11__TH CONGRESS
___ SESSION

H.R./S_____

To ensure the privacy of personal information, the protection of consumers, and the promotion of innovation.

_____

In the _____

_____

A BILL

To protect the privacy of personal information of consumers, the promotion of innovation, and provide national uniformity of regulation. This bill shall be known as the Federal Consumer Privacy Act.

SECTION 1. DEFINITIONS.

In this Act, the following definitions shall apply:

(1) AGGREGATED INFORMATION.—The term "aggregated information" means deidentified information that relates to a group or category of consumers.

(2) BUSINESS.—The term "business" means

(A) a sole proprietorship, partnership, limited liability company, corporation, association, or other legal

entity engaged in interstate commerce, and that has annual receipts in excess of the U.S. Small Business Administration size standard for the business' industry, as calculated by the U.S. Small Business Administration.

(B) A service provider is not a business to the extent it is acting in its capacity pursuant to Subsection (9).

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

(4) CONSUMER.—The term "consumer" means a natural person, in his or her personal capacity (but not in his or her capacity as an Employee), in the United States whose personal information is collected, used, or shared by such business.

(5) DATA HYGIENE. — The term "data hygiene" means activities to ensure that data is accurate, complete and current.

(6) DEIDENTIFIED INFORMATION.—The term "deidentified information" means personal information from which identifiers have been removed.

(7) PERSONAL INFORMATION.—The term "personal information" means information that identifies a consumer. Information is

not personal information if it is aggregated information, deidentified information, pseudonymized information or publicly available information that is lawfully made available to the general public.

(8) PSEUDONYMIZED INFORMATION.—The term "pseudonymized information" means information processed in such a manner that it can no longer be attributed to a specific consumer without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information do not identify, or cannot reasonably identify, a natural person.

(9) SERVICE PROVIDER.—The term "service provider" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that processes personal information on behalf of a business; provided that a contract between the business and the service provider prohibits the service provider from retaining, using, or disclosing the personal information for any purpose other than the purposes authorized under the relevant contract, or

as otherwise permitted by this Act, or other applicable law, rule or regulation or for the service provider's internal compliance purposes.

(10) THIRD PARTY.—A third party is a business that does not collect personal information directly from a consumer. A third party is not a service provider and is not an affiliate, parent or subsidiary entity of the business.

SECTION 2. NOTICE AND TRANSPARENCY.

(a) NOTICE.—A business shall provide clear and conspicuous notice of how it collects, uses and shares personal information in an easily accessible format such as through a website.

(b) TRANSPARENCY.—A business shall, upon receipt of a verifiable request directly from the individual consumer, disclose to that consumer within a reasonable time period—

(1) The categories of the personal information pertaining that to the consumer collected, used or shared by the business;

(2) The business or commercial purpose for collecting, using or sharing such personal information; and

(3) The categories of third parties with whom the business shares such personal information.

(c) REQUESTS. —A business is not obligated to provide the information required in Section 2(b) to the same consumer more than once in a 12-month period.

(d) INTERFERENCE WITH OTHER OBLIGATIONS.—The disclosure requirements of Section 2 shall not supersede or impair a consumer reporting agency or a commercial credit reporting agency's disclosure obligations under the Fair Credit Reporting Act.

SECTION 3. CONSENT TO SHARE INFORMATION.

(a) OPT-OUT CONSENT.—A business, including a third party, must honor the verifiable request received directly from the individual consumer to not share the consumer's personal information with third parties. This shall be known as opt-out consent.

(b) EXCEPTIONS.—The opt-out consent provisions in Section 3(a) shall not apply to a business or its authorized third-party or service provider that shares consumer's personal information:

(1) With or from a consumer reporting agency subject to or as authorized by the Fair Credit Reporting Act or a commercial credit reporting agency; OR

(2) To complete the transaction for which the personal information was collected, provide a good or service

requested by the consumer or that is reasonably anticipated within the context of a business' ongoing business relationship with the consumer, bill or collect for such good or service or otherwise perform a contract between the business and the consumer; OR

(3) To detect, protect against or prevent actual or potential fraud, unauthorized transactions, theft, shoplifting, claims, or other liability; to detect or prevent security incidents including national security; to detect, protect against or prevent actual or potential malicious or illegal activity; to monitor and detect financial crimes and further anti-money laundering initiatives; and identify, investigate or prosecute those responsible for any of the foregoing activities; OR

(4) To debug or identify and repair errors that impair existing intended functionality; OR

(5) To comply with the Electronic Communications Privacy Act, or other legal or regulatory obligations under federal, state or local laws as referenced in Section 5 below; OR

(6) To engage in research and measurement purposes where the data is protected through appropriate security measures; OR

(7) For uses by the business or its service providers that are reasonably aligned with, related to, or compatible with the purposes for which the data was originally collected; OR

(8) To comply with a legal or regulatory obligation or as authorized by federal, state, or local law; OR

(9) To exercise or defend legal claims; OR

(10) To protect the safety or property of natural persons or of the business; OR

(11) To conduct product recalls; OR

(12) For reasonable network management, inventory management, financial reporting and accounting, analytics, product or service delivery, improvement or forecasting; OR

(13) For other lawful purposes compatible with the context in which the consumer provided the personal information, including for data hygiene.

SECTION 4. RIGHT TO DATA DELETION.

(a) DATA DELETION.—A business, including a third party, shall make a good faith effort to delete and require its service providers to

delete personal information upon a verifiable request received directly from the individual consumer.

(b) EXCEPTIONS.—A business shall not be required to comply with a consumer's request to delete the consumer's personal information under section 4(a) more than once in any 12 month period, nor when the personal information is used by the business—

(1) As authorized for consumer reporting agencies by the Fair Credit Reporting Act or in the performance of activities as a commercial credit reporting agency; OR

(2) To complete the transaction for which the personal information was collected, provide a good or service requested by the consumer or that is reasonably anticipated within the context of a business's ongoing business relationship with the consumer including but not limited to rewards or loyalty programs, bill or collect for such good or service, or otherwise perform a contract between the business and the consumer; OR

(3) To detect, protect against or prevent actual or potential fraud, unauthorized transactions, theft, shoplifting, claims, or other liability; to detect or prevent security incidents

including national security; to detect, protect against or prevent actual or potential malicious or illegal activity; to monitor and detect financial crimes and further anti-money laundering initiatives; and identify, investigate or prosecute those responsible for any of the foregoing activities; OR

(4) To debug or identify and repair errors that impair existing intended functionality; OR

(5) To exercise free speech, ensure the right of another consumer to exercise his or her right of free speech, or exercise another right provided for by law; OR

(6) To comply with the Electronic Communications Privacy Act, or other legal or regulatory obligations under federal, state or local laws as referenced in Section 5 below; OR

(7) To engage in research and measurement purposes where the data is protected through appropriate security measures; OR

(8) For uses by the business or its service providers that are reasonably aligned with, related to, or compatible with the purpose for which the data was originally collected, including data hygiene; OR

(9) To comply with a legal or regulatory obligation or as authorized by federal, state, or local law; OR

(10) To exercise or defend legal claims; OR

(11) To protect the safety or property of natural persons or businesses; OR

(12) For reasonable network management, inventory management, financial reporting and accounting, analytics, product, service or service delivery, improvement or forecasting; OR

(13) For other lawful purposes compatible with the context in which the consumer provided the information, including data hygiene; OR

(14) For data stored in back-up systems, legacy systems, or otherwise not readily accessible or where identifying and deleting such personal information creates undue burden.

SECTION 5. OBLIGATIONS NOT APPLICABLE.

(a) A business shall not be obligated to comply with this Act to the extent compliance restricts the business' ability to:

(1) Comply with federal, state, or local laws that do not relate to the privacy of personal information; OR

(2) Comply or respond to a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities; OR

(3) Cooperate with law enforcement agencies concerning conduct or activity that a business, service provider, or third party reasonably and in good faith believes may violate federal, state, or local law; OR

(4) Exercise or defend actual or reasonably anticipated legal claims; OR

(5) Collect, use, retain, create or share information that is aggregated information, deidentified information, or pseudonymized information, or publicly available information that is lawfully made available to the general public; OR

(6) Engage in activities that are protected by the First Amendment; OR

(7) Collect, use, or share information about employees, independent contractors, temporary workers and applicants for the aforementioned roles.

(a) This Act shall not be construed to require a business to do the following:

(1) Re-identify deindentified data or otherwise link data in a form that renders it personal information;

(2) Retain personal information about a consumer that would not otherwise be retained in the ordinary course of business; OR

(3) Comply with a request to exercise any of the rights in Sections 2 through 4 if the business is unable to verify, using commercially reasonably efforts, the identity of the consumer making the request.

Section 6. Safe Harbors.

(a) GUIDELINES.—A business may satisfy the requirements of this Act by following a set of guidelines issued by persons approved under subsection (1).

(1) DEEMED COMPLIANCE.—A business will be deemed to be in compliance with the requirements of this Act if that business complies with such guidelines that, after notice and comment, are approved by the Commission upon making a

determination that the guidelines meet the requirements of this Act.

(2) EXPEDITED RESPONSE TO REQUESTS.—The Commission shall act upon requests for safe harbor treatment within 180 days of the filing of the request, and shall set forth in writing its conclusions with regard to such requests.

(3) APPEALS.—Final action by the Commission on a request for approval of guidelines, or the failure to act within 180 days on a request for approval of guidelines, submitted under subparagraph (1) may be appealed to a district court of the United States of appropriate jurisdiction as provided for in section 706 of title 5, United States Code.

(b) LIABILITY.— A business shall not be liable for the failure of another person to fulfill a legal duty or obligation related to personal information, including any such failure that results in a violation of this Act.

SECTION 7. ENFORCEMENT.

(a) GENERAL APPLICATION.—The Commission shall enforce the requirements of the Act. Notwithstanding section 5(a)(2) of the Federal Trade Commission Act, the Commission shall have

authority over common carriers subject to the Communications Act of 1934 to enforce this Act.

(b) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—A violation of this Act shall be treated as an unfair or deceptive act or practice in or affecting commerce for purposes of section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)). [***The Chamber recognizes that businesses not under FTC jurisdiction are subject to the jurisdiction of other agencies and will be subject to enforcement by those agencies. The U.S. Chamber adopted privacy principles that apply to all industry sectors that handle consumer data and are not specific to any subset of industry sectors. These principles shall be applied consistently across all industry sectors. The Chamber will continue to actively engage policymakers and stakeholders to ensure in accordance with its principles consistent enforcement across sectors.***]

(c) OPPORTUNITY TO CORRECT.—Section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) is amended by inserting at the end the following: "(O) OPPORTUNITY TO CURE PRIVACY DEFICIENCIES.—Before proceeding with an enforcement action as authorized by this Section, the Commission shall notify a business

that it has a reason to believe that the business has failed to comply with the Federal Consumer Privacy Act in a manner that is not willful or reckless. The Commission shall give a business reasonable time to cure non-willful or non-reckless violations before undertaking an enforcement action authorized by this Section.

(d) PRIVATE RIGHTS OF ACTION.—This Act shall not be construed to authorize a person to bring a civil action against an alleged violator of the Act.

SECTION 8. RELATION TO OTHER LAWS.

(a) PREEMPTION OF STATE LAW.—The provisions of this Act shall supersede any provisions of the statutes, laws, regulations, rules, ordinances, requirements, or the equivalent, of any State, or any locality or political subdivision of a State, including, but not limited to, any tort, duty, or consumer protection or unfair practice law, to the extent that such provisions relate to, or serve as the basis for enforcement action as it relates to, the privacy or security of personal information. No State, or any locality or political subdivision of a State, shall adopt, maintain, enforce, impose, or

continue in effect any such provision after the effective date of this Act.

(b) OTHER FEDERAL LAWS.

(1) IN GENERAL.—Except as otherwise provided in paragraph (2) this Act shall supersede any other Federal statute or regulation relating to the privacy or security of personal information.

(2) This Act shall not be construed as superseding any of the following laws:

(A) The Children's Online Privacy Protection Act (15 U.S.C. § 6501 et seq.);

(B) The Communications Assistance of Law Enforcement Act (47 U.S.C. § 1001 et seq.);

(C) Section 227 of the Communications Act of 1934 (47 U.S.C. 227);

(D) The Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);

(E) The Health Insurance Portability and Accountability Act (Public Law 104-191);

(F) The Electronic Communications Privacy Act;

(G)The Driver Privacy Protection Act (15 U.S.C. § 2721 et seq); AND

(H) The Federal Aviation Act, as amended (49 U.S.C. § 40101 et seq.), and the provisions of such other Federal statutes and regulations not superseded by this Act shall continue to apply in lieu of this Act.

[***The Chamber recognizes that robust federal privacy laws already apply to many sectors of the economy. A federal law should work to harmonize or replace sectoral privacy approaches unless there is a meaningful reason to keep an existing sectoral law. Although the Chamber recognizes the importance of allowing data protection, privacy, or consumer protection laws like HIPAA and the Federal Aviation Act, as amended (49 U.S.C. § 40101 et seq.) to remain in place, the Chamber will continue to actively engage policymakers and stakeholders about how other sectoral laws should interact with a new privacy framework. The Commission's authority may need to be modified if certain sectoral laws are eliminated. The Chamber's position is that a new privacy framework should not impose dual enforcement of federal agencies upon regulated entities.]***