116TH CONGRESS
1ST SESSION

S. _____

_____

IN THE SENATE OF THE UNITED STATES

January 28, 2019

[Senators Introducing and Co-Sponsoring]

_____

A BILL

To improve the protection of personal privacy by enacting nationwide standards governing for profit and non-profit private sector organizations' collection, use and sharing of personal data consistent with the Fair Information Practice Principles.

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; GENERAL APPLICATION

(a) Short Title. - This Act may be cited as the "Innovative and Ethical Data Use Act of 2018"

(b) Table of Contents. - The table of contents for this Act is as follows:

Sec. 1. Short title; table of contents.

Sec. 2. Findings.

Sec. 3. Definitions.

Sec. 4. Implementation of Fair Information Practice Principles through establishment of a comprehensive privacy and data security program.

Sec. 5. Oversight of third parties by a covered entity.

Sec. 6. Federal Trade Commission rulemaking authority; Technology neutrality requirement; Enforcement; Penalties for non-compliance.

Sec. 7. Sanction safe harbor.

Sec. 8. Federal Trade Commission guidance; International coordination; Congressional reporting.

Sec. 9. Federal Trade Commission resources.

Sec. 10. Preemption.

Sec. 11. Savings.

Sec. 12. Effective date.

SECTION 2. FINDINGS

Congress finds that—

(a) Individuals need to feel confident that data that relates to them will not be used to harm them, their families, or society.

(b) The use of personal data by organizations can greatly benefit individuals and society, and innovation in this use often results in economic growth for the United States.

(c) Organizations that create, collect, use, process, store, transfer, disseminate, disclose, or dispose of personal data should institute a comprehensive privacy and data security program consistent with the codification of the Fair Information Practice Principles.

(d) A comprehensive privacy and data security program should include administrative, technical, and physical privacy protections which are appropriate to the size and complexity of an organization, and the nature and scope of the organization's activities with respect to personal data, as well as the privacy risk associated with personal data, including its misuse by other organizations that transfer or receive that data. To be effective, data security and privacy considerations must be part of the day-to-day operations of organizations.

(e) The consumer privacy and data security program should be designed to—

(1) Consider and protect an individual's privacy throughout the information life cycle;

(2) Facilitate individuals' control over their personal data and enable them to participate in decision-making regarding the processing of their personal data;

(3) Ensure the confidentiality, integrity, availability, and security of personal data;

(4) Protect against unauthorized access, acquisition, disclosure, destruction, alteration, or use of personal data;

(5) Protect against reasonably anticipated threats and vulnerabilities to the security of personal data or to the legitimate privacy interests of individuals, including following standard industry practices regarding installing hardware and software security updates;

(6) Identify, assess, and mitigate privacy risk on an ongoing basis;

(7) Prevent the use of personal data in any manner inconsistent with the original purpose for which that personal data was collected, unless subsequently permitted; and

(8) Prevent the use or application of outputs from machine learning, algorithms, predictive analytics or similar analysis that would violate any state or federal law or regulation to wrongly discriminate against individuals or facilitate such discrimination, or deny any individual the exercise of any Constitutionally-protected right or privilege.

SECTION 3. DEFINITIONS

In this Act, the following definitions shall apply:

(a) COLLECT.—The term "collect" means—

(1) Buying, renting, gathering, obtaining, receiving, inferring, creating or accessing any personal data pertaining to an individual by any means; or

(2) Obtaining personal data relating to an individual, either actively or passively, or by observing the individual's behavior.

(3) EXCLUSIONS.—The term "collection" does not include the obtaining of personal data solely for facilitating the transmission, routing, or connections by which digital personal data and other data is transferred between or among covered entities, or to and from the individual to whom the personal data relates when the collector does not access, review, or modify the content of that personal data, or otherwise perform or conduct any analytical, algorithmic or machine learning processes on such personal data.

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

(c) CONSUMER PRIVACY AND DATA SECURITY PROGRAM.—The term "consumer privacy and data security program" means the program described in section 4 of this Act.

(d) COVERED ENTITY.—The term "covered entity" means—

(1) Any person 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));

(2) Notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.);

(3) Notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any non-profit 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) of the Internal Revenue Code of 1986;

(4) Organizations that are related to the covered entity by common ownership or corporate control; and

(5) Third parties, as defined by section 3(l) of this Act;

(6) EXCLUSIONS.—The term "covered entity" does not include

(A) Persons, as described in sections 3(d)(1) - (4) of this Act, that have fewer than 25 employees, collect or utilize the personal data of fewer than 50,000individuals, or that derive less than half of all revenue annually from the sale of personal data; or

(B) Persons, as described in sections 3(d)(1) - (4) of this Act, to the extent they offer services related to the transmission, routing, or connections by which digital personal data and other data is transferred between or among covered entities, or to and from the individual to whom the personal data relates, but which services do not access, review, or modify the content of that personal data, or otherwise perform or conduct any analytical, algorithmic or machine learning processes on such personal data, other than to:

(i) Ensure the security of the data and the networks, systems, software, hardware or devices employed by the covered entity; or

(ii) Aid in the efficiency of the transmission of the personal data and other data sent or received with the personal data.

(C) To the extent a person, as described in sections 3(d)(1) - (4) of this Act, offers services covered by section 3(d)(B) as well as other services not covered by section 3(d)(B), this exclusion applies only to the conduct or services explicitly covered by section 3(d)(B).

(D) Organizations covered by Health Insurance Portability and Accountability Act of 1996 (Pub.L. 104-191), the Family Educational Rights and Privacy Act (Pub.L.93-380), the Fair Credit Reporting Act (Pub.L. 91-508) or the Financial Services Modernization Act of 1999 (Pub.L. 106-102), are excluded from the provisions of this Act to the degree the specific uses of data are covered by the privacy provisions of those laws.

(e) DUTY OF CARE.—The term "duty of care" means for a covered entity to take reasonable risk-based measures not to intentionally process personal data in a manner that would have the reasonably foreseeable consequence of directly causing a natural person to suffer significant physical injury or unmerited substantial financial loss, unless:

(1) it was reasonably foreseeable that such injury or loss may have been outweighed by potential benefits to that natural person; or

(2) that natural person has explicitly consented to such processing.

(f) IDENTIFIABLE NATURAL PERSON.—The term "identifiable natural person" means a person who can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, biometric, mental, economic, cultural or social identity of that natural person.

(g) NATURAL PERSON.—The term "natural person" means a human being, naturally born, versus a legally-generated juridical person.

(h) PERSON.—The term "person" means any natural or legal person, which may include any partnership, corporation, trust, estate, cooperative, association, or other entity.

(i) PERSONAL DATA.—The term 'personal data' means any information relating to an identified or identifiable natural person, other than those specific categories of personal data which the Commission exempts from this definition by promulgation of a final rule as deemed appropriate to carry out the purpose of this Act.

(j) PRIVACY RISK.—The FTC shall issue a final rule in accordance with this section to provide more guidance on potential adverse consequences that would fall underneath this definition. The term "privacy risk" means potential adverse consequences to individuals and society arising from the processing of personal data, including, but not limited to:

(1) Direct or indirect financial loss or economic harm;

(2) Physical harm;

(3) Psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma;

(4) Significant inconvenience or expenditure of time;

(5) Adverse outcomes or decisions with respect to an individual's eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;

(6) Stigmatization or reputational harm;

(7) Disruption and intrusion from unwanted commercial communications or contacts;

(8) Price discrimination;

(9) Effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless

reasonably foreseeable, contemplated by, or expected by the covered entity assessing privacy risk, that significantly:

(A) Alters that individual's experiences;

(B) Limits that individual's choices;

(C) Influences that individual's responses; or

(D) Predetermines results; or

(10) 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 that personal data will not be collected or used.

(11) Other potential adverse consequences, consistent with the provisions of this section, as determined by the Commission and promulgated through a rule.

(k) PROCESSING.—The term "processing" means any operation or set of operations that is performed on personal data or on sets of personal data, such as collection, creation, generation, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transfer, dissemination or otherwise making available, combination, erasure, or destruction;

(l) THIRD PARTY.—The term "third party" means, with respect to any covered entity, a person that is not related to the covered entity by common ownership or corporate control, and when such person processes personal data at the direction of a covered entity, using the means and instrumentalities for processing personal data provided by the covered entity, or when the person processes personal data obtained from the covered entity.

SECTION 4. IMPLEMENTATION OF FAIR INFORMATION PRACTICE PRINCIPLES THROUGH ESTABLISHMENT OF A COMPREHENSIVE PRIVACY AND DATA SECURITY PROGRAM.

(a) COLLECTION LIMITATION.—No covered entity shall collect any personal data that is not relevant and necessary to accomplish the specified purpose(s) required in section 4(c).

(b) DATA QUALITY.—A covered entity shall only process personal data that is relevant to the purposes for which they are to be processed, and, to the extent necessary for those purposes. To the extent reasonable for the purpose of the processing, the data should be complete, accurate, and should be updated by the covered entity as necessary to maintain accuracy.

(c) PURPOSE SPECIFICATION.—The purposes for which personal data are processed shall be included in the notices required by section 4(f). Such description of the purposes shall be described clearly and specifically in relation to the intended uses of the personal data by the covered entity.

(1) *Time of Specification.*—The purpose must be specified not later than at the time of collection by the covered entity, unless impossible or impracticable.

(d) USE LIMITATION.—The Commission shall issue a final rule in accordance with this section to provide additional information on the types of uses that fall under section 4(d)(2)(C), and the risk/benefits analysis required in the section 4(d)(3). A covered entity shall only process personal data consistent with the provisions of section 4(d):

(1) *Permitted Processing.*—A covered entity shall be allowed to process personal data:

(A) for any purpose for which the individual to whom the personal data relates provides explicit consent, unless otherwise prohibited by law, regulation or public policy;

(B) as required by law or regulation, including the lawful request of a government agency; or

(C) any uses that satisfy the language of consistent uses under section 4(d)(3).

(2) *Prohibited Uses*.—Notwithstanding paragraph (d)(1) of this section, a covered entity shall not process personal data when the covered entity knows, or has reason to know, that the processing of the personal data will likely:

(A) violate one or more state or federal laws or regulations, including the provisions of this Act; or

(B) interfere with, or deny, individuals their rights and privileges under the United States Constitution.

(C) violate the duty of care to the individual as defined in section 3(e).

(D) Only the forms of processing or the specific processing activity that are prohibited by the requirements of section 4(d)(2)(A), (B) or (C) above shall be prohibited. Processing activities that do not meet the requirements shall not be prohibited and instead must satisfy the requirements of either 4(d)(1) or 4(d)(3) to be permitted.

(3) *Consistent Uses*.—A covered entity shall be allowed to process personal data for purposes consistent with the purposes specified pursuant to section 4(c). The determination of whether a specific processing activity is consistent shall be documented and based on a risk/benefits analysis, taking into consideration the following factors:

(A) the degree to which technical or operational measures have been taken to de-identify the data so as to reduce the likelihood of privacy risk to the individual;

(B) the degree to which the individual to whom the personal data relates would reasonably expect the processing of the personal data given the specified purpose;

(C) the likelihood and severity of privacy risks to that individual;

(D) the potential benefits to that individual;

(E) the privacy risks and potential benefits to other individuals as appropriate; and

(F) the potential risks and benefits to society, including, but not limited to, the potential impact on the economy, free expression, democratic participation, scientific advancement, public welfare, and the public good.

(4) *Automated Processing.*—Processing of personal data by algorithmic, machine learning, or artificial intelligence processing or predictive analytics, without human intervention, shall only be done after the covered entity conducts an assessment, specific to the automated processing, which:

(A) determines, through objective means, that such processing, and the results of such processing, are reasonably free from bias and error, and that the data quality obligations of section 4(b) are met;

(B) analyzes privacy risks, as defined in section 3(j) of this Act, to the individual. Such assessment shall include the identification of reasonably foreseeable privacy risks, if any, and mitigation of such privacy risk to that individual from that processing, including the potential ethical and legal consequences of processing for the individual; and

(C) concludes that, after all reasonable steps are taken to mitigate privacy risk, the automated processing does not cause, or is not likely to cause, substantial privacy risk.

(e) SECURITY SAFEGUARDS.—A covered entity shall develop, document, implement, and maintain a comprehensive data security program that contains administrative, technical, and physical safeguards for personal data that are appropriate to the size and complexity of the covered entity, the nature and scope of the covered entity's activities, and the sensitivity of any personal data processed by the covered entity. Such data security program shall, at a minimum implement reasonable processes, procedures, and tools to:

(1) safeguard the security, confidentiality, integrity, and availability of personal data;

(2) protect against any anticipated threats or hazards to the security or integrity of such personal data; (3) protect against unauthorized processing of such personal data; and(4) take reasonable efforts to incorporate security updates provided by the manufacturers of hardware and software products consistent with coordinated vulnerability disclosure best practices.

(f) OPENNESS.—The Commission shall issue a final rule to provide more detail on the requirements for the notices required under this section 4(f). In issuing regulations, a covered entity shall provide individuals, government agencies and the public with information concerning its data practices regarding personal data.

(1) *Explicit Notice.*—A covered entity shall provide explicit notice to an individual prior to the collection from that individual of personal data that is likely to create significant privacy risk. Collections that require explicit notice include, but are not to be limited to:

(A) geolocation data;

(B) biometric data;

(C) data about racial or ethnic origin;

(D) data related to an individual's religion or religious practice;

(E) physical and mental health data, including any past or present information regarding an individual's medical history; mental or physical condition; medical treatment; or diagnosis by a health care professional;

(F) sexual life data, including concepts such as sexual activity, sexual orientation, sexual preference and/or sexual behavior; or

(G) genetic data.

(H) Exclusions—Explicit Notice is not required if:

(i) providing the notice is not reasonably feasible,

(ii) providing the notice would defeat the purpose of providing privacy protection for the individual to whom the data relates,

(iii) providing the notice would cause the organization to violate the law, or

(iv) a similar notice is already required by another law.

(2) *General Notice*.—A covered entity shall publish, and make publicly available on an ongoing basis, a privacy policy generally articulating the processing practices of the covered entity.

(A) The privacy policy shall include information communicating how individuals may:

(i) access personal data that is processed about them;

(ii) correct erroneous personal data;

(iii) halt further processing of that data by the covered entity or any third party; or

(iv) obtain deletion of the personal data relating to the individual, and any analysis or predictions based upon the processing of that personal data.

(B) The privacy policy shall be:

(i) clear, conspicuous, drafted in plain language and published in a prominent location;

(ii) made publicly accessible prior to collection or, where notice prior to collection is impossible or impracticable, the privacy policy will be made publicly accessible before additional processing of that personal data by the covered entity and in all cases before processing is completed that creates privacy risk.

(3) *Complete Notice.*—A covered entity shall publish and make publicly available on an ongoing basis a reasonably full and complete description of the covered entity's collection and processing of personal data, including but not limited to the:

(A) categories of personal data processed by the covered entity;

(B) details on the type of processing of those personal data types;

(C) purposes for the processing of that personal data by the covered entity;

(D) involvement of any third parties in the processing of personal data;

(E) reasonably foreseeable use of that personal data, if any, by any third party.

(F) application of machine learning, algorithmic processing or artificial intelligence to that personal data by the covered entity, or any third party;

(G) predictive analysis concerning that personal data;

(H) mechanisms established to demonstrate accountability in compliance with section 4(h); and

(I) foreseeable privacy risk related to the processing of the personal data by the covered entity or a third party, including the foreseeable privacy risk created from or by the application of machine learning, algorithmic processing or artificial intelligence to that personal data.

(g) INDIVIDUAL PARTICIPATION.—The Commission shall issue a final rule in accordance with this section to provide more clarity on the requirements of section 4(g)(6). A covered entity shall provide any individual with a readily available means of promptly obtaining:

(1) confirmation of whether personal data concerning the individual is processed by the covered entity;

(2) descriptions of the categories of personal data that are processed by the covered entity;

(3) plain language explanations of the specific types of personal data collected about the requesting individual and the processing of the personal data concerning the individual, including any undertaken by a third-party;

(4) reasonable access to the personal data and the ability to correct erroneous personal data;

(5) correction or supplementation of the personal data with additional information offered voluntarily by the individual to address data quality requirements as described in section 4(b).

(6) reasonable obscurity of personal data processed and maintained in a publicly available format under the control of the covered entity or by a third party, where the availability of that personal data creates or is likely to create significant privacy risk to the individual that is disproportionate to the public benefit of the availability of the personal data.

(A) For purposes of this section, personal data that is sold for a fee shall be deemed publicly available.

(B) The requirements set forth in this section shall not come into effect until the Commission publishes the guidance described in section 8(a)(4)(f) below;

(C) EXCLUSION.—No individual may demand that a covered entity obscure accurate information that an individual committed and was convicted of a crime, unless that information would be expunged or otherwise removed from official records pursuant to state or federal law or regulation, including by operation of a pardon.

(7) EXCEPTION.—Nothing in this section shall require a covered entity to take actions that jeopardize the safety of the individual or rights and freedoms of others under the United States Constitution.

(h) ACCOUNTABILITY.—The Commission shall issue a final rule in accordance with this section to provide more detail on the necessary policies, processes and personnel required to comply with this section. A covered entity shall ensure compliance with this Act by developing and implementing an ongoing accountability program that includes:

(1) POLICIES.—internal publication of written policies and procedures implementing the requirements of this Act.

(2) INTERNAL LEADERSHIP, STAFFING, AND OVERSIGHT.—appointment of a data privacy leader responsible for developing and implementing the covered entity's consumer privacy and data security program, and related policies and practices.

(A) The data privacy leader shall report to senior management and shall be supported by appropriate resources and personnel. Without limitation to other covered entities, a small or medium sized covered entity shall allocate oversight resources in relation to its size and complexity, and the nature and scope of its data holdings and activities with personal data.

(A) Senior management shall be responsible for appropriate reporting and oversight of the privacy program.

(B) The data privacy leader shall develop and implement the covered entity's programs, policies and practices.

(3) STAFFING AND DELEGATION.—dedication of resources to ensure that the privacy program is appropriately staffed by adequately trained personnel. Without limitation to other covered entities, staffing and delegation decisions in small and medium-sized organizations should reflect the particular circumstances of the organization and its activities, and the nature, size and sensitivity of its data holdings.

(4) EDUCATION AND AWARENESS.—an up-to-date education and awareness program to keep employees, contractors and third parties aware of data protection obligations.

(5) ONGOING RISK ASSESSMENT AND MITIGATION.—a process to identify, assess, and mitigate reasonably forseeable privacy risk, including privacy risk raised by new products, services, technologies, methods of processing, and business models. Such process shall:

(A) identify reasonably foreseeable internal and external threats that could result in unauthorized access, destruction, acquisition, disclosure, or use of personal data or of systems containing personal data;

(B) assess the likelihood and potential severity of privacy risk created by the processing of personal data, and from unauthorized access, destruction, acquisition, disclosure, or use of personal data;

(C) assess the sufficiency of its technical, physical, and administrative controls to identify and mitigate privacy risk from unauthorized access, destruction, acquisition, disclosure, or processing of personal data;

(D) assess the effectiveness of efforts to properly destroy and dispose of such personal data, including through the disposal or retirement of hardware or the transition to new software;

(E) assess the privacy risk to an individual from the misuse of personal data by either the covered entity or third parties;

(F) assess the privacy risk from the use of algorithmic, machine learning or artificial intelligence processing of personal data. Such assessment shall include determinations of:

(i) the relevancy, accuracy, and adequacy of the data used to train the algorithm or analytical tool;

(ii) the degree to which a covered entity employee or contractor should be involved in the decision making or oversight of the results of the processing; and

(iii) whether it is likely the processing will result in substantial privacy risk.

(G) assess the potential to reduce or mitigate privacy risk by the deployment of privacy enhancing technologies; and

(H) nothing in this section shall require a covered entity to request another party to violate coordinated vulnerability disclosure best practices.

(6) PROGRAM RISK ASSESSMENT OVERSIGHT AND VALIDATION.—a periodic assessment, and in any event no less than annually, of the accountability program and supporting processes to ensure compliance with this section. The results of these assessments, and any recommendations for changes to the program, shall be reported to the appropriate personnel within the covered entity, including senior management.

(7) INCIDENT MANAGEMENT AND COMPLAINT HANDLING.—procedures for responding to data breaches and for addressing inquiries and complaints concerning personal data.

(8) INTERNAL ENFORCEMENT.—procedures for internal enforcement of the covered entity's policies and discipline for non-compliance.

(9) REDRESS.—procedures to provide remedies for privacy risk. The redress mechanisms shall be appropriate to the specific issue as well as to the size and complexity of the covered entity and the nature and scope of the covered entity's activities and data holdings. The redress mechanism shall be readily and easily accessible by the individuals to whom they are offered.

SECTION 5. OVERSIGHT OF THIRD PARTIES BY A COVERED ENTITY

(a) In the event a covered entity engages a third party to process personal data, the covered entity shall—

(1) exercise appropriate due diligence in the selection of the third party for responsibilities related to personal data, and take reasonable steps to maintain appropriate controls for the privacy and security of the personal data at issue;

(2) require the third party by contract to implement and maintain appropriate measures designed to meet the objectives and requirements required by section 4 of this Act; and

(3) implement an assessment process to periodically, and in no event less than annually, determine whether the third party is in compliance with the provisions of this Act. The assessment process shall reflect the particular circumstances of the covered entity including its size and complexity and the nature and scope of the covered entity's data holdings and activities with respect to personal data and the relative privacy risk such processing is likely to create for individuals.

(b) 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. Nothing in this section shall prohibit covered entities from providing assistance or support to other covered entities for the sole purpose of coming into compliance with the provisions of this Act.

SECTION 6. FTC RULEMAKING AUTHORITY; TECHNOLOGY NEUTRALITY REQUIREMENT; ENFORCEMENT; PENALTIES FOR NON-COMPLIANCE

(a) RULEMAKING.—

(1) AUTHORITY.—The Commission shall, in accordance with section 553 of title 5, United States Code, issue such regulations it determines to be necessary to carry out the specific sections of this Act in which such a rule is noted.

(2) AUTHORITY TO GRANT EXCLUSIONS.—The regulations prescribed under this section may include such additional exclusions from this Act as the Commission considers consistent with the purposes of this Act.

(3) LIMITATION.—In promulgating rules under this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware, nor prescribe or otherwise require that computer software or hardware products or services be designed, developed, or manufactured in a particular manner.

(b) ENFORCEMENT.—

(1) IN GENERAL.—The Attorney General and the Commission may enforce violations of this Act.

(2) CRIMINAL ACTIONS BY THE ATTORNEY GENERAL OF THE UNITED STATES.—

(A) IN GENERAL.—The Attorney General may bring an action for a criminal violation in the appropriate United States district court against any company officer 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, can be construed as acting knowingly under this statute. Providing the certification without conducting the review as described in section 7, or verifying that the review was conducted and completed, may constitute a conscious effort to avoid learning the truth.

(B) CRIMINAL PENALTIES.—Whoever provides the certification as set forth in section 7 knowing that the periodic 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.

(3) CIVIL ACTIONS BY THE COMMISSION.—

(A) IN GENERAL.—Compliance with the requirements imposed under this subtitle may be enforced pursuant to the Federal Trade Commission Act (15 U.S.C. 41 et seq.) by the Commission with respect to persons subject to this Act. All of the functions and powers of the Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person with the requirements imposed under this title.

(B) CIVIL PENALTIES.—

(i) A violation of the provisions of section 4 or 5 of this Act shall be subject to a civil penalty in an amount that is not greater than $16,500 per individual for whom the covered entity processed personal data in violation of the terms of the Act.

(ii) CIVIL PENALTY CAP.—Notwithstanding (3)(B)(i) of this section, no civil penalty shall be imposed under this Act in excess of $1,000,000,000 arising out of the same acts or omissions.

(iii) CRITERIA FOR CIVIL PENALTIES.—When determining the amount of civil penalties the Commission will take into consideration the degree of privacy risk created by the processing of the covered entity, the intent of the covered entity, the degree of culpability, any history of similar prior conduct, ability to pay, effect on the ability to continue to do business, the degree to which the covered entity put in place appropriate controls as described in section 4(h), what efforts the covered entity took to mitigate the privacy risk, and such other matters as justice may require.

(4) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed under this Act shall constitute an unfair or deceptive act or practice in commerce in violation of regulations 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 and shall be subject to enforcement by the Commission under that Act with respect to any covered entity, irrespective of whether that covered entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act.

(A) The Commission shall have the authority to seek equitable relief as it deems appropriate, including restitution, consumer redress and disgorgement.

(5) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(A) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that a covered entity has violated provisions of this Act, the State, as *parens patriae,* may bring a civil action on behalf of the residents of that State to—

(i) enjoin that act or practice;

(ii) enforce compliance with the provisions of this Act;

(iii) obtain damages, restitution, or other compensation on behalf of residents of the State; or

(iv) impose a civil penalty in an amount that is not greater than $16,500 per individual for whom the covered entity processed personal data.

(v) Notwithstanding section 6(b)(5)(iv) , no civil penalty shall be imposed under this Act in excess of $1,000,000,000, arising out of the same acts or omissions.

(vi) When determining the amount of civil penalties attorney general of the state will take into consideration the degree of privacy risk created by the processing of the covered entity, the intent of the covered entity, the degree to which the covered entity put in place appropriate controls as described in section 4(h) and what efforts the covered entity took to mitigate the privacy risk.

(B) NOTICE.—

(i) IN GENERAL.—Before filing an action under this subsection, the attorney general of the State involved shall provide to the Attorney General of the United States and the Commission—

(aa) a written notice of that action; and

(bb) a copy of the complaint for that action.

(ii) EXCEPTION.—Subparagraph (i) shall not apply with respect to the filing of an action by an attorney general of a State under this subsection if the attorney general of a State determines that it is not feasible to provide the notice described in this subparagraph before the filing of the action.

(iii) NOTIFICATION WHEN PRACTICABLE.—In an action described under subparagraph (ii), the attorney general of a State shall provide the written notice and the copy of the complaint to the Attorney General of the United States and the Commission as soon after the filing of the complaint as practicable.

(iv) FEDERAL PROCEEDINGS.—Upon receiving notice under paragraph (iii), the Attorney General of the United States and the Federal Trade Commission shall have the right to—

(aa) move to stay the action, pending the final disposition of a pending Federal proceeding or action as described in this Act;

(bb) initiate an action in the appropriate United States district court pursuant to this Act and move to consolidate all pending actions, including State actions, in such court;

(cc) intervene in an action brought under section 6(b)(5)(A); and

(dd) file petitions for appeal.

(C) PENDING PROCEEDINGS.—If the Commission initiates a federal civil action for a violation of this subtitle, or any regulations thereunder, no attorney general of a State may bring an action for a violation of this subtitle that resulted from the same or related acts or omissions against a defendant named in the Federal civil action.

(D) RULE OF CONSTRUCTION.—For purposes of bringing any civil action described in section 6(b)(5)(A), nothing in this subtitle 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—

(i) conduct investigations;

(ii) administer oaths and affirmations; or

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

(4) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under section 6(b)(2) may be brought in—

(i) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(ii) another court of competent jurisdiction.

(B) SERVICE OF PROCESS.—In an action brought under section 6(b)(2), process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

SECTION 7. SANCTION SAFE HARBOR.

(a) CIVIL PENALTIES SAFE HARBOR.—A covered entity shall:

(1) not be subject to the civil penalties described in sections 6(b)(3) or 6(b)(5)(A), if a corporate officer certifies in writing to the Commission that it has conducted a thorough review of compliance with this Act, and specifically of the accountability program required by section 4(h), and such review does not reveal any material non-compliance with the requirements of this Act for which reasonable plans have not been put in place to mitigate.

(2) annually recertify compliance with this Act to be qualified for the protection of the safe harbor described in this section.

(3) notwithstanding the above, this safe harbor shall not exempt a covered entity from equitable remedies provided under section 6(b)(4)(A) or 6(b)(5)(A)(i-iii).

(b) REPEATED VIOLATIONS.—The safe harbor provided in section 7(a) shall not be valid if:

(1) the Commission determines the covered entity has committed repeated violations of this Act;

(2) the Commission has provided written notice to the covered entity of the repeated violations, specifically informing the covered entity of the termination of its safe harbor status; and

(3) the Commission has not provided subsequent written notice that the covered entity has taken actions sufficient to mitigate the risk of future violations and specifically reinstating the safe harbor status for the covered entity.

SECTION 8. FEDERAL TRADE COMMISSION GUIDANCE; INTERNATIONAL COORDINATION; REPORTS TO CONGRESS.

(a) FEDERAL TRADE COMMISSION GUIDANCE.—Not later than one year after the date of enactment of this Act, and at least annually thereafter, the Commission shall publish:

(1) a report to Congress on recommendations to modify existing federal privacy laws which have become unnecessary or inconsistent by the provisions of this Act on whether there are additional state laws that should not be preempted by the provisions of this Act, and for government funding for the research of privacy enhancing technologies.

(2) guidance for covered entities to achieve and maintain compliance with this Act; and

(3) materials intended to assist individuals in understanding the requirements of covered entities pursuant to this Act, and the rights of individuals afforded pursuant to this Act.

(4) guidance and materials to assist covered entities with compliance with this Act, which shall include, but shall not be limited to:

(A) examples of types of data included within the definition of personal data;

(B) guidance on the analysis required for ethical uses of personal data for automated processing under section 4;

(C) guidance on the analysis required on the ethical considerations of automated uses of personal data under section 4(d)(4);

(D) guidance on examples of, and the process to determine, the situations where Explicit Notice is required under section 4(f);

(E) guidance on the form and necessary detail required in the General and Complete Notices required under section 4(f);

(F) guidance on how to provide reasonable obscurity as required in section 4(g)(6);

(G) guidance on the assessment process for third parties as required in section 5;

(H) guidance on the requirements and format for the certification described in section 7; and

(I) guidance on how covered entities can implement privacy enhancing technologies that can mitigate privacy risk as described in section 4(h)(5)(G).

(b) INTERNATIONAL COORDINATION AND COOPERATION.—Where necessary, the Commission shall coordinate any enforcement actions undertaken pursuant to this Act

with the Data Protection Authorities or similar offices of foreign nations in a manner consistent with authorities codified at section 6, subsections (j)-(k) of the Federal Trade Commission Act (15 U.S.C. 46).

(c) REPORTS TO CONGRESS.—Not later than 180 days after the date of enactment of this Act, and at least annually thereafter, the Commission shall submit to Congress and make available on a public website a report concerning the effectiveness of this Act, compliance by covered entities, violations of this Act and enforcement actions undertaken, if any, to resolve those violations, enforcement priorities and resources needed by the Commission to fully implement and enforce this Act and regulations promulgated pursuant to this Act.

SECTION 9. FTC RESOURCES

(a) APPOINTMENT OF ATTORNEYS.—Notwithstanding any other provision of law, the Director of the Bureau of Consumer Protection of the Commission may, without regard to the civil service laws (including regulations), appoint not more than 250 additional personnel in attorney positions in the Division of Privacy and Identity Protection of the Bureau of Consumer Protection.

(b) APPOINTMENT OF SUPPORT PERSONNEL.—Notwithstanding any other provision of law, the Director of the Bureau of Consumer Protection of the Federal Trade Commission may, without regard to the civil service laws (including regulations), appoint not more than 250 additional personnel in project management, technical and administrative support positions in the Division of Privacy and Identity Protection of the Bureau of Consumer Protection.

(c) AUTHORIZATION OF APPROPRIATIONS.—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.

SECTION 10. PREEMPTION.

(a) PREEMPTION.—For a covered entity that is subject to this subtitle, the provisions of this subtitle shall preempt any civil provisions of the law of any State or political subdivision of a State to the degree they are focused on the reduction of privacy risk through the regulation of personal data collection and processing activities.

(b) CONSUMER PROTECTION LAWS.—Except as provided in subsection (a), this section shall not be construed to limit the enforcement, or the bringing of a claim pursuant to any State consumer protection law by an attorney general of a State, other than the extent to which those laws regulate personal data collection and processing.

(c) PROTECTION OF CERTAIN STATE LAW.—Nothing in this Act shall be construed to preempt the applicability of—

(1) State constitutional, trespass, contract, data breach notification or tort law, other than to the degree such laws are substantially intended to govern personal data collection and processing; or

(2) any other state law to the extent that the law relates to acts of fraud, wiretapping or the protection of social security numbers.

(3) any state law to the extent it provides additional provisions to specifically regulate the covered entities as defined in the Health Insurance Portability and Accountability Act of 1996 (Pub.L. 104-191), the Family Educational Rights and Privacy Act (Pub.L. 93-380), the Fair Credit Reporting Act (Pub.L. 91-508) or the Financial Services Modernization Act of 1999 (Pub.L. 106-102).

(4) Private contracts based on any state law that require a party to provide additional or greater personal data privacy or data security protections to an individual than does this Act.

(d) PRESERVATION OF FTC AUTHORITY.—Nothing in this Act may be construed in any way to limit the authority of the Federal Trade Commission under any other provision of law.

(e) FCC AUTHORITY.—Insofar as any provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.), including but not limited to section 222 of the Communications Act of 1934 (47 U.S.C. 222), or any regulations promulgated under such Act apply to any person, partnership, or corporation subject to this Act with respect to privacy policies, terms of service, and practices covered by this Act, such provision of the Communications Act of 1934 or such regulations shall have no force or effect, unless such regulations pertain to emergency services.

SECTION 11. SAVINGS.—Nothing in this Act may be construed in any way to limit an individual's rights and privileges under the U.S. Constitution, including, but not limited to, those protections of free speech and assembly.

SECTION 12. EFFECTIVE DATE.

(a) EFFECTIVE DATE.—This Act shall take effect on the expiration of the date that is 180 days after the date of enactment of this Act.

(b) NO RETROACTIVE APPLICABILITY.—This Act shall not apply to any conduct that occurred before the effective date under subsection (a).