The Online Civil Rights and Privacy Act of 2019

SECTION 1 – PURPOSES

The purposes of this Act are to prevent and remedy discrimination and to promote equal opportunity; to prevent and remedy unfair and deceptive practices involving the processing of personal information; to give individuals the right to access and control their own personal information; to protect the privacy and information security of individuals; and to provide transparency as to the privacy and information security practices of covered entities. This Act is a remedial civil rights and consumer protection statute that shall be generously and broadly construed to effectuate these purposes.

SECTION 2 – DEFINITIONS

(a) BIOMETRIC INFORMATION – The term "biometric information" means any personal information generated from the measurement or specific technological processing of an individual's unique biological, physical, or physiological characteristics. Biometric information includes measurements of, but is not limited to, fingerprints, voice prints, iris scans, facial characteristics, identifying DNA (deoxyribonucleic acid) information, gait, or other unique biological characteristics, including any mathematical code or algorithmic model generated or extracted from measurements of these characteristics. Biometric information does not include writing samples, written signatures, photographs, demographic data or physical descriptions such as height, weight, hair color, or eye color.

(b) COMMISSION – The term "Commission" means the Federal Trade Commission.

(c) COVERED ENTITY – The term "covered entity" means any person that processes more than a de minimis amount of personal information in or affecting interstate commerce, as well as entities related to that person by common ownership or corporate control. Such term does not include:

(1) the federal Government; the Government of any State; the Government of any Indian tribe; or any political subdivision, department, agency, component entity, or instrumentality of said Governments;

(2) any employee, officer, agent, contractor, or organization working on behalf of such an entity described in paragraph (1), when processing personal information directly on behalf of such entity and only as relates to such processing; or

(3) A natural person, unless acting in a commercial capacity that does not qualify as a small business.

(d) DATA BROKER – The term "data broker" means a covered entity, or affiliate or subsidiary of a covered entity, that (1) discloses the personal information of any individual to a third party, and (2) with whom that individual does not have a direct relationship.

(e) DISCLOSING – The term "disclosing" or "disclose" or "disclosure" means any action, set of actions, or omission in which a person makes information available to another person, intentionally or unintentionally. This includes but is not limited to sharing; publishing; selling; leasing; licensing; providing access; and negligently, recklessly, or intentionally failing to restrict access.

(f) INDIVIDUAL – The term "individual" means a natural person residing in the United States.

(g) PERSONAL DEVICE – The term "personal device" means an electronic device that is (1) capable of sending, routing, or receiving communications to or from another electronic device, and (2) intended for use by a single individual or single household or, if used outside of a home, by no more than ten individuals at once.

(h) PERSONAL HEALTH INFORMATION – The term "personal health information" means information regarding the medical history of, the physical or mental health of, or the provision of health care to an individual.

(i) PERSONAL INFORMATION – The term "personal information" means any information held by a covered entity—regardless of how the information is collected, inferred, derived, created, or obtained—that is linked or reasonably linkable to an individual or a personal device. Information is reasonably linkable to an individual or personal device if it can be used on its own or in combination with other reasonably available information, regardless of whether such other information is held by the covered entity, to identify an individual or a personal device.

(1) "Personal information" shall not include information processed within the scope of employment by an employer in connection with employment status of workers. This exclusion does not include information about applicants.

(j) PRIVACY RISK – The term "privacy risk" means the potential for adverse consequences to individuals and/or society arising from the processing of personal information, including but not limited to:

(1) Direct or indirect financial harm;
(2) Physical harm or threats to persons or property;
(3) Psychological harm, including anxiety, embarrassment, fear, and other mental harm;
(4) Discrimination in goods, services, or economic opportunities—such as housing, employment, credit, insurance, education, or healthcare—on the basis of a person or class of persons' actual or perceived race, color, ethnicity, national origin, religion, sex, gender, gender identity, sexual orientation, or disability;

(5) Harassment, including sexual harassment;
(6) Bias-related crimes and threats;
(7) Interference with or surveillance of First Amendment-protected activities by state actors;
(8) Interference with the right to vote or with free and fair elections;
(9) Interference with due process or equal protection under law;
(10) Stigmatization or reputational harm;
(11) Disruption or intrusion from unwanted commercial solicitations, such as spam email, junk mail, or unwanted robocalls;
(12) Adverse effects on an individual arising from the processing of personal information that are not reasonably foreseeable to the average person; or
(13) Other adverse consequences that affect an individual's private life, including private family matters, actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation of seclusion or access control.

(k) PROCESSING – The term "processing" or "process" means any action or set of actions performed on or with personal information, including but not limited to collection, acquisition, access, analysis, creation, generation, derivation, decision making, recording, alteration, organization, structuring, storage, retention, use, disclosure, transmission, sale, licensing, disposal, destruction, or other handling of personal information.

(l) SERVICE PROVIDER – The term "service provider" means a person that processes personal information on behalf of a covered entity.

(m) SMALL BUSINESS – The term "small business" means a person
(1) that is not an affiliate or subsidiary of a covered entity, directly or indirectly;
(2) that is not a service provider;
(3) that has no more than 50 workers;
(4) that has no more than $500 million in annual revenue;
(5) that processes the personal information of no more than 100,000 individuals; and
(6) whose website, computer application, or internet-enabled service has no more than one million monthly active users.

(n) STATE – The term "State" means any State of the United States, the District of Columbia, the Commonwealth of Puerto Rico, and any territory or possession of the United States;

(o) THIRD PARTY – The term "third party" means a covered entity that
(1) accesses personal information from or discloses personal information to a second covered entity in connection with a contractual relationship or commercial transaction; and

(2) is not a service provider of the second covered entity.

The term "third party" includes any affiliate or related corporate entity that holds itself out to the public as separate from the second covered entity, such that a reasonable individual would not expect it to be related to the second covered entity or expect that it may have access to personal information accessible to the second covered entity.

SECTION 3 – DISCRIMINATORY PRACTICES AND EQUAL OPPORTUNITY

(a) DISCRIMINATION IN ECONOMIC OPPORTUNITIES. – It is unlawful to process personal information (1) for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for (2) housing, employment, credit, insurance, or education opportunities, (3) in a manner that discriminates against or otherwise makes the opportunity unavailable on the basis of a person or class of persons' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.

(1) Burden of Proof in Disparate Impact Cases. – The unlawful processing of personal information based on disparate impact is established under this subsection only if (A) a complaining party demonstrates that the processing of personal information causes a disparate impact on the basis of a protected characteristic; and (B) the respondent fails to demonstrate that the challenged processing of information is necessary to achieve one or more substantial, legitimate, nondiscriminatory interests or (C) the complaining party shows that an alternative policy or practice could serve that interest with a less discriminatory effect.

(2) Separability of Components of a Processing of Personal Information. – With respect to demonstrating that a particular processing of personal information causes a disparate impact as described in paragraph (a)(1), the complaining party shall demonstrate that any particular challenged component of the processing of personal information causes a disparate impact, except that if the components of the respondent's processing of personal information are not reasonably capable of separation for analysis, the processing of personal information may be analyzed as a whole.

(A) Machine learning algorithms are presumed to be not capable of separation for analysis unless respondent proves otherwise by a preponderance of the evidence.

(b) DISCRIMINATION IN PUBLIC ACCOMMODATIONS. – It is unlawful to process personal information in a manner that segregates, discriminates in, or otherwise makes unavailable the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation on the basis of a person or class of persons' actual or perceived race,

color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, or disability.

(1) Place of Public Accommodation. – The term "place of public accommodation" means any type of business considered a place of public accommodation pursuant to 42 U.S.C. § 2000a(b) or 42 U.S.C. § 12181(7), as well as any business that offers goods or services through the internet to the general public.

(2) Disparate Impact Cases. – The standards for disparate impact cases stated in paragraphs (a)(1)-(2) of this section shall apply to disparate impact cases with respect to this paragraph.

(3) Interference with Rights and Privileges. – It is unlawful for any person to

(A) withhold, deny, deprive, or attempt to withhold, deny, or deprive, any person of any right or privilege secured by this paragraph;

(B) intimidate, threaten, coerce, or attempt to intimidate, threaten, or coerce, any person with the purpose of interfering with any right or privilege secured by this paragraph; or

(C) punish or attempt to punish any person for exercising or attempting to exercise any right or privilege secured by this paragraph.

(c) VOTER SUPPRESSION AND INTIMIDATION. – It is unlawful to process personal information in a manner that intentionally deprives, defrauds, or attempts to deprive or defraud any person of their free and fair exercise of the right to vote in a federal, State, or local election. Intentionally depriving, defrauding, or attempting to deprive or defraud means:

(1) Intentional deception as to the times, places, or methods of voting; eligibility to vote; counting of ballots; adjudication of elections; explicit endorsements by any person of a candidate; or 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, or coercion to prevent, interfere with, retaliate against, deter, or attempt to prevent, interfere with, retaliate against, or deter

(A) voting or registering to vote in a federal, State, or local election; or

(B) giving support or advocacy in a legal manner toward a candidate in a federal, State, or local election.

(d) DUTY TO INTERRUPT CIVIL RIGHTS VIOLATIONS. – A covered entity that is not a small business has a duty to prevent or aid in preventing violations of subsections (a)-(c) of this section. Such covered entity shall be liable if:

(1) a person violates any of subsections (a)-(c) of this section;

(2) the covered entity had actual knowledge of the violation, or made conscious effort to avoid obtaining actual knowledge of the violation, before it occurred or while it was ongoing;

(3) the covered entity had the ability to prevent, halt, or materially aid in preventing or halting the violation;
(4) the covered entity neglected or refused to prevent, halt, or materially aid in preventing or halting the violation; and
(5) the violation caused an injury.

(e) AUDITING FOR DISCRIMINATORY PROCESSING. –
(1) A covered entity that is not a small business shall annually audit its personal information processing practices to:
(A) Determine that the processing practices work as intended and do not discriminate in a manner prohibited by this section;
(B) Analyze privacy risks to the public, and to any individual or class of individuals whose personal information is being processed; and
(C) Identify and implement reasonable measures to mitigate those privacy risks.
(2) The Commission shall promulgate regulations, in conjunction with the transparency regulations specified in Section 7, to implement this subsection. This subsection shall go into effect upon the promulgation of such regulations or two years after the enactment of this Act, whichever is sooner.

(f) UNFAIR OR DECEPTIVE ADVERTISING, TARGETING, PERSONALIZATION, AND DELIVERY PRACTICES. – Within two years of the date of enactment of this Act, the Commission shall promulgate regulations to define and prohibit unfair or deceptive advertising, targeting, personalization, and delivery practices. Practices that violate subsections (a)-(c) of this section are per se unfair or deceptive. In specifying additional unfair or deceptive practices, the Commission shall consider:
(1) Established public policy, such as civil rights laws, that can guide the Commission's determinations of what constitutes an unfair or deceptive practice;
(2) The methods available or used to target, personalize, and deliver online advertisements, and their effects;
(3) Research of and methodologies for measuring discrimination, including disparate impact, in advertising, targeting, personalization, and delivery practices;
(4) The role of all actors in the digital advertising ecosystem, including advertisers; social media platforms; search engines; websites and applications that carry advertisements; advertising networks; data brokers; personal device manufacturers; and other relevant entities;
(5) Harms caused by predatory or manipulative marketing practices targeting marginalized or vulnerable populations, including on the actual or perceived basis of race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, personal health information, lawful source of income, disability, age, criminal record, or immigration status;

(6) Whether, and at what age, minors are able to distinguish between regular content and paid advertisements;
(7) Methods for fairly promoting equal opportunity in housing, employment, credit, insurance, education, or healthcare, through targeted outreach to underrepresented populations in a fair and non-predatory manner;
(8) How to increase diversity and inclusion by fairly promoting content generated by and small businesses owned by members of underrepresented populations; and
(9) Other privacy risks posed by advertising, targeting, personalization, and delivery practices.

(g) EXCEPTIONS. – Nothing in this section shall limit covered entities from processing personal information for (1) the purpose of advertising, marketing, or soliciting economic opportunities to underrepresented populations in a fair, non-deceptive, and non-predatory manner; or (2) legitimate internal testing for the purpose of preventing unlawful discrimination or otherwise determining the extent or effectiveness of the covered entity's compliance with this Act.

(h) RULE OF CONSTRUCTION. – Nothing in this section shall be construed to limit the Commission or any other entity's authority to enforce against unfair, deceptive, or abusive practices or other practices prohibited by other laws or regulations. Nothing in this section shall be construed to preempt or limit the rights of individuals under other laws or regulations.

SECTION 4 – UNFAIR PROCESSING PRACTICES

(a) PERMISSIBLE PROCESSING. – In general, a covered entity shall process personal information only to the extent that such processing is relevant to and necessary for a purpose specified in the covered entity's privacy notice, as described in section 7, and not otherwise restricted by this Act or other laws. If such processing is not reasonably foreseeable to an ordinary individual based on the nature of the covered entity and the nature of an individual's relationship with that covered entity, and is not otherwise restricted, the covered entity may process the personal information only after obtaining an individual's affirmative express consent. A covered entity may also process personal information to the extent necessary to comply with a requirement of this Act or other laws.

(b) PROHIBITED PROCESSING. – It is unlawful for a covered entity to engage in the following processing practices when those practices are not required to provide the product, service, or specific feature that an individual has requested:

(1) BIOMETRIC INFORMATION TRACKING. – The processing of biometric information to identify an individual, to verify an individual's identity, or to track an individual's activities or location without specifically identifying them.

(2) PRECISE LOCATION INFORMATION. – The processing of precise location information generated by a personal device, either in real time or in historical logs. Location information is precise, regardless of the technological mechanism used, if it is sufficient to identify a location with greater accuracy than the relevant ZIP code or is otherwise reasonably likely to identify an individual's home or workplace.

(3) TRACKING OF CHILDREN UNDER THE AGE OF 13. – The disclosure of children's personal information to third parties, and the processing of children's personal information for targeted advertising purposes, where a covered entity has actual knowledge that it is processing personal information from a child under the age of thirteen or where such personal information is obtained from services, products, or specific features directed to children under the age of thirteen.

(4) CONTENT OF COMMUNICATIONS. – The disclosure to third parties of the contents of communications or the parties to a communication.

(5) SENSOR RECORDINGS. – The processing of personal information collected through the microphone, camera, or other sensors of a personal device capable of measuring environmental conditions. This includes but is not limited to personal information involving the measurement of chemicals, light, radiation, air pressure, speed, weight or mass, positional or physical orientation, magnetic fields, temperature, and sound. This does not include the measurement or use of such environmental information in a manner that does not process personal information.

(6) PERSONAL HEALTH INFORMATION. – The processing of personal health information.

(7) SEXUAL LIFE INFORMATION. – The processing of personal information related to an individual's sexual life, including their sexual activity, relationships, orientation, preferences, communications, or behavior.

(c) OTHER PROHIBITED UNFAIR PRACTICES. – Except as otherwise provided in this Act, it shall be unlawful for a covered entity to:

(1) Charge an extra fee or raise prices when an individual exercises their rights under this Act.

(2) Terminate, refuse to provide, degrade goods or services to, or otherwise retaliate against, an individual who exercises their rights under this Act.

(3) Require an individual to arbitrate disputes that arise under this Act or otherwise waive legal rights.

(d) RIGHT TO PETITION. – A person may petition the Commission, pursuant to Section 553 of Title 5, United States Code, to declare a practice to be unfair or deceptive under this Act.

The Commission shall declare a practice to be unfair or deceptive and promulgate regulations prohibiting or restricting that practice if it finds that the practice causes or contributes to material and unreasonable privacy risks or if it finds the practice is otherwise contrary to the public interest because it is inconsistent with the purposes of this Act. As part of its evaluation of the petition, the Commission shall make factual findings on:

(1) The likelihood, nature, scope, and severity of privacy risks directly and indirectly posed by the practice to individuals and society;

(2) If the practice involves the direct processing of personal information by a covered entity, the degree to which such processing is reasonably foreseeable to an ordinary individual;

(3) The practicality and ability of individuals to limit or avoid the practice in the market, evaluating in particular—

(A) If the relevant market is not national, regional variations in market competitiveness;

(B) the options available to low income and vulnerable individuals;

(C) the complexity of the practice and the ability of individuals to understand how it works and how it affects them; and

(4) Whether the practice is predatory toward a particular class of individuals on the basis of their actual or perceived race, color, ethnicity, religion, national origin, immigration status, sex, gender, gender identity, sexual orientation, familial status, biometric information, personal health information, income, age, disability, level of education, or criminal record;

(5) The potential benefits of the practice to individuals and society;

(6) The ability of covered entities to provide goods and services requested by individuals at reasonable cost without engaging in the practice; and

(7) The necessity of the practice for safety, security, fraud prevention, legal process, technical support, or mitigating other more serious privacy risks.

(e) EXCEPTIONS. – Nothing in this section shall limit covered entities from processing personal information when necessary for:

(1) detecting and preventing security incidents; protecting against malicious, deceptive, fraudulent, or illegal activity; or prosecuting those responsible for that activity;

(2) preventing imminent danger to the personal safety or property of an individual or group of individuals;

(3) identifying or repairing errors that impair existing intended functionality;

(4) engaging in public or peer reviewed scientific, medical, historical, social science, or statistical research in the public interest that adheres to all other applicable ethical standards or laws, with informed consent;

(5) legitimate internal testing for the purpose of preventing unlawful discrimination or otherwise determining the extent or effectiveness of the covered entity's compliance with this Act;

(6) complying with a federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; and

(7) any other exception specified by the Commission by regulation that is consistent with the purposes of this Act and narrowly tailored to serve the public interest. When considering new exceptions, the Commission shall prioritize the minimization and prevention of privacy risks.

Authorization under one of these exceptions to process personal information is strictly limited to the purpose of the exception and does not authorize any processing for any other purpose.

(f) RULE OF CONSTRUCTION – Nothing in this section shall be construed to limit the Commission or any other entity's authority to enforce against unfair, deceptive, or abusive practices or other practices prohibited by other laws or regulations. Nothing in this section shall be construed to preempt or limit the rights of individuals under other laws or regulations.

SECTION 5 – DECEPTIVE PROCESSING PRACTICES

(a) It is unlawful for a covered entity to make material misrepresentations with respect to the processing of personal information, whether or not any individual is in fact misled, deceived, or damaged thereby. A covered entity's express statements are presumptively material.

(b) Such misrepresentations include but are not limited to:

(1) Notices, reports, settings, interfaces, or other representations that have a tendency to mislead individuals as to how their personal information is being processed;

(2) The use of false pretenses, fraudulent statements, misleading interfaces, or other misrepresentations to induce the disclosure of personal information or consent to process personal information;

(3) A misleading omission of material information;

(4) Representing that processing has a method, approval, certification, characteristic, use, benefit, quality, standard, or grade that it does not have;

(5) Representing that the covered entity has a sponsorship, approval, status, affiliation, or certification that the covered entity does not have;

(6) Misrepresenting as to a material fact which has a tendency to mislead;

(7) Misrepresenting as to the information security practices of the covered entity;

(8) Claiming that personal information is encrypted when it is not, or misrepresenting the security or extent of the encryption;
(9) Representing that processing is necessary for a purpose when it is not;
(10) Representing that personal information has been de-identified, destroyed, erased, or disposed of when it has not;
(11) Misrepresenting the identities of service providers or third parties to whom the covered entity discloses personal information; and
(12) Representing that the covered entity has complied with an individual's request with regard to access to, correction, or deletion of their personal information, when it has not.

(c) When evaluating whether a representation is misleading, courts and the Commission shall consider the totality of the covered entity's relevant representations from the perspective of a reasonable ordinary individual under the circumstances. When the covered entity targets representations to a specific group, courts and the Commission shall evaluate the representations from the perspective of a reasonable ordinary member of that group. Non-misleading disclosures in a privacy notice or annual privacy report are insufficient to cure an otherwise deceptive practice.

(d) RULE OF CONSTRUCTION – Nothing in this section shall be construed to limit the Commission or any other entity's authority to enforce against unfair, deceptive, and abusive practices or other practices prohibited by other laws or regulations. Nothing in this section shall be construed to preempt or limit the rights of individuals under other laws or regulations.

SECTION 6 – INDIVIDUAL RIGHTS TO PERSONAL INFORMATION

(a) INDIVIDUAL RIGHTS. – Subject to exceptions promulgated by the Commission under subsection (d), an individual has the following rights with respect to personal information pertaining to the individual that is held by covered entities:

(1) The right to access personal information and the names of third parties to whom the covered entity discloses such personal information.

(2) The right to dispute the accuracy or completeness of personal information processed for the purpose of determining eligibility or making offers for housing, employment, credit, insurance, education, or healthcare opportunities.

(3) The right to delete personal information that is held by or derived from the individual's current or former account with the covered entity, unless that personal information is publicly available from other sources.

(4) The right to request that the covered entity cease processing personal information, unless that personal information is publicly available from other sources.

(5) The right to transmit or transfer personal information from one covered entity to another covered entity, or to obtain a copy of such personal information.

(b) COVERED ENTITY DUTIES. – A covered entity shall:

(1) Make available an accessible, conspicuous, and easy-to-use means for individuals to make a complaint or request, or otherwise exercise their rights under this Act;

(2) Respond to an individual's complaint or request within a reasonable period of time;

(3) Provide a response explaining the outcome of the individual's complaint or request;

(4) Provide a reasonable opportunity to appeal adverse determinations;

(5) Provide information about how to contact the Commission; and

(6) If the covered entity has a direct relationship with the individual, provide these resources at least via the same medium(s) and language(s) that the individual routinely uses to interact with the covered entity.

(c) DATA PORTABILITY WORKING GROUP. – Not later than six months after the date of enactment of this Act, the National Institute of Standards and Technology shall establish a working group to make recommendations on the implementation of paragraph (a)(5), to promote common frameworks and cooperation to foster the interoperable portability of personal information, and to address reasonable limitations on portability. Such group shall include equal numbers of industry representatives, public interest representatives, and technical experts. This working group shall promulgate a data portability standard within eighteen months of the date of the establishment of the working group, and shall review the standard at least once every three years thereafter.

(d) EXCEPTIONS AND IMPLEMENTATION. – Within two years of the enactment of this Act, the Commission shall promulgate regulations implementing this section and establishing reasonable exceptions, such as for the provision of service and business administration; the security, safety, and rights of the individual, the covered entity, and others; peer-reviewed scientific or academic research in the public interest; journalism related to public figures or public concerns; the needs of small businesses; and other legal obligations, rights, and privileges.

(1) The Commission shall consider the recommendations of the National Institute of Standards and Technology working group with regard to the implementation of paragraph (a)(5).

(2) Subsections (a) and (b) of this section shall become effective when the Commission promulgates these regulations, or three years after the date of enactment of the Act, whichever is sooner.

(e) RULE OF CONSTRUCTION. – Nothing in this section shall be interpreted to require a covered entity to take an action that would transform information that is not personal information into personal information. Nothing in this section shall be construed to limit the Commission or any other entity's authority to enforce against unfair, deceptive, and abusive practices or other practices prohibited by other laws or regulations. Nothing in this section shall be construed to preempt or limit the rights of individuals under other laws or regulations.

SECTION 7 – TRANSPARENCY

(a) A covered entity has a duty to inform individuals how it processes and secures their personal information.

(b) PRIVACY NOTICES. – A covered entity that is not a small business shall make available a notice that provides relevant information describing its privacy and information security policies, practices, and procedures in a manner that is conspicuous, accessible, not misleading, machine-readable, and easy to understand. The notice shall include:

(1) the types of personal information that the covered entity processes and a general description of how it obtains such information;
(2) the general purposes of processing, and ways in which the covered entity processes personal information, including whether and how the covered entity customizes its products, services, or prices based on an individual's personal information;
(3) the names of third parties, including affiliates, and categories of service providers to whom the covered entity discloses personal information and the purpose for which the covered entity makes each type of disclosure;
(4) a description of how individuals may exercise their rights under the Act or otherwise control the covered entity's processing of their personal information;
(5) a description of the method by which the covered entity will notify individuals of material changes to its data policies;
(6) the effective date of the notice; and
(7) any other information that the Commission, by regulation, deems appropriate.

(c) ANNUAL PRIVACY REPORT. – A covered entity that is not a small business shall publish an annual privacy report that is thorough and not misleading. Within two years, the Commission shall promulgate regulations implementing this paragraph. These regulations shall prioritize covered entities' provision of information regarding such covered entities' processing practices and security policies while also protecting intellectual property.

(1) The annual report shall include:

(A) the types of personal information the covered entity processes and a detailed description of how it obtains or derives each type of information;

(B) A detailed list of all purposes for which the covered entity processes personal information, including a detailed description of whether and how the covered entity customizes its products, services, or prices based on an individual's personal information;

(C) a description of how the covered entity uses personal information to make decisions or recommendations, including a description of scoring, filtering, ranking, recommending, or decision-making done by systems that are entirely or substantially automated;

(D) a list of third parties and service providers to whom the covered entity discloses personal information;

(E) a description of the covered entity's approach to identifying and mitigating privacy risks, including:

(i) the designation of an employee responsible for monitoring the covered entity's privacy practices covered by this Act;

(ii) the manner in which the covered entity educates and trains its workers on privacy risks and data processing obligations;

(iii) the procedures by which a covered entity audits, monitors, and addresses privacy risks pursuant to Section 3(e), and a report of the findings of the most recent audit; and

(iv) a data retention policy that details how long the covered entity retains different types of personal information in days, months, or years, or indefinitely, and why it retains the personal information for that length of time;

(F) any material changes to the covered entity's policies or practices related to personal information processing and privacy since the prior report;

(G) any material security incidents or violations of the company's privacy program, the covered entity's response, and an assessment of the effects of the incidents or violations on persons whose personal information was involved; and

(H) any other information that the Commission, by regulation, deems appropriate.

(2) The chief executive officer, chief privacy officer, chief operating officer, chief information security officer, or a senior officer of equivalent stature of the covered entity must certify, under oath, the information contained in the annual privacy report. The officer must certify that:

(A) They have reviewed the disclosures;
(B) Based on their knowledge, the disclosures do not contain any untrue statement of fact or misleading statement, or omit a material fact;
(C) They are responsible for establishing, maintaining, and regularly evaluating the effectiveness of the covered entity's internal information security and privacy controls;
(D) They have included information in the disclosure sufficient to understand the covered entity's compliance with this Act and any significant changes in the covered entity's internal information security and privacy controls since the previous report.

(d) MODEL PRIVACY NOTICES FOR SMALL BUSINESSES. – Within two years of the enactment of this Act, the Commission shall promulgate regulations specifying transparency requirements for covered entities that are also small businesses. The Commission shall consider the need for individuals to understand how such covered entities process personal information, the types of information addressed in subsection (b), the scope of privacy risks from data processing by small businesses, and the cost of compliance to small businesses. These regulations shall include model privacy notices for small business that are also covered entities that, if used appropriately, presumptively satisfy the transparency requirements of this section.

(e) REGISTRY OF DATA BROKERS. – Within three years of the enactment of this Act, the Commission shall promulgate regulations creating an online public registry of data brokers and a process for registration. The registry shall be designed to be accessible to the general public. Once the registry is established, data brokers who are not small businesses must register and be in good standing in order to process personal information.

(1) A data broker's registration shall include links to the data broker's most recent privacy notice and annual privacy report, and brief descriptions of:
(A) the identity of the data broker and, if it is a subsidiary of another company, its corporate ownership;
(B) the primary business activity of the data broker;
(C) the types of personal information the data broker processes;
(D) how the data broker acquires personal information;
(E) the types of persons to whom the data broker discloses personal information; and
(F) sufficient information for individuals to be able to contact the data broker and exercise their rights under this Act.

(2) In addition to other enforcement measures under this Act, the Commission may temporarily suspend or permanently revoke the registration of a data broker that violates the Act.

SECTION 8 – PROTECTION OF PERSONAL INFORMATION

(a) INFORMATION SECURITY

(1) A covered entity has a duty to secure personal information that it processes, protect such personal information's integrity, and prevent its unauthorized processing and disclosure.

(2) A covered entity shall establish and implement reasonable policies, practices, and procedures to satisfy this duty, taking into consideration:

(A) the nature, scope, and complexity of the activities engaged in by such covered entity;
(B) the size of the covered entity;
(C) the types and magnitude of privacy risks posed by the covered entity's processing of personal information;
(D) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and
(E) the cost of implementing such administrative, technical, and physical safeguards.

(3) For covered entities that are not small businesses, the policies, practices, and procedures required in paragraph (2) shall include, at a minimum:

(A) a written security policy with respect to the processing of personal information;
(B) a procedure for holistically assessing the privacy risks posed by the covered entity's activities;
(C) the identification of an officer or other senior employee as the point of contact with responsibility for the management of information security;
(D) a procedure for identifying and assessing any reasonably foreseeable vulnerabilities in the system or systems maintained by such covered entity that contain personal information, which shall include regular monitoring for a breach of security of such system or systems;
(E) a procedure for taking preventive and corrective action designed to mitigate against identified vulnerabilities, which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software, and for regularly testing or otherwise monitoring the effectiveness of these safeguards;

(F) a procedure for determining if personal information is no longer needed to provide the goods, services, or specific features requested by the individual, and for disposing of data containing personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or indecipherable;

(G) a procedure for overseeing persons who have access to personal information;

(H) a procedure for training and supervision of workers for implementation of the policies, practices, and procedures required by this subsection;

(I) procedures for internal enforcement of the covered entity's policies and discipline for non-compliance;

(J) procedures for receiving and responding to information security threats reported by external technical experts and researchers;

(K) a written plan or protocol for internal and public response in the event of a breach of security that reasonably accounts for the need to promptly inform affected persons, the Commission, and law enforcement, as appropriate; and

(L) any other measures that the Commission, by regulation, deems appropriate.

(4) Within one year of the effective date of this Act, the Commission shall promulgate non-binding guidance to small businesses to assist with their compliance with the information security requirements of this subsection.

(b) DATA BREACHES – Within one year of the effective date of this Act, the Commission shall promulgate regulations establishing data breach notification requirements for covered entities. The Commission shall consider the range and scope of privacy risks posed by different types and sizes of data breaches, when and how it is appropriate to notify affected individuals and the public generally, when and how to notify the Commission and law enforcement, along with other data breach notification laws, and considerations for covered entities that are also small businesses.

(c) THIRD PARTIES AND SERVICE PROVIDERS

(1) If a covered entity has actual knowledge that a third party, service provider, or another covered entity has violated the Act, the covered entity shall promptly report the violation to the Commission.

(2) It shall be a violation of this Act for a covered entity to provide substantial assistance or support, financial or otherwise, to any person when that covered entity knows or consciously avoids knowing that the person is engaged in acts or practices that violate this Act.

(3) Third Parties. – A covered entity shall not disclose personal information to a third party unless that third party is contractually bound to meet the same privacy and security obligations as the covered entity. A covered entity shall exercise reasonable oversight and take reasonable actions to ensure a third party's compliance with such contractual provisions.

(A) A covered entity shall not further disclose personal information it has acquired from a third party, without explicit prior consent from the individual to whom the personal information pertains.

(B) A covered entity that facilitates access to personal information by other covered entities shall be obligated to limit access to and seek proof of destruction of personal information if the first covered entity has actual knowledge that another covered entity has violated this Act.

(4) Service Providers. – A covered entity may not disclose personal information to a service provider unless the covered entity enters into a contractual agreement with the service provider that prohibits the service provider from processing the personal information for any purpose other than the purposes for which the covered entity shared such personal information with the service provider, and that requires the service provider to meet the same privacy and security obligations as the covered entity. Such service provider shall not further disclose or process personal information it has acquired from the covered entity except as explicitly authorized by the contract. A covered entity shall exercise reasonable oversight and take reasonable actions to ensure its service providers' compliance.

SECTION 9 – RULEMAKING AUTHORITY FOR THE FEDERAL TRADE COMMISSION

Except where another agency is explicitly specified, the Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations it determines to be necessary to carry out this Act.

SECTION 10 – ENFORCEMENT

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION. –

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES. – A violation of this Act shall be treated as an unfair or deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. § 57a) regarding unfair or deceptive acts or practices.

(2) POWERS OF COMMISSION. – The Commission shall enforce 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.

(3) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS. – Notwithstanding Sections 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. §§ 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act with respect to:

(A) Common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.);

(B) Organizations not organized to carry on business for their own profit or that of their members.

(b) ENFORCEMENT BY STATES. –

(1) Civil action. – In any case in which the attorney general of a State, or other official or agency designated by a State to enforce this Act, has reason to believe that an interest of the residents of that State has been or is adversely affected by any person who violates this Act or regulations promulgated pursuant to this Act, such State attorney general, official or agency, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States.

(2) Rights of the Federal Trade Commission. – Except where not feasible, the State shall notify the Commission in writing of any civil action under subsection (b) prior to initiating such civil action. Upon receiving notice with respect to a civil action, the Commission shall have the right to intervene in such action on its own behalf.

(c) ENFORCEMENT BY THE DEPARTMENT OF JUSTICE CIVIL RIGHTS DIVISION

The Attorney General of the United States may bring a civil action to enforce subsections (a)-(d) of Section 3 of this Act in an appropriate district court of the United States. The Attorney General shall, where reasonable and appropriate, consult with the Commission prior to the initiation of such civil action.

(d) PRIVATE RIGHT OF ACTION. –

(1) Any person may bring an action seeking relief from a violation of this Act or regulations promulgated pursuant to this Act in an appropriate district court of the United States on their own behalf or on behalf of themselves and the general public.

(2) A nonprofit organization may, on behalf of itself or any of its members, on behalf of an individual or class of individuals, or on any such behalf and on behalf of the general public, bring an action seeking relief from a violation of this Act or

regulations promulgated pursuant to this Act in an appropriate district court of the United States.

(e) REMEDIES. –

(1) In any case brought by a state actor under this Act, the court may award the following:

(A) Injunctive relief, including preliminary injunctions, to prevent further violations of and compel compliance with the Act;

(B) Civil penalties. – The greater of (i) up to $16,500 per violation; or (ii) up to 4% of the annual revenue of the covered entity, if the defendant is a covered entity;

(C) Other appropriate relief, including restitution, to redress harms to individuals or to mitigate all substantial privacy risks; and

(D) Any other relief that the court determines proper.

(2) In any case brought by a private party under this Act, the court may award the following:

(A) Injunctive relief, including preliminary injunctions, to prevent further violations of and compel compliance with the Act;

(B) $16,500 per violation or treble actual damages, whichever is greater;

(C) Reasonable attorneys' fees and costs;

(D) If the defendant is a covered entity, punitive damages up to 4% of the annual revenue of the covered entity;

(E) Other appropriate relief to mitigate all substantial privacy risks to the affected individual(s); and

(F) Any other relief which the court determines proper.

(3) CALCULATING DAMAGES AND CIVIL PENALTIES. – When calculating damages and civil penalties, the court shall consider the number of affected individuals, the severity of the violation, and the size and revenues of the covered entity. Each individual whose information was unlawfully processed counts as a separate violation. Each provision of the Act that was violated counts as a separate violation.

(f) CRIMINAL ACTIONS BY THE ATTORNEY GENERAL FOR FALSE REPORTING. –

(1) The Attorney General may bring an action for a criminal violation in the appropriate United States district court against any person who completes a certification to the Commission under Section 7 of this Act, and who knew that the statements required by the certification are not true. Reckless disregard of whether a statement is true, or a conscious effort to avoid learning the truth, shall be construed as acting knowingly under this statute. Providing the certification without conducting the

assessment(s) required for the annual privacy report, or without verifying that the assessment(s) was conducted and completed, may constitute a conscious effort to avoid learning the truth.

(2) Criminal Penalties. – Whoever provides the certification as set forth in Section 7 knowing that the annual privacy report accompanying the statement contains false or inaccurate information shall be fined not more than $1,000,000 or imprisoned not more than 10 years.

SECTION 11 – PERSONNEL FOR THE COMMISSION AND CONGRESSIONAL OFFICE OF TECHNOLOGY ASSESSMENT

(a) ADDITIONAL PERSONNEL FOR THE BUREAU OF CONSUMER PROTECTION AT THE FEDERAL TRADE COMMISSION

Notwithstanding any other provision of law, the Director of the Bureau of Consumer Protection of the Commission may appoint not more than 100 additional personnel in the Division of Privacy and Identity Protection of the Bureau of Consumer Protection; and may appoint not more than 150 additional personnel to the Division of Enforcement of the Bureau of Consumer Protection. There is authorized to be appropriated to the Director of the Bureau of Consumer Protection such sums as may be necessary to carry out this section.

(b) ESTABLISHMENT OF A BUREAU OF TECHNOLOGY AT THE FEDERAL TRADE COMMISSION

(1) Establishment. – There is established within the Federal Trade Commission the Bureau of Technology to be headed by a Director of Technology.

(2) Organization. – The personnel and assets of the Office of Technology Research and Investigation at the Bureau of Consumer Protection shall be transferred to the Bureau of Technology. The Director of the Bureau shall have the authority to organize the Bureau and establish offices under the Bureau as is necessary to carry out the Bureau's functions. Notwithstanding any other provision of law, the Director of the Bureau of Technology may appoint not more than 250 additional personnel. There is authorized to be appropriated to the Director of the Bureau of Technology such sums as may be necessary to carry out this section.

(3) Duties. – It shall be the duty of the Bureau of Technology to advise the Commission on the impact of current and future technological developments on issues, regulations, and cases falling within the Commission's authorities, including on developments with regard to their impacts on privacy, competition, equal opportunity, and consumer protection.

(c) RE-ESTABLISHMENT OF A CONGRESSIONAL OFFICE OF TECHNOLOGY ASSESSMENT

There is appropriated, for salaries and expenses of the Office of Technology Assessment as authorized by the Technology Assessment Act of 1972 (2 U.S.C. § 471 et seq.), $2,500,000.

SECTION 12 – REPORTS TO CONGRESS

(a) Not later than two years after the effective date of this Act, and at least biennially thereafter, the Commission shall submit a public report to Congress concerning the effectiveness of this Act; developments in the state of the art of personal information processing; compliance by covered entities; violations of this Act and enforcement actions undertaken, if any to resolve those violations; and enforcement priorities and resources needed by the Commission to fully implement and enforce this Act and regulations promulgated pursuant to this Act.

(b) Not later than two years after the effective date of this Act, and at least triennially thereafter, the Department of Housing and Urban Affairs shall submit a public report to Congress concerning personal information processing practices that may result in housing discrimination and disparities in housing opportunities.

(c) Not later than two years after the effective date of this Act, and at least triennially thereafter, the Department of Labor shall submit a public report to Congress concerning personal information processing practices that may result in employment discrimination and disparities in employment opportunities.

(d) Not later than two years after the effective date of this Act, and at least triennially thereafter, the Consumer Financial Protection Bureau shall submit a public report to Congress concerning personal information processing practices that may result in lending discrimination and disparities in access to credit by consumers.

(e) Not later than two years after the effective date of this Act, and at least triennially thereafter, the Department of Education shall submit a public report to Congress concerning personal information processing practices that may result in education discrimination and disparities in education opportunities.

(f) Not later than two years after the effective date of this Act, and at least triennially thereafter, the Department of Health and Human Services shall submit a public report to Congress concerning personal information processing practices that may result in healthcare or health insurance discrimination and disparities in healthcare or health insurance.

(g) Not later than two years after the effective date of this Act, and at least triennially thereafter, the Department of Veterans Affairs shall submit a public report to Congress concerning personal information processing practices that may result in discrimination against veterans or disparities in opportunities for veterans.

SECTION 13 – EFFECTIVE DATE

The provisions of this Act that apply to covered entities shall apply beginning on the date two years after the date of enactment, unless otherwise noted.

SECTION 14 – RELATION TO OTHER LAW

(a) The provisions of this Act shall preempt any State law only to the extent that such State law is inconsistent with the provisions of this Act and only if the Commission has affirmatively determined, on a case-by-case basis, that such State law is preempted. The Commission shall not presume that more restrictive State laws are inconsistent with the provisions of this Act.

(b) This Act shall not be construed to preempt, modify, or limit the rights granted by or the enforcement of any federal law or any of the following State laws:
   (1) Consumer protection laws of general applicability;
   (2) Laws that address the processing or privacy of health, education, or financial information;
   (3) Civil rights laws, including laws addressing discrimination, equal opportunity, online harassment, civil actions for bias-related crimes, or sexual harassment;
   (4) Laws that govern the privacy rights or other protections of workers and worker information;
   (5) Trespass, contract, tort, or criminal law;
   (6) Laws that address notification requirements in the event of a data breach; or
   (7) Other laws to the extent that those laws relate to acts of fraud.

SECTION 15 – SEVERABILITY

If any provision of this Act, or the application thereof to any person, is held unconstitutional or otherwise invalid, the validity of the remainder of the Act and the application of such provision to other persons shall not be affected thereby.