[DISCUSSION DRAFT]

H. R. __

To establish consumer privacy protections and data security for individuals whose personal information is collected, used, and shared by certain entities, to require safeguards on the collection and use of such information and restrictions on the sharing of such information, to properly safeguard their data, and to amend the Federal Trade Commission Act to implement various enforcement abilities to the Commission's practices, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

_____ introduced the following bill; which was referred to the Committee on _____

A BILL

To establish consumer privacy protections and data security for individuals whose personal information is collected, used, and shared by certain entities, to require safeguards on the collection and use of such information and restrictions on the sharing of such information, to properly safeguard their data, and to amend the Federal Trade Commission Act to implement various reforms to the Commission's practices, and for other purposes.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Control Our Data Act".

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

TITLE I—CONSUMER PRIVACY AND SECURITY OF DATA CONTAINING PERSONAL INFORMATION

SEC. 101. DEFINITIONS.

As used in this title, the following definitions apply:

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

(2) COVERED ENTITY.—The term "covered entity"

(A) means any organization, corporation, trust, partnership, estate, cooperative association, sole proprietorship, unincorporated association, or other entity, including such covered entity's affiliates, over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2));

(B) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers; and

(C) not withstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), any nonprofit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) o the Internal Revenue Code of 1986.

(3) DATA BROKER.—

(A) the term "Data Broker":

(i) Includes a covered entity, or affiliate or subsidiary of a covered entity, that regularly collects, uses, or shares personal information and sells or licenses to any third-party or is otherwise compensated for disclosing information for the third party's own purposes; and

(ii) Includes a covered entity whose principal source of revenue is derived from selling personal information to any third-party or is otherwise compensated for the disclosure of such collection, use, or sharing of personal information.

(B) does not include a commercial entity to the extent that such entity collects, uses, and shares information collected by and received from a nonaffiliated third-party concerning individual who are current or former customers or employees of the third party to provide benefits for the employees or directly transact business with the customers.

(4) PERSONAL INFORMATION. — the term "personal information" —

(A) Means any information that is linked or reasonably linkable to a specific individual; and

(B) Does not include –

(i) Information that is collected, used, or shared solely for the purpose of employment of an individual, including any information regarding an individual that pertains to such individual in his or her capacity as an owner, director, or employee of a partnership, corporation, trust, estate, cooperative, association, or other type of entity;

(ii) Aggregate information;

(iii) Deidentified information;

(iv) Information that is rendered unusable, unreadable, or indecipherable such as because the information is redacted, tokenized, or encrypted;

(v) Information legally obtained from a publicly available source, including information obtained from a news report, periodical, or other widely distributed media, or from Federal, State, or local government records; or,

(vi) Pseudonymized information.

(5) SENSITIVE INFORMATION.— The term "sensitive information" means—

(A) Health information;

(B) Biometric information;

(C) Precise geolocation information;

(D) Social security numbers;

(E) Drivers license number, or other government issued identification number;

(F) The contents and parties to communications;

(G) Financial information, including bank account numbers, credit card numbers, debit card numbers, or insurance policy numbers;

(H) any information pertaining to children under 13 years of age; or

(I) genetic information, including DNA.

(6) THIRD PARTY.—The Term "Third Party" means a person or covered entity to the extent that which the covered entity or person is not a service provider or a co-branded affiliate, that access or receives personal information from, or discloses personal information to, a covered entity.

(7) Small to Mid-Size Entities. — the term "small to mid-size entity" means a covered entity that:

(A) has an annual gross revenue of less than $25 million in assets;

(B) collect, use, share the personal information of 50,000 or less individuals; or

(C) derive 50% or less of annual revenue from selling consumer information.

(8) Large Entities. —The term "large entities means a covered entity that:

(A) has an annual gross revenue of more than $25 million in assets;

(B) collect, use, share the personal information of 50,000 or more individuals; or

(C) derive 50% or more of annual revenue from selling consumer information.

(9) Legitimate Purpose.—For purposes of section 105 of this title, legitimate purpose means—

(A) a purpose that was specified at the time the personal information was collected; or

(B) a purpose that is otherwise consistent with the requirements of section 104 of this title.

SEC. 102. TRANSPARENCY OF COMPANY PRIVACY POLICIES AND INDIVIDUAL RIGHTS TO ACCESS, CORRECT, AND DELETE PERSONAL INFORMATION.

(a) PRIVACY POLICIES.—

(1) IN GENERAL.—A covered entity shall maintain and conspicuously post on the primary Internet website of the covered entity or otherwise make available a privacy policy that shall include the following:

(A) Each category of personal information collected, used, or shared by the covered entity and the purposes for such collection, use, or sharing;

(B) The means by which the covered entity collects such personal information;

(C) Each category of third-party persons or entities with whom the covered entity shares such information;

(D) The rights of an individual to access, correct, and delete personal information collected, used, or shared by the covered entity about such individual, as set forth in subsection (c), and the processes for exercising such rights;

(E) The process by which a covered entity notifies an individual of material changes to the privacy policy of the covered entity required by this subsection;

(F) The process by which a covered entity responds to web browser “do not track” signals or other mechanisms that provide an

individual the ability to exercise choice regarding the collection of personal information;

(G) The effective date of the privacy policy, and any revisions to such policy; and

(H) whether a covered entity collects personal information about individuals over time and across different websites or mobile applications when an individual uses the covered entity's website or mobile application.

(2) DISCLOSURE OF PERSONAL INFORMATION SHARED WITH THIRD PARTIES.—If a covered entity sells or otherwise shares personal information with a data broker or other third-party persons or entities or collects, uses, or shares personal information for targeted advertising, such covered entity shall disclose the nature of such collection, use, or sharing of information along with the privacy policy required under paragraph (1).

(3) SUMMARY.—Each covered entity shall maintain and conspicuously post on the primary Internet website of the covered entity or otherwise make available a summary of the covered entity's privacy policy that states in plain, understandable terms—

(A) how the covered entity collects personal information;

(B) the purposes for which the covered entity collects such information; and

(C) each category of third-party persons or entities with which the covered entity shares such information, if applicable.

(b) NOTICE TO INDIVIDUALS BEFORE COLLECTING PERSONAL INFORMATION.—

(1) NOTICE.—Each covered entity shall provide an individual with clear and understandable information at or before the point of collection of personal information regarding—

(A) how a covered entity collects such personal information, including whether such information is collected by auditory means;

(B) each category of such personal information that a covered entity collects, uses, or shares;

(C) the purposes for which a covered entity collects, uses, or shares such personal information;

(D) the rights of an individual with regard to accessing, correcting, and deleting personal information pertaining to that individual that is collected, used, or shared by the covered entity, as set forth in subsection (c), and the processes for exercising such rights; and

(E) each category of third-party persons or entities with which a covered entity shares such information.

(2) NOTICE OF ANY CHANGE IN POLICIES.—If a covered entity materially changes its privacy policy, such covered entity shall provide an individual with clear and understandable information about such changes prior to the collection of any additional personal information.

(c) INDIVIDUAL RIGHTS REGARDING PERSONAL INFORMATION.—

(1) RIGHTS AND OBLIGATIONS.—

(A) CONFIRMATION.—Upon a verifiable request by an individual, a covered entity shall, without undue delay, provide confirmation to the individual as to whether the covered entity collects, uses, or shares the personal information of such individual.

(B) ACCESS.—Upon a verifiable request by an individual, a covered entity that collects the personal information of an individual shall disclose, without undue delay, to the individual—

(i) each category of personal information about the individual;

(ii) each category of sources from which the personal information is collected;

(iii) the purpose for which the covered entity collects, uses, or shares the personal information of the individual; and

(iv) each category of third-party persons or entities with which the covered entity shares the personal information of the individual.

(C) CORRECTION.—Upon a verifiable request by an individual, a covered entity shall, without undue delay, provide the individual the ability to dispute the accuracy or completeness of any personal information the covered entity has collected and, if necessary, the ability to correct such information.

(D) DELETION.—Upon a verifiable request by an individual, a covered entity that operates a website or mobile application shall be required to delete the account or profile of the individual, and any personal information that the covered entity has collected pertaining to that individual.

(E) OBJECTION.— Upon a verifiable request by an individual, a covered entity may not collect, use, or share the sensitive information of such individual.

(2) EXCEPTIONS.—Any obligation imposed under paragraph (1) shall not apply to the extent that such obligation restricts the ability of a covered entity to—

(A) fulfill a payment, complete a service, or notify individuals of product recalls;

(B) develop products, improve its services, complete data analytics, and research;

(C) conduct its own marketing or advertising that does not involve the sharing of personal information to a third party;

(D) comply with Federal, State, or local laws, rules, or regulations;

(E) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by Federal, State, local, authorities;

(F) cooperate with law enforcement agencies concerning conduct or activity that the covered entity reasonably and in good faith believes may violate Federal, State, or local law;

(G) investigate, exercise, or defend legal claims;

(H) collect, use, retain, sell, or otherwise disclose personal information that is deidentified or aggregated;

(I) prevent or detect identity theft, fraud, or other criminal activity;

(J) perform a contract to which the individual making a request under paragraph (1) is a party or in order to take steps at the request of the individual prior to entering into a contract;

(L) perform a task carried out in the public interest or in the exercise of official authority vested in the covered entity;

(M) collect, use, or share personal information of an individual for one or more specific purposes where the individual has given his or her consent to the collection, use, or sharing of their information; or

(N) prevent, detect, or respond to security incidents, ransomware, harassment, malicious or deceptive activities, or any illegal activity, preserve the integrity or security of systems, or investigate, report, or prosecute those responsible for any illegal action that involves the personal information of an individual.

(3) EXCLUSION FOR EVIDENTIARY PRIVILEGE.—The obligations imposed under paragraph (1) do not apply where compliance by a covered entity would violate an evidentiary privilege under Federal, State, or local laws and do not prevent a covered entity from providing personal information concerning an individual to a person covered by an evidentiary privilege under Federal, State, or local laws as part of a privileged communication.

(4) NONLIABILITY OF THIRD PARTIES.—A covered entity that has disclosed personal information to a third-party person or entity is not in violation of this subsection, if the recipient collects, uses, or shares such personal information in violation of this subsection, provided that, at the time of disclosing the personal information, the disclosing covered entity did not have actual knowledge that the recipient intended to commit a violation. A third-party person or entity receiving personal data from a covered entity is likewise not liable under this section for the obligations of a covered entity to which it provides services.

(d) RESPONSE TO INDIVIDUAL RIGHTS REQUESTS.—

(1) TIMELINESS.—A covered entity shall comply with a verifiable request under subsection (c)(1) within a reasonable time, but not later than 30 days after the date on which the request is submitted by an individual. The time period to provide the required information may be extended once by an additional 30 days when reasonably necessary, provided the individual is provided notice of the extension within the first 30-day period.

(2) PERIOD OF APPLICABILITY.—The disclosure of the requested information under this section shall cover the 12-month period preceding the receipt by the covered entity of the verifiable request.

(3) DENIAL OF A REQUEST.—If a covered entity denies a verifiable request under subsection (c)(1) on the basis of an exemption described in subsection (c)(2), the covered entity shall inform the individual within a reasonable time, but no later than 30 days after receiving the request of the reasons for the denial and the means for appealing such denial.

(4) PROHIBITION ON FEES.—A covered entity may not charge a fee to an individual for making a request under subsection (c)(1) if the individual does not submit a request more than once in a single month, and twice in 12-month period.

(A) If an individual submits more than one request every month, or two in a 12-month period, the covered entity may charge such individual a reasonable fee.

(B) If an individual submits an illegitimate or non-verifiable request, the covered entity may charge such individual a reasonable fee regardless of how many requests such individual has made in a 12-month period.

(e) VERIFICATION.—

(1) LIMITATIONS OF COVERED ENTITY OBLIGATION.—A covered entity is not required to collect, use, share, or otherwise maintain personal information, or reverse any pseudonymization or deidentification that has been applied to personal information for the purpose of verification under subsection (c)(1).

(2) UNABLE TO VERIFY.—If a covered entity cannot, through reasonable efforts, verify an individual making a request under subsection (c)(1), the covered entity shall notify the individual without undue delay and shall have no obligation to complete the request of the individual under such subsection.

(f) FTC RULEMAKING AND GUIDANCE.—

(1) REGULATIONS.—The Commission may prescribe regulations under section 553 of title 5, United States Code, to—

(A) modify or add to the information each covered entity must include in the disclosure required by subsection (a)(3); or

(B) add to the information a covered entity must provide to an individual at or before the point of collection of personal information pursuant to subsection (b)(1).

(2) GUIDANCE.—Not later than 1 year after the date of enactment of this Title, the Commission shall issue guidance on how to comply with the provisions of subsection (c).

(g) FTC STUDY ON EFFECTIVELY COMMUNICATING SHORT-FORM PRIVACY STATEMENTS.—

(1) STUDY.—Not later than 180 days after the date of the enactment of this Title, the Commission shall conduct a study to determine the most effective method of communicating common privacy practices in short-form privacy statements, graphic icons, or other means determined by the Commission that disclose how a covered entity collects personal information, the purposes for which the covered entity collects such information, and, if applicable, the category of third parties or data brokers the covered entity shares such information with. After the completion of such study, the Commission shall submit a report to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate with the results of the study.

SEC. 103. SENSITIVE INFORMATION.

(a) EXPRESS PRIOR CONSENT.—A covered entity may collect or use the sensitive information of an individual, or share such information with a third-party person or entity, only if such covered entity obtains express consent prior to the collection, use, or sharing of such information from such individual.

(b) SEPARATE CONSENT.—A covered entity shall request such consent for the collection, use, or sharing of such sensitive information separate from the original consent such individual provided to use the product or service of the covered entity.

SEC. 104. LEGITIMATE PURPOSE FOR COLLECTION, USE, OR SHARING OF PERSONAL INFORMATION.

(a) IN GENERAL.—A covered entity may only collect, use, or share personal information in a manner that is consistent with—

(1) the explanation in the privacy policy and disclosures of the covered entity as required by section 102;

(2) the purposes of:

(A) fulfilling a transaction, including billing and auditing related to the order, and necessary customer support such as product development and improvement; or

(B) providing a product or service specifically requested and approved by the individual.

(3) the reasonable expectations of the individual to whom such information pertains;

(4) complying with a legal obligation or specifically authorized by law;

(5) necessary to—

(A) verify identify and the detection and prevention of fraudulent, malicious, or illegal activity, or prosecute persons responsible for such activity;

(B) defend against actual or potential security threats;

(C) prevent imminent danger to the personal safety of an individual or groups of individuals, including from cybersecurity threats; or

(D) network management and security, including debugging to identify and repair errors that impair existing functionality.

(b) RESTRICTION.—A covered entity may not collect, use, or share personal information for a purpose that is materially different from the purposes for which the personal information was originally collected or subsequently authorized by the individual, unless the covered entity obtains express consent prior to such additional collection, use or sharing of such information.

SEC. 105. RETENTION.

(a) IN GENERAL.—A covered entity may only retain personal information for as long as such personal information is relevant to a legitimate purpose.

SEC. 106. PRIVACY BY DESIGN.

(a) POLICIES, PRACTICES, AND PROCEDURES.—A covered entity shall establish and implement reasonable policies, practices, and procedures regarding the collection, use, and sharing of personal information to—

(1) comply with Federal, State, or local laws, rules, or regulations related to personal information the covered entity collects, uses, or shares;

(2) consider the mitigation of privacy risks related to the products and services of the covered entity, including their design, development, and implementation; and

(3) implement reasonable training and safeguards within the covered entity to promote compliance with all privacy laws applicable to personal information the covered entity collects, uses, or shares and mitigate privacy risks.

(b) FACTORS TO CONSIDER.—The policies, practices, and procedures established by a covered entity under subsection (a), shall correspond with—

(1) the size of the covered entity and the nature, scope, and complexity of the activities engaged in by the covered entity;

(2) the sensitivity of the personal information collected, used, or shared by the covered entity;

(3) the volume of personal information collected, used, or shared by the covered entity;

(4) the number of individuals to which the personal information collected, used, or shared by the covered entity relates; and

(5) the cost of implementing the program.

(c) ADDITIONAL REQUIREMENTS FOR LARGE ENTITIES.— A large entity shall designate at least one appropriately qualified employee who reports directly to the highest official at the covered entity as a privacy protection officer who shall, either directly or through a supervised designee or designees—

(1) establish processes to enforce the privacy policies, practices, and procedures of the covered entity to comply with all applicable laws;

(2) establish processes to periodically review and update the privacy policies, practices, and procedures of the covered entity as necessary;

(3) conduct regular and comprehensive audits to ensure the policies, practices, and procedures of the covered entity work to ensure the company is in compliance with all applicable laws;

(4) develop a program to educate and train employees about compliance requirements;

(5) Maintain updated clear, and understandable records of all data security practices undertaken by the covered entity; and

(6) Serve as the point of contact between the covered entity and enforcement authorities.

(d) COMMISSION GUIDANCE.—Not later than 1 year after the date of enactment of this Title, the Commission shall issue guidance as to what constitutes reasonable policies, practices, and procedures as required by this section.

SEC. 107. RISK ASSESSMENT AND MITIGATION.

(a) RISK ASSESSMENT.—

(1) REQUIREMENT.—Not later than 1 year after enactment of this Title, a covered entity shall conduct, to the extent not previously conducted, a risk assessment of each of its practices relating to the collection, use, and sharing of personal information and an additional risk assessment any time there is a change in such practices that materially increases the risk to individuals. Such risk assessments shall take into account the type of personal information to be collected, used or shared by the covered entity, including the extent to which the personal information is sensitive information and the context in which the personal information is to be collected, used, or shared.

(2) RISK-BENEFIT ANALYSIS.—Risk assessments conducted under paragraph (1) shall identify and weigh the benefits that may flow directly or indirectly from the collection, use, or sharing of personal information to the covered entity, the individual to whom such information pertains, a third-party person or entity, and the public, against the potential risks to the rights of the individual, as mitigated by safeguards that can be employed to reduce such risks.

(3) FACTORS TO INCLUDE IN ASSESSMENT.—In assessing privacy risks, the covered entity may include reviews of—

(A) categories of data and sources;

(B) systems;

(C) the flow of information;

(D) a third party person or entity and any service provider; and

(E) the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, are used to secure personal data.

(b) CONFIDENTIAL TREATMENT OF INFORMATION.—A covered entity shall make the risk assessment available to the Commission upon request and any information submitted to the Commission under this section shall be considered privileged and confidential and exempt from public disclosure in the same manner as matters exempt from disclosure under section 552(b)(4) of title 5, United States Code.

(c) RISK MITIGATION.—A covered entity shall take reasonable actions to mitigate the privacy risks identified under this section, which may include—

(1) anonymization of personal data, or pseudonymization of personal data where anonymization is not possible; or

(2) encryption, blockchain and distributed ledger technologies, or any other emerging technologies that is more protective of personal data if appropriate to the collection and use of such personal data.

SEC. 108. THIRD PARTY SHARING.

(a) INVESTIGATION AND NOTIFICATION REQUIREMENTS.—If a covered entity has entered into a contract with a third-party person or entity to share or permit the collection of personal information with respect to a website or mobile application operated by the covered entity, the covered entity shall—

(1) upon discovering that the third-party person or entity has violated a term of such contract relating to the use and treatment of user

data, conduct in good faith a reasonable and prompt investigation of the nature of the violation; and

(2) if the investigation produces evidence that the third-party person or entity's conduct constitutes a violation of this Title, promptly notify the Commission and appropriate State Attorney General, including—

(A) the name and contact information of the third-party person or entity;

(B) the nature of the violation; and

(C) any information about the actions of the third-party person or entity that resulted in the violation of the term of the contact.

(b) CONFIDENTIAL TREATMENT OF INFORMATION.—Any information submitted to the Commission under this section shall be considered privileged and confidential and exempt from public disclosure in the same manner as matters exempt from disclosure under section 552(b)(4) of title 5, United States Code.

SEC. 109. DATA SECURITY.

(a) DATA SECURITY.—

(1) IN GENERAL.— A covered entity shall develop, implement, and maintain reasonable administrative, technical, and physical security measures, policies, practices, and procedures to protect and secure personal information against unauthorized access and acquisition.

(2) FACTORS TO BE CONSIDERED.—The reasonable administrative, technical, and physical security measures, policies, practices, and procedures required under paragraph (1) shall be appropriate to—

(A) the size and complexity of the covered entity;

(B) the nature and scope of the activities of the covered entity;

(C) the cost of available tools to improve security and reduce vulnerabilities to unauthorized access and acquisition of such information;

(D) the sensitivity of the personal information collected, used, and shared by the covered entity; and

(E) the current state of the art in administrative, technical, and physical safeguards for protecting such information.

(b) ADDITIONAL REQUIREMENTS FOR LARGE ENTITIES.—As part of the reasonable safeguards required under subsection (a)(1), a covered entity shall—

(1) designate an officer, employee, or employees to maintain such safeguards;

(2) identify material internal and external risks to the security and confidentiality of personal information and assess the sufficiency of any safeguards in place to control such risks;

(3) implement safeguards designed to control any identified or reasonably foreseeable risks;

(4) maintain reasonable procedures for the security of personal information by a third-party person to require that such person maintains reasonable administrative, technical, and physical safeguards designed to protect the security of such personal information; and

(5) evaluate the safeguards and make reasonable adjustments to those safeguards in light of any material changes in technology, internal or external threats to personal information, and the covered entities own changing business arrangements or operations.

(c) FTC GUIDELINES.—Not later than 1 year after the date of enactment of this Title, the Commission shall issue guidance on what is considered reasonable for the requirement under this section.

(d) REBUTTABLE PRESUMPTION.—If a covered entity establishes that it has complied with the guidance of the Commission issued under subsection (c), it shall be presumed that such covered entity has complied with this section such that if the Commission seeks to pursue an enforcement action arising out of the unauthorized

acquisition of personal information maintained by the covered entity, the Commission must establish by clear and convincing evidence that the covered entity nonetheless lacked reasonable safeguards required by subsection (a)(1).

SEC. 110. SELF-REGULATORY GUIDELINES AND SAFE HARBOR.

(a) IN GENERAL.—A covered entity or group of covered entities may apply to the Commission for approval of one or more sets of self-regulatory guidelines governing the collection, use, sharing, and security of personal information by a covered entity.

(b) APPLICATION.—Such application shall include—

(1) a description of how the proposed guidelines will meet or exceed the requirements of this title;

(2) a description of the entities or activities the proposed guidelines are designed to cover;

(3) a list of the covered entities, that are known at the time of application, that intend to adhere to the guidelines; and

(4) the identity of an independent organization to be approved by the Commission under subsection (c)(2)(B) to conduct reviews of and compliance with such guidelines in order to ensure that the covered entity or entities meet or exceed the requirements of this Title.

(c) COMMISSION REVIEW.—

(1) PUBLIC COMMENT.—As soon as feasible after the receipt of proposed guidelines submitted pursuant to subsection (a), the Commission shall provide an opportunity for public comment on such proposed guidelines.

(2) APPROVAL OF APPLICATION.—The Commission shall approve an application regarding proposed guidelines under subsection (a) if the applicant demonstrates that such guidelines—

(A) meet or exceed requirements of this title; and

(B) provide for the regular review and validation by an independent organization not associated with the covered entity and approved by the Commission to conduct such reviews in order to ensure that the covered entity continues to meet or exceed the requirements of this title.

(3) DETERMINATION.—Within 90 days after the date on which the application is received by the Commission, the Commission shall issue a determination approving or denying an application regarding the proposed guidelines submitted pursuant to subsection (a) and providing the reasons for approving or denying such application.

(d) SAFE HARBOR PROTECTION.—A covered entity shall be considered to be in compliance with this title if the covered entity is in compliance with guidelines approved by the Commission pursuant to this section.

SEC. 111. ANTI-DISCRIMINATION.

(a) PROHIBITED CONDUCT.— A covered entity may not, through the collection use or sharing of personal information, discriminate against or make an economic opportunity unavailable on the basis of race, color, religion, national origin, sex, age, political ideology, or disability of a persons or class of persons.

(b) EXCEPTIONS.—Nothing in this section shall prohibit a covered entity from using or sharing personal information for the purpose of advertising, marketing, or soliciting economic opportunities to underrepresented populations.

SEC. 112. ONE NATIONAL STANDARD.

(a) PREEMPTION OF STATE LAW.—

(1) IN GENERAL.—No State or political subdivision of a State may maintain, enforce, prescribe, or continue in effect any law, rule, regulation, requirement, standard, or other provision having the force and effect of law of any State, or political subdivision of a State, related to the collection, use, or sharing of personal information by or on behalf of a covered entity.

(2) RULE OF CONSTRUCTION.—This subsection shall not be construed to—

(A) limit the enforcement of any State or political subdivision of a State consumer protection law;

(B) preempt the applicability of State trespass, contract, or tort law; and

(C) preempt the applicability of any State law to the extent that the law relates to acts of fraud, unauthorized access to personal information, or notification of unauthorized access to personal information.

(b) PRESERVATION OF AUTHORITY.—

(1) IN GENERAL.—Nothing in this title may be construed in any way to limit the authority of the Commission under any other provision of law.

(2) APPLICATION OF OTHER LAW.—Notwithstanding any other provision of law, neither any provision of the Communications Act of 1934 (47 U.S.C. 51 et. seq.) nor any regulation promulgated by the Federal Communications Commission shall apply to any covered entity with respect to the collection, use, or sharing of individuals' information, unless such provision or regulation pertain solely to 9-1-1 calls.

SEC. 113. ENFORCEMENT AND CONSUMER RESTITUTION.

(a) ENFORCEMENT BY FEDERAL TRADE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this title shall be treated as an unfair and 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(a)(1)(B)) regarding unfair or deceptive acts or practices. Notwithstanding section 5 of such Act, the maximum civil penalties for violations of this title shall be as specified in paragraph (3), as applicable.

(2) POWERS OF COMMISSION.—The Commission shall enforce this title 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 title, and any covered entity subject to the Commission's authority who violates this title 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.).

(3) CIVIL PENALTIES.—

(A) FIRST OFFENSE CIVIL PENALTIES.—

(i) A large entity with $3 billion in annual revenue, 300 monthly active social media users, and generates three quarters of its revenue in online advertising shall be subject to a civil penalty of not more than $100,000 for each violation or $100,000 for each knowing violation.

(ii) A large entity shall be subject to a civil penalty of not more than $43,792 for each violation or $43,792 for each knowing violation.

(iii) A small to mid-size entity shall not be subject to a civil penalty if a violation constitutes the covered entity's first violation of this Title.

(B) SUBSEQUENT VIOLATIONS.—

(i) A large entity shall be subject to a civil penalty of not more than $100,000 for each violation or $100,000 for each intentional violation.

(ii) A small to mid-size entity shall be subject to a civil penalty of not more than $43,792 for each violation or $43,792 for each intentional violation.

(C) PENALTY FACTORS.—In determining the amount of such a civil penalty, the Commission shall consider-

(i) the degree of culpability of a covered entity;

(ii) whether a violation was knowing or intentional;

(iii) any history of prior similar conduct by the covered entity;

(iv) the covered entity's ability to pay;

(v) the effect on the covered entity's ability to continue to do business;

(vi) whether the covered entity identified and took measures to correct the violation;

(vii) the economic impact as determined by the Bureau of Economics at the Commission; and

(vii) any other matters as justice may require.

(D) ADJUSTMENT FOR INFLATION.—Beginning on the date that the Consumer Price Index is first published by the Bureau of Labor Statistics that is after one year after the date of enactment of this Title, and each year thereafter, the amounts specified in subparagraphs (A) and (B) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

(4) Small business ability to seek judicial intervention.—A small to mid-size entity may immediately seek judicial intervention in a district court of the United States of appropriate jurisdiction to determine the validity of any action taken by the Commission under this Title. The small to mid-size entity shall not be required to pay any penalties until the completion of the determination by the Federal court.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by any covered entity that violates this title, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State exclusively in a district court of the United States of appropriate jurisdiction to—

(A) enjoin further violation of such section by the covered entity;

(B) compel compliance with such section; or

(C) obtain civil penalties pursuant to subsection (a).

(2) CONSOLIDATION OF ACTIONS BROUGHT BY TWO OR MORE STATE ATTORNEYS GENERAL.—Whenever a civil action under this subsection is pending and another civil action or actions are commenced pursuant to this subsection in a different Federal district court that involve one or more common questions of fact, a covered entity the covered entity that is the defendant in such actions may elect for such action or actions to be transferred for the purposes of consolidated pretrial proceedings and trial to the United States District Court for the District of Columbia; provided, however, that no such action shall be transferred if pretrial proceedings in that action have been concluded before a subsequent action is filed by a State Attorney General.

(3) INTERVENTION BY THE COMMISSION.—

(A) NOTICE AND INTERVENTION.—In all cases, the attorney general of a State shall provide prior written notice of any action under paragraph (1) to the Commission and provide the Commission with a copy of its complaint, except in any case in which such prior notice is not feasible, in which case such attorney general shall serve such notice immediately upon instituting such action. The Commission may not bring a separate action after an action has been initiated by the attorney general of a State, but the Commission shall have the right—

(i) to intervene in the State action;

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

(iii) to file petitions for appeal.

(B) PENDING PROCEEDINGS.—If the Commission initiates a Federal civil action for a violation of this title, no State attorney general may bring an action for a violation of this title that resulted from the same violations against a covered entity named in the civil action initiated by the Commission. If the Commission has instituted or intervened in a proceeding or a civil action for a violation of this title, no additional State attorney general may bring an action under this subsection against any covered entity in such civil action for any violation of this title alleged in the complaint.

(4) RULE OF CONSTRUCTION.—For purposes of bringing any civil action under paragraph (1), nothing in this title shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(A) conduct investigations;

(B) administer oaths or affirmations; or

(C) compel attendance of witnesses or the production of documentary and other evidence.

(5) ACTIONS BY OTHER STATE OFFICIALS.—

(A) OTHER STATE OFFICERS.—In addition to civil actions brought by attorneys general under paragraph (1), any other consumer protection officer of a State who is authorized by the State to do so may bring a civil action under paragraph (1), subject to the same requirements and limitations that apply under this subsection to civil actions brought by attorneys general.

(B) SAVINGS PROVISION.—Nothing in this subsection may be construed to prohibit an authorized official of a State from initiating or continuing any proceeding in a court of the State for a violation of any civil or criminal law of the State.

(c) ABILITY TO CURE ALLEGED VIOLATIONS.—After notification of any alleged violation of this title by the Commission, a covered entity shall have 30 days after the date on which such notification is received to move to cure such violations. A

covered entity that fails to move to cure any alleged violation within 30 days may be subject to civil penalties pursuant to this section.

(d) FTC STUDY ON HARM.—Not later than 1 year after the date of enactment of this Title, the Commission shall conduct a study to determine what constitutes a privacy harm to individuals based on actions by covered entities with respect to the collection, use, and sharing of personal information. Such study shall include a description of how the Commission prioritizes enforcement actions to address the specific privacy harms the Commission identifies in the study.

(e) FTC GUIDANCE.—No guidelines issued by the Commission with respect to this title shall confer any rights on any person, State, or locality, nor shall operate to bind the Commission or any person to the approach recommended in such guidelines. In any enforcement action brought pursuant to this title, the Commission shall allege a specific violation of a provision of this title. The Commission may not base an enforcement action on, or execute a consent order based on, practices that are alleged to be inconsistent with any such guidelines, unless the practices allegedly violate a provision of this title.

(f) CONSUMER RESTITUTION AND ACCESS TO ENFORCEMENT.—Nothing in this Title shall be construed to establish a private right of action for a violation of this Title. Not later than three years after the enactment of this Title, the Commission shall report to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate the implementation of the nationwide standard, status of cooperation with State Attorneys General, economic analysis related to any administrative action, and any detailed justification for broader enforcement tools.

SEC. 114. BUREAU OF CONSUMER PRIVACY PROTECTION AND DATA SECURITY.

(a)ESTABLISHMENT.– The Chairman of the Commission shall establish a new administrative unit in the Commission to be known as the Bureau of Consumer Privacy Protection and Data Security, which shall—

(1) Administer and enforce this part and other consumer privacy or data security laws or regulations within the Commission’s jurisdiction;

(2) Educate consumers regarding their rights under this Title;

(3) Provide guidance to covered entities regarding their obligations under this Title; and

(4) Provide support and assistance to small and mid-size entities seeking to comply with this Title.

(b)APPOINTMENTS.—

(1) Director.—The Chairman of the Commission shall appoint a Director of the Bureau of Consumer Privacy and Data Security.

(2) Personnel.—

(A) In General.—The Director of the Bureau of Consumer Privacy and Data Security may, without regard to the civil service laws (including regulations), appoint not less than 250 certified professionals for the purpose of implementing subsection (a)

(B) Appointment of Technologists.—In appointing certifies professionals under subparagraph (A), the Director of the Bureau of Privacy shall appoint at least 25 certified technologists.

(C) Technologists Defined.—The term "technologists" means individuals, other than attorneys, with training and expertise regarding microeconomic and macroeconomic theory, state of the art information technology, information security, network, software development, computer science, and other related fields and applications.

(D) Appointment of Psychologists.—In appointing certified professionals under subparagraph (A), the Director of the Bureau of Privacy shall appoint at least 5 psychologists, 2 of which have experience in the well-being of children and teens.(c) OFFICE OF BUSINESS MENTORSHIP.—

(1) In General.—

(A) The Director of the Bureau of Consumer Privacy and Data Security shall establish within the Bureau an Office of Business Mentorship to provide guidance and consultation to covered entities regarding compliance with this Title.

(B) Covered entities may petition the Commission through this office for tailored guidance as to how to comply with the requirements of this Title.

(2) Personnel.—The Director of the Bureau of Consumer Privacy and Data Security shall assign not less than 25 employees of the Bureau of Consumer Privacy and Data Security to staff the Office of Businesses Mentorship, of which 15 must be certified professionals.

(3) Small Business Support.—The Director of the Bureau of Consumer Privacy and Data Security shall assign not less than 5 employees of the Office of Business Education to provide additional support to covered entities with fewer than 50 employees.

(4) Rule of Construction.—No provision of this section shall be construed to limit the authority of the Commission under any other provision of law.

SEC. 115. SPECIAL REQUIREMENTS ON DATA BROKERS

(a) NOTICE ON WEBSITE OF DATA BROKERS.—An data broker shall place a clear and conspicuous notice on the internet website of the data broker (if the data broker maintains such a website) notifying consumers that the entity is a data broker using specific language that the Commission shall determine through rulemaking and providing a link to the website established under subsection (c).

(b) REQUIRED AUDIT LOG OF ACCESSED AND TRANSMITTED INFORMATION.—Not later than 1 year after the date of enactment of this Title, the Commission shall promulgate regulations to require a data broker to establish measures that facilitate the auditing of any internal or external access to, or disclosure of, any personal information relating to an individual that was collected, used, or shared by such data broker.

(c) FTC REGISTRY OF DATA BROKERS.—

(1) Not later than 1 year after the date of enactment of this Title, the Commission shall promulgate regulations to require each data broker that collects, uses, or shares personal information of more than 250,000

or more individuals to register with the Commission and provide—(A) A legal name of the data broker and any other related entities through which the data broker collects, uses, or shares personal information

(B) A description of the categories of information the data broker collects, uses, or shares

(C) The contact information of the data broker, including a telephone number, e-mail address, a website, and a physical mailing address; and

(D) A link to a website through which an individual may easily exercise the rights under subsection (b) of this Section.

(2) The Commission shall establish and maintain on an internet website a searchable central registry of data brokers that—

(A) Is accessible to the general public to identify individual data brokers;

(B) For each data broker, provides the information described in paragraph (1); and

(C) Provides links to individual data brokers through which an individual may exercise the rights provided under subsection (b) of this Section.

(D) Provide consumers a “Do Not Contact” registry link to submit verifiable requests that data brokers with public facing websites that fully or partially display consumers’ date of birth, phone numbers, email addresses, mailing addresses, and advertise services to disclose other information in return for compensation, and are not defined as a consumer reporting agency under the Fair Credit Reporting Act, must remove the consumers’ data or be subject to the penalties of the Act.

TITLE II – GRANTING THE FEDERAL TRADE COMMISSION ADDITIONAL AUTHORITIES UNDER SECTION 13(B) OF THE FEDERAL TRADE COMMISSION ACT

SEC. 202. FTC AUTHORITY TO SEEK PERMANENT INJUNCTIONS AND OTHER EQUITABLE RELIEF.

(a) EQUITABLE RELIEF.—Section 13 of the Federal Trade Commission Act (15 U.S.C. 53) is amended—

(1) In subsection (b)—

(A) in paragraph (1) by inserting "has violated," after "corporation";

(B) in paragraph (2—

(i) by striking "that" and inserting "that either (A)"; and

(ii) by striking "final," and inserting "final; or (B) the permanent enjoining thereof or the ordering of equitable relief under subsection (e),"; and

(C) in the matter following paragraph (2)—

(i) by striking "to enjoy any such act or practice";

(ii) by striking "Upon" and inserting "In a suit under paragraph (2)(A), upon";

(iii) by striking "without bond";

(iv) by striking "proper cases" and inserting "a suit under paragraph (2)(B)";

(v) by striking "injunction." and inserting "injunction, equitable relief under subsection (e), or such other relief

as the court determines to be just and proper, including temporary or preliminary equitable relief.";

(vi) by striking "Any suit" and inserting "Any suit under this subsection";

(vii) by striking "In any suit under this section" and inserting "In an such suit"; and

(1) by adding at the end the following:

(b) Equitable Relief Respecting Unfair or Deceptive Acts or Practices.—

(1) Restitution; Contract Recission and Reformation; Refunds; Return of Property.—In a suit brough under subsection (b)(2)(B), if the violation of law that gives rise to the suit involves conduct that a reasonable person would have known under the circumstances was unfair or deceptive (within meaning of section 5(a)(1)), the Commission may seek, and the court may order, with respect to such violation—

"(A) restitution for loss that the court has a sound basis to conclude resulted from such violation;

"(B) rescission or reformation of contracts;

"(C) refund of money; or

"(D) return of property.

(2) Disgorgement.—In a suit brough under subsection (b)(2)(B), if the violation of law that gives rise to the suit involves conduct that a reasonable person would have known under the circumstances was unfair or deceptive (within meaning of section 5(a)(1)), the Commission may seek, and the court may order, disgorgement of any unjust enrichment that the court has a sound basis to conclude that a person, partnership, or corporation obtained as a result of such violation.

(3) Calculation.— Any amount that a person, partnership, or corporation is ordered to pay under paragraph (2), with respect to a violation, shall be offset by any amount such person, partnership, or corporation is ordered to pay, and the value of any property such person, partnership, or corporation is ordered to return, under paragraph (1) with respect to such violation.

(4) Limitations period.—

(A) In General.—A court may not order equitable relief under this subsection with respect to any violation occurring before the period that begins on the date that is 5 years before the date on which the Commission files the suit in which such relief is sought.

(B) Calculation.—For purposes of calculating the beginning of the period described in subparagraph (A), any time during which an individual against which the equitable relief is sought is outside of the United States shall not be counted.

(C) Effect on certain conduct.—Notwithstanding subparagraph (A), a court may order equitable relief under this subsection with respect to a violation occurring before the period described in such subparagraph, if the Commission proves that the person, partnership, or corporation against which such relief is sought engaged, after such violation, in intentionally deceptive or fraudulent conduct or fraudulent conduct that prevented the Commission from bringing the suit in which such relief is sought within such period."

(c) CONFORMING AMENDMENT.—Section 16(a)(2)(A) of the Federal Trade Commission Act (15 U.S.C. 56(a)(2)(A)) is amended by striking "(relating to injunctive relief)".

(d) APPLICABILITY.—The amendments made by this section shall apply with respect to any action or proceeding that is commenced on or after, the date of the enactment of this title.