American Data Privacy and Protection Act Draft Legislation
Section by Section Summary

Section 1. Short Title; Table of Contents.
The title of the Act will be the "American Data Privacy and Protection Act."

Section 2. Definitions.
The Act defines "covered entity" to include any entity that collects, processes, or transfers covered data and is subject to the jurisdiction of the Federal Trade Commission (FTC), including nonprofits, and telecommunications common carriers. "Covered data" is defined as information identifying, linked, or reasonably linkable to an individual or device linkable to an individual. This includes derived data and unique identifiers, but does not include de-identified data, employee data, or publicly available information (each of which is separately defined).

"Sensitive covered data" is also defined and subject to heightened requirements. Any information related to individuals under 17 is sensitive. Sensitive covered data also includes government-issued identifiers not required to be displayed in public such as social security and passport numbers; past, present, and future health, diagnosis, disability, or treatment information; financial account, debit card, and credit card numbers along with any access code, password, or credentials; biometric information; genetic information; past or present precise geolocation information; private communications such as voicemail, email, text or information identifying parties to communications; any account or device log-in credentials; information revealing race, ethnicity, national origin, religion, union membership status, sexual orientation, or sexual behavior that violates an individual's reasonable expectations on disclosure; information revealing online activities over time and across third party online services; calendar, address book, phone, text, photos, audio and video recordings maintained for private use on a device; photos or videos of naked or undergarment-clad private areas; and information revealing individuals access to or viewing of TV, cable, or streaming media services.
Any other covered data collected, processed, or transferred for the purpose of identifying sensitive covered data is also considered sensitive. The FTC is granted rulemaking authority under the Administrative Procedure Act (APA) to include additional categories of covered data within the sensitive covered data definition where those categories require similar protection as a result of new methods for collecting or processing covered data.

"Biometric information" and "genetic information" are each specifically defined.
"Third-party collecting entities" (commonly referred to as data brokers or information brokers), "service providers", and "third parties" are all defined subsets of covered entities. "Large Data Holders" are covered entities with gross revenues above $250 million [and / that] collected, processed, or transferred covered data of over 5 million individuals/devices or the sensitive covered data of 100,000 individuals/devices in the most recent calendar year.

"Collecting" means acquiring covered data by any means. "Processing" means any operation or set of operations performed on covered data. "Transferring" means to disclose, make available, or license covered data by any means or in any way. Together these terms dictate the actions of covered entities and individuals with respect to covered data.

"Targeted advertising" means displaying to an individual or unique identifier an online advertisement that is selected based on knowns and assumptions derived from covered data collected. It does not include responses to an individual's specific request; first-party advertising based on individual's visit to or use of a service that offers a product or service that is the subject of the advertisement; contextual advertising when an advertisement is displayed based on the content of a webpage or online service; or processing of data solely used for measuring or reporting advertising metrics.

Other key definitions include affirmative express consent and algorithm.

Title I – Duty of Loyalty

Section 101. Data Minimization.

The Act imposes a baseline duty on all covered entities not to unnecessarily collect or use covered data in the first instance, regardless of any consent or transparency requirements. Specifically, covered entities are prohibited from collecting, processing, or transferring covered data beyond what is reasonably necessary, proportionate, and limited to provide specific products and services requested by individuals, communicate with individuals in a manner they reasonably anticipate given the context of their relationship with the covered entity, or for a purpose expressly permitted by the Act.

The FTC must issue guidance to help establish what is "reasonably necessary, proportionate, and limited" to comply with this section.

Section 102. Loyalty Duties.

To prevent harmful uses of particular sensitive data and ensure covered entities are protecting individual privacy, covered entities are prohibited from and significantly restricted in engaging in certain data practices regarding specific types of covered data except for very limited circumstances. This includes responding to a warrant or meeting heightened conditions for obtaining express affirmative consent of the individual when collecting, processing, or transferring biometric information, genetic information, aggregated internet browsing and search history, physical activity information, and transferring precise geolocation information to third parties. Social Security numbers, password information, and nonconsensual intimate images are subject to further restrictions.

Section 103. Privacy by Design.

Covered entities have a duty to implement reasonable policies, practices, and procedures for collecting, processing, and transferring covered data. These should correspond to the entity's size, complexity, activities related to covered data, the types and amount of covered data the entity engages with, and the cost of implementation compared to the risks posed. Privacy by design must also take into account the particular privacy risks related to individuals under age 17. The FTC must issue guidance on reasonable policies, practices, and procedures within one year of enactment.

Section 104. Loyalty to Individuals with Respect to Pricing.

Covered entities may not condition or effectively condition the provision or termination of services or products to individuals by having individuals waive any privacy rights in the Act.

This prohibition does not prevent covered entities from differentiating the price of or levels of services based on an individual providing financial information necessarily collected and used for payment when an individual specifically requests a product. Covered entities are also not prevented from offering loyalty programs that provide discounts in exchange for continued business, provided they otherwise comply with the Act.

Title II – Consumer Data Rights

Section 201. Consumer Awareness.

Within 90 days of enactment, the FTC must publish a public web page describing all provisions of the Act in plain language, listed separately to help advise individuals and covered entities of their rights and obligations under the Act. The web page must be updated for changes in law.

Section 202. Transparency.

Covered entities must provide individuals with privacy policies detailing their data collection, processing, transfer, and security activities in a readily available and understandable manner. Such policies must include contact information, the affiliates of the covered entity that it transfers covered data to, and the purposes for each category of covered data the covered entity collects, processes, and transfers. Covered entities must specify the third-party collecting entities to whom they transfer covered data and for what purposes.

Privacy policies must also state how individuals may exercise their rights under the Act and how long the entity intends to retain covered data. Privacy policies must be provided in all languages in which covered entities conduct business related to the covered data. Any material changes to a privacy policy require covered entities to notify individuals and provide an opportunity to withdraw consent before further processing the covered data of those individuals. Covered entities must specify whether any covered data they handle is made available to China, Russia, Iran, or North Korea.

Finally, large data holders must provide short-form notices of their covered data practices pursuant to minimum requirements established in FTC regulations under the APA.

Section 203. Individual Data Ownership and Control.

Individuals have the right to access, correct, delete, and portability of, covered data that pertains to them. The right to access includes obtaining covered data in a human-readable and downloadable format that individuals may understand without expertise, the names of any other entities their data was transferred to, the categories of sources used to collect any covered data, and the purposes for transferring the data. The rights to correct and delete covered data also require covered entities to notify other entities to whom covered data was transferred of the corrected information or desire to have the covered data deleted.

To the extent technologically feasible, individuals also have the right to export their covered data in a portable format. Covered entities are not required to comply with individual requests under this section where they are unable to verify the identity of the individual making the request. These individual rights are subject to covered entities rights to limited permissive exceptions for covered data use, such as complying with law enforcement or judicial proceedings. The timing

for covered entities to respond to such requests depends on whether covered entities are large data holders or meet the requirements of small and mid-sized entities.

The FTC is authorized to promulgate APA regulations as necessary to establish processes for compliance with this section, taking into consideration various characteristics of different covered entities and their activities with respect to covered data.

Section 204. Right to Consent and Object.
Sensitive covered data may not be collected, processed, or transferred to a third party without the express affirmative consent of the individual to whom it pertains. Individuals must be provided the means to provide and withdraw consent by the same clear, conspicuous, and easy to use means. Individuals may opt out of the transfer of any covered data to a third party.
Covered entities engaged in targeted advertising must provide individuals with clear and conspicuous means to opt out prior to any targeted advertising and at all times afterwards.

Section 205. Data Protections for Children and Minors.
Covered entities are subject to additional requirements for covered data with respect to individuals under age 17. Targeted advertising is expressly prohibited [if covered entities have actual knowledge that an individual is under 17]/[to any individual under 17]. Covered entities may not transfer the covered data of individuals between 13 and 17 years old to third parties without express affirmative consent [where the covered entity has actual knowledge the individual is between 13 and 17].

This section establishes a Youth Privacy and Marketing Division at the FTC, which shall be responsible for addressing privacy and marketing concerns with respect to children and minors. The division must submit annual reports to Congress and hire staff that includes experts in youth development, data protection, digital advertising, and data analytics.

This section also requires the FTC Inspector General to submit a report to Congress every two years analyzing the fairness and effectiveness of the safe harbor provisions in the Children's Online Privacy Protection Act of 1998 (COPPA). These reports must be published on the FTC web site.

Notably, there are several other important provisions with heightened or specific call-outs to children and minors throughout the legislation.

Section 206. Third-party collecting entities.
Third-party collecting entities must place a clear and conspicuous notice on their web site and/or mobile application informing individuals they are a third-party collecting entity using language specified by FTC regulations. The FTC must promulgate regulations under the APA that require third-party collecting entities to allow for auditing of any access to or disclosure of covered data related to individuals that is processed by the third-party collecting entity.

Third-party collecting entities that process covered data of more than 5,000 individuals must annually register with the FTC. Registration includes paying a $100 fee, providing information about the third-party collecting entity's activities, providing contact information, and creating a

link to a website where individuals may exercise their audit rights under this section. Third-party collecting entities face civil fines for failing to register or provide the notice required by this section.

Finally, the FTC must establish and maintain an online, public, searchable registry of registered third-party collecting entities that allows individuals to look up information on third-party collecting entities, links to and contact information of the third-party collecting entities, and a link and mechanism by which individuals may submit a single request to all registered third-party collecting entities to have all covered data about them deleted within 30 days.

Section 207. Civil Rights and Algorithms.
Covered entities may not collect, process, or transfer covered data in a manner that discriminates on the basis of race, color, religion, national origin, gender, sexual orientation, or disability. This does not prevent covered entities from diversifying an applicant, participant, or customer pool. As applicable, the FTC is required to transmit any information it obtains regarding potential discriminatory uses of covered data to federal executive agencies with authority to initiate proceedings related to such a violation. The FTC must submit annual reports to Congress on the information it sends to these agencies under this section and how that information relates to federal civil rights laws.

This section also requires large data holders that use algorithms to assess their algorithms annually and submit annual algorithmic impact assessments to the FTC. These assessments must describe steps the entity has taken or will take to mitigate potential harms from algorithms, including any harms specifically related to individuals under 17. These assessments must also seek to mitigate algorithmic harms related to advertising for housing, education, employment, healthcare, insurance, or credit, access to or restrictions on places of public accommodation, and any disparate impact on the basis of an individual's race, color, religion, national origin, gender, sexual orientation, or disability status.

Algorithmic evaluations must occur at the design phase of an algorithm, including any training data that is used to develop the algorithm. To the extent possible, entities must also meaningfully consult with independent auditors when conducting their assessments.

The FTC must publish guidance regarding compliance with this section. The FTC is also granted rulemaking authority under the APA to promulgate regulations establishing processes for submitting algorithmic assessments and excluding any algorithms it deems to present minimal risks to individuals.

Finally, the FTC must, in consultation with the Department of Commerce (DOC), conduct a study using its section 6(b) authority to review the algorithmic impact assessments received under this section. Within three years of enactment, the FTC and DOC must submit a report to Congress containing the results of the study. An additional report is required three years after the initial submission as well as whenever the FTC deems it necessary.

Section 208. Data Security and Protection of Covered Data.

Covered entities must implement and maintain data security practices and procedures that protect and secure covered data against unauthorized use and acquisition. In determining whether such protections are reasonable, the FTC must consider the entity's size, complexity, activities related to covered data, the types and amount of covered data the entity engages with, the current state of the art in protecting covered data, and the cost of available tools.

This section provides specific requirements covered entities must meet to assess vulnerabilities, take preventive and corrective action, evaluate their systems, and for the retention and disposal of covered data. Covered entities must provide training to all employees with access to covered data and designate an officer or employee to maintain and implement their data security practices. Entities regulated by and in compliance with the data security requirements in the Gramm-Leach Bliley Act and the Health Insurance Portability and Accountability Act (HIPAA) will be deemed in compliance with this section.

The FTC may promulgate regulations under the APA to establish processes for compliance with this section.

Section 209. General Exceptions.
Notwithstanding other provisions in the Act, covered entities may generally collect, process, or transfer covered data for specific purposes where it is reasonably necessary, proportionate, and limited to the specific purpose. Such exceptions include completing transactions, processing covered data already collected to perform system maintenance, diagnostics, or internal research, addressing security incidents, guarding against illegal activity and fraud, complying with legal obligations, preventing death or serious physical injury, effectuating product recalls, and conducting research in the public interest that meets specific requirements for human subjects research.

The section also provides exemptions for certain small and medium-sized covered entities. Those entities that for the prior three years earned gross annual revenues of $41 million or less, did not collect or process the covered data of 100,000 individuals in a year (except for processing payments and promptly deleting covered data for requested products/services), and did not derive more than half their revenue from transferring covered data are exempt from the data portability requirements. These covered entities may choose to delete, rather than correct, an individual's covered data upon receiving a verified request in section 203 and are fully excluded from the data security requirements in section 208(a) except for data retention obligations as well as and section 301(c)'s requirement to designate a privacy and data security officer.

Section 210. Unified Opt-Out Mechanisms.
The FTC must conduct a study to determine the feasibility of created centralized opt-out mechanisms to ease individuals exercise of their rights to opt-out of covered data transfers in section 204(c), targeted advertising in section 204(d), and the single request to all registered third-party collecting entities to have all covered data about them deleted in section 206(c)(3)(D). If the FTC finds that a centralized mechanism for any or all of the rights would be feasible, it must promulgate APA regulations establishing such mechanisms for covered entities to allow individuals to make these designations.

Title III – Corporate Accountability

Section 301. Executive Responsibility.

The CEOs (or equivalent) and privacy officers at large data holders must annually certify that their company maintains reasonable internal controls and reporting structures for compliance with the Act. This certification must be based on a review conducted by the certifying officers within 90 days of submission.

All covered entities must designate one or more privacy and data security officers who must implement privacy and data security programs and ensure ongoing compliance with the Act. Large data holders must also designate at least one of these officers as the privacy protection officer to report directly to the entity's highest official. That officer is responsible for establishing processes, conducting regular comprehensive audits, developing training and education programs for employees, maintaining records, and serving as the point of contact with enforcement authorities as related to the privacy and security requirements of the Act.

Large data holders must also conduct privacy impact assessments weighing the benefits of its covered data practices against the potential consequences to individual privacy on a biennial basis and have them approved by the privacy protection officer.

In assessing the privacy risks, the large data holder may include reviews of the means by which technologies, including blockchain and distributed ledger technologies and other emerging technologies, are used to secure personal information.

Section 302. Service Providers and Third Parties.

Service providers and third parties each have responsibilities related to covered data. In so far as a covered entity acts as a service provider, it may only collect or process covered data for the purposes directed by the covered entity it got the data from and may not transfer such data to another entity without express affirmative consent of the individual to whom it pertains. Service providers generally have the same responsibilities as other covered entities under the Act, with the exception that, given their non-consumer facing role, they are only required to assist the covered entities they process covered data for from fulfilling requests by individuals to exercise their rights under sections 203 and 204 of the Act.

Third parties cannot process covered data beyond the expectations of a reasonable individual. Such entities are generally subject to the same responsibilities as other covered entities under the Act, except for the rights to consent and object under Section 204 with respect to data collected in their capacity as third parties.

Covered entities must conduct reasonable due diligence in selecting service providers and deciding to transfer covered data to third parties. The FTC must issue guidance to help covered entities comply with this section, including to help alleviate potentially unreasonable compliance burdens on small entities.

Section 303. Technical Compliance Programs.

Within 120 days of enactment, the FTC must promulgate regulations under the APA to establish processes for covered entities to submit technical compliance programs for approval. Such

programs are to be specific to particular technologies, products, services, or methods regarding covered data. Such programs will establish compliance guidelines and be publicly available to individuals whose data is processed by participating entities.

The FTC, state attorneys general, and courts in private litigation must consider a covered entity's history of compliance with any approved program when bringing or hearing an enforcement action against that entity.

Section 304. Commission Approved Compliance Guidelines.
Non-third-party collecting entities that meet the small and medium-sized covered entities criteria in section 209(c) are eligible to participate in FTC approved compliance guidelines for handling covered data. Applications for approval must include how the guidelines will meet or exceed the Act's requirements, the entities or activities the guidelines intend to cover, any covered entities known at the time of submission who want to participate, and a description of how entities will be independently assessed for compliance. Compliance with any approved guidelines must be assessed by an independent organization not associated with any covered entity participant and that organization must be identified in the application for approval.

The FTC has 180 days from receipt to approve a submission. Material changes to the guidelines must also be submitted for approval, which the FTC must respond to in 90 days. The FTC may withdraw approval at any time by notifying the participating covered entities its basis for doing so, beginning a 90-day timeline to cure the deficiency in the guidelines and submit the proposed cure to the FTC for approval.

An entity eligible to participate in approved guidelines will be deemed in compliance with the Act if in compliance with the guidelines, but will remain subject to enforcement if alleged to not be in compliance with the Act.

Section 306. Digital Content Forgeries.
Within a year after enactment and annually after that DOC must publish a report on digital content forgeries. The report will define, describe, and assess digital content forgeries, including the methods to identify and take counter-measures against them.

<u>Title IV – Enforcement, Applicability, and Miscellaneous</u>
Section 401. Enforcement by the Federal Trade Commission.
The FTC must establish a new bureau to carry out its authority under the Act that is comparable to the current Bureaus of Consumer Protection and Competition. That bureau must be fully operational within a year of enactment and include an office of business mentorship to assist covered entities with compliance.

Violations of the Act will be treated as violations of a rule defining an unfair or deceptive act or practice under the FTC Act, meaning it may obtain civil penalties for initial and subsequent violations, among other relief. The FTC may generally enforce the Act akin to any other violation under the FTC Act, but it may not bring an action under section 5(b) of that Act to stop the same conduct that it brings an enforcement against under this Act.

This section establishes a relief fund for victims of entities violating the Act. Any relief the FTC or the Department of Justice obtains enforcing the Act that cannot be provided directly to harmed individuals will be deposited there and be available to the FTC, without fiscal year limitation, to provide relief to individuals harmed by violations under the Act. To the extent money in the fund cannot be used to compensate harmed individuals, the FTC may use funds for the office of business mentorship or to engage in technological research.

Section 402. Enforcement by State Attorneys General.
State Attorneys General and chief consumer protection enforcement officers may bring cases in federal court for injunctive relief, to obtain damages, penalties, restitution, or other compensation, and to obtain reasonable attorney's fees and other litigation costs. The FTC retains the right to intervene upon receiving required notice from state enforcement officers and no state enforcement may occur once the FTC or its deputy has initiated an enforcement action regarding that conduct. States retain all of their existing investigatory and administrative powers and rights to bring enforcement actions arising solely under existing state law.

Section 403. Enforcement by Individuals.
Starting four years after the date the Act takes effect, persons or classes of persons may generally bring a civil action in federal court seeking compensatory damages, injunctive relief, declaratory relief, and reasonable attorney's fees and litigation costs. This right applies to claims alleging violations of specified prohibited uses of covered data, the individual rights in sections 102, 104, 202, 203, 204, protections for children and minors against targeted advertising and the unlawful transfer of covered data in section 205(a)-(b), rights exercisable against registered third-party collecting entities in section 206, civil rights violations under section 207, data security protections under section 208, and rights exercisable against service providers and third parties under section 302.
Individuals must notify the FTC and the attorney general of their state of residence of their intent to bring such an action; those agencies then have 60 days to determine if they wish to bring suit. Demands for monetary payments sent to covered entities prior to the end of this period or after one of the agencies has opted to bring an action will be considered to be made in bad faith. All demand letters must provide a statement and link to the FTC web site established by section 201 of the Act that describes a covered entity's rights under the Act.

The FTC's Bureau of Economics must conduct annual studies beginning five years after enactment regarding the impact of demand letters under the act and report these findings to Congress.

Covered entities may not enforce pre-dispute arbitration agreements or joint action waivers with respect to minors. Pre-dispute joint action waivers for arbitration or administrative proceedings are precluded in all cases. When individuals seek injunctive relief against covered entities or any relief against small and medium sized covered entities meeting the criteria in section 209, those entities have a limited right to cure the alleged deficiency. Covered entities must be provided 45 days written notice identifying specific provisions the entity allegedly violated. When a cure is achieved, demands for injunctive relief may be reasonably dismissed.

Section 404. Relationship to Federal and State Laws.

Existing federal law and the authority of federal agencies is generally not limited except where specified in the Act. Covered entities subject to and in compliance with the related data privacy and security requirements of certain specified federal laws shall be held to be in compliance with the related laws of the Act solely and exclusively to the extent that covered data is subject to the requirements in the other laws. The FTC must issue guidance for implementation of these provisions. [In so far as covered entities are providers of broadband internet access service, satellite carriers, or cable operators] no law or regulation of the FCC shall apply to that entity with respect to the collecting, processing, or transferring covered data under the Act.
State laws covered by the provisions of the Act are preempted, subject to a list of specified state laws to be preserved. That list includes generally applicable consumer protection laws; civil rights laws; employee and student privacy protections; data breach notification laws; contract and tort law; criminal laws regarding fraud, theft, identity theft, unauthorized access to electronic devices, and unauthorized use of personal information; laws on cyberstalking, cyberbullying, nonconsensual pornography, and sexual harassment; unrelated public sector and safety laws; laws addressing public records and criminal justice information; laws addressing bank, financial, and tax records, Social Security numbers, credit cards, credit reporting, credit repair, credit clinics, and check-cashing services; facial recognition, electronic surveillance, wiretapping, and telephone monitoring laws; the Illinois Biometric and Genetic Information Privacy Acts; laws addressing unsolicited email and phone calls; laws addressing medical information, records, and HIV status or testing; the confidentiality of library records; and Section 1798.150 of the California Civil Code, as amended. State common law rights or remedies and statutes creating remedies for civil relief are not preempted or displaced by the Act, but violations of the Act shall not be pleaded as an element of any such cause of action.

Section 405. Severability.
If any provision of the Act is held invalid, the remainder of the Act will remain valid to the furthest extent possible.

Section 406. COPPA.
The Act does not relieve or change existing obligations under COPPA. Within 180 days of enactment, the FTC must amend its existing COPPA rules to reference additional requirements to covered entities under this Act.

Section 407. Authorization of Appropriations.
The Act authorizes the FTC to be appropriated the sums necessary to carry out the Act.

Section 408. Effective Date.
[Except as otherwise provided,] the Act will take effect [180] days after the date of enactment.