ONLINE CIVIL RIGHTS ACT

LAWYERS' COMMITTEE FOR CIVIL RIGHTS UNDER LAW

DECEMBER 2023

Table of Contents

SECTION 1 – PURPOSES.

The purposes of this Act are to prevent and remedy algorithmic discrimination and to promote equal opportunity; to require that algorithmic systems are safe and effective prior to deployment and through post-deployment monitoring; to give individuals the right to opt-out and appeal decisions made by algorithmic systems; to protect the data security of individuals; and to provide transparency as to the algorithmic and data practices of developers and deployers.

SECTION 2 – DEFINITIONS.

(1) ABNORMALLY DANGEROUS ACTIVITY. – The term "abnormally dangerous activity" means an activity that creates a foreseeable and highly significant risk of physical, psychological, or economic harm. In determining whether an activity is abnormally dangerous, the following factors shall be considered, examining the totality of the circumstances:

- (A) The existence of a high degree of risk of harm to a person or property.
- (B) The likelihood that the harm that results will be great.
- (C) The inability to eliminate the risk by the exercise of reasonable care.
- (D) The extent to which the activity is not a matter of common usage.
- (E) The inappropriateness of the activity to the place where it is carried on.
- (F) The extent to which the activity's value to the community is outweighed by its dangerous attributes.

(2) 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 developer or deployer that meets the requirements of subparagraph (B).
- (B) REQUEST REQUIREMENTS.—The requirements of this subparagraph with respect to a request from a developer or deployer 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 developer or deployer'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 developer or deployer's product or service.
  - (ii) The request includes a description of the processing purpose for which the individual's consent is sought and—
  - (iii) clearly states the specific categories of personal data that the developer or deployer shall collect, process, and transfer necessary to effectuate the processing purpose; and
    - (I) 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 personal data to be collected, processed, or transferred by the developer or deployer for such processing purpose.
  - (iv) The request clearly explains the individual's applicable rights related to consent.
  - (v) The request is made in a manner reasonably accessible to and usable by individuals with disabilities.
  - (vi) The request is made available to the individual in each covered language in which the developer or deployer provides a product or service for which authorization is sought.
  - (vii) 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.

(viii) Processing or transferring any personal 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 developer or deployer may not infer that an individual has provided affirmative express consent to an act or practice from the inaction of the individual or the individual's continued use of a service or product provided by the covered entity.

(D) PRETEXTUAL CONSENT PROHIBITED.—A developer or deployer 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 personal data.

(3) COLLECT; COLLECTION.—The terms "collect" and "collection" mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring personal data by any means.

(4) CONSEQUENTIAL ACTION.—The term "consequential action" means an act that is likely to have or contribute to a material effect on the impact of, access to, eligibility for, cost of, terms of, or conditions of any of the following:

(A) Employment, including hiring, pay, independent contracting, worker management, promotion, termination, and labor relations.

(B) Education and vocational training, including assessment, proctoring, academic integrity, accreditation, certification, admissions, financial aid, and scholarships.

(C) Housing and lodging, including rental and short-term housing and lodging, home appraisals, rental subsidies, and publicly-supported housing.

(D) Essential utilities, including electricity, heat, water, municipal trash or sewage services, internet and telecommunications service, and public transportation.

(E) Health care, including mental health care, dental, vision, and adoption services.

(F) Credit, banking, and other financial services.

(G) Insurance.

(H) The criminal justice system, immigration enforcement, border control, and child protective services, including risk and threat assessments, bail determinations, sentencing, parole, surveillance, unmanned vehicles and machines, and predictive policing.

(I) Legal services, including court-appointed counsel services and alternative dispute resolution services.

(J) Elections, including voting, redistricting, voter eligibility and registration, support or advocacy for a candidate for office, distribution of voting information, election security, and administration.

(K) Government benefits and services, as well as identity verification, fraud prevention, and assignment of penalties.

(L) Public accommodations.

(M) Abnormally dangerous activities.

(N) Any other service, program, or opportunity which has a comparable legal, material, or similarly significant effect on an individual's life as determined by the Federal Trade Commission through rules promulgated pursuant to section 553 of title 5, United States Code.

(5) COVERED ALGORITHM.—The term "covered algorithm" means—

(A) —

(i) a computational process that uses machine learning, natural language processing, artificial intelligence techniques, or other computational processing techniques of similar or greater complexity; or

(ii) a deterministic computational process derived from a process described in clause (i); and

(B) that, with respect to a consequential action—

(i) creates or facilitates the creation of a product or information;

(ii) promotes, recommends, ranks, or otherwise affects the display or delivery of material information;

(iii) makes a decision; or

(iv) facilitates human decision making.

(6) COVERED LANGUAGE.—The term "covered language" means the ten languages with the most speakers in the United States, according to the most recent United States Census.

(7) 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 developer or deployer—

(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 developer or deployer—

(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.

(8) DEPLOYER.—The term "deployer" means any person, other than an individual acting in a non-commercial context, that uses a covered algorithm. This definition shall not be interpreted to be mutually exclusive from "Developer".

(9) DEVELOPER.—The term "developer" means any person, other than an individual acting in a non-commercial context, that designs, codes, customizes, or produces a covered algorithm, or substantially modifies a covered algorithm, whether for its own use or for use by a third party. This definition shall not be interpreted to be mutually exclusive from "Deployer".

(10) DISPARATE IMPACT.— The term "disparate impact" means an unjustified differential effect on a person or group of people on the basis of one or more actual or perceived protected characteristics.

(A) A differential effect is unjustified if—

(i) a respondent fails to show that the action, policy, or practice causing the differential effect is necessary to achieve one or more substantial, legitimate, and nondiscriminatory interests; or

(ii) once a respondent shows such interest, a complainant shows that an alternative action, policy, or practice could serve that interest with less differential effect.

(B) With respect to demonstrating that a covered algorithm causes or contributes to a differential effect, the covered algorithm is presumed to be not capable of separation for analysis and may be analyzed holistically, unless a respondent proves otherwise by a preponderance of the evidence.

(11) HARM.—The term "harm" means a non-de minimis adverse effect on an individual or group of individuals.

(12) INDEPENDENT AUDITOR.—The term "independent auditor" means a person that conducts a pre-deployment evaluation or impact assessment of a covered algorithm in a manner that exercises objective and impartial judgment on all issues within the scope of such evaluation or assessment. A person is not an independent auditor of a covered algorithm if they—

(A) are or were involved in using, developing, offering, licensing, or deploying the covered algorithm;

(B) at any point during the pre-deployment evaluation or impact assessment, has an employment relationship with a developer or deployer that uses, offers, or licenses the covered algorithm; or

(C) at any point during the pre-deployment evaluation or impact assessment, has a direct financial interest or a material indirect financial interest in a developer or deployer that uses, offers, or licenses a covered algorithm.

(13) INDIVIDUAL.—The term "individual" means a natural person in the United States.

(14) LARGE BUSINESS.—

(A) IN GENERAL.—The term "large business" means a developer or deployer that, in the most recent calendar year—

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

(ii) develops or deploys a covered algorithm that is likely to have or contribute to a material effect on at least 1,000,000 individuals; or

(iii) possesses the personal data of more than 5,000,000 individuals or devices that identify or are linked or reasonably linkable to 1 or more individuals, excluding personal 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.

(B) EXCLUSIONS.—The term "large business" does not include any instance in which the developer or deployer would qualify as a large business solely on the basis of collecting or processing—

(i) email addresses;

(ii) 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 developer or deployer.

(C) REVENUE.—For purposes of determining whether any developer or deployer is a large business, the term "revenue", with respect to any developer or deployer that is not organized to carry on business for its own profit or that of its members—

(i) means the gross receipts the developer or deployer 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.

(15) PERSONAL DATA.—

(A) IN GENERAL.—The term "personal 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 "personal data" does not include—

(i) de-identified data;

(ii) employee data; or

(iii) publicly available information.

(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.

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

(17) PROTECTED CHARACTERISTIC.—The term "protected characteristic" means one or more of the following actual or perceived traits: race, color, ethnicity, national origin, religion, sex (including sexual orientation and gender identity), disability, limited English proficiency, biometric information, familial status, source of income, or income level (not including the ability to pay for a specific good or service being offered).

(18) PUBLIC ACCOMMODATION.—

(A) The term "public accommodation" means—

(i) a business that offers goods or services to the general public, regardless of whether it is operated for profit and regardless of whether it operates from a physical facility;

(ii) a park, road, or pedestrian pathway open to the general public;

(iii) public transportation; or

(iv) publicly-owned or -operated facilities open to the general public.

(B) The term "public accommodation" does not include a private club or group not open to the general public, as described in section 201(e) of the Civil Rights Act of 1964 (42 U.S.C. 2000a(e)).

(19) 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.

(20) STATE DATA PROTECTION AUTHORITY.—The term "state data protection authority" means an independent public authority that supervises, investigates, and regulates data protection and security law in a State, including handling complaints lodged against violations of state and relevant national laws.

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

TITLE I – CIVIL RIGHTS

SEC. 101. DISCRIMINATION.

(a) IN GENERAL.—A developer or deployer shall not offer, license, or use a covered algorithm in a manner that discriminates in, causes a disparate impact, or otherwise makes unavailable the equal enjoyment of goods, services, or other activities or opportunities as related to a consequential action on the basis of a protected characteristic.

(b) EXCEPTIONS.—This section shall not apply to—

(1) the offer, license, or use of a covered algorithm for the sole purpose of—

(A) a developer's or deployer's self-testing to identify, prevent, or mitigate discrimination or otherwise to ensure compliance with obligations under federal law; or

(B) expanding an applicant, participant, or customer pool to increase diversity or redress historic discrimination.

(2) 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)).

SEC. 102. PRE-DEPLOYMENT EVALUATIONS AND POST-DEPLOYMENT IMPACT ASSESSMENTS.

(a) PRE-DEPLOYMENT EVALUATIONS.—A developer or deployer that develops or deploys a covered algorithm or makes material changes to a previously deployed covered algorithm shall, prior to deploying, licensing, or offering the covered algorithm in interstate commerce, conduct a pre-deployment evaluation as follows:

(1) PRELIMINARY EVALUATION.—As a first step, the developer or deployer shall evaluate whether it is plausible that use of the covered algorithm may result in a harm. If it is not plausible, the developer or deployer shall record a finding of no plausible impact. If it is plausible, the developer or deployer shall proceed to conduct a full pre-deployment evaluation. When conducting this preliminary evaluation of a material change to a previously deployed covered algorithm, the developer or deployer may limit the scope of its inquiry to whether use of the covered algorithm may result in a harm as a result of the material change.

(2) DEVELOPER FULL PRE-DEPLOYMENT EVALUATION.—

(A) A developer shall engage an independent auditor to evaluate—

(i) the covered algorithm's design;

(ii) the manner in which the covered algorithm makes or contributes to consequential actions;

(iii) the potential for the covered algorithm to produce a harm;

(iv) the potential for the covered algorithm to result in disparate treatment or effects on the basis of protected characteristics; and

(v) appropriate risk mitigation measures.

(B) This evaluation shall include a detailed review and description, sufficient for a person having ordinary skill in the art to understand the functioning, risks, uses, benefits, limitations, and other pertinent attributes of the covered algorithm, including—

(i) the purpose of the covered algorithm;

(ii) intended benefits, limitations, uses, and deployment contexts, including a description of the baseline process being enhanced or replaced by the covered algorithm if applicable;

(iii) the covered algorithm's methodology;

(iv) the inputs the covered algorithm is designed to use;

(v) the outputs the covered algorithm is designed to produce and actually produces in testing;

(vi) how the covered algorithm was trained and tested, including—

(I) measures used to test performance of the covered algorithm; and

(II) defined benchmarks and goals that correspond to those measurements, including whether there was sufficient training and testing on demographic groups that are reasonably likely to use or be affected by the covered algorithm;

(vii) the necessity and proportionality of the methodology of the covered algorithm in relation to its stated purpose;

(viii) alternatives and recommendations to prevent or mitigate harm;

(ix) what reasonable steps to search for and implement less discriminatory alternatives to the covered algorithm were taken;

(x) any consultation with relevant stakeholders;

(xi) which, protected characteristics were used, if any, for testing and evaluation, and how and why they were used;

(xii) any other algorithmic system incorporated into the development of the covered algorithm, regardless of whether such precursor algorithmic system itself involves a consequential action;

(xiii) the data used to develop, test, maintain, or update the covered algorithm, including—

(I) the types of data used, from where the data was collected, and how the data was collected, inferred, and processed;

(II) the legal authorization for collecting and processing the data, including any affirmative express consents provided by individuals to whom any data pertains and limitations placed on the use of such data; and

(III) an explanation of how the data used is representative, proportional, and appropriate to the development and intended uses of the covered algorithm; and

(xiv) other pertinent development and risk mitigation information as prescribed by rules promulgated by the Federal Trade Commission pursuant to section 553 of title 5, United States Code.

(C) The independent auditor shall produce a report of its findings and recommendations to the developer.

(3) DEPLOYER FULL PRE-DEPLOYMENT EVALUATION.—

(A) A deployer shall engage an independent auditor to evaluate—

(i) the manner in which the covered algorithm will be used to make or contribute to consequential actions;

(ii) the potential for the covered algorithm to produce a harm;

(iii) the potential for the covered algorithm to result in disparate treatment or effects on the basis of protected characteristics; and

(iv) appropriate risk mitigation measures.

(B) This evaluation shall include a detailed review and description, sufficient for a person having ordinary skill in the art to understand the functioning, risks, uses, benefits, limitations, and other pertinent attributes of the covered algorithm, including—

(i) the purpose for which the covered algorithm will be deployed;

(ii) the necessity and proportionality of the covered algorithm in relation to its planned use, including intended benefits, limitations, and a description of the baseline process being enhanced or replaced by the covered algorithm if applicable;

(iii) the inputs that the deployer plans to use, including—

(I) the types of data to be used and how the data will be collected, inferred, and processed;

(II) the legal authorization for collecting and processing the data, including any affirmative express consents provided by individuals to whom any data pertains and limitations placed on the use of such data; and

(III) an explanation of how the data used is representative, proportional, and appropriate to the deployment of the covered algorithm;

(iv) the outputs the covered algorithm is expected to produce;

(v) the potential for the covered algorithm to produce a harm in the context in which the covered algorithm will be deployed;

(vi) alternatives and recommendations to prevent or mitigate harm in the context in which the covered algorithm will be deployed;

(vii) a description of any consultation with relevant stakeholders; and

(viii) other pertinent development and risk mitigation information as prescribed by rules promulgated by the Federal Trade Commission pursuant to section 553 of title 5, United States Code.

(C) The independent auditor shall produce a report of its findings and recommendations to the deployer.

(b) DEPLOYER ANNUAL IMPACT ASSESSMENTS.—A deployer that uses a covered algorithm in interstate commerce shall annually conduct an impact assessment as follows:

(1) PRELIMINARY ASSESSMENT.—As a first step, the deployer shall evaluate whether it is plausible that the use of the covered algorithm over the preceding year resulted in harm. If it is not plausible, the deployer shall record a finding of no plausible impact. If it is plausible, the deployer shall proceed to conduct a full impact assessment.

(2) FULL IMPACT ASSESSMENT.—A deployer shall engage an independent auditor to assess the impact of the covered algorithm over the preceding year.

(A) This assessment shall include—

(i) a statement of the purpose of the covered algorithm and its intended benefits, uses, and deployment contexts;

(ii) a detailed description of the types of data inputted into the covered algorithm, including—

(I) documentation of how input data is represented and complete descriptions of each field;

(II) the types of data processed and how the data was collected, inferred, and processed;

(III) the legal authorization for collecting and processing the data, including any affirmative express consents provided by individuals to whom any data pertains and limitations placed on the use of such data;

(IV) an explanation of how the data used is representative, proportional, and appropriate to the deployment of the covered algorithm; and

(V) whether and to what extent the data inputted into the covered algorithm was used to train the covered algorithm;

(iii) the outputs produced by the covered algorithm, including whether and to what extent the covered algorithm produced the outputs it was expected to produce;

(iv) a detailed description of how the covered algorithm was used to make a consequential action;

(v) whether and to what extent the covered algorithm was used and performed as the developer intended and any measures considered to evaluate use and performance;

(vi) a detailed description of the extent to which the covered algorithm produced disparate treatment or effects on the basis of protected characteristics, including the methodology for such evaluation and an explanation, if one is known, as to how the covered algorithm produced or likely produced such disparity;

(vii) the harms actually produced and reasonably likely to have been produced by the covered algorithm;

(viii) actions taken to prevent or mitigate harms, including how relevant staff are informed of, trained about, and implement such policies and practices;

(ix) alternatives and recommendations to prevent and mitigate harms going forward; and

(x) other pertinent assessment criteria and risk mitigation recommendations as prescribed by rules promulgated by the Federal Trade Commission pursuant to section 553 of title 5, United States Code.

(B) The independent auditor shall produce a report of its findings and recommendations to the deployer.

(c) DEVELOPER ANNUAL REVIEW OF ASSESSMENTS.—Within 30 days of completion of an impact assessment, a deployer shall provide the summary of the impact assessment to the developer of the covered algorithm. Annually, the developer shall conduct a review of the impact assessments from its deployers to—

(1) assess how deployers are using its covered algorithm, including whether they are using it as intended and the methodology for assessing such use;

(2) assess the types of data deployers are inputting into the covered algorithm and the types of outputs the covered algorithm is producing;

(3) assess whether deployers are complying with their contractual agreements with the developer and whether any remedial action is necessary;

(4) compare a covered algorithm's performance in real-world conditions versus pre-deployment testing, including the methodology used to evaluate such performance;

(5) assess whether the covered algorithm is causing harm or is reasonably likely to be causing harm;

(6) assess whether the covered algorithm is causing, or is reasonably likely to be causing, disparate treatment or effects on the basis of protected characteristics, and if so, how and for which protected characteristics;

(7) determine whether the covered algorithm needs modification;

(8) determine whether any other action is appropriate to ensure that the covered algorithm remains safe and effective; and

(9) undertake any other assessments and responsive actions as prescribed by rules promulgated by the Federal Trade Commission pursuant to section 553 of title 5, United States Code.

(d) COMBINING DEVELOPER AND DEPLOYER OBLIGATIONS.—If a person is both the developer and deployer of a covered algorithm, they may conduct combined pre-deployment evaluations and annual assessments so long as each combined evaluation or assessment satisfies all requirements for both developers and deployers.

(e) REPORTING AND RETENTION REQUIREMENTS.—

(1) REPORTING.—A developer or deployer that conducts a full pre-deployment evaluation, full annual impact assessment, or developer review of assessments shall—

(A) submit the evaluation, assessment, or review to the Federal Trade Commission within 30 days of completion;

(B) upon request, make the evaluation, assessment, or review available to Congress; and

(C) publish a summary of the evaluation, assessment, or review on their website in a manner that is easily accessible to individuals and submit such summaries to the Federal Trade Commission within 30 days of completion.

(2) RETENTION.—A developer or deployer shall retain all pre-deployment evaluations and impact assessments, whether preliminary or full, and developer reviews, for at least five years.

(3) TRADE SECRETS AND PRIVACY.—A developer or deployer may redact and segregate any trade secret (as defined in section 1839 of title 18, United States Code) from public disclosure under this section. A developer or deployer shall redact and segregate personal data from public disclosure under this subsection.

(f) RULEMAKING.—

(1) IN GENERAL.—The Federal Trade Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations implementing this section.

(2) SUMMARIES.—Within 18 months of the date of enactment of this Act, the Federal Trade Commission shall promulgate rules, pursuant to section 553 of title 5, United States Code, specifying what information a deployer or developer shall include and shall not include in a summary of an evaluation, assessment, or developer review. In such rules, the Federal Trade Commission shall consider the need to protect the privacy of personal data as well as the need for information sharing by deployers and developers to execute this section and inform the public. For summaries submitted by deployers to developers for developer annual reviews of assessments, the Federal Trade Commission shall specify the extent to and process by which a developer may request additional information from the deployer and the purposes for which a developer is permitted to use such additional information.

SEC. 103. DECEPTION AND VOTING.

(a) IN GENERAL.—It shall be unlawful for a developer or deployer to use a covered algorithm in a manner that intentionally deprives, defrauds, or attempts to deprive or defraud any individual of the right to vote in a Federal, State, or local election, including—

(1) intentional deception regarding—

(A) the time, place, or method of voting or registering to vote;

(B) the eligibility requirements to vote or register to vote;

(C) the counting and canvassing of ballots;

(D) the adjudication of elections;

(E) explicit endorsements by any person or candidate; or

(F) any other material information pertaining to the procedures or requirements for voting or registering to vote in a Federal, State, or local election; or

(2) intentionally using deception, threats, intimidation, fraud, or coercion to prevent, interfere with, retaliate against, deter, or attempt to prevent, interfere with, retaliate against, or deter an individual from—

(A) registering to vote;

(B) voting in a Federal, State, or local election;

(C) supporting or advocating for a candidate in a Federal, State, or local election; or

(D) serving as or executing the responsibilities of an election worker, including processing or scanning ballots, or tabulating, canvassing, or certifying voting results.

TITLE II – DUTY OF CARE

SEC. 201. DUTY OF CARE.

(a) IN GENERAL.—It shall be unlawful for a developer or deployer to offer, license, or use a covered algorithm in a manner that is not safe and effective.

(b) SAFE.—For purposes of subsection (a), a covered algorithm is safe if—

(1) the developer or deployer has taken reasonable measures to prevent and/or mitigate harms identified by a pre-deployment evaluation or impact assessment as stipulated in Section 102 (a) and 102 (b);

(2) use of the covered algorithm as intended is not likely to result in a violation of this Act; and

(3) the developer or deployer evaluates the possibility of not offering, licensing, or using the covered algorithm or removing a covered algorithm from use, and reasonably concludes that—

(A) use of the covered algorithm is not likely to result in substantial harm to individuals;

(B) the benefits to individuals affected by the covered algorithm likely outweigh the costs to such individuals;

(C) individuals can reasonably avoid being affected by the covered algorithm; and

(D) use of the covered algorithm is not likely to result in deceptive practices.

(c) EFFECTIVE.—For purposes of subsection (a), a covered algorithm is effective if the developer or deployer has taken reasonable steps to ensure that—

(1) the covered algorithm functions at a level that would be considered reasonable performance by a person with ordinary skill in the art;

(2) the covered algorithm functions in a manner that is consistent with its expected performance and publicly advertised performance;

(3) the covered algorithm functions in a manner that is consistent with any publicly advertised purpose or use; and

(4) any data used in the design, development, deployment, or use of covered algorithms is relevant and appropriate to the deployment context and the publicly advertised purpose.

(d) DECEPTIVE MARKETING OF A PRODUCT OR SERVICE.—A developer or deployer shall not engage in deceptive advertising, marketing, or other public statements regarding a covered algorithm that they develop or deploy.

(e) OFF-LABEL USE.—It shall be unlawful for a developer to knowingly offer or license a covered algorithm for any use other than an intended use evaluated in the pre-deployment evaluation.

(f) ABNORMALLY DANGEROUS ACTIVITIES.—It shall be unlawful for a developer or deployer to offer, license, or use a covered algorithm to engage in an abnormally dangerous activity.

SEC. 202. GOVERNANCE.

(a) IN GENERAL.—A deployer or developer shall establish, document, implement, and maintain a governance program that contains reasonable administrative and technical safeguards to map, measure, manage, and govern the reasonably foreseeable risks of harm associated with the use or intended use of a covered algorithm, including all compliance measures required under this Act. The safeguards required by this subsection shall be appropriate to—

(1) the use or intended use of the covered algorithm;

(2) the deployer's or developer's role as a deployer or developer;

(3) the size, resources, and sophistication of the deployer or developer;

(4) the nature, context, and scope of the activities of the deployer or developer in connection with the covered algorithm;

(5) the volume, nature, and sensitivity of the data collected or processed by the covered algorithm;

(6) the current state of the art (and limitations thereof) in administrative and technical safeguards; and

(7) the technical feasibility and cost of available tools, assessments, and other means used by a deployer or developer to map, measure, manage, and govern the risks associated with a covered algorithm.

(b) The governance program of a large business shall:

(1) Designate an executive officer who shall annually certify to the Federal Trade Commission in good faith that the developer or deployer is compliant with this Act.

(2) Identify and implement safeguards to address reasonably foreseeable risks of harm resulting from the use or intended use of a covered algorithm.

(3) Conduct an annual and comprehensive review of policies, practices, and procedures to ensure compliance with this Act.

(4) Evaluate and make reasonable adjustments to administrative and technical safeguards in light of material changes in technology, the risks associated with the covered algorithm, the state of technical standards, and changes in business arrangements or operations of the deployer or developer.

(5) Ensure that covered algorithms are developed and deployed with consultation from communities likely to be affected by the covered algorithm, other relevant stakeholders, and domain experts to identify concerns, risks, and potential impacts of the system.

(6) Provide for ongoing training and education for all relevant employees, contractors, or other agents regarding reasonably foreseeable risks of harms associated with the use of a covered algorithm and any improved methods of developing or performing pre-deployment evaluations or impact assessments based on industry best practices.

(c) REQUIREMENTS.—A certification submitted under subsection (b) shall be based on a review of the effectiveness of the internal controls and reporting structures of the large business that is conducted by the certifying executive officer not more than 90 days before the submission of the certification. A certification submitted under subsection (b) 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.

SEC. 203. RELATIONSHIPS BETWEEN DEVELOPERS AND DEPLOYERS.

(a) DEVELOPER RESPONSIBILITIES.—A developer shall—

(1) assist a deployer in responding to a request made by an individual under this Act, by either—

(A) providing appropriate technical and organizational measures, taking into account the nature of the processing and the information reasonably available to the developer, for the deployer to comply with such a request; or

(B) fulfilling a request by a deployer to execute an individual rights request that the deployer has determined should be complied with, by—

(i) complying with the request pursuant to the deployer's instructions; or

(ii) providing written verification to the deployer that it does not hold personal 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 303;

(2) upon the reasonable request of the deployer, make available to the deployer information necessary to demonstrate the compliance of the deployer with the requirements of this Act, which may include making available a report of the pre-deployment evaluation or annual review of assessments conducted by the developer and providing information necessary to enable the deployer to conduct and document an impact assessment or pre-deployment evaluation required by Section 102 (a) and (b);

(3) at the deployer's direction, delete or return all personal data to the deployer as requested at the end of the provision of services, unless retention of the personal data is required by law; and

(4) allow and cooperate with reasonable assessments by the deployer or the deployer's designated assessor; alternatively, the developer may arrange for a qualified and independent assessor to conduct an assessment of the developer's policies and technical and organizational measures in support of the obligations under this Act using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The developer shall provide a report of such assessment to the deployer upon request.

(b) CONTRACTS BETWEEN DEVELOPERS AND DEPLOYERS.—

(1) REQUIREMENTS.—A developer may only offer or license a covered algorithm to a deployer pursuant to a written contract between the developer and deployer, and only if the contract—

(A) sets forth the data processing procedures of the developer with respect to collection, processing, or transfer performed on behalf of the deployer;

(B) clearly sets forth—

(i) instructions for collecting, processing, or transferring data;

(ii) instructions for deploying the covered algorithm as intended;

(iii) the nature and purpose of collecting, processing, or transferring;

(iv) the type of data subject to collecting, processing, or transferring;

(v) the duration of processing; and

(vi) the rights and obligations of both parties, including a method by which the developer shall notify the deployer of material changes to its privacy practices or its covered algorithm;

(C) does not relieve a developer or deployer of any requirement or liability imposed on such developer or deployer under this Act; and

(D) prohibits both the developer and deployer from combining data received from or collected on behalf of the other party with data the developer or deployer received from or collected on behalf of another party, if such combining is not necessary to effectuate a purpose described in Section 301(c).

(2) CONTRACT TERMS.—Each developer shall retain copies of previous contracts entered into in compliance with this subsection with each deployer to which it provides requested products or services.

(c) THIRD PARTIES.—

(1) A third party shall not process or transfer personal data received from a developer or deployer for a purpose other than contracted. Third parties may reasonably rely on representations made by the developer or deployer that transferred the personal data if the third party conducts reasonable due diligence on the representations of the developer or deployer and finds those representations to be credible.

(2) RULEMAKING.—Not later than 2 years after the date of enactment of this Act, the Federal Trade Commission shall promulgate rules pursuant to section 553 of title 5, United States Code, regarding compliance with this subsection, taking into consideration the burdens on developers, deployers, and third parties meeting the requirements of this section.

(d) RULE OF CONSTRUCTION.—Solely for the purposes of this section, the requirements for developers to contract with, assist, and follow the instructions of deployers shall be read to include requirements to contract with, assist, and follow the instructions of a government entity if the developer is providing a service to a government entity.

SEC. 204. HUMAN ALTERNATIVES AND OTHER PROTECTIONS.

(a) RIGHT TO HUMAN ALTERNATIVES.—

(1) Within 2 years of the Effective Date of this Act, the Federal Trade Commission shall promulgate rules pursuant to section 553 of title 5, United States Code, identifying the circumstances and manner in which a deployer shall provide individuals with a means of opting-out of the use of a covered algorithm with regard to a consequential action concerning the individual, and to instead have such consequential action undertaken by a human.

(2) When promulgating rules pursuant to paragraph (a)(1), the Federal Trade Commission shall consider—

(A) how to ensure that notices and requests are clear and conspicuous, in plain language, easy to execute, and at no cost to individuals;

(B) specific types of consequential actions for which a human alternative is appropriate, considering magnitude of the action and risk of harm;

(C) the extent to which a human alternative would be beneficial to individuals and the public interest;

(D) the extent to which a human alternative can prevent or mitigate harm;

(E) risks of harm to individuals beyond the requestor if a human alternative is allowed or not allowed;

(F) the technical and economic feasibility of providing a human alternative in different circumstances;

(G) how to ensure that notices to individuals are effective, timely, and useful; and

(H) any other considerations the Federal Trade Commission deems appropriate to balance the need to give individuals' control over consequential actions related to them with considerations of practical feasibility and effectiveness.

(b) INDIVIDUAL AUTONOMY.—

(1) A developer or deployer may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of any individual right under this Act or individual choice 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 right.

(c) RIGHT TO APPEAL.—

(1) Within 2 years of the Effective Date of this Act, the Federal Trade Commission shall promulgate rules pursuant to section 553 of title 5, United States Code, identifying the circumstances and manner in which a developer or deployer shall provide individuals with a means to appeal to a human a consequential action resulting from the developer or deployer's use of a covered algorithm.

(2) When promulgating the rules pursuant to paragraph (c)(1), the Federal Trade Commission shall—

(A) ensure that the appeal mechanism is clear and conspicuous, in plain language, easy-to-execute, and no cost to individuals;

(B) ensure that the appeal mechanism is proportionate to the consequential action;

(C) ensure that the appeal mechanism is reasonably accessible, timely, usable, effective, and non-discriminatory;

(D) require, where appropriate, a mechanism for individuals to identify and correct any personal data used by the covered algorithm;

(E) specify training requirements for human reviewers; and

(F) consider any other circumstances, procedures, and other matters the Federal Trade Commission deems appropriate to balance the need to give individuals a right to appeal consequential actions related to them with considerations of practical feasibility and effectiveness.

(d) PROHIBITION OF RETALIATION.—

(1) A developer or deployer shall not discriminate or retaliate against an individual because the individual exercised any of their rights under this Act or refused to waive any of their rights under this Act, including, but not limited to, by actually denying or threatening to deny equal enjoyment of goods, services, or other activities or opportunities in relation to a consequential action.

(2) Nothing in this subsection shall prohibit a developer or deployer from denying service, charging an individual a different price or rate, or providing a different level or quality of goods or services to the consumer, if that differential in service is necessary and directly related to the value provided to the developer or deployer by the covered algorithm.

(3) This subsection does not prohibit a developer or deployer from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this Act.

(e) WHISTLEBLOWER PROTECTION.—A developer or deployer may not, directly or indirectly, discharge, demote, suspend, threaten, harass, or in any other manner discriminate or retaliate against an individual for reporting or attempting to report a violation of this Act.

TITLE III – DATA SECURITY

SEC. 301. DATA MINIMIZATION.

(a) DEPLOYER DATA MINIMIZATION, IN GENERAL.—A deployer may not collect, process, or transfer personal data unless the collection, processing, or transfer is limited to what is necessary and proportionate to—

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

(2) effect a purpose permitted under subsection (c).

(b) DEVELOPER DATA MINIMIZATION, IN GENERAL.—A developer may not collect, process, or transfer personal data unless the collection, processing, or transfer is limited to what is necessary and proportionate to—

(1) develop a specific covered algorithm, to the extent the individual to whom the data pertains has given affirmative express consent for development of that specific covered algorithm; or

(2) effect a purpose permitted under subsection (c).

(c) PERMISSIBLE PURPOSES.—A developer or deployer may collect, process, or transfer personal data for any of the following purposes if the collection, processing, or transfer is limited to what is necessary and proportionate to such purpose:

(1) 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.

(2) With respect to personal data previously collected in accordance with this Act, notwithstanding this provision—

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

(B) to develop, maintain, repair, or enhance a product or service for which such data was collected, not including the development of a covered algorithm;

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

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

(E) to protect against spam; or

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

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

(4) To fulfill a product or service warranty.

(5) To prevent, detect, protect against, or respond to a security incident. For purposes of this paragraph, the term "security" is defined as network security, medical alerts, fire alarms, access control security, and natural disaster response. This paragraph does not permit, however, the transfer of personal data for payment or other valuable consideration to a government entity.

(6) To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity. For purposes of this paragraph, 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. This paragraph does not permit, however, the transfer of personal data for payment or other valuable consideration to a government entity.

(7) To comply with a legal obligation imposed by Federal, Tribal, State, or local law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the developer or deployer.

(8) To prevent an individual, or group of individuals, from suffering harm where the developer or deployer believes in good faith that the individual, or group of individuals, is at risk of death, serious physical injury, or other serious health risk. This paragraph does not permit, however, the transfer of personal data for payment or other valuable consideration to a government entity.

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

(10) —

(A) 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.

(B) Not later than 18 months after the date of enactment of this Act, the Federal Trade Commission should issue guidelines to help deployers ensure the privacy of affected users and the security of personal data, particularly as data is being transferred to and stored by researchers. Such guidelines should consider risks as they pertain to projects using personal 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.

(11) 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 developer or deployer.

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

(13) 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 developer or deployer's assets, only if the developer or deployer, in a reasonable time prior to such transfer, provides each affected individual with—

(A) a notice describing such transfer, including the name of the entity or entities receiving the individual's personal data and their privacy policies as described in Section 401; and

(B) a reasonable opportunity to withdraw any previously given affirmative express consents in accordance with the requirements of Section 301 (b) and Section 401 (e).

(14) To conduct a pre-deployment evaluation, impact assessment, or developer review consistent with Section 102.

(15) To ensure the data security and integrity of personal data, as described in Section 302 and Section 303.

(d) RULEMAKING.—The Federal Trade Commission shall have authority to promulgate rules implementing this section pursuant to section 553 of title 5, United States Code.

SEC. 302. DATA SECURITY AND PROTECTION OF PERSONAL DATA.

(a) ESTABLISHMENT OF DATA SECURITY PRACTICES.—

(1) IN GENERAL.—A developer or deployer shall establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and secure personal data against unauthorized access and acquisition.

(2) CONSIDERATIONS.—The reasonable administrative, technical, and physical data security practices required under paragraph (1) shall be appropriate to—

(A) the size and complexity of the developer or deployer;

(B) the nature and scope of the developer or deployer's collecting, processing, or transferring of personal data;

(C) the volume and nature of the personal data collected, processed, or transferred by the developer or deployer;

(D) the sensitivity of the personal data collected, processed, or transferred;

(E) the current state of the art (and limitations thereof) in administrative, technical, and physical safeguards for protecting such personal data; and

(F) the cost of available tools to improve security and reduce vulnerabilities to unauthorized access and acquisition of such personal data in relation to the risks and nature of the personal data.

(b) SPECIFIC REQUIREMENTS.—The data security practices of the developer and deployer required under subsection (a) shall include, for each respective entity's own system or systems, at a minimum, the following practices:

(1) ASSESS VULNERABILITIES.—Identifying and assessing any material internal and external risk to, and vulnerability in, the security of each system maintained by the developer or deployer that collects, processes, or transfers personal data, or a third party that collects, processes, or transfers personal data on behalf of the developer or deployer, including unauthorized access to or risks to such personal data, human vulnerabilities, access rights, and the use of third parties. With respect to large business, such activities shall include a plan to receive and reasonably respond to unsolicited reports of vulnerabilities by any entity or individual and by performing a reasonable investigation of such reports.

(2) PREVENTIVE AND CORRECTIVE ACTION.—Taking preventive and corrective action designed to mitigate reasonably foreseeable risks or vulnerabilities to personal data identified by the developer or deployer, consistent with the nature of such risk or vulnerability and the developer or deployer'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.

(3) EVALUATION OF PREVENTIVE AND CORRECTIVE ACTION.—Evaluating and making reasonable adjustments to the action described in paragraph (2) in light of any material changes in technology, internal or external threats to personal data, and the developer or deployer's own changing business arrangements or operations.

(4) INFORMATION RETENTION AND DISPOSAL.—Disposing of personal data in accordance with a retention schedule that shall require the deletion of personal 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 personal data to make such data permanently unreadable or indecipherable and unrecoverable to ensure ongoing compliance with this section. Third parties shall establish practices to delete or return personal data to a developer or deployer as requested at the end of the provision of services unless retention of the personal data is required by law, consistent with Section 303.

(5) TRAINING.—Training each employee with access to personal data on how to safeguard personal data and updating such training as necessary.

(6) DESIGNATION.—Designating an officer, employee, or employees to maintain and implement such practices.

(7) INCIDENT RESPONSE.—Implementing procedures to detect, respond to, or recover from security incidents, including breaches.

(c) REGULATIONS.—The Federal Trade Commission may promulgate, in accordance with section 553 of title 5, United States Code, technology-neutral regulations to establish processes for complying with this section. The Federal Trade Commission shall consult with the National Institute of Standards and Technology in establishing such processes.

SEC. 303. INDIVIDUAL DATA OWNERSHIP AND CONTROL.

(a) ACCESS TO, AND CORRECTION, DELETION, AND PORTABILITY OF, PERSONAL DATA.—In accordance with subsections (b) and (c), a developer or deployer shall provide an individual, after receiving a verified request from the individual, with the right to—

(1) access—

(A) in a human and machine-readable format that a reasonable individual can understand and download from the internet, the personal data (except personal data in a back-up or archival system) of the individual making the request that is collected, processed, or transferred by the developer or deployer or any service provider of the developer or deployer within the 24 months preceding the request;

(B) the categories of any third party, if applicable, and an option for consumers to obtain the names of any such third party as well as and the categories of any service providers to whom the developer or deployer has transferred for consideration the personal data of the individual, as well as the categories of sources from which the personal data was collected; and

(C) a description of the purpose for which the developer or deployer transferred the personal data of the individual to a third party or service provider;

(2) correct any verifiable substantial inaccuracy or substantially incomplete information with respect to the personal data of the individual that is processed by the developer or deployer and instruct the developer or deployer to make reasonable efforts to notify all third parties or service providers to which the developer or deployer transferred such personal data of the corrected information;

(3) delete personal data of the individual that is processed by the developer or deployer and make reasonable efforts to notify all third parties to which the developer or deployer transferred such personal data of the individual's deletion request; and

(4) to the extent technically feasible, export to the individual or directly to another entity the personal data of the individual that is processed by the developer or deployer, including inferences linked or reasonably linkable to the individual but not including other derived data, without licensing restrictions that limit such transfers in—

(A) a human-readable format that a reasonable individual can understand and download from the internet; and

(B) a portable, structured, documented, interoperable, and machine-readable format.

(b) INDIVIDUAL AUTONOMY.—A developer or deployer may not condition, effectively condition, attempt to condition, or attempt to effectively condition the exercise of a right described in subsection (a) through—

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

(2) 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 right.

(c) TIMING.—

(1) IN GENERAL.—Subject to subsections (d) and (e), each request under subsection (a) shall be completed by any—

(A) large business within 5 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual; or

(B) developer or deployer that is not a large business within 30 days of such request from an individual, unless it is demonstrably impracticable or impracticably costly to verify such individual.

(2) EXTENSION.—A response period set forth in this subsection may be extended once by 30 additional days when reasonably necessary, considering the complexity and number of the individual's requests, so long as the developer or deployer informs the individual of any such extension within the initial response period, together with the reason for the extension.

(d) FREQUENCY AND COST OF ACCESS.—A developer or deployer—

(1) shall provide an individual with the opportunity to exercise each of the rights described in subsection (a); and

(2) with respect to—

(A) the first 2 times that an individual exercises any right described in subsection (a) in any 12-month period, shall allow the individual to exercise such right at no cost; and

(B) any time beyond the initial 2 times described in subparagraph (A), may allow the individual to exercise such right for a fee, reasonably related to the cost to the developer or deployer for complying with such request, for each request.

(e) VERIFICATION AND EXCEPTIONS.—

(1) REQUIRED EXCEPTIONS.—A developer or deployer may not permit an individual to exercise a right described in subsection (a), in whole or in part, if the developer or deployer—

(A) cannot reasonably verify that the individual making the request to exercise the right is the individual whose personal data is the subject of the request or an individual authorized to make such a request on the individual's behalf;

(B) reasonably believes that the request is made to interfere with a contract between the developer or deployer and another individual;

(C) determines that the exercise of the right would require access to or correction of another individual's personal data;

(D) reasonably believes that the exercise of the right would require the developer or deployer to engage in an unfair or deceptive practice under section 5 of the Federal Trade Commission Act (15 U.S.C. 45); or

(E) reasonably believes that the request is made to further fraud, support criminal activity, or the exercise of the right presents a data security threat.

(2) ADDITIONAL INFORMATION.—If a developer or deployer cannot reasonably verify that a request to exercise a right described in subsection (a) is made by the individual whose personal data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the developer or deployer—

(A) may request that the individual making the request to exercise the right provide any additional information necessary for the sole purpose of verifying the identity of the individual; and

(B) may not process or transfer such additional information for any other purpose.

(3) PERMISSIVE EXCEPTIONS.—

(A) IN GENERAL.—A developer or deployer may decline, with adequate explanation to the individual, to comply with a request to exercise a right described in subsection (a), in whole or in part, that would—

(i) require the developer or deployer to retain any personal data collected for a single, one-time transaction, if such personal data is not processed or transferred by the developer or deployer for any purpose other than completing such transaction;

(ii) be demonstrably impracticable or prohibitively costly to comply with, and the developer or deployer shall provide a description to the requestor detailing the inability to comply with the request;

(iii) require the developer or deployer to attempt to re-identify de-identified data;

(iv) require the developer or deployer to maintain personal data in an identifiable form or collect, retain, or access any data in order to be capable of associating a verified individual request with personal data of such individual;

(v) result in the release of trade secrets or other privileged or confidential business information;

(vi) require the developer or deployer to correct any personal data that cannot be reasonably verified as being inaccurate or incomplete;

(vii) interfere with a valid law enforcement request, 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 developer or deployer from being able to maintain a confidential record of deletion requests, maintained solely for the purpose of preventing personal data of an individual from being recollected after the individual submitted a deletion request and requested that the developer or deployer no longer collect, process, or transfer such data;

(x) fall within an exception enumerated in the regulations promulgated by the Federal Trade Commission pursuant to subparagraph (D); or

(xi) with respect to requests for deletion—

(I) unreasonably interfere with the provision of products or services by the developer or deployer to another person it currently serves;

(II) delete personal data that relates to a public figure and for which the requesting individual has no reasonable expectation of privacy;

(III) delete personal data reasonably necessary to perform a contract between the developer or deployer and the individual;

(IV) delete personal data that the developer or deployer needs to retain in order to comply with professional ethical obligations;

(V) delete personal data that the developer or deployer reasonably believes may be evidence of unlawful activity or an abuse of the developer or deployer's products or services; or

(VI) 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 personal data that would unreasonably interfere with the provision of education services by or the ordinary operation of the school or institution.

(B) PARTIAL COMPLIANCE.—In a circumstance that would allow a denial pursuant to subparagraph (A), a developer or deployer shall partially comply with the remainder of the request if it is possible and not unduly burdensome to do so.

(C) NUMBER OF REQUESTS.—For purposes of subparagraph (A)(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.

(D) FURTHER EXCEPTIONS.—The Federal Trade Commission may, by regulation as described in subsection (g), establish additional permissive exceptions necessary to protect the rights of individuals, alleviate undue burdens on covered entities, prevent unjust or unreasonable outcomes from the exercise of access, correction, deletion, or portability rights, or as otherwise necessary to fulfill the purposes of this section. In establishing such exceptions, the Federal Trade Commission should consider any relevant changes in technology, means for protecting privacy and other rights, and beneficial uses of personal data by developers or deployers.

(f) REGULATIONS.—Not later than 2 years after the date of enactment of this Act, the Federal Trade Commission shall promulgate regulations, pursuant to section 553 of title 5, United States Code, as necessary to establish processes by which developers and deployers are to comply with the provisions of this section. Such regulations shall take into consideration—

(1) the size of, and the nature, scope, and complexity of the activities engaged in by the developer or deployer, including whether the developer or deployer is a large business or nonprofit organization;

(2) the sensitivity of personal data collected, processed, or transferred by the developer or deployer;

(3) the volume of personal data collected, processed, or transferred by the developer or deployer;

(4) the number of individuals and devices to which the personal data collected, processed, or transferred by the developer or deployer relates; and

(5) after consulting the National Institute of Standards and Technology, standards for ensuring the deletion of personal data under this Act where appropriate.

(g) ACCESSIBILITY.—A developer or deployer shall facilitate the ability of individuals to make requests under subsection (a) in any covered language in which the developer or deployer provides a product or service. The mechanisms by which a developer or deployer enables individuals to make requests under subsection (a) shall be readily accessible and usable by individuals with disabilities.

TITLE IV – TRANSPARENCY

SEC. 401. NOTICE AND DISCLOSURE.

(a) IN GENERAL.—Each developer or deployer shall make publicly available, in a clear, conspicuous, not misleading, plain language, and easy-to-read and readily accessible manner, a disclosure that provides a detailed and accurate representation of its practices with regard to the collection, processing, and transfer of personal data.

(b) CONTENT OF DISCLOSURE.—A developer or deployer shall publish a disclosure that includes, at a minimum, the following:

(1) The identity and the contact information of—

(A) the developer or deployer to which the disclosure applies (including the developer or deployer's points of contact and generic electronic mail addresses, as applicable for inquiries concerning the covered algorithm or related to individual rights under this Act); and

(B) any other entity within the same corporate structure as the developer or deployer to which personal data is transferred by the deployer.

(2) A link to the website containing the developer or deployer's summaries of pre-deployment evaluations, full annual impact assessments, or developer review of assessments.

(3) The categories of personal data the developer or deployer collects or processes.

(4) The processing purposes for each category of personal data the developer or deployer collects or processes.

(5) Whether the developer or deployer transfers personal data and, if so, each third party to which the deployer transfers personal data, and the purposes for which such data is transferred to such categories of third parties including government entities, except for a transfer to a governmental entity pursuant to a court order or law that prohibits the developer or deployer from disclosing such transfer.

(6) The length of time the developer or deployer intends to retain each category of personal data, or, if it is not possible to identify that timeframe, the criteria used to determine the length of time the developer or deployer intends to retain categories of personal data.

(7) A prominent description of how an individual can exercise the rights described in this Act.

(8) A general description of the developer or deployer's practices for compliance with Section 201, Section 301, Section 302, and Section 303.

(9) The effective date of the disclosure.

(10) Whether or not any personal data collected by the developer or deployer is transferred to, processed in, stored in, or otherwise accessible to the People's Republic of China, Russia, Iran, or North Korea.

(c) LANGUAGES.—The disclosure required under subsection (a) shall be made available to the public in each covered language in which the developer or deployer operates or provides service.

(d) ACCESSIBILITY.—The developer or deployer shall also provide the disclosures under this section in a manner that is reasonably accessible to and usable by individuals with disabilities.

(e) MATERIAL CHANGES.—

(1) AFFIRMATIVE EXPRESS CONSENT.—If a developer or deployer makes a material change to its disclosure, the developer or deployer shall notify each individual affected by such material change before implementing the material change with respect to any prospectively collected personal data and, except as provided in Section 301 (c), provide a reasonable opportunity for each individual to withdraw previously given consents to any further materially different collection, processing, or transfer of previously collected personal data under the changed policy.

(2) NOTIFICATION.—The developer or deployer shall take all reasonable electronic measures to provide direct notification regarding material changes to the disclosure to each affected individual, in each covered language in which the disclosure is made available, and taking into account available technology and the nature of the relationship.

(3) LOG OF MATERIAL CHANGES.—Each developer or deployer shall retain copies of previous versions of its disclosure for at least 10 years beginning after the date of enactment of this Act and publish them on its website. Such developer or deployer 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 disclosure 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 paragraph shall not apply to any previous versions of a developer or deployer's disclosure, or any material changes to such disclosure, that precede the date of enactment of this Act.

(f) SHORT-FORM NOTICE

(1) IN GENERAL.—A developer or deployer shall provide a short-form notice regarding a covered algorithm it develops, offers, licenses, or uses in a manner that is—

(A) concise, clear, conspicuous, in plain language, and not misleading;

(B) readily accessible to the individual

(i) for a deployer, based on what is reasonably anticipated within the context of the relationship between the individual and the deployer; or

(ii) for a developer, based on the expectations of a reasonable person who is likely to be affected by the covered algorithm;

(C) inclusive of an overview of individual rights and disclosures to draw attention to data practices that may be unexpected to a reasonable person or that involve a consequential action; and

(D) no more than 500 words in length.

(2) If a developer or deployer has a relationship with an individual, the developer or deployer shall provide the short-form notice to that individual upon the individual's first interaction with the covered algorithm. If a developer or deployer does not have a relationship with the individual, the developer or deployer shall provide the short-form notice in a clear, conspicuous, accessible, and not misleading manner on their website.

(3) RULEMAKING.—The Federal Trade 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 paragraph (1), which shall not exceed the content requirements in subsection (b) and shall include templates or models of short-form notices.

SEC. 402. EXPLANATIONS.

(a) IN GENERAL.—A deployer shall provide a clear, conspicuous, easy-to-use, no-cost, and accessible mechanism for an individual to request an explanation as to whether and how a covered algorithm used by the deployer affects or affected the individual. A deployer shall provide an explanation, upon request, in the following circumstances related to a consequential action and may choose to provide an explanation in other circumstances:

(1) An adverse action involving government benefits or services.

(2) Pre-trial detention, arrest, prosecution, bail determinations, sentencing, parole determinations, or any other matter involving the criminal justice system, immigration enforcement, child protective services, or civil enforcement by a government.

(3) An adverse action involving essential utilities.

(4) An adverse action involving housing, employment, financial services, insurance, healthcare, or education.

(5) The determination of an insurance premium or an interest rate for a loan.

(6) Any other circumstance designated by regulation pursuant to subsection (f).

(b) ADVERSE ACTION.—As used in this section, the term "adverse action" means a decision that—

(1) restricts access to or materially impairs enjoyment of an opportunity, good, service, benefit, or activity;

(2) provides or offers an opportunity, good, service, benefit, or activity in a manner materially different from the manner requested by the individual; or

(3) imposes a detriment, penalty, demerit, punishment, or other material and negative consequence on an individual.

(c) IDENTITY VERIFICATION.—A deployer shall take reasonable measures to verify the identity of a requester and to ensure that it is disclosing the explanation only to the affected individual. A deployer may request information from the requester that is necessary to validate the individual's request. Any such information obtained in this manner may not be used for any other purpose. The Federal Trade Commission may establish other requirements by regulation pursuant to subsection (f).

(d) FORMAT.—An explanation provided pursuant to this section shall be in plain language, accessible to individuals with disabilities, and available in each covered language in which the deployer operates or provides service. The Federal Trade Commission may establish other requirements by regulation pursuant to subsection (f).

(e) CONTENT OF EXPLANATION.—An explanation provided pursuant to this section shall—

(1) explain why the covered algorithm produced the result it produced for this specific individual;

(2) be truthful, accurate, and scientifically valid;

(3) identify at least the three most significant factors used to inform the decision;

(4) include a summary of an individual's rights under this act;

(5) include the developer or deployer's points of contact and electronic mail addresses, as applicable for inquiries concerning the covered algorithm or related to individual rights under this Act; and

(6) any other information designated by regulation pursuant to subsection (f).

(f) RULEMAKING.—The Federal Trade Commission may promulgate rules, pursuant to section 553 of title 5, United States Code, to implement this section.

(g) GUIDANCE.—Within 2 years of the date of enactment, the Federal Trade Commission shall publish guidance on explanations for covered algorithm decisions, including templates or models for explanations, as appropriate.

SEC. 403. CONSUMER AWARENESS.

(a) NOTICE OF CONSUMER RIGHTS.—

(1) IN GENERAL.—Not later than 90 days after the date of enactment of this Act, the Federal Trade Commission shall publish, on the public website of the Federal Trade Commission, a webpage that describes each provision, right, obligation, and requirement of this Act, listed separately for individuals and for deployers and developers, and the remedies, exemptions, and protections associated with this Act, in plain and concise language and in an easy-to-understand manner.

(2) UPDATES.—The Federal Trade Commission shall update the information published under subsection (a) on a quarterly basis as necessitated by any change in law, regulation, guidance, or judicial decisions.

(3) ACCESSIBILITY.—The Federal Trade Commission shall publish the information required to be published under subsection (a) in the ten languages with the most users in the United States, according to the most recent United States Census.

(b) ANNUAL REPORT.—

(1) Not later than 2 years after the effective date described in this section, and annually thereafter, the Federal Trade Commission shall publish publicly on the website of the Federal Trade Commission a report describing and summarizing the information from pre-deployment evaluations, impact assessments, and developer reviews submitted to it by developers and deployers that—

(A) is accessible and machine readable in accordance with the 21st Century Integrated Digital Experience Act (44 U.S.C. 3501 note); and

(B) describes broad trends, aggregated statistics, and anonymized information about performing impact assessments of covered algorithms, for the purposes of updating guidance related to impact assessments and summary reporting, oversight, and making recommendations to other regulatory agencies.

(c) PUBLICLY ACCESSIBLE REPOSITORY.—

(1) Not later than 180 days after the Federal Trade Commission promulgates the regulations required under this annual reporting section, the Federal Trade Commission shall develop a publicly accessible repository to publish the summaries of pre-deployment evaluations, impact assessments, and developer reviews submitted to the Federal Trade Commission under Section 201.

(2) The Federal Trade Commission shall publish new summaries in the repository within 30 days of receipt unless it has good cause to delay publication.

(3) The Federal Trade Commission shall design the repository established under paragraph (1) to—

(A) be publicly available and easily discoverable on the website of the Federal Trade Commission;

(B) allow users to sort and search the repository by multiple characteristics (such as by developer or deployer and date reported) simultaneously;

(C) allow users to make a copy of or download the information obtained from the repository, including any subsets of information obtained by sorting or searching as described in clause (ii), in accordance with current guidance from the Office of Management and Budget, such as the Open, Public, Electronic, and Necessary Government Data Act (44 U.S.C. 101 note);

(D) be in accordance with user experience and accessibility best practices such as those described in the 21st Century Integrated Digital Experience Act (44 U.S.C. 3501 note); and

(E) include information about design, use, and maintenance of the repository, including any other information about the design, use, and maintenance the Federal Trade Commission determines.

SEC. 404. LABELING AI-GENERATED CONTENT.

(a) LABELING REQUIREMENTS.—

(1) IN GENERAL.—A deployer who uses a covered algorithm to generate, in whole or in part, an image, text, video, audio, or other media, and who publishes such content for a commercial purpose, shall include on any output, in a clear, conspicuous, and accessible manner a disclaimer consisting of—

(A) either—

(i) the following statement: "AI Disclaimer: This output was generated by artificial intelligence."; or

(ii) a symbol, similar in size and design to the copyright symbol, that consists of the letters "AI" in a circle; and

(B) the output's metadata information, including an identification of the media as being generated by a covered algorithm, the identity of the covered algorithm used to generate the media, and the date and time the media was created.

(2) DECEPTIVE ELECTION-RELATED CONTENT.—A deployer who uses a covered algorithm to generate, in whole or in part, an image, text, video, audio, or other media, and intentionally publishes such content, shall also include the disclaimer described in paragraph (1) if—

(A) the content depicts an image or video of a candidate for federal, state, or local office;

(B) the content includes audio simulating, altering, or distorting the voice of a candidate for federal, state, or local office; or

(C) the content depicts information about the time, place, manner, or requirements for voting or registering to vote.

(3) DEVELOPER REQUIREMENTS.—

(A) A developer who offers the ability to use a covered algorithm to generate or publish the content discussed in paragraphs (1) or (2) shall provide deployers of the covered algorithm a mechanism to comply with the labeling requirements of this section.

(B) To the extent technically feasible, a developer shall make the disclaimers required under paragraphs (1) and (2) permanent or unable to be easily removed.

(4) RULEMAKING.—Within 2 years of the Effective Date of this Act, the Federal Trade Commission shall promulgate rules, pursuant to section 553 of title 5, United States Code, regarding the time, place, manner, and other appropriate requirements for the use of this disclaimer, including accessibility for persons with disabilities. The Federal Trade Commission may also create exceptions to paragraphs (1) and (2) in specific circumstances where it would be obvious to a reasonable person that the media is a synthetic depiction of an actual item, place, person, or event.

(5) For a period of five years following the effective date of this Act, the Federal Trade Commission shall undertake reasonable efforts to educate the public about the meaning and use of the disclaimer required by this subsection. At the conclusion of such period, the Federal Trade Commission shall report to Congress on the adoption of and effectiveness of this labeling requirement.

(b) UNIFORM LABELING RESEARCH STUDY.—

(1) The Director of the National Institute of Standards and Technology shall establish a research study on matters relating to the development of uniform labeling requirements and technical standards for content generated in part or whole by a covered algorithm, including advice on—

(A) standard labeling and/or watermarking protocols across deployment contexts, including the best practices of instituting such requirements;

(B) explainability, including the ability for a reasonable individual to understand the contents of any required label;

(C) provenance, including the ability for an individual to trace the origin of content generated by covered algorithms; and,

(D) tools for detecting and authenticating content generated by covered algorithms.

(2) No later than 1 year after the date of the enactment of this Act, and not less frequently than once every 3 years thereafter, the Director of the National Institute of Standards and Technology shall submit to the President, the Federal Trade Commission, and Congress a report on the findings and recommendations under subsection (b)(1).

TITLE V – ENFORCEMENT

SEC. 501. ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF THE FEDERAL TRADE COMMISSION.—

(A) IN GENERAL.—Except as provided in paragraphs (3), (4), and (5), the Federal Trade Commission shall enforce this Act and the regulations promulgated under this Act 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 Act.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates this Act or a regulation promulgated under this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act (15 U.S.C. 41 et seq.).

SEC. 502. ENFORCEMENT BY STATES.

(a) CIVIL ACTION.—In any case in which the attorney general or State Data Protection Authority of a State has reason to believe that an interest of the residents of that State has been, may be, or is adversely affected by a violation of this Act or a regulation promulgated under this Act by a developer or deployer, the attorney general may bring a civil action in the name of the State, or as parens patriae on behalf of the residents of the State. Any such action shall be brought exclusively in an appropriate Federal district court of the United States. In such an action, a court may award—

(1) injunctive relief;

(2) damages, restitution, or other compensation on behalf of the residents of such State;

(3) civil penalties in the amount of $15,000 per violation, or 4% of defendant's average gross annual revenue over the preceding three years, whichever is greater;

(4) reasonable attorneys' fees and litigation costs; and

(5) any other relief the court deems just and reasonable.

(b) RIGHTS OF THE FEDERAL TRADE COMMISSION.—

(1) IN GENERAL.—Except as provided in paragraph (2), the attorney general or State Data Protection Authority of a State shall notify the Federal Trade Commission in writing prior to initiating a civil action under subsection (a). Such notification shall include a copy of the complaint to be filed to initiate such action. Upon receiving such notification, the Federal Trade Commission may intervene in such action as a matter of right pursuant to the Federal Rules of Civil Procedure.

(2) FEASIBILITY.—If the notification required by paragraph (1) is not feasible, the attorney general or State Privacy Authority shall notify the Federal Trade Commission immediately after initiating the civil action.

(c) RULE OF CONSTRUCTION.—Nothing in this section may be construed to prevent the attorney general of a State from exercising the powers conferred on the attorney general.

SEC. 503. PRIVATE RIGHT OF ACTION.

(a) ENFORCEMENT BY PERSONS.—

(1) IN GENERAL.—Any person or class of persons may bring a civil action against a developer or deployer for a violation of this Act or a rule promulgated pursuant to this Act in any court of competent jurisdiction.

(2) RELIEF.—In a civil action brought under paragraph (1), the court may award—

(A) treble actual damages or $15,000 per violation, whichever is greater;

(B) nominal damages;

(C) punitive damages;

(D) injunctive relief;

(E) declaratory relief;

(F) reasonable attorney's fees and litigation costs; and

(G) any other relief the court deems just and reasonable.

(3) RIGHTS OF THE FEDERAL TRADE COMMISSION AND STATE ATTORNEYS GENERAL.—

(A) IN GENERAL.—Prior to a person bringing a civil action under paragraph (1), such person shall notify the Federal Trade Commission and the attorney general of the State where such person resides in writing that such person intends to bring a civil action under such paragraph. Upon receiving such notice, the Federal Trade Commission and State attorney general shall each or jointly make a determination and respond to such person not later than 60 days after receiving such notice, as to whether they will intervene in such action pursuant to the Federal Rules of Civil Procedure. If a state attorney general does intervene, they shall only be heard with respect to the interests of the residents of their State.

(B) RETAINED AUTHORITY.—Subparagraph (A) may not be construed to limit the authority of the Federal Trade Commission or any applicable State attorney general or State Privacy Authority to later commence a proceeding or civil action or intervene by motion if the Federal Trade Commission or State attorney general does not commence a proceeding or civil action within the 60-day period.

(b) ARBITRATION AGREEMENTS AND PRE-DISPUTE JOINT ACTION WAIVERS.—

(1) PRE-DISPUTE ARBITRATION AGREEMENTS.—Notwithstanding any other provision of law, no pre-dispute arbitration agreement or pre-dispute joint action waiver is enforceable with regard to a dispute arising under this Act.

(2) DEFINITIONS.—For purposes of this subsection:

(A) PRE-DISPUTE ARBITRATION AGREEMENT.—The term "pre-dispute arbitration agreement" means any agreement to arbitrate a dispute that has not arisen at the time of the making of the agreement.

(B) PRE-DISPUTE JOINT-ACTION WAIVER.—The term "pre-dispute joint-action waiver" means an agreement, whether or not part of a pre-dispute arbitration agreement, that would prohibit or waive the right of 1 of the parties to the agreement to participate in a joint, class, or collective action in a judicial, arbitral, administrative, or other related forum, concerning a dispute that has not yet arisen at the time of the making of the agreement.

SEC. 504. NO SECTION 230 IMMUNITY.

(c) SECTION 230 OF THE COMMUNICATIONS ACT OF 1934 (47 U.S.C. 230) IS AMENDED–

(1) in subsection (e), by adding at the end the following:

"(6) NO EFFECT ON CLAIMS RELATED TO GENERATIVE ARTIFICIAL INTELLIGENCE.—Nothing in this section (other than subsection (c)(2)) shall be construed to impair or limit any claim in a civil action or charge in a criminal prosecution brought under Federal or State law against the provider or user of an interactive computer service if the conduct underlying the claim or charge involves information created or developed, in whole or in part, through the use or provision of generative artificial intelligence by the provider or user of the interactive computer service."; and

(2) in subsection (f), by adding at the end the following:

"(5) GENERATIVE ARTIFICIAL INTELLIGENCE.—The term 'generative artificial intelligence' means an artificial intelligence system that is capable of generating novel text, video, images, audio, and other media based on prompts or other forms of data provided by a person.".

SEC. 505. SEVERABILITY.

If any provision of this Act, or the application thereof to any person or circumstance, is held invalid, the remainder of this Act, and the application of such provision to other persons not similarly situated or to other circumstances, shall not be affected by the invalidation.

TITLE VI – FEDERAL RESOURCES

SEC. 601. OCCUPATIONAL SERIES RELATING TO ALGORITHM AUDITING.

(a) ALGORITHM AUDITING FIELDS.—Not later than 270 days after the date of the enactment of this Act, the Director of the Office of Personnel Management shall exercise the authority of the Director under section 5105 of title 5, United States Code, to establish a new occupational series and associated policies covering Federal Government positions in the field of algorithm auditing, as described in GAO report GAO-21-519SP "Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities," including algorithm auditing practices, platform auditing, evaluation and assessment of artificial intelligence systems, computer security, independent evaluation and audits of computer systems, data science, statistics, and related fields.

SEC. 602. UNITED STATES DIGITAL SERVICE ALGORITHM AUDITORS.

(a) Within 180 days after the date of the enactment of this Act, the Administrator of the United States Digital Service shall establish a track for algorithm auditing and begin to hire algorithm audit practitioners.

(b) Once hired, algorithm auditing track personnel and projects shall give prioritization to efforts of the Federal Trade Commission.

(c) The Administrator of the United States Digital Service shall work with the Federal Trade Commission to ensure the algorithm auditing track staffing and expertise meets their needs.

SEC. 603. ADDITIONAL FEDERAL RESOURCES.

(a) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Federal Trade Commission and other federal agencies enumerated in this Act such sums as may be necessary to carry out this Act.

(b) FTC PERSONNEL.—Notwithstanding any other provision of law, the Federal Trade Commission may hire no more than 500 additional personnel to accomplish the work of the Federal Trade Commission related to unfair or deceptive acts or practices relating to the development or deployment of covered algorithms, data security, identity theft, data abuses, and related matters, and carrying out this Act.

lawyerscommittee.org
digitaljustice@lawyerscommittee.org