115TH CONGRESS
2D SESSION

S. _____

To amend the Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, or share personal information, to protect personal information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

_____

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

A BILL

To amend the Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, or share personal information, to protect personal information, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Consumer Data Protection Act''.

SEC. 2. DEFINITIONS.

In this Act:

(1) AUTOMATED DECISION SYSTEM.—The term ''automated decision system'' 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, that impacts consumers.

(2) AUTOMATED DECISION SYSTEM IMPACT ASSESSMENT.—The term ''automated decision system impact assessment'' means a study evaluating an automated decision system and the automated decision system's development process, including the design and training data of the automated decision system, for impacts on accuracy, fairness, bias, discrimination, privacy, and security that includes, at a minimum—

(A) a detailed description of the automated decision system, its design, its training, data, and its purpose;

(B) an assessment of the relative benefits and costs of the automated decision system in light of its purpose, taking into account relevant factors, including—

(i) data minimization practices;

(ii) the duration for which personal information and the results of the automated decision system are stored;

(iii) what information about the automated decision system is available to consumers;

(iv) the extent to which consumers have access to the results of the automated decision system and may correct or object to its results; and

(v) the recipients of the results of the automated decision system;

(C) an assessment of the risks posed by the automated decision system to the privacy or security of personal information of consumers and the risks that the automated decision system may result in or contribute to inaccurate, unfair, biased, or discriminatory decisions impacting consumers; and

(D) the measures the covered entity will employ to minimize the risks described in subparagraph (C), including technological and physical safeguards.

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

(4) CONSUMER.—The term ''consumer'' means an individual.

(5) COVERED ENTITY.—The term ''covered entity''—

(A) means a person, partnership, or corporation over which the Commission has jurisdiction under section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2); and

(B) does not include a person, partnership, or corporation that—

(i) with respect to the most recent fiscal year had—

(I) not greater than $50,000,000 in average annual gross receipts for the 3-taxable-year period preceding the fiscal year, as determined in accordance with paragraphs (2) and (3) of section 448(c) of the Internal Revenue Code of 1986; and

(II) personal information on less than—

(aa) 1,000,000 consumers; and

(bb) 1,000,000 consumer devices;

(ii) is not substantially owned, operated, or controlled by a person, partnership, or corporation that does not meet the requirements under clause (i); and

(iii) is not a data broker or other commercial entity that, as a substantial part of their business, collects, assembles, or maintains personal information concerning an individual who is not a customer or an employee of that entity in order to sell or trade the information or provide third-party access to the information.

(6) DATA PROTECTION IMPACT ASSESSMENT.—The term ''data protection impact assessment'' means a study evaluating the extent to which an information system protects the privacy and security of personal information the system processes.

(7) EXECUTIVE CAPACITY.—The term ''executive capacity'' means an assignment within an organization in which the employee primarily—

(A) directs the management of the organization or a major component or function of the organization;

(B) establishes the goals and policies of the organization, component, or function;

(C) exercises wide latitude in discretionary decision-making; and

(D) receives only general supervision or direction from higher level executives, the board of directors, or stockholders of the organization.

(8) HIGH-RISK AUTOMATED DECISION SYSTEM.—The term ''high-risk automated decision system'' means an automated decision system that—

(A) taking into account the novelty of the technology used and the nature, scope, context, and purpose of the automated decision system, poses a significant risk—

(i) to the privacy or security of personal information of consumers; or

(ii) of resulting in or contributing to inaccurate, unfair, biased, or discriminatory decisions impacting consumers;

(B) makes decisions, or facilitates human decision making, based on systematic and extensive evaluations of consumers, including attempts to analyze or predict sensitive aspects of their lives, such as their work performance, economic situation, health, personal preferences,

interests, behavior, location, or movements, that—

(i) alter legal rights of consumers; or

(ii) otherwise significantly impact consumers;

(C) involves the personal information of a significant number of consumers regarding race, color, national origin, political opinions, religion, trade union membership, genetic data, biometric data, health, gender, gender identity, sexuality, sexual orientation, criminal convictions, or arrests;

(D) systematically monitors a large, publicly accessible physical place; or

(E) meets any other criteria established by the Commission in regulations issued under section 7(b)(1).

(9) HIGH-RISK INFORMATION SYSTEM.—The term ''high-risk information system'' means an information system that—

(A) taking into account the novelty of the technology used and the nature, scope, context, and purpose of the information system, poses a significant risk to the privacy or security of personal information of consumers;

(B) involves the personal information of a significant number of consumers regarding race, color, national origin, political opinions, religion, trade union membership, genetic data, biometric data, health, gender, gender identity, sexuality, sexual orientation, criminal convictions, or arrests;

(C) systematically monitors a large, publicly accessible physical place; or

(D) meets any other criteria established by the Commission in regulations issued under section 7(b)(1).

(10) INFORMATION SYSTEM.—The term ''information system''—

(A) means a process, automated or not, that involves personal information, such as the collection, recording, organization, structuring, storage, alteration, retrieval, consultation, use, sharing, disclosure, dissemination, combination, restriction, erasure, or destruction of personal information; and

(B) does not include automated decision systems.

(11) JOURNALISM.—The term ''journalism'' means the gathering, preparing, collecting,

photographing, recording, writing, editing, reporting, or publishing of news or information that concerns local, national, or international events or other matters of public interest for dissemination to the public.

(12) PERSONAL INFORMATION.—The term ''personal information'' means any information, regardless of how the information is collected, inferred, or obtained that is reasonably linkable to a specific consumer or consumer device.

(13) SHARE.—The term ''share''—

(A) means the actions of a person, partnership, or corporation transferring information to another person, partnership, or corporation; and

(B) includes actions to knowingly—

(i) share, exchange, transfer, sell, lease, rent, provide, disclose, or otherwise permit access to information; or

(ii) enable or facilitate the collection of personal information by a third party.

(14) STORE.—The term ''store''—

(A) means the actions of a person, partnership, or corporation to retain information; and

(B) includes actions to store, collect, assemble, possess, control, or maintain information.

(15) THIRD PARTY.—The term ''third party'' means any person, partnership, or corporation that is not—

(A) the person, partnership, or corporation, whether a covered entity or not, that is sharing the personal information;

(B) solely performing an outsourced function of the person, partnership, or corporation sharing the personal information if—

(i) the person, partnership, or corporation is contractually or legally prohibited from using, storing, or sharing the personal information after the conclusion of the outsourced function; and

(ii) the person, partnership, or corporation is complying with regulations promulgated under subparagraphs (A) and (B) of section 7(b)(1), regardless of whether the person, partnership, or corporation is a covered entity; or

(C) a person, partnership, or corporation for whom the consumer gave opt-in consent for

the covered entity to disclose the personal information of the consumer.

(16) USE.—The term ''use'' means the actions of a person, partnership, or corporation in using information, including actions to use, process, or access information.

SEC. 3. NONECONOMIC INJURY.

The first sentence of section 5(n) of the Federal Trade Commission Act (15 U.S.C. 45(n)) is amended by inserting '', including those involving noneconomic impacts and those creating a significant risk of unjustified exposure of personal information,'' after ''cause substantial injury''.

SEC. 4. CIVIL PENALTY AUTHORITY.

Section 5 of the Federal Trade Commission Act (15 U.S.C. 45) is amended—

(1) in subsection (b)—

(A) in the fifth sentence, by inserting '', and it may, in its discretion depending on the nature and severity of the violation, include in the cease and desist order an assessment of a civil penalty, which shall be not more than an amount that is the greater of $50,000 per violation, taken as an aggregate sum of all violations, and 4 percent of the total annual gross

revenue of the person, partnership, or corporation for the prior fiscal year'' before the period at the end;

(2) in subsection (l)—

(A) in the first sentence, by striking ''of not more than $10,000 for each violation'' and inserting '', which shall be not more than an amount that is the greater of $50,000 per violation, taken as an aggregate sum of all violations, and 4 percent of the total annual gross revenue of the person, partnership, or corporation for the prior fiscal year'';

(3) in subsection (m)(1)—

(A) in subparagraph (A), in the second sentence, by striking ''of not more than $10,000 for each violation'' and inserting '', which shall be not more than an amount that is the greater of $50,000 per violation, taken as an aggregate sum of all violations, and 4 percent of the total annual gross revenue of the person, partnership, or corporation for the prior fiscal year''; and

(B) in subparagraph (B), in the matter following paragraph (2), by striking ''of not more than $10,000 for each violation'' and in-

serting ", which shall be not more than an amount that is the greater of $50,000 per violation, taken as an aggregate sum of all violations, and 4 percent of the total annual gross revenue of the person, partnership, or corporation for the prior fiscal year".

SEC. 5. ANNUAL DATA PROTECTION REPORTS.

(a) REPORTS.—

(1) IN GENERAL.—Each covered entity that has not less than $1,000,000,000 per year in revenue and stores, shares, or uses personal information on more than 1,000,000 consumers or consumer devices or any covered entity that stores, shares, or uses personal information on more than 50,000,000 consumers or consumer devices shall submit to the Commission an annual data protection report describing in detail whether, during the reporting period, the covered entity complied with the regulations promulgated in accordance with subparagraphs (A) and (B) of section 7(b)(1). To the extent that the covered entity did not comply with these regulations, this statement shall include a description of which regulations were violated and the number of consumers whose personal information was impacted.

(2) REGULATIONS.—Not later than 2 years after the date of enactment of this Act, the Federal Trade Commission shall promulgate regulations in accordance with section 553 of title 5, United States Code, carrying out this subsection.

(b) FAILURE OF CORPORATE OFFICERS TO CERTIFY PRIVACY AND DATA SECURITY REPORTS.—

(1) IN GENERAL.—Chapter 63 of title 18, United States Code, is amended by adding at the end the following:

"§ 1352. Failure of corporate officers to certify data protection reports

''(a) DEFINITION.—In this section, the term 'covered entity' has the meaning given the term in section 2 of the Consumer Data Protection Act.

''(b) CERTIFICATION OF ANNUAL DATA PROTECTION REPORTS.—Each annual report filed by a company with the Federal Trade Commission pursuant to section 5(a) of the Consumer Data Protection Act shall be accompanied by a written statement by the chief executive officer, chief privacy officer (or equivalent thereof), and chief information security officer (or equivalent thereof) of the company.

''(c) CONTENT.—The statement required under subsection (b) shall certify that the annual report fully com-

plies with the requirements of section 5(a) of the Consumer Data Protection Act.

''(d) CRIMINAL PENALTIES.—Whoever—

''(1) certifies any statement as set forth in subsections (b) and (c) of this section knowing that the annual report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than the greater of $1,000,000 or 5 percent of the largest amount of annual compensation the person received during the previous 3-year period from the covered entity, imprisoned not more than 10 years, or both; or

''(2) intentionally certifies any statement as set forth in subsections (b) and (c) of this section knowing that the annual report accompanying the statement does not comport with all the requirements set forth in this section shall be fined not more than $5,000,000 or 25 percent of the largest amount of annual compensation the person received during the previous 3-year period from the covered entity, imprisoned not more than 20 years, or both.''.

(2) TECHNICAL AND CONFORMING AMENDMENT.—The table of sections for chapter 63 of title 18, United States Code, is amended by adding at the end the following:

''1352. Failure of corporate officers to certify data protection reports.''.

SEC. 6. "DO NOT TRACK" DATA SHARING OPT OUT.

(a) REGULATIONS.—Not later than 2 years after the date of enactment of this Act, the Commission shall promulgate regulations, in accordance with section 553 of title 5, United States Code, to—

(1) implement and maintain a ''Do Not Track'' data sharing opt-out website—

(A) that allows consumers to opt-out of data sharing, view their opt-out status, and change their opt-out status;

(B) the effect of which opt-out is to prevent—

(i) covered entities from sharing the personal information of the consumer with third parties, including personal information shared with or stored by the covered entity prior to the opt-out unless—

(I) the sharing is necessary for the primary purpose for which the consumer provided the personal information; and

(II) the third party with whom the personal information was shared does not retain the personal information for secondary purposes; and

(ii) covered entities from storing or using personal information of the consumer that has been shared with them by non-covered entities, not including personal information shared with or stored by the covered entity prior to the opt-out;

(C) that is reasonably accessible and usable by consumers; and

(D) that enables consumers to make use of the features described in subparagraph (A) through an Application Programming Interface;

(2) as part of the implementation of the opt-out website described in paragraph (1)—

(A) maintain a record of the opt-out status of consumers enrolled through the opt-out website, including the date and time when the consumer opted out;

(B) enable consumers to convey their opt-out status to covered entities in 1 or more privacy-protecting ways through technological means determined by the Commission, such as through a consumer's web browser or operating system;

(C) enable covered entities to determine whether a particular consumer is enrolled in the

opt-out website in a privacy-preserving way that does not result in the disclosure of any personal information other than a consumer's opt-out status to that covered entity; and

(D) enable covered entities to make use of the mechanism described in subparagraph (C) through an Application Programming Interface, for which the Commission may charge a reasonable fee to cover the costs of operating the opt-out registry and access to the system;

(3) require that a covered entity be bound by the opt-out of a consumer when the opt-out is conveyed through the opt-out website implemented and maintained by the Commission—

(A) immediately for new customers; and

(B) within 30 days for existing customers or consumers who are not customers, unless, after the consumer has opted out in the manner described in paragraph (1)(A), the covered entity receives, in accordance with the procedures described in paragraph (10), consent from the consumer to not be bound by the consumer's opt-out;

(4) require covered entities that store or use personal data on consumers with which they—

(A) do not have a direct relationship; or

(B) otherwise do not have the ability to determine the consumer's opt-out preference through one of the technological means established pursuant to paragraph (2)(B);

to make a good-faith effort to determine the consumer's opt-out status at least as frequently as determined by the Commission, through the Application Programming Interface maintained by the Commission pursuant to paragraph (2)(D);

(5) permit covered entities to not be bound by the consumer's opt-out for—

(A) disclosures made to the government that are either required or permitted by law;

(B) disclosures made pursuant to an order of a court or administrative tribunal;

(C) disclosures made in response to a subpoena, discovery request, or other lawful process provided that such process is accompanied by a protective order that—

(i) prohibits the parties from using or disclosing the personal information for any purpose other than the litigation or proceeding for which such personal information was requested; and

(ii) requires the return to the covered entity or destruction of the personal information (including all copies made) at the end of the litigation or proceeding; or

(D) disclosures made to investigate, protect themselves and their customers from, or recover from fraud, cyber attacks, or other unlawful activity;

(6) establish standards and procedures, including through an Application Programming Interface, for a covered entity to request and obtain consent from a consumer who has opted-out in the manner described in paragraph (1)(A) for the covered entity to not be bound by the opt-out, provided such standards and procedures—

(A) require the covered entity to provide the consumer, at the time the covered entity is seeking consent, in accordance with paragraph (10), and in a form that is understandable to a reasonable consumer—

(i) a list of each third party with whom the personal information of the consumer will or may be shared by the covered entity;

(ii) a description of the personal information of that consumer that will or may be shared; and

(iii) a description of the purposes for which the personal information of that consumer will or may be shared;

(B) if the covered entity requires consent as a condition for providing a product or service, require the covered entity to—

(i) notify the consumer that he or she can obtain a substantially similar product or service in exchange for monetary payment or other compensation rather than by permitting the covered entity to share the consumer's personal information, as provided in subsection (b)(1)(B); and

(ii) with respect to the notice described in clause (i)—

(I) make the notice in a clear and conspicuous manner; and

(II) include the cost of the fee, if any, and instructions for obtaining the substantially similar product or service described in clause (i);

(C) if the covered entity does not require consent as a condition for providing a product or service, require the covered entity to clearly and conspicuously notify the consumer that the consumer may refuse to provide consent but still obtain the product or service; and

(D) require the covered entity to notify the consumer of his or her right, and how to exercise that right, to later withdraw consent for the covered entity to not be bound by the consumer's opt-out;

(7) not less frequently than every 2 years, examine the information that is presented to consumers in accordance with the procedures described in paragraph (6) to make sure that the information is useful, understandable, and to the extent possible, does not result in notification fatigue;

(8) establish standards and procedures requiring that when a non-covered entity that is not the consumer shares personal information about that consumer with a covered-entity, the covered entity shall make reasonable efforts to verify the opt-out status of the consumer whose personal information has been shared with the covered entity, after which

the covered entity may only store or use that personal information—

(A) if the consumer has not opted-out in the manner described in paragraph (2)(A); or

(B)(i) if the non-covered entity knowingly enabled or facilitated the collection of personal information by the covered entity and the covered entity itself receives consent from the consumer to store or use the consumer's personal information in accordance with paragraph (9); or

(ii) if the non-covered entity otherwise shares the information with the covered-entity and the consumer has given consent in accordance with paragraph (9) to the covered entity or non-covered entity for the non-covered entity to share the consumer's personal information with the specific covered entity;

(9) establish standards and procedures for a person, partnership, or corporation to request and obtain consent from a consumer, in accordance with paragraph (8)(B) that clearly identifies the covered entity that will be storing or using the personal information and provides the consumer, at the time the person, partnership, or corporation is seeking

consent, in accordance with paragraph (10), and in a form that is understandable to a reasonable consumer—

(A) the name and contact information of the person, partnership, or corporation from whom the personal information of that consumer is to be obtained;

(B) a description of the personal information of that consumer that will be shared; and

(C) a description of the purposes for which the personal information of that consumer will be shared;

(10) detail the standardized form and manner in which certain information related to sharing shall be disclosed to consumers, which shall, to the extent that the Commission determines to be practicable and appropriate, be in the form of a table that—

(A) contains clear and concise headings for each item of such information; and

(B) provides a clear and concise form for stating each item of information required to be disclosed under each such heading; and

(11) permit a consumer to withdraw his or her consent to a covered entity to not be bound by the

consumer's opt-out at any time, including through an Application Programming Interface.

(b) ACTS PROHIBITED.—

(1) IN GENERAL.—It shall be unlawful for any covered entity to condition its products or services upon a requirement that consumers—

(A) change their opt-out status through the opt-out website maintained by the Commission pursuant to subsection (a)(2); or

(B) give the covered entity consent to not be bound by the consumer's opt-out status, unless the consumer is also given an option to pay a fee to use a substantially similar service that is not conditioned upon a requirement that the consumer give the covered entity consent to not be bound by the consumer's opt-out status.

(2) FEE.—The fee described in paragraph (1)(B) shall not be greater than the amount of monetary gain the covered entity would have earned had the average consumer not opted-out.

(c) ENFORCEMENT BY THE COMMISSION.—A violation of subsection (b) shall be treated as a violation of a rule defining an unfair or deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

SEC. 7. DATA PROTECTION AUTHORITY.

(a) ACTS PROHIBITED.—It is unlawful for any covered entity to—

(1) violate a regulation promulgated under subsection (b); or

(2) knowingly provide substantial assistance to any person, partnership, or corporation whose actions violate this Act.

(b) REGULATIONS.—

(1) IN GENERAL.—Not later than 2 years after the date of enactment of this section, the Commission shall promulgate regulations, in accordance with section 553 of title 5, United States Code, that—

(A) require each covered entity to establish and implement reasonable cyber security and privacy policies, practices, and procedures to protect personal information used, stored, or shared by the covered entity from improper access, disclosure, exposure, or use;

(B) require each covered entity to implement reasonable physical, technical, and organizational measures to ensure that technologies or products used, produced, sold, offered, or leased by the covered entity that the covered entity knows or has reason to believe store, process, or otherwise interact with personal information are

built and function consistently with reasonable data protection practices;

(C) require each covered entity to designate at least 1 employee who reports directly to an employee acting in an executive capacity in the covered entity, to coordinate its efforts to comply with and carry out its responsibilities under this Act, including any request or challenge related to the sharing of personal information;

(D) require each covered entity to provide, at no cost, not later than 30 business days after receiving a written request from a verified consumer about whom the covered entity stores personal information—

(i) a reasonable means to review any stored personal information of that verified consumer, including the manner in which the information was collected and the date of collection, in a form that is understandable to a reasonable consumer;

(ii) a reasonable means to challenge the accuracy of any stored personal information of that verified consumer, including—

(I) by providing publicly accessible contact information for any employee responsible for overseeing such a challenge; and

(II) implementing a reasonable process for responding to such challenges, including the ability of the covered entity to terminate an investigation of information disputed by a consumer under this clause, and providing notice to the consumer of such termination, if the covered entity reasonably determines that the dispute by the consumer is frivolous or irrelevant, including by reason of a failure by a consumer to provide sufficient information to investigate the disputed information;

(iii) a list of each person, partnership, or corporation with whom the personal information of that verified consumer was shared by the covered entity that—

(I) does not include—

(aa) disclosures to governmental entities pursuant to a

court order or law that prohibits the covered entity from revealing that disclosure to the consumer;

(bb) disclosures of personal information to third parties when the personal information of the consumer was made available to and readily accessible by the general public with the consent of the verified consumer and shared with the third party through a mechanism available to any member of the general public; or

(cc) disclosures of information about the verified consumer that the covered entity did not obtain from that consumer, if revealing that disclosure of information would expose another consumer to likely harm; and

(II) except as provided in subparagraph (I), includes, at a minimum—

(aa) the name and contact information of each person, part-

nership, or corporation with whom the personal information of that verified consumer was shared;

(bb) a description of the personal information of that verified consumer that was shared, in a form that is understandable to a reasonable consumer;

(cc) a statement of the purposes for which the personal information of that verified consumer was shared;

(dd) if the covered entity claims consent from the consumer as the basis for sharing, a statement of the circumstances surrounding that consumer consent, specifically when, where, and how the consent was obtained and by whom the consent was obtained; and

(ee) a statement of when the personal information of that

verified consumer was shared; and

(iv) for any personal information about that verified consumer stored by the covered entity that the covered entity did not obtain directly from that verified consumer, a list identifying—

(I) the name and contact information of each person, partnership, or corporation from whom the personal information of that verified consumer was obtained;

(II) a description of the personal information, in a form that is understandable to a reasonable consumer;

(III) a statement of the purposes for which the personal information of that verified consumer was obtained by the covered entity; and

(IV) a statement of the purposes for which the personal information of that verified consumer was shared with the covered entity;

(E) detail the standardized form and manner in which the information in subparagraph

(D) shall be disclosed to consumers which shall, to the extent the Commission determines to be practicable and appropriate, be in the form of a table that—

(i) contains clear and concise headings for each item of information; and

(ii) provides a clear and concise form for stating each item of information required to be disclosed under each such heading;

(F) require each covered entity to correct the stored personal information of the verified consumer if, after investigating a challenge by a verified consumer under subparagraph (D), the covered entity determines that the personal information is inaccurate;

(G) require each covered entity to conduct automated decision system impact assessments of—

(i) existing high-risk automated decision systems, as frequently as the Commission determines is necessary; and

(ii) new high-risk automated decision systems, prior to implementation;

provided that a covered entity may evaluate similar high-risk automated decision systems that present similar risks in a single assessment;

(H) require each covered entity to conduct data protection impact assessments of—

(i) existing high-risk information systems, as frequently as the Commission determines is necessary; and

(ii) new high-risk information systems, prior to implementation;

provided that a covered entity may evaluate similar high-risk information systems that present similar risks in a single assessment;

(I) require each covered entity to conduct the impact assessments under subparagraphs (G) and (H), if reasonably possible, in consultation with external third parties, including independent auditors and independent technology experts; and

(J) require each covered entity to reasonably address in a timely manner the results of the impact assessments under subparagraphs (G) and (H).

(2) CONSULTATION.—The Commission shall promulgate regulations under subparagraphs (A) and (B) of paragraph (1) in consultation with the National Institute of Standards and Technology.

(3) OPTIONAL PUBLICATION OF IMPACT ASSESSMENTS.—The impact assessments under subparagraphs (G) and (H) may be made public by the covered entity at its sole discretion.

(c) PREEMPTION OF PRIVATE CONTRACTS.—It shall be unlawful for any covered entity to commit the acts prohibited in subsection (a), regardless of specific agreements between entities or consumers.

(d) ENFORCEMENT BY THE COMMISSION.—

(1) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of subsection (a) shall be treated as a violation of a rule defining an unfair or deceptive act or practice under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(2) POWERS OF THE COMMISSION.—

(A) IN GENERAL.—The Commission shall enforce this section 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 section.

(B) PRIVILEGES AND IMMUNITIES.—Any person who violates subsection (a) 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) AUTHORITY PRESERVED.—Nothing in this section shall be construed to limit the authority of the Commission under any other provision of law.

SEC. 8. BUREAU OF TECHNOLOGY.

(a) ESTABLISHMENT.—There is established in the Federal Trade Commission a bureau to be known as the Bureau of Technology (referred to in this section as the ''Bureau'').

(b) CHIEF TECHNOLOGIST.—The Bureau shall be headed by a chief technologist, who shall be appointed by the Chairman of the Commission.

(c) STAFF.—

(1) IN GENERAL.—Except as provided in paragraph (2), the Director of the Bureau may, without regard to the civil service laws (including regulations), appoint and terminate 50 additional personnel with expertise in management, technology,

digital design, user experience, product management, software engineering, and other related fields to technologist and management positions to enable the Bureau to perform the duties of the Bureau.

(2) EXCEPTED SERVICE.—Not fewer than 40 of the additional personnel appointed under paragraph (1) shall be appointed to positions described in section 213.3102(r) of title 5, Code of Federal Regulations.

(d) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Bureau such sums as are necessary to carry out this section.

SEC. 9. ADDITIONAL PERSONNEL IN THE BUREAU OF CONSUMER PROTECTION.

(a) IN GENERAL.—Notwithstanding any other provision of law, the Director of the Bureau of Consumer Protection of the Federal Trade Commission may, without regard to the civil service laws (including regulations), appoint—

(1) 100 additional personnel in the Division of Privacy and Identity Protection of the Bureau of Consumer Protection; and

(2) 25 additional personnel in the Division of Enforcement of the Bureau of Consumer Protection.

(b) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to the Director of the Bureau of Consumer Protection such sums as may be necessary to carry out this section.

SEC. 10. COMPLAINT RESOLUTION.

The Commission shall create rules and guidance establishing procedures for the resolution of complaints by consumers regarding covered entities that improperly use, store, or share the personal information of consumers, including procedures to—

(1) properly process and store complaints;

(2) provide a consumer with email updates regarding the status of the consumer's complaint;

(3) create an online portal that allows a consumer to log in and track the status of the consumer's complaint;

(4) review and forward complaints to the correct person, partnership, corporation, government agency, or other entity; and

(5) process and store each response from a person, partnership, corporation, government agency, or other entity to which a complaint was forwarded.

SEC. 11. APPLICATION PROGRAMMING INTERFACES.

The Commission shall, in consultation with the National Institute of Standards and Technology and relevant

stakeholders, including consumer advocates and independent technology experts—

(1) standardize Application Programming Interfaces necessary to permit consumers and covered entities to programmatically avail themselves of the rights and responsibilities created by this Act;

(2) permit and enable consumers to securely delegate the ability to make requests on their behalf; and

(3) require covered entities to implement the Application Programming Interfaces, as appropriate.

SEC. 12. NEWS MEDIA PROTECTIONS.

Covered entities engaged in journalism shall not be subject to the obligations imposed under this Act to the extent that those obligations directly infringe on the journalism, rather than the business practices, of the covered entity.