CONSUMER DATA PRIVACY & SECURITY ACT

Senator Jerry Moran

Section 1: Short Title

This act may be cited as the "*Consumer Data Privacy and Security Act*."

Section 2: Definitions

This section defines terms used throughout the act, including *collection*, *covered entity*, *personal data*, *processing*, *sensitive personal data*, *service provider*, *small business*, *third party*, and other critical terms that carefully and clearly delineate the scope of the act.

Section 3: Collection and Processing of Personal Data

This section establishes notice and consent requirements expected of covered entities, third parties, and service providers as it pertains to their specific relationship to the personal data in question. A covered entity, including a third party, shall not collect or process personal data of an individual unless the individual has consented for a specific purpose or in accordance with a permissible purpose as described in this section.

This section allows for third parties to collect and process personal data if the covered entity, from whom the third party received the personal data, gave proper notice that the third party would collect or process the personal data for a specific purpose and the individual consented. It also establishes notice and consent requirements for different or additional collection or processing, while establishing a duty for third parties to exercise reasonable due diligence prior to reliance on representations from a covered entity.

This section requires express affirmative consent from the individual for a covered entity to collect or process the personal data of the individual if the action involves sensitive personal data of the individual or discloses the personal data of the individual to a third party. Notice to the individual, prior to consent, shall be concise, meaningful, timely, prominent, and easy-to-understand, and the covered entity shall provide an individual the means to withdraw previously given consent.

Section 4: Right to Know

This section requires a covered entity to make its privacy policy available to the public in a clear and prominent location and in easy-to-understand language. It also requires past versions of the privacy policy to remain publicly available. The content of a privacy policy shall include:

- Identity and contact information for the appropriate representative of the covered entity for the purposes of privacy inquiries;
- Descriptions of each category of personal data collected and the purposes of collection and processing;
- Descriptions of relevant retention periods, if possible, and determining criteria for the deletion or de-identification of such personal data;
- Whether and for what purposes the covered entity discloses personal data to third parties, the categories of personal data disclosed to third parties, and the types of third parties to which those categories of data are disclosed;

- Whether and for what purposes the covered entity receives personal data from third parties, the categories of personal data received from third parties, and the types of third parties to which those categories of personal data are received;
- Description of notification process related to material changes in the privacy policies and practices of the covered entity;
- Description of how the individual may avoid or minimize the collection and processing of their personal data; and
- The effective date of the privacy policy.

This section establishes specific exceptions to the privacy policy requirement, including in-person transactions, compliance with laws or other legal requirements, prevention of imminent danger to the personal safety of an individual, and protection against security threats, abuse, fraud, theft, unauthorized transaction, or any other unlawful activity.

If there is a material change to the privacy policy, this section requires a covered entity to notify each individual whose personal data is collected or processed by the covered entity, or a service provider on behalf of the covered entity, with a description of the material change and not process any sensitive personal data of the individual that was collected before the effective date of the material change in a matter that is inconsistent with the privacy policy at the applicable time of the original express affirmative consent. If technically feasible, the covered entity shall provide the notice of the material change directly to the affected individual. If direct notification of a material change is impossible or demonstrably impracticable, the covered entity shall publish the notice in a reasonably prominent location and publish a reasonable time prior further processing.

Section 5: Individual Control

This section requires covered entities to provide reasonably accessible, clear, conspicuous, and easy-to-use means to individuals to exercise their rights to access, accuracy and correction, and erasure with respect to their personal data at no additional cost to the individual.

This section establishes a “right to access,” which requires a covered entity to confirm whether or not it has collected or processed the personal data of the individual submitting a verified request and, if so, provide the individual a copy or accurate representation of the personal data of that individual and a list of third parties to which the covered entity disclosed the personal data. The covered entity would also be required to provide the personal data generated and submitted by an individual in a structured, commonly-used, and machine readable format and transmit such information to another entity without constraints or conditions.

This section creates a “right to accuracy and correction,” which requires a covered entity to establish reasonable procedures to ensure that the personal data that the covered entity collects and processes, with respect to the individual, is accurate, up-to-date and provides individuals the ability to submit a verified request to dispute the accuracy and completeness of the personal data while requesting appropriate correction.

This section provides a “right to erasure,” which requires a covered entity to delete or de-identify the personal data of the individual upon request without undue delay, while also directing any associated service providers to do the same with the personal data in question.

This section allows any individual to exercise each of the rights described at least twice in any 12-month period while allowing the covered entity to charge a reasonable fee or refuse to act on the request if the individual submits a manifestly unfounded, frivolous, or excessive request. This section also requires a covered entity to verify the identity of the individual making the request while laying out a reasonable effort to conduct such verification.

This section also describes specific situations in which the covered entity shall decline to act on a request while requiring appropriate notice of the reasons of declination.

This section also clarifies that "small businesses," as defined in this act, are not required to comply with the consumer controls of "right to access" or "right to accuracy and correction" due to the resource-intensive nature of these apparatuses. However, "small businesses" would still be required to comply with the "right to erasure" with special considerations related to timeliness.

This section also authorizes the FTC to consult with and solicit comments from consumer data industry representatives on the issuance of guidance describing nonbinding best practices related to consumer controls.

Section 6: Security

This section requires each covered entity and service provider to develop, document, implement, and maintain a comprehensive data security program that contains reasonable administrative, technical, and physical safeguards designed to protect personal data from unauthorized access and related harmful disclosures.

The safeguards must be appropriate to the size, complexity, and resources of the entity; the nature and scope of the activities of the entity; the technical feasibility and cost of available tools to reduce vulnerabilities; the sensitivity of the personal data involved; and the potential of economic loss or physical injury to the individual if unauthorized disclosure occurs.

A comprehensive data security program required under this section must:

- Include a designated employee responsible for managing the safeguards;
- Be designed to identify material internal and external risks to the security and confidentiality of the personal data handled by the entity;
- Implement safeguards designed to control the risks identified in its risk assessments while regularly assessing the effectiveness of the safeguards;
- Maintain reasonable procedures to ensure that service providers and third parties to whom the personal data is transferred have similarly effective safeguards; and
- Maintain reasonable flexibility to adjust the safeguards in light of any material changes in technology and business arrangements.

Section 7: Accountability

This section applies only to "applicable entities" that collect and process the personal data of more than 20,000,000 individuals or the sensitive personal data of more than 1,000,000 individuals. Applicable entities would be required to designate an employee to serve as the privacy officer who is responsible for overseeing its policies and practices related to the collection and processing of personal data.

This section also requires applicable entities to conduct privacy impact assessments when it intends to begin a new collection or processing activity or to make a material

change in its processing of personal data. The assessment shall take into consideration the nature and volume of the personal data and the potential for the new processing activity or material change to be a proximate cause of harm to individuals to whom the personal data pertains. The applicable entity's privacy officer would be required to approve the finding of any such assessment and be required to be documented.

This section mandates that applicable entities shall implement a comprehensive privacy program to safeguard the privacy and security of the personal data collected and processed for the life cycle of development and operational purposes of its products and services.

Section 8: Rules Relating to Service Providers

This section pertains to the rules relating to service providers and covered entities that enter into contractual arrangements with such service providers. Any covered entity that discloses personal data to a service provider, who by definition collects and processes personal data on behalf of and at the direction of the covered entity, shall:

- Take reasonable steps to identify whether a service provider has established appropriate procedures and controls for ensuring the privacy and security of the personal data to comply with this act; and
- Investigate any circumstances in which a reasonable person would determine that there is a high probability that the service provider is not in compliance with a requirement described in the section.

In determining whether a covered entity has acted reasonably in complying with these provisions, the FTC shall take into account the size, complexity, and resources of the covered entity and the risk of harm reasonably expected to occur as a result of the covered entity disclosing personal data to a service provider without complying with the section.

A contract in this section would require the service provider to only collect and process the personal data as directed by the covered entity, establish the purposes and means of collecting and processing personal data with which such service provider shall be required to comply, and include reasonable representations that the service provider has established appropriate procedures and controls to comply with this act. Contracts may not relieve a covered entity or service provider of the requirements imposed on them by this legislation.

This section requires service providers to inform the covered entity, from which it received personal data, when it is required to process personal data to comply with a legal requirement unless prohibited by law. If a service provider amends its policies or practices relating to personal data that is relevant for the provisions of this section, it shall provide reasonable notice of such change to any covered entity on whose behalf the service provider collects and processes data.

This section also requires service providers to either provide a covered entity appropriate technical and organizational measures for the covered entity to comply with the privacy control requests or respond to the covered entity that provides the service provider with a privacy control request received under Section 5. A service provider is required to comply with a covered entity's request to delete, de-identify, or return personal data after completion of a service or function for which the data was disclosed to the service provider.

A service provider shall make available to the covered entity information necessary to demonstrate the service provider's compliance, insofar as such information is technically available to the service provider. Service providers may engage a subcontractor for processing personal data covered in a contract after providing a covered entity, from which it received personal data, an opportunity to object and, pursuant to an agreement, to meet obligations of the service provider with respect to the personal data.

Similar to a covered entity, in determining whether a service provider has acted reasonably in complying with these provisions, the FTC shall take into account the size, complexity, and resources of the service provider and the risk of harm reasonably expected to occur as a result of noncompliance by the service provider.

Section 9: Enforcement

This section specifies that a violation of this act or regulation promulgated under this act shall be treated as an unfair or deceptive act or practice in violation of Section 5 of the FTC Act. The FTC would also have jurisdiction to enforce this act with respect to common carriers and nonprofit organizations. The section also authorizes the FTC to utilize "first-time" civil penalty authority for violations of this act, and the amount of the civil penalty shall be determined based on a number of factors including the degree of harm associated with the privacy and security of the personal data in question, the intent of the covered entity, and the size, complexity, and resources of the covered entity among others.

This section also authorizes state attorney generals to bring civil action on behalf of the residents of their state, as parens patriae, for violations of this act or regulations promulgated by this act. If pursuing civil action, the state attorney general would be required to notify the FTC in writing no later than 10 days before initiating a civil action. The FTC would be authorized to intervene in any civil action brought by the state attorney general. Civil actions brought by two or more state attorney generals would be required to be consolidated. Finally, if the FTC institutes an enforcement action under this section with respect to a violation of this act, state attorney generals would not be permitted to institute a civil action against any defendant named in the complaint raised by the FTC.

This section makes clear that nothing in this act shall be construed to provide a private right of action.

Section 10: Relation to Other Laws

This section expressly preempts any provision of a law, rule, regulation, or other requirement of any state or locality to the extent that such provision relates to the privacy or security of personal data. This section also preserves certain state and local laws that pertain to specific categories that this comprehensive federal privacy law is not intended to supersede including consumer data breach notification laws, rules of criminal or civil procedure, laws relating to fraud or public safety, laws pertaining to employment and employment-related data, laws pertaining to discrimination, and sector-specific, state-level laws that apply to non-preemptive federal privacy frameworks.

This section also specifically clarifies that the provisions of this act are not to be interpreted to be superseding, the following federal laws:

- The Children's Online Privacy Protection Act
- The Communications Assistance for Law Enforcement Act
- Section 227 of the Communications Act of 1934

- Title V of the Gramm-Leach-Bliley Act
- The Fair Credit Reporting Act
- The Health Insurance Portability and Accountability Act
- The Health Information Technology for Economic and Clinical Health Act
- The Family Educational Rights and Privacy Act of 1974
- The Electronic Communications Privacy Act
- The Driver's Privacy Protection Act of 1994
- The Federal Aviation Act of 1958

This section also clarifies that no provisions of the Communications Act or regulations under the act (or amendments to the law) shall apply to covered entities with respect to the collection, processing, or security of personal data under this act, except to the extent that such provision pertains to "911" lines or other emergency lines.

Section 11: Commission Resources

This section requires the FTC Chairman to appoint no fewer than 440 additional individuals to serve as personnel to enforce this act and other laws relating to the privacy and security of personal data. It also requires the FTC to submit to Congress a report that includes an assessment of the resources available to carry out this act and what is needed to effectively carry it out. Finally, this section authorizes "such sums as may be necessary to carry out this section."

Section 12: Guidance and Reporting

This section requires the FTC to coordinate any enforcement action it pursues with relevant data protection authorities established in foreign countries. Additionally, the Secretary of Commerce, in consultation with the FTC, shall consistently report to Congress on the coordinated efforts to achieve international interoperability with foreign data protection authorities.

This section also requires the FTC to annually report to Congress on the effectiveness of the act, compliance outcomes including violations and enforcement actions, priorities of the FTC in enforcement, and resources needed to fully implement and enforce the provisions of the act. Finally, the Comptroller General of the United States shall report to the President and Congress on any identified inconsistencies between the act and other privacy and security laws, the impact of the act on small businesses, recommendations related to technological and economic trends, and enforcement activities carried out by the FTC.

Section 13: Severability

This section clarifies that if any provision of this act is held to be unconstitutional, the application of other provisions of this act shall not be affected.

Section 14: Effective Date

This section states that this act shall take effect on the date that is one year after the date of enactment, except that section 10 shall take effect upon the date of enactment of this act.