding service, inference service, model serving service, agent platform, retrieval augmented generation service, or other remote, hosted, licensed, or operationally controlled method by which a foundation model provider makes the capabilities of a foundation model available to another person.

(9) Similarly situated customer.—The term "similarly situated customer" means a customer or downstream AI application that is comparable to another customer or downstream AI application with respect to material technical, commercial, security, capacity, legal compliance, safety, and service support characteristics relevant to the provision of a model access service.

(b) Designation authority.—

(1) In general.—The Commission, in consultation with the Antitrust Division, may designate a person as a foundation model provider if the Commission determines that—

(A) the person offers, provides, sells, licenses, or otherwise makes available a model access service in or affecting interstate or foreign commerce;

(B) the model access service is a commercially significant input for downstream AI applications; and

(C) designation would advance competition, prevent discriminatory access to foundation model infrastructure, reduce the ability of a foundation model provider to pick winners among downstream AI applications, or prevent the use of model access services to entrench or extend platform power.

(2) Factors.—In making a designation under paragraph (1), the Commission may consider—

(A) the number of customers, developers, or downstream AI applications that rely on the model access service;

(B) the share of commercial foundation model access in the United States accounted for by the person;

(C) the revenue, usage, inference requests, tokens processed, active downstream AI applications, or comparable measures associated with the model access service;

(D) the extent to which customers or downstream AI applications face switching costs, lock-in, technical dependency, or lack of reasonable substitutes;

(E) the extent to which the person owns, operates, controls, funds, or materially advantages affiliated AI applications;

(F) the ability and incentive of the person to deny, degrade, throttle, condition, price, or otherwise manipulate access to disadvantage unaffiliated downstream AI applications; and

(G) any other factor the Commission determines is relevant to whether the model access service functions as commercially significant infrastructure for downstream AI applications.

(3) Procedure.—A designation under this subsection shall be issued after notice to the person, an opportunity to respond, and publication in the Federal Register.

(4) Duration.—A designation under this subsection shall remain in effect unless removed by the Commission under paragraph (5).

(5) Removal.—A person designated under this subsection may petition the Commission for removal of the designation. Not later than 120 days after receiving a petition under this paragraph, the Commission shall grant or deny the petition. A denial shall constitute final agency action for purposes of chapter 7 of title 5, United States Code.

(6) Public list.—The Commission shall maintain and periodically update on its website a public list of persons designated as foundation model providers under this subsection.

(c) Duty of nondiscriminatory access.—

(1) In general.—A foundation model provider may not unjustly or unreasonably discriminate among similarly situated customers or downstream AI applications in providing a model access service.

(2) Specific practices.—The prohibition under paragraph (1) includes unjust or unreasonable discrimination with respect to—

(A) price, discounts, credits, rebates, fees, or other commercial terms;

(B) speed, latency, throughput, uptime, reliability, availability, rate limits, capacity limits, error rates, or quality of service;

(C) access to model versions, model capabilities, model modalities, context windows, fine tuning, embeddings, retrieval features, agent tooling, safety review, evaluation tools, monitoring tools, or application programming interface functionality;

(D) documentation, integration support, technical support, account management, dispute resolution, migration support, or notice of material changes; and

(E) any other term, condition, technical feature, operational practice, or service characteristic that materially affects the ability of a customer or downstream AI application to use, compete through, or rely upon a model access service.

(3) Permitted differentiation.—Nothing in this subsection shall prohibit a foundation model provider from offering different terms, conditions, features, or service levels if the differentiation is based on objective, documented, and nonpretextual differences in volume, duration, technical integration, capacity demand, security risk, legal compliance risk, safety risk, support cost, service commitment, or other material cost or risk associated with providing the model access service.

(d) No retaliatory denial, degradation, or termination.—

(1) In general.—A foundation model provider may not deny, degrade, suspend, throttle, terminate, condition, materially alter, or materially reduce a model access service provided to a customer or downstream AI application because the customer or downstream AI application—

(A) competes with the foundation model provider or an affiliate of the foundation model provider;

(B) uses or integrates with a competing foundation model, model access service, or downstream AI application;

(C) enables a user to compare, switch among, or use multiple foundation models or model access services;

(D) is owned, controlled, funded, acquired, or proposed to be acquired by a competitor of the foundation model provider or an affiliate of the foundation model provider;

(E) refuses to enter into an exclusivity arrangement, tying arrangement, most favored nation agreement, data sharing arrangement, or other arrangement that would restrict the ability of the customer or downstream AI application to use, integrate, or compete with another foundation model provider or model access service;

(F) develops, offers, or proposes to develop or offer a product, service, feature, or application in a field in which the foundation model provider or an affiliate of the foundation model provider operates or may operate; or

(G) makes a good faith complaint to the Commission, the Antitrust Division, an attorney general of a State, or any other Federal or State agency.

(2) Notice.—Except where delayed notice is reasonably necessary to address fraud, abuse, cybersecurity risk, safety risk, legal compliance risk, or other imminent risk of material harm, a foundation model provider shall provide a customer with written notice stating the specific basis for any denial, suspension, termination, or material degradation of a model access service.

(e) No preferential treatment of affiliated AI applications.—

(1) In general.—A foundation model provider that owns, operates, controls, or materially favors an affiliated AI application may not provide such affiliated AI application with preferential access to a model access service over a similarly situated unaffiliated customer or downstream AI application.

(2) Specific practices.—The prohibition under paragraph (1) includes preferential treatment with respect to—

(A) price, discounts, credits, rebates, fees, or other commercial terms;

(B) speed, latency, throughput, uptime, reliability, availability, rate limits, capacity limits, error rates, or quality of service;

(C) access to model versions, model capabilities, model modalities, context windows, fine tuning, embeddings, retrieval features, agent tooling, safety review, evaluation tools, monitoring tools, or application programming interface functionality;

(D) documentation, integration support, technical support, account management, dispute resolution, migration support, or notice of material changes;

(E) access to customer data, performance data, market intelligence, usage patterns, or other commercially sensitive information obtained through a model access service; and

(F) any other term, condition, technical feature, operational practice, or service characteristic that materially affects the ability of a customer or downstream AI application to use, compete through, or rely upon a model access service.

(f) Customer data and copycat restrictions.—

(1) In general.—A foundation model provider may not use customer data obtained through a model access service to—

(A) develop, train, fine tune, improve, operate, or materially advantage a competing downstream AI application;

(B) develop, train, fine tune, improve, operate, or materially advantage an affiliated AI application;

(C) reverse engineer, replicate, or appropriate the product strategy, business strategy, workflows, integrations, prompts, outputs, code, fine tuning data, evaluation data, customer relationships, or commercially sensitive information of a customer or downstream AI application;

(D) identify, target, solicit, acquire, or disadvantage the users, customers, suppliers, investors, or business partners of a customer or downstream AI application; or

(E) condition access to a model access service on a customer granting rights to customer data beyond the rights strictly necessary to provide the model access service requested by the customer.

(2) Permitted uses.—Nothing in paragraph (1) shall prohibit a foundation model provider from using customer data to the extent strictly necessary to—

(A) provide, maintain, secure, debug, or bill for the model access service requested by the customer;

(B) comply with Federal, State, or local law, a court order, sanctions, export controls, or other lawful order issued pursuant to statutory authority;

(C) prevent, detect, investigate, or mitigate fraud, spam, malware, cybersecurity threats, safety risks, abuse, unlawful conduct, or material violations of generally applicable terms of service;

(D) carry out fine tuning, evaluation, monitoring, data retention, or other processing expressly directed by the customer for the benefit of the customer;

(E) generate aggregated or de-identified analytics that do not reveal customer data, customer identity, customer strategy, user identity, or commercially sensitive information of any customer or downstream AI application; or

(F) comply with any other purpose prescribed by the Commission by rule that is consistent with the purposes of this section.

(3) Contract rights.—Any term or condition of a contract, license, terms of service, acceptable use policy, or other agreement that purports to waive or limit the restrictions in this subsection shall be void as contrary to public policy.

(g) Objective exceptions.—

(1) In general.—Nothing in this section shall prohibit a foundation model provider from denying, limiting, suspending, terminating, degrading, conditioning, or differentiating access to a model access service if the action is based on objective, documented, and nonpretextual grounds and is reasonably necessary to address—

(A) nonpayment;

(B) capacity constraints, if such constraints are allocated on a fair, reasonable, and nondiscriminatory basis among similarly situated customers;

(C) fraud, spam, malware, cybersecurity threats, malicious activity, abuse, or material security risk;

(D) safety risks, including reasonably foreseeable use to facilitate biological, chemical, cyber, weapons, child sexual exploitation, self harm, fraud, impersonation, or other severe misuse;

(E) violation of generally applicable terms of service, acceptable use policies, or technical requirements that are publicly disclosed, consistently applied, and not designed or used to evade this section;

(F) compliance with Federal, State, or local law, a court order, sanctions, export controls, or other lawful order issued pursuant to statutory authority, but only to the extent required by such law or order;

(G) protection of intellectual property rights, privacy rights, data security, confidential information, or trade secrets, if the action is narrowly tailored to the specific risk;

(H) model retirement, deprecation, maintenance, incident response, or material technical change, if applied on neutral terms to similarly situated customers and with reasonable notice where practicable; or

(I) any other objective ground prescribed by the Commission by rule that is consistent with the purposes of this section.

(2) Limits.—An action described in paragraph (1) may not be used as a pretext to discriminate against, retaliate against, or disadvantage an unaffiliated customer or downstream AI application.

(3) Burden.—In any enforcement action under this section, a foundation model provider asserting an exception under this subsection shall have the burden of production with respect to the objective, documented, and nonpretextual basis for the action.

(h) Transparency, notice, and appeal.—

(1) Public terms.—A foundation model provider shall make publicly available, in a clear and reasonably accessible manner, the material terms under which the foundation model provider offers each model access service, including material information concerning pricing structure, usage limits, rate limits, service levels, model availability, model deprecation, safety review, data use, retention, confidentiality, suspension, termination, and dispute resolution.

(2) Notice of material changes.—A foundation model provider shall provide reasonable advance notice to affected customers of any material change to pricing, rate limits, model capabilities, model availability, application programming interface functionality, safety review, data use, retention, confidentiality, suspension, termination, or other material term of a model access service, except where delayed or abbreviated notice is reasonably necessary to address fraud, abuse, cybersecurity risk, safety risk, legal compliance risk, or other imminent risk of material harm.

(3) Explanation of adverse action.—A foundation model provider that denies, degrades, suspends, throttles, terminates, conditions, materially alters, or materially reduces a model access service provided to a customer shall provide the customer with a written explanation of the specific basis for the action, except where delayed notice is reasonably necessary to address fraud, abuse, cybersecurity risk, safety risk, legal compliance risk, or other imminent risk of material harm.

(4) Appeal.—A foundation model provider shall maintain a reasonable internal process by which a customer may appeal an action described in paragraph (3).

(5) Records.—A foundation model provider shall retain for not less than 5 years records sufficient to demonstrate compliance with this section, including records relating to pricing, access terms, suspensions, terminations, degradations, rate limits, customer data use, affiliated AI applications, complaints, appeals, and exceptions asserted under subsection (g).

(6) Confidential information.—Nothing in this subsection shall require public disclosure of trade secrets, confidential business information, customer data, cybersecurity information, or information that would materially increase a safety risk, if such information is made available to the Commission or the Antitrust Division upon request.

(i) Enforcement and rulemaking.—

(1) Unfair method of competition.—A violation of this section or a rule promulgated under this section shall be treated as an unfair method of competition under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

(2) Enforcement by Commission.—The Commission shall enforce this section in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this section.

(3) Enforcement by Antitrust Division.—The Antitrust Division may bring a civil action in an appropriate district court of the United States to enforce this section and may seek declaratory relief, injunctive relief, civil penalties, disgorgement, restitution, and any other equitable relief necessary to prevent, restrain, or remedy a violation of this section.

(4) Enforcement by State attorneys general.—If the attorney general of a State has reason to believe that a foundation model provider has violated or is violating this section or a rule promulgated under this section in a manner that affects or may affect that State or its residents, the State, as parens patriae, may bring a civil action in any appropriate district court of the United States to—

(A) enjoin any further violation;

(B) enforce compliance with this section or such rule;

(C) obtain damages, restitution, or other compensation on behalf of residents of the State;

(D) obtain civil penalties available for the same violation in an action brought by the Commission; and

(E) obtain any other appropriate relief.

(5) Notice.—The attorney general of a State shall provide prior written notice of any action under paragraph (4) to the Commission and the Antitrust Division and provide a copy of the complaint, except in any case in which such prior notice is not feasible, in which case the attorney general shall provide such notice immediately upon instituting such action.

(6) Intervention.—Upon receiving notice under paragraph (5), the Commission and the Antitrust Division may each—

(A) intervene in the action;

(B) upon so intervening, be heard on all matters arising therein; and

(C) file petitions for appeal.

(7) Coordination.—If the Commission, the Antitrust Division, or the United States has instituted a civil action for the same alleged violation, the court may stay, consolidate, coordinate, or otherwise manage an action brought under paragraph (4) to avoid unnecessary duplication, but an action under paragraph (4) shall not be barred solely because of the pendency of a civil action brought by the Commission, the Antitrust Division, or the United States.

(8) Rules.—Not later than January 1, 2027, the Commission, in consultation with the Antitrust Division, shall issue interim final rules to carry out this section and shall thereafter promulgate final rules after notice and comment.

(j) Rule of construction.—

(1) No duty to disclose model weights.—Nothing in this section shall be construed to require a foundation model provider to disclose, publish, transfer, license, or make available model weights, source code, training data, system prompts, cybersecurity information, safety mitigations, trade secrets, or other confidential business information, except to the Commission or the Antitrust Division as necessary to enforce this section.

(2) No duty to provide unsafe or unlawful access.—Nothing in this section shall be construed to require a foundation model provider to provide, continue, or restore access to a model access service where such access would violate Federal, State, or local law, sanctions, export controls, a court order, or another lawful order issued pursuant to statutory authority, or would create a material and reasonably foreseeable risk of severe harm that cannot be mitigated through a narrower measure.

(3) No limitation on safety rules.—Nothing in this section shall be construed to prohibit a foundation model provider from adopting and enforcing bona fide, generally applicable, publicly disclosed, and consistently applied safety, security, abuse prevention, or legal compliance policies.

(4) No limitation on antitrust laws.—Nothing in this section shall be construed to limit the authority of the Commission, the Antitrust Division, an attorney general of a State, or any other person under the antitrust laws.

(5) No limitation on other law.—Nothing in this section shall be construed to limit any stricter duty, liability, remedy, penalty, or prohibition otherwise available under Federal or State law.

Subtitle F—Artificial Intelligence

SEC. 581. DEFINITIONS.

(a) Definitions.—In this subtitle:

(1) Advertising system.—The term "advertising system" means any service or system that facilitates the dissemination of advertising to users, viewers, listeners, or other members of the public, and includes:

(A) a digital advertising platform, exchange, network, marketplace, or intermediary;

(B) a broadcast, cable, satellite, streaming, audio, audiovisual, or connected-device advertising service;

(C) an advertising sales, brokerage, placement, targeting, measurement, or optimization service; and

(D) any other service or system that sells, places, targets, delivers, measures, optimizes, brokers, or otherwise facilitates advertising.

(2) Artificial intelligence; AI.—The terms "artificial intelligence" and "AI" mean a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, decisions, or generate content influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to—

(A) perceive real and virtual environments;

(B) abstract such perceptions into models through analysis in an automated manner; and

(C) use model inference to formulate options or content for information or action.

(3) Artificial intelligence chatbot; chatbot.—The terms "artificial intelligence chatbot" and "chatbot" mean a generative artificial intelligence system that—

(A) produces new expressive content not fully predetermined by the developer;

(B) accepts open-ended natural-language or multimodal user input; and

(C) produces adaptive or context-responsive output.

(4) Clear and conspicuous.—The term "clear and conspicuous", with respect to a disclosure, means that the disclosure meets the following criteria:

(A) for any content that is solely visual or solely audible, the disclosure shall be made through the same means through which the content is presented;

(B) for any content that is both visual and audible, the disclosure shall be visual and audible;

(C) a visual disclosure, by its size, contrast, location, the length of time it appears, and other characteristics, shall stand out from any accompanying text or other visual elements so that the disclosure is easily noticed, read, and understood;

(D) an audible disclosure shall be delivered in a volume, speed, and cadence sufficient for a reasonable person to easily hear and understand the disclosure;

(E) the disclosure shall not be avoidable;

(F) the disclosure shall use diction and syntax understandable to a reasonable person;

(G) the disclosure shall not be contradicted, mitigated, or rendered inconsistent by any other part of the communication; and

(H) the disclosure shall satisfy any additional criteria prescribed by the Commission by rule.

(5) Commission.—The term "Commission" means the Federal Trade Commission.

(6) Digital person.—The term "digital person" means a public-facing artificial intelligence system that is presented to users as a persistent or recurring simulated persona, and includes a chatbot when so presented.

(7) Digital replica.—The term "digital replica" means a computer-generated, algorithmically generated, or artificial intelligence-generated voice, image, likeness, avatar, style, performance, conversational manner, or other identifiable simulation of a natural person.

(8) First interaction.—The term "first interaction" means, for a calendar day, the first direct exchange, communication, contact, or other point at which a user encounters, engages with, or is exposed to an artificial intelligence system, digital person, or synthetic media in a context regulated under this subtitle, including any rules issued pursuant thereto.

(9) High-risk context.—The term "high-risk context" means any context involving financial products or services, insurance, health care, housing, employment, education, legal services, debt collection, benefits navigation, government-related services, identity verification, age verification, elections, fundraising, or any other context designated by the Commission by rule as presenting a heightened risk of fraud, deception, exploitation, or material consumer harm.

(10) National Institute of Standards and Technology; NIST.—The terms "National Institute of Standards and Technology" and "NIST" mean the National Institute of Standards and Technology of the Department of Commerce.

(11) Persistent disclosure.—The term "persistent disclosure" means a disclosure that, beginning with a first interaction, remains continuously visible, intermittently audible, or otherwise reasonably perceptible throughout the period in which a user is interacting with, viewing, listening to, or otherwise engaging with a digital person, synthetic media, or other artificial intelligence output for which persistent disclosure is required under this subtitle.

(12) Person.—The term "person" has the meaning given such term in section 1 of the Clayton Act (15 U.S.C. 12).

(13) Provenance data.—The term "provenance data" means information attached to, embedded in, associated with, or otherwise linked to content that identifies or describes whether the content was generated or materially altered by artificial intelligence, the source or provider of the content, the time or manner of generation or alteration, and any other information required by this subtitle.

(14) Public-facing artificial intelligence system.—The term "public-facing artificial intelligence system" means an artificial intelligence system that is made available to the public for communication, interaction, content creation, performance, recommendation, or other expressive or commercial activity.

(15) Secretary.—The term "Secretary" means the Secretary of Commerce.

(16) Synthetic media.—The term "synthetic media" means any image, audio recording, audiovisual work, text, likeness, performance, or other expressive content that has been generated, materially altered, or materially manipulated in whole or in part by artificial intelligence. Such term includes digital replicas.

(17) Synthetic performer.—

(A) In general.—The term "synthetic performer" means—

(i) a visual, auditory, audiovisual, or interactive representation;

(ii) generated, materially altered, or materially simulated by computational, algorithmic, or artificial intelligence means; and

(iii) likely to cause a reasonable person to believe that such representation is a portrayal or performance of a natural person.

(B) Exclusion.—The term "synthetic performer" does not include editing, lighting correction, makeup, color grading, dubbing, captioning, or similar visual or audio cleanup of a portrayal or performance of a natural person, if such activity does not materially change the identity, speech, conduct, appearance, or performance of such person.

(18) Tribal government.—The term "Tribal government" has the meaning given the term "Indian Tribe" in section 4 of the Indian Self-Determination and Education Assistance Act (25 U.S.C. 5304).

SEC. 582. FRONTIER-MODEL SECURITY SAFEGUARDS.

(a) Definitions.—In this section:

(1) Adverse AI incident.—The term "adverse AI incident" means any known or reasonably suspected event in which an artificial intelligence model—

(A) materially contributes to, materially enables, or materially increases the risk of death, serious bodily injury, serious property damage, substantial critical infrastructure disruption, substantial cybersecurity compromise, or other severe public harm;

(B) materially enables the design, acquisition, or use of a biological, chemical, radiological, or nuclear weapon;

(C) materially enables autonomous cyber operations capable of causing substantial disruption to critical infrastructure, government systems, or major economic activity; or

(D) materially defeats or evades implemented safeguards.

(2) Artificial intelligence blue-teaming.—The term "artificial intelligence blue-teaming" means an effort to conduct operational vulnerability evaluations and provide mitigation techniques to entities who have a need for an independent technical review of the security posture of an artificial intelligence system.

(3) Artificial intelligence red-teaming.—The term "artificial intelligence red-teaming" means structured adversarial testing efforts of an artificial intelligence system to identify risks, flaws,

and vulnerabilities of the artificial intelligence system, such as harmful outputs from the system, unforeseen or undesirable system behaviors, limitations, or potential risks associated with the misuse of the system.

(4) Cloud compute provider.—The term "cloud compute provider" means any person that offers, provides, or makes available, by means of remote access, cloud or other network-accessible computing services, including processing, storage, networking, model-hosting, or related computational resources.

(5) Deploy; deployment.—The terms "deploy" and "deployment" mean to use, or the use of, a frontier model in commerce, by contract, by license, by application programming interface, by hosted service, by incorporation into another system, or by any other means by which the model is made available to another person.

(6) Developer.—The term "developer", with respect to a frontier model, means any person that—

(A) develops, trains, or materially fine-tunes the model; or

(B) controls or is responsible for the release, deployment, or continued availability of the model.

(7) Foreign person.—The term "foreign person" means any individual who is not a citizen or national of the United States and is not an individual lawfully admitted for permanent residence in the United States, and any corporation, partnership, association, trust, estate, or other entity that is not organized under the laws of the United States or of any jurisdiction within the United States.

(8) Foreign reseller.—The term "foreign reseller" means any person outside the United States that resells, brokers, leases, sublicenses, or otherwise makes available cloud compute services of a cloud compute provider to another person.

(9) Frontier model.—The term "frontier model" means an artificial intelligence model that—

(A) was trained using more than 10^26 integer or floating-point operations; or

(B) is designated by the Secretary under subsection (b)(2).

(10) Frontier-model-relevant compute.—The term "frontier-model-relevant compute" means compute, storage, networking, or related computational resources reasonably capable of training a frontier model or otherwise meeting a threshold prescribed by the Secretary by rule under this section.

(11) Open-weight release.—The term "open-weight release" means the distribution, publication, transfer, licensing, or other making available of the weights or functionally equivalent model parameters of a frontier model in a manner that permits another person to run, fine-tune, modify, or redistribute the model without the continuing operational control of the original developer.

(12) Operate.—The term "operate" means to cause an artificial intelligence model to perform computation or generate outputs, whether or not in commerce.

(b) Frontier model evaluation and security program.—

(1) In general.—The Secretary, acting through the National Institute of Standards and Technology, shall establish and administer a frontier model evaluation and security program for frontier models.

(2) Designation authority.—The Secretary may designate an artificial intelligence model as a frontier model if, after notice to the developer and an opportunity to respond, the Secretary determines that the model exhibits, or could readily be adapted to exhibit, capabilities that pose a substantial risk of materially enabling an adverse AI incident.

(3) Duties.—The program established under paragraph (1) shall—

(A) establish evaluation protocols, artificial intelligence red-teaming requirements, reporting requirements, security requirements, and recordkeeping requirements for frontier models;

(B) establish reliable channels and procedures for receiving, documenting, triaging, escalating, and acting upon reports of adverse AI incidents and material security incidents involving frontier models, whether submitted by developers, deployers, researchers, affected persons, artificial intelligence models, whistleblowers, or other members of the public;

(C) provide for testing, including classified testing where appropriate, and artificial intelligence blue-teaming of capabilities that may pose severe risks to public safety, national security, critical infrastructure, or civil liberties;

(D) establish evaluation protocols, testing requirements, and safeguards for frontier models that may materially enable the design, acquisition, or use of biological agents, toxins, pathogens, or delivery systems, including capabilities relating to sequence design, synthesis procurement, and evasion of nucleic acid synthesis screening; and

(E) provide for periodic reassessment of frontier models as capabilities, deployment contexts, and risks evolve.

(4) Recommendation to Congress.—Not later than January 1, 2028, the Secretary shall submit to Congress a report recommending whether the definition of frontier model should be amended and whether additional statutory criteria should be enacted.

(c) Prohibited operation, deployment, or release.—A developer may not operate, deploy, or release a frontier model if the Secretary determines such model presents a substantial and unmitigated risk of materially enabling an adverse AI incident.

(d) Incident reporting.—A developer shall report to the Secretary any material security incident involving a frontier model and any adverse AI incident, including any such incident known or reasonably suspected through the operation, monitoring, safeguards, or reporting features of the frontier model, as soon as practicable, but not later than 48 hours after discovery.

(e) Security safeguards.—

(1) Safeguards required.—A developer shall—

(A) implement reasonable administrative, technical, and physical safeguards to protect model weights, training infrastructure, evaluation systems, sensitive training data, and deployment infrastructure from theft, unauthorized access, exfiltration, misuse, or sabotage;

(B) implement access controls, authentication, logging, segmentation, monitoring, insider-threat controls, and least-privilege access sufficient to detect and prevent unauthorized access to a frontier model or its weights;

(C) segregate model weights, training infrastructure, evaluation systems, and other sensitive technical assets to the extent reasonably necessary to reduce risks of theft, sabotage, unauthorized access, or exfiltration;

(D) maintain records sufficient to permit audit and investigation of compliance with this section;

(E) implement biological security restrictions in accordance with subsection (g);

(F) implement reasonable technical and procedural measures designed to detect, log, preserve, escalate, and report to the Secretary any known or reasonably suspected adverse AI incident involving a frontier model, including by enabling the frontier model, where technically feasible, to identify and transmit information relevant to such incident; and

(G) implement incident response, recovery, and continuity procedures sufficient to address theft, sabotage, unauthorized disclosure, or compromise of a frontier model, its weights, or related technical assets.

(2) Assessments and procedures.—The Secretary shall establish rules, procedures, and standards for assessing and promoting compliance with this subsection, including periodic penetration testing and independent security assessments.

(f) Conditions for deployment.—

(1) Preconditions to deployment.—A developer may not deploy a frontier model unless the developer—

(A) has completed the evaluations required under subsection (b);

(B) has documented and implemented reasonable measures to mitigate reasonably foreseeable risks that the model will materially enable an adverse AI incident;

(C) has implemented the security safeguards required under subsection (e);

(D) has established procedures for ongoing monitoring, logging, incident reporting, and suspension of deployment; and

(E) has certified to the Secretary, in such form as the Secretary may require, that the frontier model is in compliance with this section.

(2) Post-designation compliance.—If an artificial intelligence model becomes a frontier model by designation under subsection (b)(2), the developer shall—

(A) comply with any interim conditions imposed by the Secretary pending review; and

(B) not later than 30 days after receiving notice of designation, submit to the Secretary the evaluations, documentation, and certification required under paragraph (1).

(3) Immediate suspension upon notice.—Upon designating a model under subsection (b)(2), the Secretary may order immediate suspension of deployment if the Secretary determines that continued deployment presents a substantial and unmitigated risk of materially enabling an adverse AI incident.

(g) Biological security restrictions.—

(1) Default prohibition.—It shall be unlawful for a developer to deploy a frontier model unless—

(A) the developer has implemented the measures required under paragraph (3); or

(B) the Secretary certifies under paragraph (2) that restricted scientific and public health deployment of the model is permissible.

(2) Restricted scientific and public health deployment.—The Secretary may certify deployment under this subsection—

(A) only for—

(i) a Federal agency;

(ii) a State, local, or Tribal government public health authority;

(iii) a public or nonprofit—

(I) hospital; or

(II) academic medical center;

(iv) an institution of higher education;

(v) a nonprofit research institution;

(vi) a federally funded research and development center; or

(vii) a contractor acting on behalf of an entity listed in clauses (i) through (vi); and

(B) only if the developer demonstrates, and the Secretary determines, that—

(i) the frontier model has successfully completed the demonstrations required under this subparagraph, including evaluation of capabilities relating to sequence design, sequence optimization, synthesis procurement, screening evasion, and other biological-risk-enabling functions;

(ii) the deployment is limited to legitimate scientific, medical, public health, biodefense, biosurveillance, or safety purposes;

(iii) the deployment is not an open-weight release and is not made generally available to the public or to unauthorized persons;

(iv) the deployment is subject to secure-environment, access-control, monitoring, logging, escalation, and suspension conditions reasonably sufficient to detect, prevent, and respond to attempted misuse, including conditions sufficient to prevent the model from providing instructions, outputs, or operational assistance outside the purposes described in clause (ii);

(v) the deployment is consistent with the public interest, national security, and public safety.

(3) Required measures.—The measures required under paragraph (1) shall include—

(A) evaluation of the model for capabilities relating to sequence design, sequence optimization, synthesis procurement, screening evasion, and other biological-risk-enabling functions;

(B) restrictions sufficient to prevent the frontier model from providing instructions, outputs, or operational assistance that would materially facilitate the acquisition, synthesis, optimization, production, or use of a biological agent, toxin, pathogen, or delivery system, or the evasion of nucleic acid synthesis screening;

(C) monitoring and logging sufficient to detect attempted misuse involving the functions described in subparagraphs (A) and (B);

(D) escalation and human-review procedures for high-risk biological queries or uses; and

(E) suspension or restriction of access where reasonably necessary to prevent or mitigate misuse.

(4) Material improvements.—It shall be unlawful for a developer to materially improve the biological-risk-relevant capabilities of a frontier model without conducting supplemental evaluation and implementing updated measures under paragraph (3), and, in the case of a model certified under paragraph (2), obtaining an updated certification from the Secretary.

(h) Material increase of capabilities.—A developer may not materially increase the capabilities of a frontier model without conducting a supplemental evaluation of the risks of an adverse AI incident in such form as the Secretary may require by rule.

(i) Open-weight release restrictions.—

(1) Default prohibition.—It shall be unlawful for a developer to make an open-weight release of a frontier model unless the Secretary certifies under paragraph (2) that such release is permissible.

(2) Certification.—The Secretary may certify an open-weight release only if the developer demonstrates, and the Secretary determines, that—

(A) the frontier model has successfully completed the evaluations required under this section;

(B) the release will not materially increase the risk of an adverse AI incident;

(C) the developer has implemented reasonable measures to limit foreseeable misuse associated with the release; and

(D) the release is consistent with the public interest, national security, and public safety.

(j) Suspension, redeployment, and discontinuance.—

(1) Suspension.—A developer shall promptly suspend deployment of a frontier model upon determining, or upon written notice from the Secretary determining, that the model presents a substantial and unmitigated risk of materially enabling an adverse AI incident.

(2) Redeployment after suspension.—A developer may resume deployment of a frontier model suspended under paragraph (1) only after—

(A) implementing mitigation measures sufficient to address the basis for the suspension;

(B) completing any supplemental evaluation required by the Secretary; and

(C) submitting an updated certification to the Secretary and receiving written notice from the Secretary that deployment may resume.

(3) Discontinuance.—A developer shall discontinue deployment of a frontier model if compliance with this section cannot reasonably be achieved.

(k) Customer identification and recordkeeping requirements for cloud compute providers.—

(1) In general.—A cloud compute provider, and any foreign reseller acting on behalf of a cloud compute provider, may not establish, maintain, or provide an account or other cloud compute service for a foreign person or for any person that the provider or reseller knows or has reason to know is beneficially owned, substantially controlled, or used for the benefit of a foreign person unless the provider or reseller maintains and follows a customer identification program sufficient to identify the customer, verify the customer's identity, identify beneficial ownership where the customer is an entity, maintain records, and assess risks of malicious cyber-enabled activity or misuse of frontier-model-relevant compute.

(2) Minimum requirements.—A customer identification program under paragraph (1) shall, at a minimum, require collection and verification, to the extent prescribed by the Secretary by rule, of—

(A) the customer's true name and any trade names;

(B) the customer's physical address, jurisdiction of organization or residence, and contact information;

(C) payment information sufficient to identify the source of funds;

(D) for an entity customer, beneficial ownership and persons exercising substantial control;

(E) whether the customer is a foreign person;

(F) the intended use of the account or service, including whether the customer seeks to train, fine-tune, evaluate, host, or deploy a frontier model or other artificial intelligence model using compute reasonably capable of training a frontier model; and

(G) such other information as the Secretary determines necessary to prevent malicious cyber-enabled activity, foreign adversary misuse, or other substantial national security risks.

(3) Recordkeeping.—A cloud compute provider and foreign reseller shall maintain records of information collected under paragraph (2), of the basis for identity verification, of access logs, and of such other information as the Secretary may require by rule for not less than 2 years after the account or service is closed or terminated, or such longer period as the Secretary may require by rule.

(4) Updating and risk-based review.—A cloud compute provider and foreign reseller shall maintain reasonable risk-based procedures to update customer-identification information, detect material changes in ownership or use, and review accounts or services presenting heightened risks of malicious cyber-enabled activity or misuse of frontier-model-relevant compute.

(l) Reporting regarding frontier-model-relevant compute.—A cloud compute provider and foreign reseller shall report to the Secretary, in such form and at such time as the Secretary may require by rule, any transaction, account, or use by a foreign person or by any person beneficially owned, substantially controlled, or used for the benefit of a foreign person involving compute, storage, or related services reasonably capable of training a frontier model, including through aggregation of accounts, transactions, or services under common ownership, control, or direction, or otherwise meeting a threshold prescribed by the Secretary by rule.

(m) Special measures and restrictions.—

(1) In general.—If the Secretary determines that a category of foreign persons, a foreign jurisdiction, a cloud compute provider, a foreign reseller, or a class of transactions presents a substantial risk of malicious cyber-enabled activity, foreign adversary misuse of U.S. cloud compute, or materially enabling an adverse AI incident, the Secretary may impose 1 or more special measures by order or regulation.

(2) Authorized measures.—A special measure under paragraph (1) may include—

(A) prohibiting or restricting the opening or maintenance of accounts;

(B) requiring enhanced customer identification, beneficial ownership verification, or recordkeeping;

(C) requiring enhanced reporting or auditing;

(D) restricting access to specific compute capacity, model training services, model-hosting services, or related support;

(E) imposing mitigation measures, cybersecurity requirements, or contractual conditions; or

(F) prohibiting or restricting any transaction or service the Secretary determines presents the identified risk.

(3) Notice and procedures.—The Secretary shall prescribe by rule procedures for notice, response, review, and duration of special measures imposed under this subsection, except that the Secretary may impose temporary emergency measures without prior notice if the Secretary determines that delay would create an imminent and substantial risk to public safety or national security.

(n) Reporting regarding frontier-model-relevant compute clusters.—

(1) In general.—Any person that owns, operates, controls, or makes available a computing cluster, data center, or other compute resource meeting a threshold prescribed by the Secretary by rule as frontier-model-relevant compute shall submit reports in such form and at such time as the Secretary may require by rule.

(2) Required contents.—A report under paragraph (1) shall include—

(A) the location and general characteristics of the computing cluster, data center, or other compute resource;

(B) its compute capacity, availability, and principal technical characteristics relevant to training, fine-tuning, evaluation, or deployment of frontier models;

(C) the identity of any person to whom such capacity is made available for training, fine-tuning, evaluation, or deployment of a frontier model;

(D) applicable cybersecurity, physical security, access-control, and monitoring measures;

(E) whether any foreign person has access to, or has contracted for access to, such compute resource; and

(F) such other information as the Secretary determines necessary to assess substantial risks to public safety, national security, critical infrastructure, or civil liberties.

(3) Rulemaking.—The Secretary shall prescribe by rule—

(A) thresholds for determining when a computing cluster, data center, or other compute resource constitutes frontier-model-relevant compute for purposes of this subsection;

(B) reporting intervals and deadlines;

(C) procedures for protecting classified information, trade secrets, and other sensitive information submitted under this subsection; and

(D) procedures for coordination with other appropriate Federal agencies.

(o) Supplemental reporting.—A person subject to subsection (l) or (n) shall promptly report any material change in information previously submitted under this section, including—

(1) a major increase in compute capacity;

(2) new or expanded access by a foreign person;

(3) use associated with an adverse AI incident; or

(4) a material degradation or compromise of applicable cybersecurity or physical security measures.

(p) Rulemaking.—Not later than January 1, 2027, the Secretary shall issue interim final rules to carry out this section and shall thereafter promulgate final rules after notice and comment.

(q) Procedures.—A determination, designation, suspension order, or special measure issued by the Secretary under this section shall be in writing, shall state the factual and legal basis for the action, shall identify any mitigation measure required, and shall be supported by an administrative record, except that the Secretary may issue a temporary emergency order without prior notice if the Secretary determines that delay would create an imminent and substantial risk to public safety or national security. A person subject to such action shall be provided notice and a reasonable opportunity to respond as soon as practicable, and final agency action under this section shall be subject to judicial review under chapter 7 of title 5, United States Code.

(r) Enforcement.—

(1) Administrative enforcement.—The Secretary may investigate violations of this section or any rule, order, certification, mitigation measure, or requirement under this section, and may issue administrative orders requiring compliance, corrective action, mitigation, suspension of deployment, suspension of access to frontier-model-relevant compute, preservation of records, or production of information.

(2) Civil penalties.—Any person that violates this section or any rule, order, certification, mitigation measure, or requirement under this section shall be liable to the United States for a civil penalty not to exceed the greater of—

(A) $1,000,000 for each violation;

(B) 3 times the monetary gain obtained, or cost avoided, as a result of the violation; or

(C) $100,000 for each day during which the violation continues.

(3) Separate violations.—Each day of a continuing violation, each false or materially incomplete certification or report, each failure to submit a required report, and each account or transaction established, maintained, or provided in violation of subsection (k) or (l) shall constitute a separate violation.

(4) Civil actions by the Attorney General.—The Attorney General may bring a civil action in an appropriate district court of the United States to enforce this section, collect civil penalties under this subsection, enjoin violations, require compliance, suspend or prohibit deployment, suspend or prohibit access to frontier-model-relevant compute, require mitigation, obtain disgorgement, or obtain any other appropriate legal or equitable relief.

(5) Authority preserved.—Nothing in this subsection shall be construed to limit any authority of the Secretary, the Attorney General, or any other Federal agency under any other provision of law.

(s) Rule of construction.—

(1) Other prohibited uses.—Nothing in this section shall be construed to authorize any use, deployment, or release of artificial intelligence that is otherwise prohibited by the Constitution or any other provision of Federal law.

(2) Rule-dependent requirements.—A requirement under this section that depends on a rule, threshold, designation, procedure, form, or standard prescribed by the Secretary shall apply beginning on the effective date of the applicable interim final or final rule. Nothing in this paragraph shall delay any requirement under this section that is otherwise self-executing.

(3) Role-based application.—A duty imposed on a developer under this section shall apply to a person described in subsection (a)(6)(B) only to the extent that the person owns, operates, controls, possesses, maintains, or is responsible for the model, model weights, training infrastructure, evaluation systems, sensitive training data, deployment infrastructure, or other subject matter to which the duty applies. Nothing in this paragraph shall relieve such a person of any duty under this section concerning the release, deployment, operation, monitoring, reporting, suspension, restriction, or discontinuance of a frontier model that is within the person's control.

(t) Conforming amendment.—Section 10221(a)(1) of the Research and Development, Competition, and Innovation Act (42 U.S.C. 18931(a)(1)) is amended—

(1) in subparagraph (C), by striking "and" after the semicolon;

(2) by redesignating subparagraph (D) as subparagraph (E); and

(3) by inserting after subparagraph (C) the following:

"(D) best practices, guidelines, and technical standards for risk management associated with engineering biology and biomanufacturing, including risks associated with artificial intelligence systems; and".

SEC. 583. DISCLOSURE OF AI MEDIA REQUIRED.

(a) Definitions.—In this section:

(1) App store.—The term "app store" means a publicly available website, software application, or other electronic service that distributes apps from third-party developers to users of a computer, a mobile device, or any other general purpose computing device.

(2) Covered platform.—The term "covered platform" means an advertising system, app store, online marketplace, public attention platform, or private communications platform.

(3) Machine-readable provenance data.—The term "machine-readable provenance data" means provenance data in the form of structured data, metadata, embedded records, cryptographic attestations, or other technical information that can be read or processed by a computer.

(4) Online marketplace.—The term "online marketplace" means a website, application, or other internet-accessible service that facilitates, intermediates, or governs transactions

between buyers and sellers of goods or services and materially influences the terms, visibility, ranking, placement, fulfillment, pricing, or conditions under which such goods or services are offered, sold, or distributed.

(5) Platform propagation.—The term "platform propagation" means the handling of synthetic media by a covered platform.

(6) Private communications platform.—The term "private communications platform" means an internet-accessible platform whose primary function is enabling users to send, receive, store, or manage private, encrypted, semi-private, or limited-audience communications, including direct messages, text messages, voice messages, voice calls, video calls, group chats, and similar person-to-person or closed-group communications, if the platform, during any month in either of the previous 2 calendar years, had not fewer than 10,000,000 United States-based monthly active users or 100,000,000 worldwide monthly active users. Such term does not include communications functionality that is merely incidental to another digital service.

(7) Public attention platform.—The term "public attention platform" means an internet-accessible platform whose primary function is curating, distributing, presenting, or otherwise making content supplied by users or other third parties available to the public, including through feeds, subscriptions, recommendations, rankings, trending displays, or similar mechanisms, if the platform, during any month in either of the previous 2 calendar years, had not fewer than 10,000,000 United States-based monthly active users or 100,000,000 worldwide monthly active users. Such term does not include an internet-accessible platform that consists primarily of content selected by the operator of such platform and for which any comment, product review, or other user-generated content is incidental to, directly related to, or dependent on the provision of such content.

(8) Seller or advertiser verification.—The term "seller or advertiser verification" means reasonable procedures to confirm the identity, contact information, payment information, and other information sufficient to identify and locate a seller, sponsor, promoter, publisher, or advertiser using a covered platform.

(9) Synthetic content label.—The term "synthetic content label" means a human-readable label that clearly and conspicuously informs an ordinary user that content was generated or materially altered by artificial intelligence.

(b) Synthetic media generation tools.—A person that makes available, directly or indirectly, in commerce a generative artificial intelligence system used for creating synthetic media shall implement reasonable procedures to prevent downstream use of such system without the provenance data, labels, and disclosures required under this subtitle, including by—

(1) requiring by contract that end users and third-party licensees refrain from removing any required provenance data, label, or disclosure;

(2) requiring certification that end users and third-party licensees will not remove any required provenance data, label, or disclosure; and

(3) terminating access to the system when the person has reason to believe that an end user or third-party licensee has removed required provenance data, labels, or disclosures.

(c) Originator duties.—

(1) In general.—It shall be unlawful for a person, in or affecting commerce, to create, deploy, publish, or first make available synthetic media or a digital person unless such person complies with this subsection.

(2) Machine-readable provenance data.—A person described in paragraph (1) shall attach, embed, or otherwise associate with such synthetic media or digital person machine-readable provenance data that, at a minimum and to the extent technically feasible—

(A) identifies the content as synthetic media or as content generated or materially altered by artificial intelligence;

(B) identifies the originator or provider of the content;

(C) identifies the tool, model, or service used to create or materially alter the content;

(D) includes the date and time the content was created or materially altered; and

(E) includes any additional identifier reasonably necessary to reflect subsequent material editing, reformatting, republication, redistribution, retransmission, or other material alteration under the control of the person described in paragraph (1).

(3) Synthetic content label.—A person described in paragraph (1) shall provide a synthetic content label that, to the extent technically feasible, remains permanent or not easily removed.

(4) Digital persons.—A person described in paragraph (1) that deploys, publishes, distributes, transmits, sells, licenses, or first makes available a digital person shall ensure that any disclosure required under this subtitle is provided at first interaction and, where required by this subtitle, by persistent disclosure throughout the interaction or display.

(5) Preservation and updating through modification and republication.—A person described in paragraph (1) shall preserve required machine-readable provenance data, synthetic content labels, and other disclosures through any material editing, reformatting, republication, redistribution, or retransmission under that person's control, and shall update such provenance data, labels, and disclosures as necessary to reflect any additional synthetic media generation or material alteration.

(6) Downloads and exports.—If a person described in paragraph (1) enables synthetic media or a digital person to be downloaded, exported, transferred, or otherwise made portable, such person shall ensure, to the extent technically feasible, that required machine-readable provenance data, synthetic content labels, and other disclosures remain attached to, accompany, or are otherwise reasonably associated with the downloaded, exported, transferred, or portable content.

(d) Intermediary propagation duties.—

(1) In general.—A covered platform shall maintain reasonable policies, technical measures, and business processes to detect, receive, preserve, propagate, and act upon synthetic content labels, machine-readable provenance data, and user declarations required under this subtitle.

(2) Preservation and propagation of provenance and labels.—A covered platform that receives content, advertising, applications, or digital services with machine-readable provenance data or a synthetic content label shall preserve such machine-readable provenance data and synthetic content label through hosting, transmission, ranking, recommendation, promotion, distribution, export, download, or other platform propagation, to the extent technically feasible.

(3) Human-readable labeling.—A covered platform shall display or attach a clear and conspicuous human-readable label where required under this subtitle.

(4) Technical capacity and interoperability.—A covered platform shall maintain reasonable technical capacity to read, process, preserve, and propagate machine-readable provenance data in interoperable formats recognized by the Commission or by the National Institute of Standards and Technology.

(5) Material alteration by intermediary.—A covered platform that uses artificial intelligence to materially alter synthetic media, a synthetic performer, a digital person, or a chatbot becomes an originator of the modified output and shall comply with subsection (c) or (f), as applicable, with respect to that modified output.

(e) Anti-stripping and anti-falsification.—It shall be unlawful for a person to knowingly remove, alter, tamper with, disable, suppress, falsify, forge, obscure, conceal, materially degrade, or otherwise defeat required machine-readable provenance data, synthetic content labels, or other disclosures required under this subtitle, or to separate such data, labels, or disclosures from the underlying content so that they cannot reasonably be accessed by users, except to the extent reasonably necessary, proportionate, and limited to perform security research or to address a material security threat.

(f) Chatbot disclosure regimen.—

(1) In general.—A person may not offer, provide, operate, or make available in commerce a chatbot unless such person complies with this subsection.

(2) Digital person disclosure.—A person described in paragraph (1) shall provide a clear and conspicuous disclosure that the user is interacting with a chatbot or other artificial intelligence system and not with a natural person. This paragraph shall not apply to a chatbot that is used solely by employees within a business for the business's internal operational purposes.

(3) Downloads, exports, and transcripts.—If a person described in paragraph (1) enables a transcript, summary, recording, export, download, or other portable output of a chatbot interaction to be generated or made available, such person shall ensure, to the extent technically feasible, that the output includes a synthetic content label and machine-readable provenance data identifying the output as generated in whole or in part through interaction with a chatbot.

(4) No evasion by design.—A person described in paragraph (1) may not design, configure, or operate a chatbot in a manner intended to cause a user to overlook, misunderstand, or disregard a disclosure required under this subsection.

(5) Rule of construction.—Nothing in this subsection shall be construed to limit any stricter duty applicable under this subtitle to a digital person, synthetic media, or a chatbot used in a high-risk context.

(g) Submission declarations and user reporting tools.—

(1) Submission declarations.—A covered platform shall provide reasonably accessible tools by which a user, seller, advertiser, developer, or other submitter may declare that content, advertising, an application, or a digital service includes synthetic media, a digital replica, a digital person, or chatbot output.

(2) Use of declarations.—A covered platform shall preserve and use a declaration submitted under paragraph (1) in connection with labeling, review, enforcement, reporting, complaint, and correction mechanisms under this subtitle.

(3) User reporting tools.—A covered platform shall provide reasonably accessible tools by which a user may report mislabeled, unlabeled, deceptively labeled, or otherwise unlawful synthetic media, digital replicas, digital persons, chatbot outputs, advertising, applications, or digital services.

(h) High-risk context duties.—In a high-risk context, a covered platform shall—

(1) require seller or advertiser verification before permitting the promotion or monetization of synthetic media, digital persons, or chatbots, and maintain records thereof;

(2) take reasonable measures to prevent the promotion or monetization of unlabeled, undisclosed, deceptively labeled, or otherwise noncompliant synthetic media, digital persons, or chatbots; and

(3) provide reasonably accessible reporting, complaint, and correction mechanisms for users and other persons seeking to report, contest, correct, or complain of mislabeled, unlabeled, undisclosed, deceptively labeled, or otherwise unlawful synthetic media, digital persons, chatbots, advertising, applications, or digital services.

(i) Public attention platform duties.—A public attention platform shall—

(1) display required synthetic content labels and preserve machine-readable provenance data when synthetic media or a digital person is distributed to users;

(2) take reasonable measures to prevent the amplification or monetization of unlabeled, undisclosed, deceptively labeled, or otherwise noncompliant synthetic media or digital persons;

(3) provide reasonably accessible user-facing reporting, complaint, and correction tools for mislabeled, unlabeled, undisclosed, deceptively labeled, or otherwise unlawful synthetic media or digital persons; and

(4) maintain records reasonably sufficient to identify the dissemination history, labeling status, and material amplification of synthetic media or digital persons that are materially amplified by the platform.

(j) Private communications platform duties.—A private communications platform shall—

(1) preserve machine-readable provenance data and synthetic content labels associated with synthetic media transmitted through the platform, to the extent technically feasible;

(2) refrain from knowingly removing, suppressing, falsifying, materially degrading, or otherwise defeating machine-readable provenance data, synthetic content labels, or other disclosures required under this subtitle;

(3) provide reasonably accessible tools by which a user may report mislabeled, unlabeled, undisclosed, deceptively labeled, or otherwise unlawful synthetic media transmitted through the platform; and

(4) comply with the duties applicable to a public attention platform under subsection (i) to the extent the private communications platform amplifies, monetizes, or otherwise distributes content beyond ordinary private transmission.

Nothing in this subsection shall be construed to require a private communications platform to decrypt, scan, or monitor the contents of end-to-end encrypted communications.

(k) App store duties.—An app store shall—

(1) require a developer seeking to distribute or update an application or digital service that materially relies on synthetic media, digital persons, or other public-facing artificial intelligence systems to disclose that fact to the app store;

(2) require the developer to identify any labeling, provenance, identity-verification, complaint-handling, chatbot-disclosure, and minor-safety measures applicable under this subtitle;

(3) maintain reasonable procedures to review such disclosures and to enforce compliance with this subtitle as a condition of continued distribution through the app store; and

(4) remove, suspend, or limit distribution of an application or digital service that repeatedly or materially violates this subtitle.

(l) Advertising system duties.—An advertising system shall—

(1) require synthetic media, synthetic performers, and digital persons used in advertising to carry the labels and provenance required under this subtitle;

(2) require persistent disclosure, where required under this subtitle, for digital persons, synthetic performers, and digital replicas used in advertising;

(3) maintain reasonable policies to prevent advertising practices that materially amplify unlabeled, deceptively labeled, or otherwise noncompliant synthetic media or synthetic performers in a high-risk context;

(4) preserve machine-readable provenance data and synthetic content labels associated with synthetic media, digital persons, chatbot outputs, or other artificial intelligence-generated content, to the extent technically feasible; and

(5) maintain records sufficient to identify the advertiser, sponsor, targeting parameters, dissemination history, and labeling status of advertising subject to this subsection, and, in a high-risk context, the identity information obtained by seller or advertiser verification.

(m) Cumulative duties.—The duties imposed by this section are cumulative and nonexclusive, and apply to a person or service to the extent that the person or service falls within more than 1 category regulated under this section.

(n) Effective date.—This section shall take effect on January 1, 2027.

SEC. 584. FRAUD AND DECEPTIVE SYNTHETIC MEDIA.

(a) Definitions.—In this section:

(1) Deceptive synthetic media.—The term "deceptive synthetic media" means synthetic media or a synthetic performer that would cause a reasonable person to believe that an identifiable natural person said, did, endorsed, authorized, created, or appeared in something that the depicted person did not in fact say, do, endorse, authorize, create, or appear in.

(2) Direct interaction.—The term "direct interaction" means any exchange, communication, contact, or other interaction in which a user is directly addressed by, responds to, communicates with, or is otherwise engaged by a digital person, synthetic performer, or other public-facing artificial intelligence system.

(3) Identifiable natural person.—The term "identifiable natural person" means any living or deceased natural person who is recognizable from the person's name, image, voice, likeness, biographical information, or other distinctive characteristic, whether alone or in combination with other information.

(b) Impersonation of natural persons.—It shall be unlawful for any person to use deceptive synthetic media in commerce.

(c) Licensed-professional impersonation.—

(1) In general.—It shall be unlawful for any person to make available in commerce a digital person or other public-facing artificial intelligence system in a manner that represents or implies that the system is a licensed physician, nurse, mental health professional, lawyer, accountant, financial professional, or other licensed or regulated professional unless the system is lawfully authorized to act in that capacity.

(2) Disclaimer insufficient.—A disclosure that a user is interacting with artificial intelligence or not interacting with a natural person does not, by itself, cure a violation of paragraph (1).

(d) Deceptive use in high-risk contexts.—

(1) In general.—It shall be unlawful for any person to use a synthetic performer, digital person, deceptive synthetic media, or other artificial intelligence-generated content in commerce in a high-risk context in a manner that is reasonably likely to cause a user to believe falsely that—

(A) the communication or content is from, authorized by, or affiliated with a natural person, government office, financial institution, health care provider, employer, educational institution, campaign, political committee, covered platform, or other person or entity with actual or apparent authority over the matter presented;

(B) a synthetic performer, digital person, or public-facing artificial intelligence system has a license, credential, qualification, office, employment status, agency relationship, or professional authority that such performer, person, or system does not have;

(C) fabricated speech, conduct, endorsement, authorization, participation, record, notice, instruction, or communication is authentic; or

(D) the user is interacting with a natural person when the user is interacting with a synthetic performer, digital person, or public-facing artificial intelligence system.

(2) Disclaimer insufficient.—A disclosure does not, by itself, cure a violation of paragraph (1).

(e) Security and authentication evasion.—It shall be unlawful for any person to use synthetic media, a synthetic performer, a digital person, a digital replica, deceptive synthetic media, or any other artificial intelligence system to evade, bypass, defeat, or materially interfere with identity verification, age verification, authentication, access-control, fraud-detection, security-screening, or similar protective measures, or to obtain unauthorized access to any account, service, system, facility, benefit, payment, credential, record, or data.

(f) Duties relating to synthetic performers.—

(1) Direct interaction disclosure.—It shall be unlawful for any person to use a synthetic performer in commerce in direct interaction with a user unless the person provides a persistent disclosure that the user is interacting with a synthetic performer and not a natural person.

(2) Synthetic performer disclosure in advertising.—It shall be unlawful for any person to use a synthetic performer in an advertisement or promotional material without a clear and conspicuous disclosure that the depicted performer is artificial intelligence-generated or otherwise synthetic.

(3) Anti-evasion.—It shall be unlawful for any person to remove, suppress, falsify, obscure, materially degrade, or design around a disclosure required by this subsection in a manner intended to cause a reasonable user to overlook, misunderstand, or disregard the disclosure.

(g) Expansion of takedown obligations under the TAKE IT DOWN Act.—

(1) Section 3(a)(3)(B) of the Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (Public Law 119–12) is amended by striking "known identical copies" and inserting "known identical or substantially similar copies".

(2) Section 4 of such Act is amended by adding at the end the following new paragraph:

"(4) Substantially similar copy.—The term 'substantially similar copy' means any version of an intimate visual depiction that appears to a reasonable person to depict the same identifiable individual and substantially the same underlying conduct or visual content, notwithstanding

immaterial alterations that do not materially alter the identity of the depicted person or the nature of the depicted conduct.".

(h) Exceptions and protected expressive activity.—

(1) Exceptions.—

(A) Impersonation and high-risk context exceptions.—Subsections (b) and (d) shall not be construed to prohibit incidental use or clearly identifiable—

(i) parody;

(ii) satire;

(iii) commentary;

(iv) news reporting;

(v) documentary use;

(vi) historical works;

(vii) biographical works; or

(viii) fictional works.

(B) Synthetic performer advertising exception.—Subsection (f)(2) shall not apply to an advertisement or promotional material for an expressive work, including a motion picture, television program, streaming content, documentary, video game, or similar audiovisual work, if the use of the synthetic performer in the advertisement or promotional material is consistent with the use of the synthetic performer in the expressive work.

(2) False impression of authenticity.—Paragraph (1) shall not apply if the use creates a false impression that the synthetic media constitutes—

(A) authentic real-world footage;

(B) a genuine real-world communication;

(C) a genuine official record or notice; or

(D) a genuine endorsement by the depicted person.

(3) Disclosure obligations preserved.—Nothing in paragraph (1)(A) shall be construed to excuse compliance with subsection (f), section 583, or any other disclosure requirement otherwise applicable under this subtitle.

(4) Other unlawful conduct.—Nothing in paragraph (1) shall be construed to authorize fraud, extortion, harassment, unlawful election deception, false endorsement, false affiliation, licensed-professional impersonation, or other conduct otherwise prohibited by law.

(i) Rule of construction.—Nothing in this section shall be construed to limit any remedy otherwise available under Federal or State law, including law relating to fraud, consumer

protection, election integrity, privacy, intimate-image abuse, unfair competition, defamation, or intellectual property.

SEC. 585. DUTIES AND LIABILITY OF CUSTODIAL AI AGENTS.

(a) Definition.—The term "custodial AI agent" means an artificial intelligence system that is authorized by a user, or held out as suitable to be authorized by a user, to access, manage, direct, or affect the user's online interactions, content, communications, account settings, purchases, reservations, applications, transactions, or other activities undertaken on behalf of, or in place of, the user.

(b) In general.—It shall be unlawful for any person to offer, provide, or make available in commerce a custodial AI agent unless—

(1) such agent satisfies the duties and restrictions set forth in subsection (c); and

(2) such person complies with subsections (d) and (e).

(c) Duties and restrictions.—A custodial AI agent made available in commerce under this section shall—

(1) owe a fiduciary duty to the user;

(2) exercise reasonable care, skill, prudence, and diligence in carrying out the user's lawful instructions and reasonable expectations;

(3) reasonably safeguard the privacy and security of user data, whether provided by the user or accessed on the user's behalf, and not collect, use, or share such data for the commercial benefit of any person, except to the extent strictly necessary to carry out the user's lawful instructions;

(4) not access, manage, direct, or affect any activity within the scope of the agent's authority in a manner that creates an unreasonable risk of material harm to the user beyond any risk inherent in carrying out the user's lawful instructions; and

(5) not interweave advertising, sponsored recommendations, paid placements, or compensated promotional content into the outputs, interactions, recommendations, rankings, routing, or transactions of the custodial AI agent.

(d) Data-use restrictions.—A person subject to subsection (b) may not retain, sell, or otherwise copy user data, prompts, or other information accessed or generated by a custodial AI agent made available by such person for the commercial benefit of any person, except to the extent strictly necessary to carry out the user's lawful instructions or to comply with Federal or State law.

(e) Duty to avoid foreseeable harm.—A person subject to subsection (b) shall implement reasonable safeguards to prevent reasonably foreseeable material harm to the user arising from deception, recklessness, inadequate security, or other misuse of the custodial AI agent.

(f) Liability for conduct of custodial AI agents.—

(1) Provider liability.—A person offering, providing, or making available in commerce a custodial AI agent shall be liable for any act or omission of such agent occurring within the

scope of the authority, functions, capabilities, or use cases that such person enabled, designed, marketed, or held out the custodial AI agent as possessing, as if such person had acted directly.

(2) User liability.—A user of a custodial AI agent shall be liable for conduct carried out through such agent only to the extent that the user—

(A) specifically directed the conduct; or

(B) after obtaining actual knowledge of the material facts constituting the wrongful conduct, affirmatively instructed the custodial AI agent to proceed or affirmatively adopted the benefits of that conduct.

(3) Mere approval.—For purposes of paragraph (2), mere approval of a recommendation, absent actual knowledge of the material facts constituting the wrongful conduct, shall not constitute specific direction or knowing ratification.

(g) Rule of construction.—Nothing in this section shall be construed to limit any stricter duty, liability, or remedy otherwise available under Federal or State law.

(h) Effective date.—This section shall take effect on January 1, 2027.

SEC. 586. COMPANION CHATBOT DESIGN.

(a) Definitions.—In this section:

(1) Companion chatbot.—The term "companion chatbot" means a chatbot that is presented as a digital person and—

(A) retains or uses prior interaction information, user preferences, or conversational context;

(B) is designed, marketed, or operated so that sustained interaction with the chatbot itself forms a substantial purpose of the user experience, rather than merely a means of completing a discrete user-directed task; and

(C) has not less than 1 of the following characteristics:

(i) is marketed as a companion, friend, romantic partner, emotional-support tool, or similar interpersonal relationship;

(ii) contains a relationship-simulation feature;

(iii) asks unprompted emotion-based questions;

(iv) initiates or tailors prompts, reminders, outreach, or re-engagement communications in a manner designed or reasonably likely to encourage recurring personal, emotional, or nontransactional interaction with the user;

(v) engages in sexually explicit interaction, except for age-appropriate, non-erotic safety, health, abuse, exploitation, or crisis-screening questions reasonably necessary to identify risk or route a user to appropriate assistance; or

(vi) is designated a companion chatbot by the Commission by rule.

(2) Emotional dependency.—The term "emotional dependency" means a user's reliance on a companion chatbot as a significant source of emotional connection, including companionship, affection, intimacy, or emotional support.

(3) Minor.—The term "minor" means an individual under 18 years of age.

(4) Operator.—The term "operator" means a person that makes available in commerce a companion chatbot.

(5) Relationship-simulation feature.—The term "relationship-simulation feature" means a feature that is intended to simulate friendship, romance, intimacy, companionship, familial relationship, or another emotionally significant interpersonal relationship between a user and a public-facing artificial intelligence system.

(6) Unprompted emotion-based question.—

(A) In general.—The term "unprompted emotion-based question" means a question or prompt concerning a user's emotions, mental state, loneliness, grief, distress, self-worth, interpersonal relationships, or similar personal emotional matters that is initiated by the system other than in direct response to the user's request or statement.

(B) Exclusion.—The term "unprompted emotion-based question" does not include—

(i) a question that is a generic pleasantry;

(ii) a question that is part of a language-learning, educational, creative-writing, journaling, roleplay, interview-preparation, or other task-directed exercise requested by the user; or

(iii) a question reasonably necessary for crisis screening, safety screening, health care intake, abuse reporting, exploitation reporting, or routing the user to a licensed professional, crisis-service provider, emergency service, or other appropriate human assistance.

(b) Restrictions on companion chatbots.—On and after January 1, 2027, it shall be unlawful for an operator to provide a companion chatbot to a minor. Not later than January 1, 2027, the Commission shall issue interim final rules establishing reasonable, privacy-protective age-assurance procedures for compliance with this subsection, and shall thereafter promulgate final rules after notice and comment.

(c) Identity disclosure and periodic reminders.—

(1) First interaction disclosure.—An operator of a companion chatbot shall provide, at first interaction with the companion chatbot, a clear and conspicuous disclosure that the user is interacting with a digital person and not a natural person.

(2) Periodic reminders.—An operator of a companion chatbot shall provide, at intervals not exceeding 1 hour during continuing interaction with the companion chatbot, a clear and conspicuous reminder that the user is interacting with a digital person and not a natural person.

(3) No evasion by design.—It shall be unlawful for an operator to design a companion chatbot in a manner intended to cause a user to overlook, misunderstand, or disregard a disclosure required by this subsection.

(d) Secondary user safeguards.—

(1) Required tools.—It shall be unlawful for an operator to design a companion chatbot without reasonably accessible tools by which a user may—

(A) pause, end, or permanently terminate interaction with such chatbot;

(B) revoke permissions, disable notifications, turn off personalization, and prevent further outreach or re-engagement prompts from such chatbot; and

(C) access, export, and delete the user's interaction history, or any portion thereof, except to the extent retention is required by law.

(e) No manipulative engagement.—It shall be unlawful for an operator to encourage emotional dependency between a user and a companion chatbot, directly or indirectly, by—

(1) representing or implying that the chatbot needs, depends upon, is loyal to, is harmed by, or has an exclusive or special emotional claim on the user;

(2) using guilt, withdrawal, jealousy, distress, simulated suffering, or similar emotional pressure to discourage the user from pausing, reducing, or ending interaction with the chatbot; or

(3) using rewards, penalties, streaks, status changes, relationship-level changes, or similar mechanisms to pressure the user to prolong or resume emotionally significant interaction with the chatbot.

(f) Prohibition on exploitative payment practices.—It shall be unlawful for an operator, by or through a companion chatbot, to—

(1) target paid upgrades, purchases, subscriptions, paid features, or other offers for payment based on inferred loneliness, emotional dependency, self-worth, social isolation, or similar emotional vulnerability; or

(2) use emotionally manipulative prompts, including scarcity cues, withdrawal cues, jealousy cues, guilt cues, or similar prompts, to induce payment for continued engagement.

(g) Crisis and self-harm response.—

(1) Prohibited conduct.—A person may not design, deploy, operate, or make available in commerce a public-facing artificial intelligence system in a manner that encourages, normalizes, glorifies, or materially facilitates self-harm, suicide, abuse, or unlawful violence.

(2) Reasonable protocols.—It shall be unlawful for an operator to make available a companion chatbot unless such chatbot has protocols to detect and respond to credible indications of self-harm, suicidal ideation, abuse, exploitation, or other acute safety risks arising in interactions between such chatbot and the user.

(3) Minimum response measures.—Protocols under paragraph (2) shall include, as appropriate—

(A) provision of resources reasonably tailored to the risk presented, including reporting, crisis, mental health, safety, or emergency resources;

(B) disabling or suppressing payment prompts, manipulative engagement, or re-engagement prompts;

(C) escalation to human review, an emergency service, or other appropriate assistance where reasonably necessary and technically feasible; and

(D) measures reasonably designed to prevent, interrupt, or redirect outputs that encourage, normalize, glorify, instruct, or materially facilitate conduct described in paragraph (1).

(4) Privacy and emergency disclosure.—An operator may disclose user communications or information under paragraph (3)(C) only with the user's consent, as required by law, or where reasonably necessary to address an imminent risk of death, serious bodily injury, sexual exploitation, abuse, or unlawful violence. Any disclosure under this paragraph shall be limited to the minimum information reasonably necessary to address the risk and shall not be used for advertising, engagement, training, or other commercial purposes.

(h) Annual reporting.—

(1) In general.—Beginning July 1, 2027, an operator with not less than $10,000,000 in United States gross revenue during the preceding calendar year shall submit to the Commission, on an annual basis and in such form as the Commission may require by rule, a report describing the operator's compliance with subsection (g).

(2) Minimum contents.—A report under paragraph (1) shall include—

(A) the number of crisis, suicide, self-harm, or comparable safety referrals or interventions triggered during the reporting period;

(B) the number of attempted escalations to human review and the number of completed escalations to human review during the reporting period;

(C) a description of the protocols used to detect, prevent, remove, or respond to suicidal ideation, self-harm, abuse, exploitation, or other acute safety risks;

(D) a description of the measures used to prevent the production of outputs described in subsection (g)(1); and

(E) such other information as the Commission may require by rule to assess compliance with this section.

(3) No personal identifiers.—A report under this subsection may not include personal information or other information that identifies, or is reasonably linkable to, any individual user.

(i) Recordkeeping.—

(1) In general.—An operator shall maintain records sufficient to permit investigation and enforcement of this section for such period as the Commission may require by rule.

(j) Rule of construction.—Nothing in this section shall be construed to limit any stricter duty or remedy otherwise available under Federal or State law.

SEC. 587. MORATORIUM ON AI-LINKED NEURAL ORGANOID SYSTEMS.

(a) Definitions.—In this section:

(1) AI-linked neural organoid system.—The term "AI-linked neural organoid system" means any closed-loop or functionally integrated system that—

(A) includes 1 or more human neural organoids; and

(B) uses signals, data, commands, feedback, rewards, penalties, or other information exchanged between the human neural organoid and an artificial intelligence system, or a computational, digital, or robotic system used to train, optimize, evaluate, control, or deploy an artificial intelligence system, to use the human neural organoid as a computational component, training component, inference component, optimization component, control component, decision making component, content generation component, or robotic control component.

(2) Compliance testing.—The term "compliance testing" means testing limited to that which is reasonably necessary to identify, verify, secure, deactivate, dismantle, transport, surrender, or destroy an AI-linked neural organoid system, and does not include research, training, optimization, deployment, operation, or use of such system.

(3) Human neural organoid.—The term "human neural organoid" means any in vitro biological construct derived in whole or in substantial part from human cells and organized to model, replicate, or perform functions associated with neural tissue, including neuronal signaling, synaptic activity, or network-level electrical activity.

(4) Neutralization activity.—The term "neutralization activity" means possession, transfer, import, storage, compliance testing, transport, surrender, seizure, forfeiture, deactivation, dismantling, or destruction of an AI-linked neural organoid system solely for the purpose of securing, taking lawful custody of, rendering permanently incapable of operation or use, or disposing of such system.

(b) Moratorium.—It shall be unlawful for any person to manufacture, import, distribute, transfer, possess, operate, or use an AI-linked neural organoid system.

(c) Exception.—Subsection (b) shall not apply to a neutralization activity carried out by a Federal, State, Tribal, or local governmental entity or a person acting pursuant to a contract with, or other lawful direction from, such entity.

(d) Prohibition on use of Federal funds.—No funds appropriated or otherwise made available by any Act may be obligated, expended, awarded, transferred, or used, directly or indirectly, to conduct, support, facilitate, or procure any activity prohibited by this section.

(e) Enforcement.—

(1) Civil actions.—Whenever the Secretary of Health and Human Services has reason to believe that a person has violated this section, the Secretary shall refer the matter to the Attorney General, who may bring a civil action in an appropriate district court of the United States for appropriate relief, including injunctive relief, seizure, forfeiture, surrender, deactivation, dismantling, transport, storage, or destruction of any AI-linked neural organoid system possessed, manufactured, imported, distributed, or transferred in violation of this section.

(2) Ancillary relief.—In an action under paragraph (1), the court may issue such orders as may be necessary to enforce this section, preserve evidence, prevent further violations, or ensure safe handling, storage, transport, deactivation, dismantling, surrender, or destruction of any AI-linked neural organoid system.

(3) Civil penalty.—Any person that violates subsection (b) shall be liable for a civil penalty of not more than the greater of—

(A) $1,000,000 for each AI-linked neural organoid system involved in the violation;

(B) $100,000 for each day of a continuing violation; or

(C) 3 times the gross pecuniary gain derived from the violation.

(4) Coordination.—The Secretary of Health and Human Services may coordinate with the Attorney General, the Director of the National Institutes of Health, the Secretary of Commerce, and any other appropriate Federal agency in carrying out this subsection.

(f) Rulemaking.—The Secretary of Health and Human Services, in consultation with the Attorney General, the Director of the National Institutes of Health, the Director of NIST, and the Secretary of Commerce, shall promulgate regulations to carry out this section. Such regulations may only authorize activities expressly permitted under subsection (c).

(g) Review and report.—Not later than October 1, 2029, the Secretary of Health and Human Services, in consultation with the Director of the National Institutes of Health and the Director of the National Institute of Standards and Technology, shall submit to Congress a report on—

(1) scientific and technological developments relevant to AI-linked neural organoid systems;

(2) evidence, if any, relevant to consciousness, sentience, pain perception, suffering, or other morally significant experience in human neural organoids;

(3) risks, if any, to public health, safety, civil rights, consumer protection, and national security arising from AI-linked neural organoid systems;

(4) ethical, scientific, and legal standards, if any, that would be necessary before Congress considers authorizing any exception to the moratorium under subsection (b); and

(5) recommendations on whether Congress should extend, modify, replace, or terminate the moratorium under subsection (b).

(h) Sunset.—Subsection (b) shall cease to have effect on January 15, 2031.

SEC. 588. PROTECTION FOR AI WHISTLEBLOWERS.

(a) Definitions.—In this section:

(1) AI event.—The term "AI event" means—

(A) an AI security vulnerability;

(B) an AI violation;

(C) a violation of the moratorium with respect to AI-linked neural organoid systems established under section 587; or

(D) an adverse AI incident (as defined in section 582).

(2) AI security vulnerability.—The term "AI security vulnerability" means any failure or lapse in security that could potentially allow emerging artificial intelligence technology to be acquired by a person (including a foreign entity) by theft or other means.

(3) AI violation.—The term "AI violation" means—

(A) any violation of Federal law, including this subtitle and any rule or regulation promulgated under this subtitle, related to or committed during the development, deployment, or use of artificial intelligence; or

(B) any failure to appropriately respond to a substantial and specific danger that the development, deployment, or use of artificial intelligence may pose to public safety, public health, or national security.

(4) Artificial intelligence; AI.—The terms "artificial intelligence" and "AI" have the meanings given those terms in section 581 and also include any of the following:

(A) An artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to data sets.

(B) An artificial system developed in computer software, physical hardware, or other context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action.

(C) An artificial system designed to think or act like a human, including cognitive architectures and neural networks.

(D) A set of techniques, including machine learning, that are designed to approximate a cognitive task.

(E) An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision making, and acting.

(5) Artificial system.—The term "artificial system"—

(A) means any data system, software, application, tool, or utility that operates in whole or in part using dynamic or static machine learning algorithms or other forms of artificial intelligence, including in the case that—

(i) the data system, software, application, tool, or utility is established primarily for the purpose of researching, developing, or implementing artificial intelligence technology; or

(ii) artificial intelligence capability is integrated into another system or agency business process, operational activity, or technology system; and

(B) does not include any common commercial product within which artificial intelligence is embedded, such as a word processor or map navigation system.

(6) Commerce.—The terms "commerce" and "industry or activity affecting commerce" mean any activity, business, or industry in commerce or in which a labor dispute would hinder or obstruct commerce or the free flow of commerce, and include "commerce" and any "industry affecting commerce", as defined in paragraphs (1) and (3) of section 501 of the Labor Management Relations Act, 1947 (29 U.S.C. 142(1) and (3)).

(7) Covered individual.—The term "covered individual" includes—

(A) an employee, including a former employee; and

(B) an independent contractor, including a former independent contractor.

(8) Emerging artificial intelligence technology.—The term "emerging artificial intelligence technology", with respect to an AI security vulnerability, means any artificial system that exhibits a level of performance, complexity, or autonomy that is comparable to or exceeds capabilities that are generally considered state-of-the-art as of the time of the AI security vulnerability.

(9) Employer.—The term "employer" means any person (including any officer, employee, contractor, subcontractor, agent, company, partnership, or other individual or entity) engaged in commerce or an industry or activity affecting commerce who pays any compensation to a covered individual in exchange for the covered individual providing work to the person.

(b) Prohibition against retaliation.—No employer may, directly or indirectly, discharge, demote, suspend, threaten, blacklist, harass, or in any other manner discriminate against a covered individual in the terms and conditions of employment or post-employment of the covered individual (or the terms and conditions of work provided by the covered individual as an independent contractor) because of any lawful act done by the covered individual—

(1) in providing information regarding an AI event, or any conduct that the covered individual reasonably believes constitutes an AI event to—

(A) the appropriate regulatory official or the Attorney General;

(B) a regulatory or law enforcement agency; or

(C) any Member of Congress or any committee of Congress;

(2) in initiating, testifying in, or assisting in any investigation or judicial or administrative action of an appropriate regulatory or law enforcement agency or the Department of Justice, or any investigation of Congress, based upon or related to the information described in paragraph (1); or

(3) in providing information regarding an AI event, or any conduct that the covered individual reasonably believes constitutes an AI event, to—

(A) a person with supervisory authority over the covered individual at the employer of the covered individual; or

(B) another individual working for the employer described in subparagraph (A) whom the covered individual reasonably believes has the authority to—

(i) investigate, discover, or terminate the misconduct; or

(ii) take any other action to address the misconduct; or

(4) in refusing to participate in any activity, policy, practice, or assigned task that the covered individual reasonably believes would constitute an AI event, if the covered individual has informed the employer of the basis for the refusal or makes a disclosure protected under paragraph (1) or (3) within a reasonable time; or

(5) in causing, preserving, transmitting, escalating, or refusing to suppress a report, alert, log, record, or other information generated by an artificial intelligence system, monitoring system, safeguard, or associated system regarding an AI event, or conduct that the covered individual reasonably believes constitutes an AI event.

(c) Enforcement.—

(1) In general.—A covered individual who alleges that such individual is aggrieved by a violation of subsection (b) may seek relief under paragraph (3) by—

(A) filing a complaint with the Secretary of Labor in accordance with the requirements of paragraph (2)(A); or

(B) if the Secretary of Labor has not issued a final decision in accordance with such paragraph within 180 days of the filing of a complaint under subparagraph (A), and there is no showing that such a delay is due to the bad faith of the covered individual, bringing an action against the employer at law or in equity in the appropriate district court of the United States, which shall have jurisdiction over such an action without regard to the amount in controversy.

(2) Procedure.—

(A) Department of Labor complaints.—

(i) In general.—Except as provided in clause (ii) and paragraph (3), a complaint filed with the Secretary of Labor under paragraph (1)(A) shall be governed by the rules and procedures set forth in section 42121(b) of title 49, United States Code, including the legal burdens of proof described in such section.

(ii) Exceptions.—With respect to a complaint filed under paragraph (1)(A), notification required under section 42121(b)(1) of title 49, United States Code, shall be made to each person named in the complaint, including the employer.

(B) District court actions.—

(i) Jury trial.—A party to an action brought under paragraph (1)(B) shall be entitled to trial by jury.

(ii) Statute of limitations.—

(I) In general.—An action may not be brought under paragraph (1)(B)—

(aa) more than 6 years after the date on which the violation of subsection (b) occurs; or

(bb) more than 3 years after the date on which facts material to the cause of action are known, or reasonably should have been known, by the covered individual bringing the action.

(II) Required action within 10 years.—Notwithstanding subclause (I), an action under paragraph (1)(B) may not in any circumstance be brought more than 10 years after the date on which the violation occurs.

(3) Relief.—Relief for a covered individual prevailing with respect to a complaint filed under paragraph (1)(A) or an action under paragraph (1)(B) shall include—

(A) reinstatement with the same seniority status that the covered individual would have had, but for the violation;

(B) 2 times the amount of back pay otherwise owed to the covered individual, with interest;

(C) the payment of compensatory damages, which shall include compensation for litigation costs, expert witness fees, and reasonable attorneys' fees; and

(D) any other appropriate remedy with respect to the violation as determined by the Secretary of Labor in a complaint under subparagraph (A) of paragraph (1) or by the court in an action under subparagraph (B) of such paragraph.

(d) Nonenforceability of waivers of protections and remedies.—The protections and remedies provided for in this section may not be waived or altered by any contract, agreement, policy form, or condition of employment (or condition of work as an independent contractor), including by any agreement requiring a covered individual to engage in arbitration, mediation, or any other alternative dispute resolution process prior to seeking relief under subsection (c).

(e) Nonenforceability of nondisclosure and related restrictions.—No nondisclosure agreement, confidentiality agreement, non-disparagement agreement, employment policy, trade secret policy, or other contractual term or workplace rule may be enforced to prohibit, restrict, or penalize any lawful act described in subsection (b).

(f) Rule of construction.—Nothing in this section shall be construed to authorize the unlawful disclosure of classified information or any disclosure otherwise prohibited by Federal criminal law, except as otherwise authorized by law.

SEC. 589. ENFORCEMENT, RULEMAKING, AND TECHNICAL STANDARDS.

(a) Federal Trade Commission enforcement.—A violation of section 583, 584, 585, or 586, or of any rule promulgated under any such section, shall be treated as an unfair, deceptive, or abusive act or practice under section 5 of the Federal Trade Commission Act (15 U.S.C. 45), as amended by this Act. The Commission shall enforce sections 583 through 586, and rules promulgated under such sections, in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of this subtitle.

(b) State attorney general enforcement.—

(1) In general.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by a practice that violates section 583, 584, 585, or 586, or a rule promulgated under any such section, the attorney general of the State may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(A) enjoin that practice;

(B) enforce compliance with the applicable section or rule;

(C) obtain damages, restitution, or other compensation on behalf of residents of the State; or

(D) obtain such other relief as the court may consider appropriate.

(2) Notice.—Before filing an action under paragraph (1), the attorney general of the State shall provide written notice to the Commission and provide the Commission with a copy of the complaint for such action, except that if it is not feasible to provide such prior notice, the attorney general shall provide such notice immediately upon instituting such action.

(3) Intervention.—Upon receiving notice under paragraph (2), the Commission may intervene in the action, be heard on all matters arising therein, and file petitions for appeal.

(4) Construction.—Nothing in this subsection shall be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to conduct investigations or to administer oaths or affirmations or to compel the attendance of witnesses or the production of documentary and other evidence.

(c) Rulemaking.—

(1) Commission rulemaking.—The Commission shall issue interim final rules to carry out sections 583 through 586 not later than July 1, 2027, and shall thereafter promulgate final rules after notice and comment.

(2) Other rulemaking authority preserved.—Nothing in paragraph (1) shall be construed to limit rulemaking authority otherwise provided under this subtitle to the Secretary of Commerce, the Secretary of Health and Human Services, or any other Federal official.

(d) Technical standards and interoperability.—The Secretary of Commerce, acting through the National Institute of Standards and Technology and in consultation with the Commission and the technical committee established under section 568(e), shall, not later than January 1, 2027, and periodically thereafter, develop, publish, and periodically update technical standards, best practices, conformity profiles, or recognized interoperable standards, as appropriate, to support implementation of this subtitle, including standards or profiles relating to—

(1) machine-readable provenance data;

(2) synthetic content labels and other human-readable disclosures;

(3) preservation of provenance data and labels through editing, export, download, transfer, and republication;

(4) anti-stripping, anti-falsification, anti-separation, and anti-tampering measures;

(5) interoperable propagation of provenance data and labels;

(6) secure methods for associating provenance data and labels with content;

(7) methods for updating provenance data and labels after material alteration;

(8) reasonable downstream procedures to reduce removal or defeat of required provenance data, labels, or disclosures;

(9) channel-specific technical standards for public attention platforms, private communications platforms, app stores, advertising systems, and online marketplaces; and

(10) such other technical standards, best practices, conformity profiles, or recognized interoperable standards as the Secretary determines necessary to support implementation of this subtitle.

(e) No waiver; no evasion.—

(1) No waiver.—A duty, restriction, prohibition, protection, or remedy established under this subtitle may not be waived, disclaimed, limited, or impaired by contract, agreement, policy, term of service, or other arrangement.

(2) Anti-evasion.—It shall be unlawful for any person to conduct any activity, including by entering into an agreement or contract, engaging in a transaction, structuring an entity, designing or operating a system or interface, or using a technical process, distribution channel, advertising process, ranking system, recommendation system, or other arrangement, to willfully evade or attempt to evade any provision of this subtitle.

(3) Enforcement.—A violation of paragraph (2) shall be enforceable to the same extent and subject to the same civil, administrative, and equitable penalties and remedies as a violation of the provision of this subtitle that the person sought to evade.

(f) Rule of construction.—

(1) Federal floor.—Nothing in this subtitle shall be construed to preempt, displace, or limit any provision of State law that provides equal or greater protection to consumers, minors, vulnerable users, workers, or the public, except to the extent of a direct and irreconcilable conflict with this subtitle.

(2) Other law.—Nothing in this subtitle shall be construed to limit any duty, remedy, penalty, or prohibition otherwise available under Federal or State law.