CONSUMER PRIVACY AND DATA SECURITY STANDARDS ACT OF 2019

PREAMBLE

Because information is the basis of knowledge, and knowledge is the basis of competitive advantage in local, national and global markets, this law establishes a fair, inclusive, and transparent process to govern the collection, use, maintenance, and disclosure of personal information.

In order for public and private sector institutions to fulfill their mandates to serve the citizens of the United States, these institutions must earn the trust of the American people by demonstrating that they access, use, maintain and disclose consumers' personal information in a manner that respects reasonable consumer interests in privacy and data security.

Precisely what constitutes an appropriate balance in the interests of institutions and individuals regarding personal information varies, depending on the sensitivity of the personal information, the importance of the institutional need, and the context in which the information is used. At times, the appropriate balance can be reflected in sector-specific statutes and regulations. At other times, more context-specific and granular governance frameworks are needed.

The American system of voluntary consensus standards established by the private sector through recognized fair, inclusive, transparent, procedures that comport with due process, in which the interests of all principal stakeholders are accounted for, has provided effective solutions to similar problems for more than one hundred years.

When public and private sector institutions make effective use of voluntary consensus standards established through due process procedures to implement solutions to urgent problems, the benefits accrue not only to private and public institutions, but also to the American people.

SEC. 1. DEFINITIONS

(a) "PERSONAL INFORMATION" refers to information that can be reasonably expected to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

(b) "COVERED ENTITY" refers to a person, partnership, association or organization over which the Federal Trade Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), and operates a website located on the internet or an online service and who collects, uses, maintains or discloses personal information from or about individuals, or on whose behalf such information is collected, used, maintained or disclosed, where such website or online service is operated for commercial purposes, including any entity that buys and sells consumer data without direct consumer interaction, and any entity offering products

or services for sale through that website or online service. Notwithstanding the limitations in the Federal Trade Commission Act on Commission authority with respect to common carriers, a covered entity also includes common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.) and Acts amendatory thereof and supplementary thereto.

(c) “COMMISSION” refers to the Federal Trade Commission.

(d) “STANDARD" includes all of the following:

(1) Common and repeated use of rules, conditions, guidelines or characteristics for products or related processes and production methods, and related management systems practices.

(2) The definition of terms; classification of components; delineation of procedures; specification of dimensions, materials, performance, designs, or operations; measurement of quality and quantity in describing materials, processes, products, systems, services, or practices; test methods and sampling procedures; or descriptions of fit and measurements of size or strength.

(e) "STANDARD" does not include the following:

(1) Professional standards of personal conduct.
(2) Institutional codes of ethics.

(f) “VOLUNTARY CONSENSUS STANDARDS” are due process standards developed or adopted by voluntary consensus standards bodies as set forth in this Act.

(g) "VOLUNTARY CONSENSUS BODIES" are organizations which plan, develop, establish, or coordinate voluntary consensus standards using agreed-upon due process procedures. A voluntary consensus standards body is defined by the following attributes:

(1) Openness
(2) Balance of interest.
(3) Due process.
(4) An appeals process.
(5) Consensus, which is defined as general agreement, but not necessarily unanimity, and includes a process for attempting to resolve objections by interested parties, as long as all comments have been fairly considered, each objector is advised of the disposition of his or her objection(s) and the reasons why, and the consensus body members are given an opportunity to change their votes after reviewing the comments.

SEC. 2. REGULATION OF UNFAIR AND DECEPTIVE ACTS AND PRACTICES WITH COLLECTION AND USE OF PERSONAL INFORMATION

(a) ACTS PROHIBITED.—In General—It is unlawful for a covered entity to collect, use, maintain, or disseminate personal information in a manner that violates the regulations prescribed by the Federal Trade Commission under subsection (d) of this Section.

(b) ENFORCEMENT.—A violation of this Act or a regulation promulgated under this Act shall be treated as a violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)) regarding unfair or deceptive acts or practices.

(c) POWERS OF COMMISSION.—Except as provided in subsection (a), the Federal Trade 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.

(d) REGULATIONS.—

(1) IN GENERAL.—Not later than 1 year after the enactment of this Act, the Commission shall promulgate under section 553 of title 5 regulations that require covered entities to collect, use, maintain and disclose personal information:

A. In accordance with reasonable security measures to protect its confidentiality, security, and integrity; and

B. In accordance with reasonable consumer interests in privacy.

(2) Such regulations may not impose direct or indirect liability on any covered entities for making a voluntary or compelled disclosure of personal information to a federal, state local or tribal law enforcement, national security, regulatory or other governmental agency for an authorized governmental purpose.

(3) Before issuing a regulation for data security and privacy, or approving any voluntary consensus standard, the Commission shall consult with the Attorney General, and with other federal agencies, as appropriate, to ensure that the standard does not hamper competition, or restrict access to personal information for authorized law enforcement, national security, or other lawful, authorized governmental purposes.

(4) ENFORCEMENT.—Subject to Section 3 of this title, a violation of a regulation prescribed under subsection (d) of this Section 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, and any person, partnership, or corporation who violates a such a regulation shall forfeit and pay to the United States a civil penalty of not more than $10,000 for each violation, which shall accrue to the United States and may be recovered in a civil action brought by the Attorney General of the United States.

(5) INCONSISTENT STATE LAW.—No State or local government may impose any liability for commercial activities or actions by a covered entity in connection with an activity involving personal information covered by the regulations promulgated by the Commission under this Section 2 of this Act or by a voluntary consensus standard approved by the Commission pursuant to Section 3 of this Act.

SEC. 3—SAFE HARBORS

(a) In prescribing regulations under this title, the Commission shall provide incentives for adoption of voluntary consensus standards, as set forth in this Act, by covered entities to implement the protections described in Section 2(d)(A) and (B) of this title.

(b) DEEMED COMPLIANCE.—Such incentives shall include provisions for ensuring that a covered entity will be deemed to be in compliance with the requirements of the regulations issued under Section 2(d)(1) of this title if the covered entity follows a voluntary consensus standard, as set forth in this Act, that, after notice and comment, is approved by the Commission pursuant to the provisions of this Act, and found by the Commission to:

(1) meet the requirements of the regulations issued under Section 2(d)(1) of this title;

(2) be the result of due process procedures set forth in Section 4 of this Act; and

(3) appropriately balance the interests of all the stakeholders, including individuals and businesses, organizations, and other entities making lawful uses of the personal information.

(c) 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.

(d) APPEALS.—Final action by the Commission on a request for approval of voluntary consensus standards, or the failure to act within 180 days on a request for approval of the voluntary consensus standard, submitted under subsection (b) may be appealed to a district court of the United States of appropriate jurisdiction as provided for in section 706 of title 5.

SEC. 4—VOLUNTARY CONSENSUS STANDARDS

(a) GUIDELINES.—A covered entity may satisfy the requirements of regulations issued under Section 2(d)(1) of this title by following a voluntary consensus standard, issued by the National Institute of Standards and Technology or by other voluntary consensus standards bodies, pursuant to this Act, and approved by the Commission under Section 3(a) and (b) of this Title.

(b) VOLUNTARY CONSENSUS STANDARDS—PROCESS—To be eligible for safe harbor status under Section 3(a) and (b), a voluntary consensus standard must be the result of a process:

(1) That follows the principles of consensus, due process and openness, depending heavily upon data gathering and compromise among a diverse range of stakeholders;

(2) That ensures that access to the standards setting process, including an appeals mechanism, was made available to anyone directly or materially affected by the standard under development;

(3) That provides all such stakeholders (including individuals, businesses, government agencies, and other entities such as consumer groups and civil society organizations), a reasonable opportunity to voluntarily contribute their knowledge, talents and efforts to the standard's development;

(4) That consistently adheres to essential due process procedures that served and protected the public interest in openness, balance, consensus and other due process safeguards;

(5) That is equitable, accessible and responsive to the requirements of all interested and affected parties;

(6) That includes a reasonable opportunity for broad-based public review and comment on draft standard, with consideration of and response to the comments submitted by voting members of the relevant consensus body and by public review of the comments, followed by incorporation of the approved changes into a draft standard; and

(7) That includes a right to appeal by any participant that believed that due process principles were not sufficiently respected during the standards development in accordance with the procedures of the standard setting organization.

(c) VOLUNTARY CONSENSUS STANDARDS.—To be eligible for safe harbor status in connection with regulations issued under Section 2(d)(1)(B), a voluntary consensus standard must

(1) Establish a clear nexus to the collection, use, maintenance and disclosure of the personal information it governs;

(2) Reasonably identify the interests of the stakeholders (including individual consumers, businesses and governments);

(3) Reasonably identify the benefits and material risks to the stakeholders arising from the proposed collection, use, maintenance and disclosure of the personal information involved;

(4) Reasonably ensure that the benefits from the proposed collection, use, maintenance and disclosure of the personal information outweigh risks, after such risks are mitigated by technological, operational or other means, presenting the supporting analysis for such assessment of costs and benefits fairly, symmetrically, and with an appropriate level of granularity;

(5) Reasonably addressing any alternatives, after disclosing all key assumptions, data and models;

(6) Reasonably addressing the requirements by the regulations promulgated under Section 2(d)(1)(B) of this Title by specifying routine uses for which consent is not required when the use and disclosure of the personal information is compatible with the purposes for which the information was collected, and non-routine uses, in which case procedures must be established to reasonably protect the interests of the individual, including as appropriate:

(A) Written consent by the individual prior to use of the information for the non-routine purpose;
(B) Transparency regarding information collection, use, maintenance, and dissemination;
(C) Procedures for consumers to access and correct information material to decisions affecting their legitimate interests; and
(D) Redress for actual damages caused by a business's failure to adhere to the standard.

(7) Establish reasonable internal controls and accountability to ensure effective implementation of the voluntary consensus standard by the covered entity.