116TH CONGRESS
1ST SESSION

S. 2968

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

IN THE SENATE OF THE UNITED STATES

DECEMBER 3, 2019

Ms. CANTWELL (for herself, Mr. SCHATZ, Ms. KLOBUCHAR, and Mr. MARKEY) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

---

A BILL

To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the ''Consumer Online Privacy Rights Act''.

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

SEC. 2. DEFINITIONS.

In this Act:

(1) AFFIRMATIVE EXPRESS CONSENT.—

(A) IN GENERAL.—The term ''affirmative express consent'' means an affirmative act by an individual that clearly communicates the individual's authorization for an act or practice, in response to a specific request that meets the requirements of subparagraph (B).

(B) REQUEST REQUIREMENTS.—The requirements of this subparagraph with respect to a request from a covered entity to an individual are the following:

(i) The request is provided to the individual in a standalone disclosure.

(ii) The request includes a description of each act or practice for which the individual's consent is sought and—

(I) clearly distinguishes between an act or practice which is necessary to fulfill a request of the individual and an act or practice which is for another purpose; and

(II) is written in easy-to-understand language and includes a prominent heading that would enable a reasonable individual to identify and understand the act or practice.

(iii) The request clearly explains the individual's applicable rights related to consent.

(C) EXPRESS CONSENT REQUIRED.—An entity shall not infer that an individual has provided affirmative express consent to an act or practice from the inaction of the individual or the individual's continued use of a service or product provided by the entity.

(2) ALGORITHMIC DECISION-MAKING.—The term ''algorithmic decision-making'' means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques that makes a decision or facilitates human decision-making with respect to covered data.

(3) BIOMETRIC INFORMATION.—

(A) IN GENERAL.—The term ''biometric information'' means any covered data generated from the measurement or specific technological processing of an individual's biological, physical, or physiological characteristics, including—

(i) fingerprints;

(ii) voice prints;

(iii) iris or retina scans;

(iv) facial scans or templates;

(v) deoxyribonucleic acid (DNA) information; and

(vi) gait.

(B) EXCLUSIONS.—Such term does not include writing samples, written signatures, photographs, voice recordings, demographic data, or physical characteristics such as height, weight, hair color, or eye color, provided that

such data is not used for the purpose of identifying an individual's unique biological, physical, or physiological characteristics.

(4) COLLECT; COLLECTION.—The terms ''collect'' and ''collection'' mean buying, renting, gathering, obtaining, receiving, accessing, or otherwise acquiring covered data by any means, including by passively or actively observing the individual's behavior.

(5) COMMON BRANDING.—The term ''common branding'' means a shared name, servicemark, or trademark.

(6) CONTROL.—The term ''control'' means, with respect to an entity—

(A) ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of the entity;

(B) control in any manner over the election of a majority of the directors of the entity (or of individuals exercising similar functions); or

(C) the power to exercise a controlling influence over the management of the entity.

(7) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(8) COVERED DATA.—

(A) IN GENERAL.—The term ''covered data'' means information that identifies, or is linked or reasonably linkable to an individual or a consumer device, including derived data.

(B) EXCLUSIONS.—Such term does not include—

(i) de-identified data;

(ii) employee data; and

(iii) public records.

(9) COVERED ENTITY.—

(A) IN GENERAL.—The term ''covered entity'' means any entity or person that—

(i) is subject to the Federal Trade Commission Act (15 U.S.C. 41 et seq.); and

(ii) processes or transfers covered data.

(B) INCLUSION OF COMMONLY CONTROLLED AND COMMONLY BRANDED ENTITIES.—Such term includes any entity or person that controls, is controlled by, is under common control with, or shares common branding with a covered entity.

(C) EXCLUSION OF SMALL BUSINESS.—Such term does not include a small business.

(10) DE-IDENTIFIED DATA.—Term ''de-identified data'' means information that cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or household, provided that the entity—

(A) takes reasonable measures to ensure that the information cannot be reidentified, or associated with, an individual, a household, or a device used by an individual or household;

(B) publicly commits in a conspicuous manner—

(i) to process and transfer the information in a de-identified form; and

(ii) not to attempt to reidentify or associate the information with any individual, household, or device used by an individual or household; and

(C) contractually obligates any person or entity that receives the information from the covered entity to comply with all of the provisions of this paragraph.

(11) DERIVED DATA.—The term ''derived data'' means covered data that is created by the derivation of information, data, assumptions, or conclusions

from facts, evidence, or another source of information or data about an individual, household, or device used by an individual or household.

(12) EMPLOYEE DATA.—The term ''employee data'' means—

(A) covered data that is collected by a covered entity or the covered entity's service provider about an individual in the course of the individual's employment or application for employment (including on a contract or temporary basis) provided that such data is retained or processed by the covered entity or the covered entity's service provider solely for purposes necessary for the individual's employment or application for employment;

(B) covered data that is collected by a covered entity or the covered entity's service provider that is emergency contact information for an individual who is an employee, contractor, or job applicant of the covered entity provided that such data is retained or processed by the covered entity or the covered entity's service provider solely for the purpose of having an emergency contact for such individual on file; and

(C) covered data that is collected by a covered entity or the covered entity's service provider about an individual (or a relative of an individual) who is an employee or former employee of the covered entity for the purpose of administering benefits to which such individual or relative is entitled on the basis of the individual's employment with the covered entity, provided that such data is retained or processed by the covered entity or the covered entity's service provider solely for the purpose of administering such benefits.

(13) EXECUTIVE AGENCY.—The term ''Executive agency'' has the meaning given such term in section 105 of title 5, United States Code.

(14) INDIVIDUAL.—The term ''individual'' means a natural person residing in the United States, however identified, including by any unique identifier.

(15) LARGE DATA HOLDER.—The term ''large data holder'' means a covered entity that, in the most recent calendar year—

(A) processed or transferred the covered data of more than 5,000,000 individuals, de-

vices used by individuals or households, or households; or

(B) processed or transferred the sensitive covered data of more than 100,000 individuals, devices used by individuals or households, or households.

(16) PROCESS.—The term ''process'' means any operation or set of operations performed on covered data including collection, analysis, organization, structuring, retaining, using, or otherwise handling covered data.

(17) PROCESSING PURPOSE.—The term ''processing purpose'' means an adequately specific and granular reason for which a covered entity processes covered data that clearly describes the processing activity.

(18) PUBLICLY AVAILABLE INFORMATION.—

(A) IN GENERAL.—The term ''publicly available information'' means—

(i) information that a covered entity has a reasonable basis to believe is lawfully made available to the general public from widely distributed media; and

(ii) information that is directly and voluntarily disclosed to the general public

by the individual to whom the information relates.

(B) LIMITATION.—Such term does not include—

(i) information derived from publicly available information;

(ii) biometric information; or

(iii) nonpublicly available information that has been combined with publicly available information.

(19) PUBLIC RECORDS.—The term ''public records'' means information that is lawfully made available from Federal, State, or local government records provided that the covered entity processes and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity.

(20) SENSITIVE COVERED DATA.—The term ''sensitive covered data'' means the following forms of covered data:

(A) A government-issued identifier, such as a Social Security number, passport number, or driver's license number.

(B) Any information that describes or reveals the past, present, or future physical

health, mental health, disability, or diagnosis of an individual.

(C) A financial account number, debit card number, credit card number, or any required security or access code, password, or credentials allowing access to any such account.

(D) Biometric information.

(E) Precise geolocation information that reveals the past or present actual physical location of an individual or device.

(F) The content or metadata of an individual's private communications or the identity of the parties to such communications unless the covered entity is an intended recipient of the communication.

(G) An email address, telephone number, or account log-in credentials.

(H) Information revealing an individual's race, ethnicity, national origin, religion, or union membership in a manner inconsistent with the individual's reasonable expectation regarding disclosure of such information.

(I) Information revealing the sexual orientation or sexual behavior of an individual in a manner inconsistent with the individual's rea-

sonable expectation regarding disclosure of such information.

(J) Information revealing online activities over time and across third party websites or online services.

(K) Calendar information, address book information, phone or text logs, photos, or videos maintained on an individual's device.

(L) A photograph, film, video recording, or other similar medium that shows the naked or undergarment-clad private area of an individual.

(M) Any other covered data processed or transferred for the purpose of identifying the above data types.

(N) Any other covered data that the Commission determines to be sensitive covered data through a rulemaking pursuant to section 553 of title 5, United States Code.

(21) SERVICE PROVIDER.—

(A) IN GENERAL.—The term ''service provider'' means a covered entity that processes or transfers covered data in the course of performing a service or function on behalf of, and at the direction of, another covered entity, but

only to the extent that such processing or transferral—

(i) relates to the performance of such service or function; or

(ii) is necessary to comply with a legal obligation or to establish, exercise, or defend legal claims.

(B) EXCLUSION.—Such term does not include a covered entity that processes or transfers the covered data outside of the direct relationship between the service provider and the covered entity.

(22) SERVICE PROVIDER DATA.—The term ''service provider data'' means covered data that is collected by or has been transferred to a service provider by a covered entity for the purpose of allowing the service provider to perform a service or function on behalf of, and at the direction of, such covered entity.

(23) SMALL BUSINESS.—

(A) IN GENERAL.—The term ''small business'' means an entity that can establish that, with respect to the 3 preceding calendar years (or for the period during which the entity has

been in existence if, as of such date, such period is less than 3 years) the entity does not—

(i) maintain annual average gross revenue in excess of $25,000,000;

(ii) annually process the covered data of an average of 100,000 or more individuals, households, or devices used by individuals or households; and

(iii) derive 50 percent or more of its annual revenue from transferring individuals' covered data.

(B) COMMON CONTROL; COMMON BRANDING.—For purposes of subparagraph (A), the annual average gross revenue, data processing volume, and percentage of annual revenue of an entity shall include the revenue and processing activities of any person that controls, is controlled by, is under common control with, or shares common branding with such entity.

(24) THIRD PARTY.—The term ''third party''—

(A) means any person or entity that—

(i) processes or transfers third party data; and

(ii) is not a service provider with respect to such data; and

(B) does not include a person or entity that collects covered data from another entity if the two entities are related by common ownership or corporate control and share common branding.

(25) THIRD PARTY DATA.—The term ''third party data'' means covered data that is transferred to a third party by a covered entity.

(26) TRANSFER.—The term ''transfer'' means to disclose, release, share, disseminate, make available, sell, license, or otherwise communicate covered data by any means to a service provider or third party—

(A) in exchange for consideration; or

(B) for a commercial purpose.

(27) UNIQUE IDENTIFIER.—The term ''unique identifier'' means an identifier that is reasonably linkable to an individual, household, or device used by an individual or household, including a device identifier, an Internet Protocol address, cookies, beacons, pixel tags, mobile ad identifiers, or similar technology, customer number, unique pseudonym, or user alias, telephone numbers, or other forms of persistent or probabilistic identifiers that can be used to

identify a particular individual, a household, or a device.

(28) WIDELY DISTRIBUTED MEDIA.—The term ''widely distributed media'' means information that is available to the general public, including information from a telephone book or online directory, a television, internet, or radio program, the news media, or an internet site that is available to the general public on an unrestricted basis, but does not include an obscene visual depiction as defined in section 1460 of title 18, United States Code.

SEC. 3. EFFECTIVE DATE.

This Act shall take effect on the date that is 180 days after the date of enactment of this Act.

TITLE I—DATA PRIVACY RIGHTS

SEC. 101. DUTY OF LOYALTY.

(a) IN GENERAL.—A covered entity shall not—

(1) engage in a deceptive data practice or a harmful data practice; or

(2) process or transfer covered data in a manner that violates any provision of this Act.

(b) DEFINITIONS.—

(1) DECEPTIVE DATA PRACTICE.—The term ''deceptive data practice'' means an act or practice involving the processing or transfer of covered data

in a manner that constitutes a deceptive act or practice in violation of section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C. 45(a)(1)).

(2) HARMFUL DATA PRACTICE.—The term ''harmful data practice'' means the processing or transfer of covered data in a manner that causes or is likely to cause any of the following:

(A) Financial, physical, or reputational injury to an individual.

(B) Physical or other offensive intrusion upon the solitude or seclusion of an individual or the individual's private affairs or concerns, where such intrusion would be offensive to a reasonable person.

(C) Other substantial injury to an individual.

SEC. 102. RIGHT TO ACCESS AND TRANSPARENCY.

(a) RIGHT TO ACCESS.—A covered entity, upon the verified request of an individual, shall provide the individual, in a human-readable format that a reasonable individual can understand, with—

(1) a copy or accurate representation of the covered data of the individual processed or transferred by the covered entity; and

(2) the name of any third party to whom covered data of the individual has been transferred by the covered entity and a description of the purpose for which the entity transferred such data to such third party.

(b) RIGHT TO TRANSPARENCY.—A covered entity shall make publicly and persistently available, in a conspicuous and readily accessible manner, a privacy policy that provides a detailed and accurate representation of the entity's data processing and data transfer activities. Such privacy policy shall include, at a minimum—

(1) the identity and the contact information of the covered entity, including the contact information for the covered entity's representative for privacy and data security inquiries;

(2) each category of data the covered entity collects and the processing purposes for which such data is collected;

(3) whether the covered entity transfers covered data and, if so—

(A) each category of service provider and third party to which the covered entity transfers covered data and the purposes for which such data is transferred to such categories; and

(B) the identity of each third party to which the covered entity transfers covered data and the purposes for which such data is transferred to such third party, except for transfers to governmental entities pursuant to a court order or law that prohibits the covered entity from disclosing such transfer;

(4) how long covered data processed by the covered entity will be retained by the covered entity and a description of the covered entity's data minimization policies;

(5) how individuals can exercise the individual rights described in this title;

(6) a description of the covered entity's data security policies; and

(7) the effective date of the privacy policy.

(c) LANGUAGES.—A covered entity shall make the privacy policy required under this section available to the public in all of the languages in which the covered entity provides a product or service or carries out any other activities to which the privacy policy relates.

(d) RIGHT TO CONSENT TO MATERIAL CHANGES.—A covered entity shall not make a material change to its privacy policy or practices with respect to previously collected covered data that would weaken the privacy protec-

tions applicable to such data without first obtaining prior affirmative express consent from the individuals affected. The covered entity shall provide direct notification, where possible, regarding material changes to affected individuals, taking into account available technology and the nature of the relationship.

SEC. 103. RIGHT TO DELETE.

A covered entity, upon the verified request of an individual, shall—

(1) delete, or allow the individual to delete, any information in the covered data of the individual that is processed by the covered entity; and

(2) inform any service provider or third party to which the covered entity transferred such data of the individual's deletion request.

SEC. 104. RIGHT TO CORRECT INACCURACIES.

A covered entity, upon the verified request of an individual, shall—

(1) correct, or allow the individual to correct, inaccurate or incomplete information in the covered data of the individual that is processed by the covered entity; and

(2) inform any service provider or third party to which the covered entity transferred such data of the corrected information.

SEC. 105. RIGHT TO CONTROLS.

(a) RIGHT TO DATA PORTABILITY.—A covered entity, upon the verified request of an individual, shall export the individual's covered data, except for derived data, without licensing restrictions—

(1) in a human-readable format that allows the individual to understand such covered data of the individual; and

(2) in a structured, interoperable, and machine-readable format that includes all covered data or other information that the covered entity collected to the extent feasible.

(b) RIGHT TO OPT OUT OF TRANSFERS.—

(1) IN GENERAL.—A covered entity—

(A) shall not transfer an individual's covered data to a third party if the individual objects to the transfer; and

(B) shall allow an individual to object to the covered entity transferring covered data of the individual to a third party through a process established under the rule issued by the Commission pursuant to paragraph (2).

(2) RULEMAKING.—

(A) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, the Commission shall issue a rule under section

553 of title 5, United States Code, establishing one or more acceptable processes for covered entities to follow in allowing individuals to opt out of transfers of covered data.

(B) REQUIREMENTS.—The processes established by the Commission pursuant to this subparagraph shall—

(i) be centralized, to the extent feasible, to minimize the number of opt-out designations of a similar type that a consumer must make;

(ii) include clear and conspicuous opt-out notices and consumer friendly mechanisms to allow an individual to opt out of transfers of covered data;

(iii) allow an individual that objects to a transfer of covered data to view the status of such objection;

(iv) allow an individual that objects to a transfer of covered data to change the status of such objection;

(v) be privacy protective; and

(vi) be informed by the Commission's experience developing and implementing the National Do Not Call Registry.

(c) SENSITIVE DATA.—A covered entity—

(1) shall not process the sensitive covered data of an individual without the individual's prior, affirmative express consent;

(2) shall not transfer the sensitive covered data of an individual without the individual's prior, affirmative express consent;

(3) shall provide an individual with a consumer-friendly means to withdraw affirmative express consent to process the sensitive covered data of the individual; and

(4) is not required to obtain prior, affirmative express consent to process or transfer publicly available information.

SEC. 106. RIGHT TO DATA MINIMIZATION.

A covered entity shall not process or transfer covered data beyond what is reasonably necessary, proportionate, and limited—

(1) to carry out the specific processing purposes and transfers described in the privacy policy made available by the covered entity as required under section 102;

(2) to carry out a specific processing purpose or transfer for which the covered entity has obtained affirmative express consent; or

(3) for a purpose specifically permitted under subsection (d) of section 110.

Covered data processing and transfers consistent with this section shall not supersede any other provision of this Act.

SEC. 107. RIGHT TO DATA SECURITY.

(a) IN GENERAL.—A covered entity shall establish, implement, and maintain reasonable data security practices to protect the confidentiality, integrity, and accessibility of covered data. Such data security practices shall be appropriate to the volume and nature of the covered data at issue.

(b) SPECIFIC REQUIREMENTS.—Data security practices required under subsection (a) shall include, at a minimum, the following:

(1) ASSESS VULNERABILITIES.—Identifying and assessing any reasonably foreseeable risks to, and vulnerabilities in, each system maintained by the covered entity that processes or transfers covered data, including unauthorized access to or risks to covered data, human vulnerabilities, access rights, and use of service providers. Such activities shall include a plan to receive and respond to unsolicited reports of vulnerabilities by entities and individuals.

(2) PREVENTIVE AND CORRECTION ACTION.—Taking preventive and corrective action to mitigate

any risks or vulnerabilities to covered data identified by the covered entity, which may include implementing administrative, technical, or physical safeguards or changes to data security practices or the architecture, installation, or implementation of network or operating software.

(3) INFORMATION RETENTION AND DISPOSAL.—Disposing covered data that is required to be deleted or is no longer necessary for the purpose for which the data was collected unless an individual has provided affirmative express consent to such retention. Such process shall include destroying, permanently erasing, or otherwise modifying the covered data to make such data permanently unreadable or indecipherable and unrecoverable and data hygiene practices to ensure ongoing compliance with this subsection.

(4) TRAINING.—Training all employees with access to covered data on how to safeguard covered data and protect individual privacy and updating that training as necessary.

(c) TRAINING GUIDELINES.—Not later than 1 year after the date of enactment of this Act, the Commission, in conjunction with the National Institute of Standards and Technology, shall publish guidance for covered entities

on how to provide effective data security and privacy training as described in subsection (b)(4).

SEC. 108. CIVIL RIGHTS.

(a) PROTECTIONS.—

(1) IN GENERAL.—A covered entity shall not process or transfer covered data on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability—

(A) for the purpose of advertising, marketing, soliciting, offering, selling, leasing, licensing, renting, or otherwise commercially contracting for a housing, employment, credit, or education opportunity, in a manner that unlawfully discriminates against or otherwise makes the opportunity unavailable to the individual or class of individuals; or

(B) in a manner that unlawfully segregates, discriminates against, or otherwise makes unavailable to the individual or class of individuals the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation.

(2) EXCEPTION.—Nothing in this section shall limit a covered entity from processing covered data for legitimate internal testing for the purpose of preventing unlawful discrimination or otherwise determining the extent or effectiveness of the covered entity's compliance with this Act.

(3) FTC ADVISORY OPINIONS.—A covered entity may request advice from the Commission concerning the covered entity's potential compliance with this subsection, in accordance with the Commission's rules of practice on advisory opinions.

(b) ALGORITHMIC DECISION-MAKING IMPACT ASSESSMENT.—

(1) IMPACT ASSESSMENT.—Notwithstanding any other provision of law, a covered entity engaged in algorithmic decision-making, or in assisting others in algorithmic decision-making for the purpose of processing or transferring covered data, solely or in part to make or facilitate advertising for housing, education, employment or credit opportunities, or an eligibility determination for housing, education, employment or credit opportunities or determining access to, or restrictions on the use of, any place of public accommodation, must annually conduct an

impact assessment of such algorithmic decision-making that—

(A) describes and evaluates the development of the covered entity's algorithmic decision-making processes including the design and training data used to develop the algorithmic decision-making process, how the algorithmic decision-making process was tested for accuracy, fairness, bias and discrimination; and

(B) assesses whether the algorithmic decision-making system produces discriminatory results on the basis of an individual's or class of individuals' actual or perceived race, color, ethnicity, religion, national origin, sex, gender, gender identity, sexual orientation, familial status, biometric information, lawful source of income, or disability.

(2) EXTERNAL, INDEPENDENT AUDITOR OR RESEARCHER.—A covered entity may utilize an external, independent auditor or researcher to conduct such assessments.

(3) AVAILABILITY.—The covered entity—

(A) shall make the impact assessment available to the Commission upon request; and

(B) may make the impact assessment public.

A covered entity may redact and segregate trade secrets as defined by section 1839 of title 18, United States Code, from public disclosure under this subsection.

(4) STUDY.—Not later than 3 years after the date of enactment of this Act, the Commission shall publish a report containing the results of a study, using the Commission's authority under section 6(b) of the Federal Trade Commission Act (15 U.S.C. 46(b)), examining the use of algorithms for the purposes described in this subsection. Not later than 3 years after the publication of the initial report, and as necessary thereafter, the Commission shall publish a new and updated version of such report.

SEC. 109. PROHIBITION ON WAIVER OF RIGHTS.

A covered entity shall not condition the provision of a service or product to an individual on the individual's agreement to waive privacy rights guaranteed by—

(1) sections 101, 105(a), and 106 through 109 of this Act; and

(2) sections 102 through 104, and 105(b) and (c) of this Act, except in the case where—

(A) there exists a direct relationship between the individual and the covered entity initiated by the individual;

(B) the provision of the service or product requested by the individual requires the processing or transferring of the specific covered data of the individual and the covered data is strictly necessary to provide the service or product; and

(C) an individual provides affirmative express consent to such specific limitations.

SEC. 110. LIMITATIONS AND APPLICABILITY.

(a) VERIFICATION OF REQUESTS.—

(1) IN GENERAL.—A covered entity shall not permit an individual to exercise a right described in sections 102 through 105(a) if—

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

(B) the covered entity reasonably believes that the request is made to interfere with a

contract between the covered entity and another individual.

(2) ADDITIONAL INFORMATION.—If a covered entity cannot reasonably verify that a request to exercise a right described in sections 102 through 105(a) is made by the individual whose covered data is the subject of the request (or an individual authorized to make such a request on the individual's behalf), the covered entity shall request the provision of additional information necessary for the sole purpose of verifying the identity of the individual and shall not process or transfer such additional information for any other purpose.

(3) BURDEN MINIMIZATION.—A covered entity shall minimize the inconvenience to consumers relating to the verification or authentication of requests.

(b) COST OF ACCESS.—A covered entity shall carry out the rights described in sections 102 through 105(a) free of charge.

(c) EXCEPTIONS TO SECTIONS 102 THROUGH 105(b).—A covered entity may decline to comply with an individual's request to exercise a right described in sections 102 through 105(b) if—

(1) complying with the request would be demonstrably impossible (for purposes of this paragraph,

the receipt of a large number of verified requests, on its own, shall not be considered to render compliance with a request demonstrably impossible);

(2) complying with the request would prevent the covered entity from carrying out internal audits, performing accounting functions, processing refunds, or fulfilling warranty claims, provided that the covered data that is the subject of the request is not processed or transferred for any purpose other than such specific activities;

(3) the request is made to correct or delete publicly available information, and then only to the extent the data is publicly available information;

(4) complying with the request would impair the publication of newsworthy information of legitimate public concern to the public by a covered entity, or the processing or transfer of information by a covered entity for such purpose;

(5) complying with the request would impair the privacy of another individual or the rights of another to exercise free speech; or

(6) the covered entity processes or will process the data subject to the request for a specific purpose described in subsection (d) of this section, and complying with the request would prevent the covered

entity from using such data for such specific purpose.

(d) EXCEPTIONS TO AFFIRMATIVE EXPRESS CONSENT.—

(1) IN GENERAL.—A covered entity may process or transfer covered data without the individual's affirmative express consent for any of the following purposes, provided that the processing or transfer is reasonably necessary, proportionate, and limited to such purpose:

(A) To complete a transaction or fulfill an order or service specifically requested by an individual, such as billing, shipping, or accounting.

(B) To perform system maintenance, debug systems, or repair errors to ensure the functionality of a product or service provided by the covered entity.

(C) To detect or respond to a security incident, provide a secure environment, or maintain the safety of a product or service.

(D) To protect against malicious, deceptive, fraudulent, or illegal activity.

(E) To comply with a legal obligation or the establishment, exercise, or defense of legal claims.

(F) To prevent an individual from suffering harm where the covered entity believes in good faith that the individual is in danger of suffering death or serious physical injury.

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

(H) To conduct scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or a similar oversight entity that meets standards promulgated by the Commission pursuant to section 553 of title 5, United States Code.

(2) BIOMETRIC INFORMATION.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations pursuant to section 553 of title 5, United States Code, identifying privacy protective requirements for the processing of biometric information for a purpose described in subparagraph (C) or (D) of paragraph (1). Such regulations shall include—

(A) strict data processing limitations, including a prohibition on the processing of biometric information unless the covered entity has a reasonable suspicion, after a specific criminal incident involving the covered entity, that the individual may engage in criminal activity;

(B) strict data transfer limitations, including a prohibition on the transfer of biometric information to a third party other than to comply with a legal obligation or to establish, exercise, or defend a legal claim; and

(C) strict transparency obligations, including requiring disclosures in a conspicuous and readily accessible manner regarding specific data processing and transfer activities.

(e) JOURNALISM EXCEPTION.—Nothing in this title shall apply to the publication of newsworthy information of legitimate public concern to the public by a covered entity, or to the processing or transfer of information by a covered entity for that purpose.

(f) APPLICABILITY OF OTHER DATA PRIVACY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.),

part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), the Family Educational Rights and Privacy Act (20 U.S.C. 1232g; part 99 of title 34, Code of Federal Regulations), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), and is in compliance with the data privacy requirements of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the related requirements of this title, except for section 107, with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this subsection.

(g) APPLICABILITY OF OTHER DATA SECURITY REQUIREMENTS.—A covered entity that is required to comply with title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.), the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. 17931 et seq.), part C of title XI of the Social Security Act (42 U.S.C. 1320d et seq.), or the regulations promulgated pursuant to section 264(c) of the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. 1320d–2 note), and is in compliance with the information security require-

ments of such regulations, part, title, or Act (as applicable), shall be deemed to be in compliance with the requirements of section 107 with respect to data subject to the requirements of such regulations, part, title, or Act. Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance describing the implementation of this subsection.

(h) IN GENERAL.—The Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations necessary to carry out the provisions of this title.

TITLE II—OVERSIGHT AND RESPONSIBILITY

SEC. 201. EXECUTIVE RESPONSIBILITY.

(a) IN GENERAL.—Beginning 1 year after the date of enactment of this Act, the chief executive officer of a covered entity that is a large data holder (or, if the entity does not have a chief executive officer, the highest ranking officer of the entity) and each privacy officer and data security officer of such entity shall annually certify to the Commission, in a manner specified by the Commission, that the entity maintains—

(1) adequate internal controls to comply with this Act; and

(2) reporting structures to ensure that such certifying officers are involved in, and are responsible for, decisions that impact the entity's compliance with this Act.

(b) REQUIREMENTS.—A certification submitted under subsection (a) shall be based on a review of the effectiveness of a covered entity's internal controls and reporting structures that is conducted by the certifying officers no more than 90 days before the submission of the certification.

SEC. 202. PRIVACY AND DATA SECURITY OFFICERS; COMPREHENSIVE PRIVACY AND DATA SECURITY PROGRAMS; RISK ASSESSMENTS AND COMPLIANCE.

(a) PRIVACY AND DATA SECURITY OFFICER.—A covered entity shall designate—

(1) 1 or more qualified employees as privacy officers; and

(2) 1 or more qualified employees (in addition to any employee designated under paragraph (1)) as data security officers.

(b) COMPREHENSIVE PRIVACY AND DATA SECURITY PROGRAMS, RISK ASSESSMENTS, AND COMPLIANCE.—An employee who is designated by a covered entity as a pri-

vacy officer or a data security officer shall be responsible for, at a minimum—

(1) implementing a comprehensive written data privacy program and data security program to safeguard the privacy and security of covered data throughout the life cycle of development and operational practices of the covered entity's products or services;

(2) annually conducting privacy and data security risk assessments, data hygiene, and other quality control practices; and

(3) facilitating the covered entity's ongoing compliance with this Act.

SEC. 203. SERVICE PROVIDERS AND THIRD PARTIES.

(a) SERVICE PROVIDERS.—A service provider—

(1) shall not process service provider data for any processing purpose other than one performed on behalf of, and at the direction of, the covered entity that transferred such data to the service provider, except that a service provider may process data to comply with a legal obligation or the establishment, exercise, or defense of legal claims;

(2) shall not transfer service provider data to a third party without the affirmative express consent, obtained by, or on behalf of, the covered entity, of

the individual to whom the service provider data is linked or reasonably linkable;

(3) shall delete or de-identify service provider data after the agreed upon end of the provision of services;

(4) is exempt from the requirements of sections 102(a), 103, 104, and 105(a) with respect to service provider data, but shall, to the extent practicable—

(A) assist the covered entity from which it received the service provider data in fulfilling requests made by individuals under such sections; and

(B) shall delete, de-identify, or correct (as applicable), any service provider data that is subject to a verified request from an individual described in section 103 or 104; and

(5) is exempt from the requirements of section 106 with respect to service provider data, but shall have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.

(b) THIRD PARTIES.—A third party—

(1) shall not process third party data for a purpose that is inconsistent with the expectations of a reasonable individual;

(2) may reasonably rely on representations made by the covered entity that transferred third party data regarding the expectation of a reasonable individual, provided the third party conducts reasonable due diligence on the representations of the covered entity and finds those representations to be credible; and

(3) upon receipt of any third party data, is exempt from the requirements of section 105(c) with respect to such data, but shall have the same responsibilities and obligations as a covered entity with respect to such data under all other provisions of this Act.

(c) ADDITIONAL OBLIGATIONS ON COVERED ENTITIES.—

(1) IN GENERAL.—A covered entity shall—

(A) exercise reasonable due diligence in selecting a service provider and conduct reasonable oversight of its service providers to ensure compliance with the applicable requirements of this section; and

(B) exercise reasonable due diligence in deciding to transfer covered data to a third party, and conduct oversight of third parties to which

it transfers data to ensure compliance with the applicable requirements of this subsection.

(2) GUIDANCE.—Not later than 1 year after the date of enactment of this Act, the Commission shall issue guidance for covered entities regarding compliance with this subsection.

(d) IN GENERAL.—The Commission shall have authority under section 553 of title 5, United States Code, to promulgate regulations necessary to carry out the provisions of this section.

SEC. 204. WHISTLEBLOWER PROTECTIONS.

(a) IN GENERAL.—A covered entity shall not, directly or indirectly, discharge, demote, suspend, threaten, harass, or in any other manner discriminate against a covered individual of the covered entity because—

(1) the covered individual, or anyone perceived as assisting the covered individual, takes (or the covered entity suspects that the covered individual has taken or will take) a lawful action in providing to the Federal Government or the attorney general of a State information relating to any act or omission that the covered individual reasonably believes to be a violation of this Act or any regulation promulgated under this Act;

(2) the covered individual provides information that the covered individual reasonably believes evidences such a violation to—

(A) a person with supervisory authority over the covered individual at the covered entity; or

(B) another individual working for the covered entity who the covered individual reasonably believes has the authority to investigate, discover, or terminate the violation or to take any other action to address the violation;

(3) the covered individual testifies (or the covered entity expects that the covered individual will testify) in an investigation or judicial or administrative proceeding concerning such a violation; or

(4) the covered individual assists or participates (or the covered entity expects that the covered individual will assist or participate) in such an investigation or judicial or administrative proceeding, or the covered individual takes any other action to assist in carrying out the purposes of this Act.

(b) ENFORCEMENT.—An individual who alleges discharge or other discrimination in violation of subsection (a) may bring an action governed by the rules, procedures, statute of limitations, and legal burdens of proof in section

42121(b) of title 49, United States Code. If the individual has not received a decision within 180 days and there is no showing that such delay is due to the bad faith of the claimant, the individual may bring an action for a jury trial, governed by the burden of proof in section 42121(b) of title 49, United States Code, in the appropriate district court of the United States for the following relief:

(1) Temporary relief while the case is pending.

(2) Reinstatement with the same seniority status that the individual would have had, but for the discharge or discrimination.

(3) Three times the amount of back pay otherwise owed to the individual, with interest.

(4) Consequential and compensatory damages, and compensation for litigation costs, expert witness fees, and reasonable attorneys' fees.

(c) WAIVER OF RIGHTS AND REMEDIES.—The rights and remedies provided for in this section shall not be waived by any policy form or condition of employment, including by a predispute arbitration agreement.

(d) PREDISPUTE ARBITRATION AGREEMENTS.—No predispute arbitration agreement shall be valid or enforceable if the agreement requires arbitration of a dispute arising under this section.

(e) COVERED INDIVIDUAL DEFINED.—In this section, the term ''covered individual'' means an applicant, current or former employee, contractor, subcontractor, grantee, or agent of an employer.

SEC. 205. DIGITAL CONTENT FORGERIES.

(a) REPORTS.—Not later than 1 year after the date of enactment of this Act, and annually thereafter, the Director of the National Institute of Standards and Technology shall publish a report regarding digital content forgeries.

(b) REQUIREMENTS.—Each report under subsection (a) shall include the following:

(1) A definition of digital content forgeries along with accompanying explanatory materials. The definition developed pursuant to this section shall not supersede any other provision of law or be construed to limit the authority of any executive agency related to digital content forgeries.

(2) A description of the common sources in the United States of digital content forgeries and commercial sources of digital content forgery technologies.

(3) An assessment of the uses, applications, and harms of digital content forgeries.

(4) An analysis of the methods and standards available to identify digital content forgeries as well as a description of the commercial technological counter-measures that are, or could be, used to address concerns with digital content forgeries, which may include the provision of warnings to viewers of suspect content.

(5) A description of the types of digital content forgeries, including those used to commit fraud, cause harm or violate any provision of law.

(6) Any other information determined appropriate by the Director.

TITLE III—MISCELLANEOUS

SEC. 301. ENFORCEMENT, CIVIL PENALTIES, AND APPLICABILITY.

(a) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION.—

(1) NEW BUREAU.—

(A) IN GENERAL.—The Commission shall establish a new Bureau within the Commission comparable in structure, size, organization, and authority to the existing Bureaus with the Commission related to consumer protection and competition.

(B) MISSION.—The mission of the Bureau established under this paragraph shall be to assist the Commission in exercising the Commission's authority under this Act and under other Federal laws addressing privacy, data security, and related issues.

(C) TIMELINE.—Such Bureau shall be established, staffed, and fully operational within 2 years of enactment of this Act.

(2) TREATMENT AS VIOLATION OF RULE.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(3) POWERS OF COMMISSION.—

(A) IN GENERAL.—Except as provided in subparagraph (C), the Commission shall enforce this Act and the regulations promulgated under this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

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

(C) INDEPENDENT LITIGATION AUTHORITY.—The Commission may commence, defend, or intervene in, and supervise the litigation of any civil action under this subsection (including an action to collect a civil penalty) and any appeal of such action in its own name by any of its attorneys designated by it for such purpose. The Commission shall notify the Attorney General of any such action and may consult with the Attorney General with respect to any such action or request the Attorney General on behalf of the Commission to commence, defend, or intervene in any such action.

(4) DATA PRIVACY AND SECURITY RELIEF FUND.—

(A) ESTABLISHMENT OF RELIEF FUND.—There is established in the Treasury of the United States a separate fund to be known as the ''Data Privacy and Security Relief Fund''

(referred to in this paragraph as the ''Relief Fund'').

(B) DEPOSITS.—

(i) DEPOSITS FROM THE COMMISSION.—The Commission shall deposit into the Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Commission commences to enforce this Act or a regulation promulgated under this Act.

(ii) DEPOSITS FROM THE ATTORNEY GENERAL.—The Attorney General of the United States shall deposit into the Relief Fund the amount of any civil penalty obtained against any covered entity in any judicial or administrative action the Attorney General commences on behalf of the Commission to enforce this Act or a regulation promulgated under this Act.

(C) USE OF FUND AMOUNTS.—Notwithstanding section 3302 of title 31, United States Code, amounts in the Relief Fund shall be available to the Commission, without fiscal year limitation, to provide redress, payments or com-

pensation, or other monetary relief to individuals affected by an act or practice for which civil penalties have been obtained under this Act. To the extent that individuals cannot be located or such redress, payments or compensation, or other monetary relief are otherwise not practicable, the Commission may use such funds for the purpose of consumer or business education relating to data privacy and security or for the purpose of engaging in technological research that the Commission considers necessary to enforce this Act.

(D) AMOUNTS NOT SUBJECT TO APPORTIONMENT.—Notwithstanding any other provision of law, amounts in the Relief Fund shall not be subject to apportionment for purposes of chapter 15 of title 31, United States Code, or under any other authority.

(b) ENFORCEMENT BY STATE ATTORNEYS GENERAL.—

(1) CIVIL ACTION.—In any case in which the attorney general of a State or a consumer protection officer of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by the engagement of any covered

entity in an act or practice that violates this Act or a regulation promulgated under this Act, the attorney general of the State, or a consumer protection officer of the State acting on behalf of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States to—

(A) enjoin that act or practice;

(B) enforce compliance with this Act or the regulation;

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

(D) obtain such other relief as the court may consider to be appropriate.

(2) NOTICE TO THE COMMISSION AND RIGHTS OF THE COMMISSION.—Except where not feasible, the State shall notify the Commission in writing prior to initiating a civil action under paragraph (1). Such notice shall include a copy of the complaint to be filed to initiate such action. If prior notice is not practicable, the State shall provide a copy of the complaint to the Commission immediately upon instituting the action. Upon receiving such notice, the

Commission may intervene in such action and, upon intervening—

(A) be heard on all matters arising in such action; and

(B) file petitions for appeal of a decision in such action.

(3) PRESERVATION OF STATE POWERS.—No provision of this section shall be construed as altering, limiting, or affecting the authority of a State attorney general or a consumer protection officer of a State to—

(A) bring an action or other regulatory proceeding arising solely under the law in effect in that State; or

(B) exercise the powers conferred on the attorney general or on a consumer protection officer of a State by the laws of the State, including the ability to conduct investigations, to administer oaths or affirmations, or to compel the attendance of witnesses or the production of documentary or other evidence.

(4) VENUE; SERVICE OF PROCESS.—

(A) VENUE.—Any action brought under paragraph (1) may be brought in the district court of the United States that meets applicable

requirements relating to venue under section 1391 of title 28, United States Code.

(B) SERVICE OF PROCESS.—In an action brought under paragraph (1), process may be served in any district in which the defendant—

(i) is an inhabitant; or

(ii) may be found.

(c) ENFORCEMENT BY INDIVIDUALS.—

(1) IN GENERAL.—Any individual alleging a violation of this Act or a regulation promulgated under this Act may bring a civil action in any court of competent jurisdiction, State or Federal.

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

(A) an amount not less than $100 and not greater than $1,000 per violation per day or actual damages, whichever is greater;

(B) punitive damages;

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

(D) any other relief, including equitable or declaratory relief, that the court determines appropriate.

(3) INJURY IN FACT.—A violation of this Act or a regulation promulgated under this Act with respect to the covered data of an individual constitutes a concrete and particularized injury in fact to that individual.

(d) INVALIDITY OF PRE-DISPUTE ARBITRATION AGREEMENTS AND PRE-DISPUTE JOINT ACTION WAIVERS.—

(1) IN GENERAL.—Notwithstanding any other provision of law, no pre-dispute arbitration agreement or pre-dispute joint action waiver shall be valid or enforceable with respect to a privacy or data security dispute arising under this Act.

(2) APPLICABILITY.—Any determination as to whether or how this subsection applies to any privacy or data security dispute shall be made by a court, rather than an arbitrator, without regard to whether such agreement purports to delegate such determination to an arbitrator.

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

(A) The term ''pre-dispute arbitration agreement'' means any agreement to arbitrate a dispute that has not arisen at the time of the making of the agreement.

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

(C) The term ''privacy or data security dispute'' means any claim relating to an alleged violation of this Act, or a regulation promulgated under this Act, and between an individual and a covered entity.

SEC. 302. RELATIONSHIP TO FEDERAL AND STATE LAWS.

(a) FEDERAL LAW PRESERVATION.—Nothing in this Act or a regulation promulgated under this Act shall be construed to limit—

(1) the authority of the Commission, or any other Executive agency, under any other provision of law; or

(2) any other provision of Federal law unless as specifically authorized by this Act.

(b) STATE LAW PRESERVATION.—Nothing in this Act shall be construed to preempt, displace, or supplant

the following State laws, rules, regulations, or requirements:

(1) Consumer protection laws of general applicability such as laws regulating deceptive, unfair, or unconscionable practices.

(2) Civil rights laws.

(3) Laws that govern the privacy rights or other protections of employees, employee information, or students or student information.

(4) Laws that address notification requirements in the event of a data breach.

(5) Contract or tort law.

(6) Criminal laws governing fraud, theft, unauthorized access to information or unauthorized use of information, malicious behavior, and similar provisions, and laws of criminal procedure.

(7) Laws specifying remedies or a cause of action to individuals.

(8) Public safety or sector specific laws unrelated to privacy or security.

(c) PREEMPTION OF DIRECTLY CONFLICTING STATE LAWS.—Except as provided in subsections (b) and (d), this Act shall supersede any State law to the extent such law directly conflicts with the provisions of this Act, or a standard, rule, or regulation promulgated under this

Act, and then only to the extent of such direct conflict. Any State law, rule, or regulation shall not be considered in direct conflict if it affords a greater level of protection to individuals protected under this Act.

(d) PRESERVATION OF COMMON LAW OR STATUTORY CAUSES OF ACTION FOR CIVIL RELIEF.—Nothing in this Act, nor any amendment, standard, rule, requirement, assessment, law or regulation promulgated under this Act, shall be construed to preempt, displace, or supplant any Federal or State common law rights or remedies, or any statute creating a remedy for civil relief, including any cause of action for personal injury, wrongful death, property damage, or other financial, physical, reputational, or psychological injury based in negligence, strict liability, products liability, failure to warn, an objectively offensive intrusion into the private affairs or concerns of the individual, or any other legal theory of liability under any Federal or State common law, or any State statutory law.

SEC. 303. SEVERABILITY.

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

SEC. 304. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Commission such sums as may be necessary to carry out this Act.

○