116TH CONGRESS
1ST SESSION

S. _____

To improve the protection of personal privacy by enacting nationwide standards governing the collection, use and sharing of personal data consistent with the Fair Information Practice Principles.

_____

IN THE SENATE OF THE UNITED STATES

May 23, 2019

[Senators Introducing and Co-Sponsoring]

_____

A BILL

To improve the protection of personal privacy by enacting nationwide standards governing the 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 2019"

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

Section 2. FINDINGS

Congress finds that –

(a) Individuals need to be 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. Use of personal data by organizations can also produce adverse consequences for individuals, such as discrimination and loss of liberty, and can produce adverse consequences to society, such as avoidance of social and commercial systems and weakening of democratic engagement.

(c) An individual has a legal interest in the lawful processing of personal data. When personal data is processed in violation of law, such violation constitutes an invasion of the individual's

legal interest. Whether or not the adverse consequences can be quantified by economic impact, monetary loss or physical harm to the individual does not indicate that a violation of an individual's legal interest did not occur or that the adverse consequence is conjectural, hypothetical or speculative.

(d) Organizations that create, collect, or process personal data, as defined by the provisions of this Act, should institute a comprehensive privacy program consistent with the codification of the Fair Information Practice Principles.

(e) A comprehensive privacy 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 an organization.

(f) A comprehensive privacy program should be designed to—

(1) consider and protect an individual’s privacy throughout the information life cycle;

(2) facilitate an individual’s control over personal data, including the ability to participate in decision-making regarding the processing of that personal data;

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

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

(5) protect against reasonably foreseeable threats and vulnerabilities to the security of personal data or to the legitimate privacy interests of an individual, including following standard industry practices regarding installation of 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 by the individual to whom the personal data relates; and

(8) prevent the use or application of outputs from machine learning, algorithmic analysis, predictive analytics, or similar analysis that would violate any state or federal law or regulation to 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) to create, gather, buy, rent, obtain, receive, infer, or access any personal data pertaining to an individual by any means; or

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

(3) EXCLUSIONS.—The term "collect" does not include the acquisition of personal data solely to facilitate 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) **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) EXCLUSIONS.—The term "covered entity" does not include—

(A) a person, otherwise covered by Section 3(c)(1)-(3) of this Act, which—

(i) has fewer than 25 employees;

(ii) collects or utilizes the personal data of fewer than 50,000 individuals; and

(iii) derives less than half of all revenue annually from the sale of personal data; or

(B) a person, otherwise covered by Section 3(c)(1)-(3) of this Act, to the extent such person—

(i) provides electronic data transmission, routing, intermediate and transient storage or connection to its system or network, when the person providing such services is not the sender or the intended recipient of the data, and does not select, access, review, or modify the content of the electronic data or otherwise perform or conduct any analytical, algorithmic or machine learning processes on such data, other than to—

(I) ensure the security of the data and the networks, systems, software, hardware or devices employed by the person; or

(II) aid in the efficiency of the transmission of the data.

(ii) Any such person shall be excluded from the definition of covered entity under this Act only to the extent the person is engaged in the provision of such transmission, routing, intermediate and transient storage, or connections as provided in Section 3(c)(4)(B).

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

(e) **INDIVIDUAL.**—The term "individual" means a living natural person.

(f) **EXPLICIT CONSENT.**—The term "explicit consent" means a clear, affirmative act establishing a freely-given, specific, and unambiguous indication of the individual's agreement to the processing of such individual's personal data.

(g) **PERSONAL DATA.**—

(1) The term "personal data" means any information relating to an identified or identifiable individual.

(2) Modified definition by rulemaking.—The Commission may, by rule promulgated under section 553 of title 5, United States Code, exempt specific categories of information from the definition of personal data under Section 3(g)(1).

(h) **PRIVACY PROGRAM.**— The term "privacy program" means the program described in Section 4 of this Act.

(i) **PRIVACY RISK.**—

(1) The term "privacy risk" means potential adverse consequences to an individual or society arising from the processing of personal data, including, but not limited to:

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

(B) Physical harm;

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

(D) Significant inconvenience or expenditure of time;

(E) Negative or harmful 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 the granting of less favorable terms), housing, education, professional certification, or the provision of health care and related services;

(F) Stigmatization or reputational harm;

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

(H) Price discrimination;

(I) 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—

(i) alter that individual's experiences;

(ii) limit that individual's choices;

(iii) influence that individual's responses; or

(iv) predetermine results or outcomes for that individual; or

(J) other demonstrable 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, observed, or used.

(2) *Modified definition by rulemaking*.—Not later than 1 year after the date of enactment of this Act, the Commission shall, by rule promulgated under section 553 of title 5, United States Code, identify the criteria and methodology to assess and evaluate privacy risk to an individual and privacy risk to society arising from the processing of personal data. Such regulations may identify potential adverse consequences that should be excluded from the definition of privacy risk as well as additional potential adverse consequences that shall be treated as privacy risk under this Act.

(j) **PROCESSING.**—The term "processing" means any operation or set of operations that is performed on personal data, including, but not limited to, creation, generation, collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure, transfer, dissemination or otherwise making available, combination, erasure, or destruction.

(k) **SOCIETAL BENEFIT.**—The term "societal benefit" means a material, objective and identifiable positive effect or advantageous outcome accruing to the public as a result of the processing of personal data. To meet the requirements of this Act, a societal benefit must—

(1) promote and enhance the well being of the general public; and

(2) be separate and distinct from any positive outcome, advantageous impact or value that accrues to a covered entity, single person or individual, or a narrow or specific group of persons.

(l) **STANDARD FOR PROCESSING.**—The term "standard for processing" means a covered entity's legal obligation when processing personal data of an individual to prevent reasonably foreseeable privacy risk to that individual. A covered entity violates the standard for processing when the covered entity acts with reckless disregard for privacy risk to an individual arising out of the processing of the individual's personal data.

(1) When determining if a covered entity violated the standard for processing in a given context, the following factors shall be considered:

(A) The covered entity's intent to undertake the processing that caused the privacy risk to the individual;

(B) The foreseeability of privacy risk to the individual;

(C) The closeness or proximity of the connection between the covered entity's processing activity and the severity of privacy risk suffered by the individual; and

(D) The availability, cost, and commonness of measures that could have been taken to mitigate the privacy risk.

(2) A covered entity may act with reckless disregard and thereby violate the standard for processing even if the covered entity does not intend to cause privacy risk. It is sufficient for the purposes of this Act that the covered entity intends to undertake the processing activity that causes the privacy risk to the individual.

(m) **THIRD PARTY.**— The term "third party" means—

(1) with respect to any covered entity, a person that is not related to the covered entity by common ownership or corporate control; and

(2) the covered entity either—

(A) engages such person to process personal data on behalf of or at the direction of the covered entity; or

(B) transfers, sells, shares, makes available, allows access or otherwise provides personal data to such person.

(3) A third party may itself be a covered entity and otherwise subject to this Act.

Section 4. IMPLEMENTATION OF FAIR INFORMATION PRACTICE PRINCIPLES THROUGH ESTABLISHMENT OF A COMPREHENSIVE PRIVACY PROGRAM.

(a) **COLLECTION LIMITATION.**— A covered entity shall not collect any personal data that is not relevant and necessary to accomplish the purpose(s) specified by the covered entity as required in Section 4(c).

(b) **DATA QUALITY.**—

(1) 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.

(2) 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 described in the notices required by Section 4(f). Such description shall be clear and specific in relation to the intended uses of the personal data by the covered entity.

(d) **USE LIMITATION.**— A covered entity may not process personal data unless the processing is consistent with the provisions of this section.

(1) *Permitted Processing.*—Except as provided in Section 4(d)(3) below, a covered entity may process personal data as follows:

(A) for any purpose for which the individual to whom the personal data relates provides explicit consent as long as the provision of consent by the individual is not 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) if, after conducting and documenting an analysis, the covered entity concludes that—

(i) the purposes of processing personal data of an individual are consistent with the purposes specified pursuant to Section 4(c), taking into account—

(I) the relationship between the individual and the covered entity; and

(II) the degree to which the individual would reasonably expect the processing of the personal data given the specified purpose; and

(ii) the processing activity does not present an unreasonable amount of privacy risk, taking into account—

(I) the likelihood and potential severity of privacy risk to the individual whose personal data is being processed;

(II) the potential benefit of the processing activity to that individual;

(III) the privacy risk and potential benefits to an individual who may be impacted by the processing whether or not the covered entity is processing the personal data of that individual; and

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

(2) *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 does the following:

(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 risk, as defined in Section 3(i) of this Act, to the individual. Such analysis 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 an unreasonable amount of privacy risk.

(3) *Prohibited Uses.*—Notwithstanding Section 4(d)(1)-(2) of this Act, a covered entity shall not process personal data when—

(A) the covered entity knows, or has reason to know, that the processing of the personal data will likely—

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

(ii) interfere with, or deny, an individual his or her rights and privileges under the United States Constitution; or

(B) the processing violates the standard for processing, as defined in Section 3*(*l).

(4) *Presumptions*.—When relying upon the provisions of this Act to process personal data, the covered entity bears the burden to establish that it has satisfied the requirements set forth in this Act.

(5) *Rulemaking.*—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, on the scope of the application of the use limitations in Section 4(d)(1)-(2) including the criteria

and methodology to assess and evaluate privacy risk and benefits arising from the processing of personal data that the Commission determines to be appropriate and consistent with the purposes of this Act.

(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 personal data;

(3) protect against unauthorized processing of personal data; and

(4) incorporate security updates provided by the manufacturers of hardware and software products consistent with coordinated vulnerability disclosure best practices

(f) **OPENNESS.**—

(1) A covered entity shall provide an individual, government agencies, and the public with information concerning the covered entity's processing of personal data.

(2) *Explicit Notice*.—A covered entity shall provide explicit notice to an individual prior to the collection of personal data from that individual that is likely to be used by the covered entity or a third party in one or more of the following ways:

(A) Identification of geolocation;

(B) Biometric identification, including, but not limited to, facial recognition;

(C) Identification of racial or ethnic origin;

(D) Determination of an individual's religion or religious practice;

(E) Analysis of 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) Analysis of sexual life, including sexual activity, sexual orientation, sexual preference, and/or sexual behavior;

(G) Analysis of DNA or genetic history;

(H) Analysis of activities inside an individual's home or equivalent location where an individual has a reasonable expectation of privacy including a hotel room, rented room, locker room, dressing room, restroom, or mobile home; or

(I) Such other processing of personal data identified by the Commission pursuant to rules promulgated under Section 4(f)(5).

(J) *Exceptions*.—Explicit Notice is not required in the following circumstances:

(i) The method or circumstances of collection of personal data from the individual was not reasonably foreseeable by the covered entity;

(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 covered entity to violate the law; or

(iv) The covered entity provides a substantially similar notice to the individual pursuant to other federal or state law.

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

(A) The privacy policy shall include information describing how an individual may—

(i) access personal data that is processed;

(ii) correct erroneous personal data;

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

(iv) contact a third party to whom the personal data was sold, shared, transferred, or otherwise provided; and

(v) obtain deletion of the personal data, and any analysis or predictions based upon the processing of that personal data.

(B) The privacy policy shall be—

(i) clear and drafted in plain language;

(ii) conspicuous and published in a prominent location;

(iii) made publicly accessible—

(I) prior to collection; or

(II) where notice prior to collection is impossible or impracticable, the privacy policy shall be made publicly accessible before additional processing of that personal data by the covered entity and before processing is completed that is reasonably likely to create privacy risk.

(4) *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:

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

(5) *Rulemaking.*—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to carry out and to facilitate the notice requirements set forth in Section 4(f) of this Act. In promulgating such regulations, the Commission shall determine the means and timing of the notices required under this section, taking into account the different media, devices, or methods through which the covered entity collects personal data.

(g) **INDIVIDUAL PARTICIPATION.**— A covered entity shall provide an individual with a readily available means of promptly obtaining the following:

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

(2) A description of each category of personal data processed by the covered entity;

(3) A plain language explanation of the specific types of personal data collected about the individual;

(4) A description of the processing of the personal data concerning the individual, including processing undertaken by a third-party;

(5) Reasonable access to the personal data;

(6) Ability to correct or supplement erroneous personal data with additional information offered voluntarily by the individual to address data quality requirements as described in Section 4(b); and

(7) 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 societal benefit of the availability of the personal data.

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

(B) The requirements set forth in this paragraph shall not come into effect until the Commission publishes the guidance described in Section 8(a)(2) below.

(8) *Exception*.—An individual may not 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.

(9) *Exclusion*.—Nothing in Section 4(g) shall require a covered entity to take an action that jeopardizes the safety of an individual or the rights and freedoms guaranteed to an individual under the Constitution of the United States.

(10) *Rulemaking*.—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to identify practical and reasonable means for a covered entity to satisfy the requirements of Section 4(g) of this Act and otherwise carry out and facilitate the requirements set forth in this *section* of this Act.

(h) **ACCOUNTABILITY.**—A covered entity shall ensure compliance with this Act by developing and implementing an ongoing accountability program that includes:

(1) *Policies*.—A covered entity shall internally publish and implement written policies and procedures implementing the requirements of this Act.

(2) *Internal Leadership, Staffing, And Oversight*.—A covered entity shall appoint a data privacy leader responsible for developing and implementing the covered entity's privacy 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.

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

(3) *Staffing*.—A covered entity shall dedicate resources to ensure that the privacy program is reasonably 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*.—A covered entity shall develop and deploy an up-to-date education and awareness program to keep any employee, contractor, and third party aware of data protection obligations.

(5) *Incident Management and Complaint Handling*.—A covered entity shall develop and implement procedures for—

(A) responding to privacy incidents, such as the misuse of personal data and unauthorized access to personal data; and

(B) addressing inquiries and complaints concerning the collection and processing of personal data.

(6) *Ongoing Risk Assessment and Mitigation.*— A covered entity shall develop, document, and implement an ongoing, entity-wide process to identify, assess, and mitigate reasonably foreseeable privacy risk, including privacy risk raised by new products, services, technologies, methods of processing, and business models. Such process shall do the following:

(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, including misuse of personal data by third parties;

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

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

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

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

(ii) The degree to which an individual employed or retained by the covered entity should be involved in the decision making or oversight of the results of the processing covered by this paragraph; and

(iii) Whether it is likely the processing will result in unreasonable privacy risk; and

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

(7) *Program Risk Assessment and Validation.*— A covered entity shall conduct a periodic assessment, in any event no less than annually, of the privacy program and supporting processes to ensure compliance with this Act. 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.

(8) *Internal Enforcement*.—A covered entity shall develop and implement procedures for internal enforcement of the covered entity's policies and discipline for non-compliance.

(9) *Redress*.—A covered entity shall develop and implement procedures to provide remedies for privacy risk. The redress mechanisms shall be appropriate to the specific issue, 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 any individual to whom it is offered.

(10) *Exclusion.*—Nothing in Section 4(h) shall require a covered entity to request another party to violate coordinated vulnerability disclosure best practices.

(11) *Rulemaking.*—Not later than 1 year after the date of the enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to identify practical and reasonable means for a covered entity to implement an accountability program, satisfy the requirements of Section 4(h) of this Act, and otherwise carry out and facilitate the requirements set forth in Section 4(h) of this Act.

Section 5. OVERSIGHT OF THIRD PARTIES BY A COVERED ENTITY.

(a) **PROCESSING ON BEHALF OF A COVERED ENTITY.**—In the event a covered entity engages a third party to process personal data on behalf of and at the direction of the covered entity, 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 by contract that the third party—

(A) shall implement and maintain appropriate measures designed to meet the objectives and requirements required by Section 4 of this Act;

(B) is prohibited from processing such personal data except on instructions from the covered entity, unless otherwise required to do so by law; and

(C) does not disclose the personal data received from or on behalf of the covered entity, or any personal data derived from such data, other than as directed by the covered entity; and

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

(b) **SELLING, SHARING, TRANSFERRING OR OTHERWISE PROVIDING OR ALLOWING ACCESS.**— In the event a covered entity transfers, sells, shares, makes available, allows access or otherwise provides personal data to a third party the covered entity shall:

(1) exercise appropriate due diligence to ensure, to the extent practicable, that—

(A) the third party has the capacity to process personal data in compliance with this Act and other applicable laws; and

(B) the third party will take reasonable steps to maintain appropriate controls for the privacy and security of the personal data at issue;

(2) require by contract that the third party shall 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 has reasonable and appropriate measure in place to comply with the provisions of this Act and any obligations imposed on the third party with respect to processing the personal data. The assessment process shall reflect the particular circumstances of the covered entity, including its size and complexity, the nature and scope of the covered entity's data holdings, and the covered entity's activities with respect to personal data, and the relative privacy risk such processing is likely to create for an individual.

(c) **MEANS AND INSTRUMENTALITY LIABILITY**.—It shall be a violation of this Act for a covered entity to provide substantial assistance or support for or related to the processing of personal data to any person when that covered entity knows or consciously avoids knowing that the person is engaged in ongoing or systemic acts or practices that violate this Act. Nothing in this section shall prohibit a covered entity from providing assistance or support to a person 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, promulgate regulations as authorized by the specific provisions of this Act. In promulgating such regulations the Commission shall consider that such regulations must be practical, reasonable, and appropriate for a covered entity taking into account—

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

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

(C) the potential privacy risk created by such processing.

(2) *Authority To Grant Exclusions*.—In promulgating rules under this Act, the Commission may implement 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) *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 officer of a covered

entity 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 of this Act, 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 of this Act 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.

(2) *Civil Actions By The Commission*.—

(A) *Unfair Or Deceptive Acts Or Practices*.—For the purpose of the exercise by the Commission of its functions and powers under the Federal Trade Commission Act (15 U.S.C. 41 *et seq.*), 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.

(B) *Powers of the Commission.*—The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any person who violates such regulations shall be subject to the penalties and entitled to the privileges and immunities provided in that Act.

(i) *Independent Litigating Authority.*—Notwithstanding Section 6(b)(2)(B), the Commission is authorized to litigate cases, by its own attorneys, before any federal court or tribunal within the judicial branch of the United States in order to enforce the provisions of this Act. Such litigation authority includes authority to initiate, defend, or appeal legal actions; enter and enforce orders issued for violations of this Act; litigate court orders related to proceedings to enforce this Act; and argue appeals of such orders or court decisions related to enforcement of this Act.

(ii) *Equitable Relief.*—The Commission shall have the authority to seek equitable relief, as it deems appropriate, including injunctive relief, restitution, consumer redress, and disgorgement.

(C) *Civil Penalties*.—

(i) *Civil Penalty Cap*.—

(I) Notwithstanding Section 6(b)(2)(C), no civil penalty shall be imposed under this Act in excess of $1,000,000,000 arising out of the same acts or omissions.

(II) The civil penalty cap set forth in Section 6(b)(2)(C)(i)(I) does not apply to civil penalties related to a violation of a Commission order or otherwise imposed pursuant to statutes or regulations enforced by the Commission.

(ii) *Criteria for Civil Penalties*.—When determining the amount of civil penalties, the Commission shall consider 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.

(3) *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.

(B) *Civil Penalty Cap.*—Notwithstanding Section 6(b)(3)(A)(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.

(C) *Criteria for Civil Penalties.*—When determining the amount of civil penalties the Commission shall consider 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.

(D) *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 a written notice of that action and a copy of the complaint for that action.

(ii) *Exception*.—Section 6(b)(3)(D)(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 Section 6(b)(3)(D)(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 Section 6(b)(3)(D)(iii), the Attorney General of the United States and the Federal Trade Commission shall have the right to—

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

(II) 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;

(III) intervene in an action brought under Section 6(b)(3)(A); and

(IV) file petitions for appeal.

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

(F) *Rule Of Construction*.—For purposes of bringing any civil action described in Section 6(b)(3)(A), nothing in this Act 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.

Section 7. SAFE HARBOR.

(a) SAFE HARBOR FOR CIVIL PENALTIES.—A covered entity shall not be subject to the civil penalties described in Section 6(b)(2) or Section 6(b)(3)(A) if—

(1) an officer of the covered entity certifies in writing to the Commission that—

(A) the covered entity has conducted a thorough review of the implementation and operation of the privacy program required by Section 4(h); and

(B) such review does not reveal any material non-compliance with the requirements of this Act; and

(2) an officer of the covered entity recertifies compliance with this Act as required in Section 7(a)(1) no less than annually.

(b) Notwithstanding Section 7(a), this safe harbor shall not exempt a covered entity from equitable remedies provided under Section 6(b)(2)(B)(i) or Section 6(b)(3)(A)(i)-(iii).

(c) REPEATED VIOLATIONS.— The safe harbor provided by this Act shall not be valid if—

(1) the Commission has reason to believe that the covered entity has committed repeated violations of this Act;

(2) the Commission has provided written notice to the covered entity of the Commission's determination that it has reason to believe that the covered entity has repeatedly violated this Act and has suspended the covered entity's 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. GUIDANCE; INTERNATIONAL COORDINATION; REPORTS TO CONGRESS.

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

(1) materials intended to assist an individual in understanding the requirements of covered entities pursuant to this Act, and the rights of an individual afforded pursuant to this Act; and

(2) guidance and materials to assist a covered entity 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(d)(2);

(C) Guidance on the analysis required on the ethical considerations of automated uses of personal data under Section 4(d)(2);

(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)(7);

(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 mitigate privacy risk as described in Section 4(h)(6)(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 eighteen months after the date of enactment of this Act, and at least bi-annually thereafter, the Commission shall submit to Congress and make

available to the public a report concerning the effectiveness of this Act. The report shall address, at a minimum, the following topics:

(1) Compliance by covered entities;

(2) Violations of this Act and enforcement actions undertaken, if any, to resolve those violations;

(3) Enforcement priorities and resources needed by the Commission to fully implement and enforce this Act;

(4) Efforts to educate individuals regarding their rights under this Act and provide guidance to covered entities regarding compliance with this Act;

(5) Regulations promulgated pursuant to this Act; and

(6) Recommendations to modify provisions of this Act or provisions of other federal privacy laws in order to avoid or eliminate inconsistent requirements, duplicative obligations, or rules that may no longer be necessary or provide a benefit to consumers.

Section 9. FTC RESOURCES.

(a) **APPOINTMENT OF ATTORNEYS.** —Notwithstanding any other provision of law, the Chair 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 Chair of the 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 Commission such sums as may be necessary to carry out this section.

Section 10. PREEMPTION.

(a) **PREEMPTION.**—For a covered entity subject to this Act, the provisions of this Act 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 Section 10(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) the constitutional, trespass, contract, data breach notification or tort law of any state, other than to the degree such laws are substantially intended to govern personal data collection and processing;

(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); or

(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 COMMISSION AUTHORITY.**—Nothing in this Act may be construed to in any way limit the authority of the 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 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.

(f) **TREATMENT OF COVERED ENTITIES GOVERNED BY OTHER FEDERAL LAW.**—Covered entities subject to 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), are excluded from the provisions of this Act to the degree specific uses of personal data are covered by the privacy provisions of those laws.

Section 11. SAVINGS.—

Nothing in this Act may be construed to in any way 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 Section 12(a).