CENTER FOR DEMOCRACY & TECHNOLOGY

SEC. 1: DEFINITIONS

(1) PERSONAL INFORMATION. -- The term "personal information" means any information held by a covered entity, regardless of how the information is collected, inferred, created, or obtained, that is linked or reasonably linkable by the covered entity to a specific covered person or consumer device. Data is linked or reasonably linkable to a covered person or consumer device if it can be used on its own or in combination with other information held by or readily accessible to the covered entity to identify a covered person or consumer device.

(A) "Personal information" shall not include information about employees or employment status collected or used by an employer pursuant to an employer-employee relationship.

(2) PERSONAL HEALTH INFORMATION. -- "Personal Health information" includes personal information that:

(A) Relates to the physical or mental health or condition of a covered person or the provision of health care to a covered person;

(B) Is processed for the purpose or in the course of providing health or wellness services; or

(C) Is derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples.

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

(4) CONSUMER DEVICE. -- The term "consumer device" means any electronic device capable of transmitting or receiving information designed to be used by a covered person for non-commercial purposes.

(5) COVERED ENTITY. -- The term "covered entity" means a person or business entity that as part of its activities processes personal information in or affecting interstate commerce. Such term does not include:

(A) the federal Government, the Government of any State, Territory, or Federal District; the Government of any Indian tribe; or any political subdivision, department, agency, component entity, or instrumentality thereof;

(B) any employee, officer, agent, contractor, or organization working on behalf of such an entity described in subparagraph (A), with regard to data processed on behalf of such entity; or

(C) a natural person, unless acting in a non-de-minimis commercial capacity.

(6) COVERED PERSON. -- The term "covered person" is a natural person residing in the United States.

(7) DATA BROKER. -- The term "data broker" means a covered entity, or affiliate or subsidiary of a covered entity, that primarily collects and sells or licenses to any other party with whom the covered entity does not have a direct relationship, the personal information of covered persons for the third party's own purposes.

(8) PROCESSING. -- The term "processing" means any operation or set of operations performed on personal information including collection, creation, organization, structuring, storage, retaining, using, disclosing, sharing, transmitting, selling, licensing, disposing of, or otherwise handling personal information.

(9) SERVICE PROVIDER. -- The term "service provider" means a person or business entity that processes personal information only on behalf of and at the direction of a covered entity.

(10) THIRD PARTY. -- The term "third party" means a covered entity that receives personal information from or transfers personal information to another covered entity and is not a service provider of the other covered entity. The term "third party" includes any affiliate or corporate entity that holds itself out to the public as separate from the other covered entity, such that an individual acting reasonably under the circumstances would not expect it to be related to the other covered entity or to have access to personal information provided to the other covered entity.

SEC. 2: INDIVIDUAL RIGHTS WITH RESPECT TO PERSONAL INFORMATION

(1) RIGHT TO ACCESS AND CORRECTION. --
- (A) Upon request, a covered entity shall provide to a covered person reasonable access to personal information the covered entity retains and the names of third parties to whom personal information is sold or licensed.
- (B) A covered person shall have, upon request, the right to dispute the accuracy or completeness of:
  - (i) Personal health information; and
  - (ii) Personal information processed for the purpose of:
    - (a) Making determinations about a covered person's educational opportunities; or

(b) Determining eligibility for credit, insurance, housing, or employment by a covered entity.

(C) A covered entity shall make available a reasonably accessible, conspicuous, and easy-to-use means for a covered person to exercise their right to access and correction. If a covered entity has a direct relationship with a covered person, it shall offer such means at least via the same medium(s) that a covered person routinely uses to interact with the covered entity.

(2) RIGHT TO DATA PORTABILITY. --

(A) Where technically feasible, a covered entity shall make available a reasonable means for a covered person to transmit or transfer personal information about the covered person retained by the covered entity to another covered entity in a structured, standardized, and machine-readable interoperable format, or otherwise download personal information for the covered person's own use.

(B) NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY CONVENING ON PORTABILITY STANDARDS. -- Not later than 1 year after the date of enactment of this Act, the Department of Commerce shall establish a working group at the National Institute of Standards and Technology to promote common frameworks and cooperation to foster the interoperable portability of personal information. The group shall prioritize addressing reasonable limitations on portability. Such group should include equal numbers of industry representatives, public interest representatives, and technical experts.

(3) RIGHT TO DELETION. --

(A) Upon request, a covered entity that retains personal information shall make available a reasonable means for a covered person to delete personal information. Covered entities may not make it unreasonably difficult for an individual to request such deletion.

(4) EXCEPTIONS. --

(A) A covered entity may decline to provide such access under subsection (1) and (2) if:

(i) A covered person cannot reasonably document or confirm his or her identity to the covered entity;

(ii) Such access is limited by law, legally recognized privilege, or other legal obligation;

(iii) A covered entity makes an individualized determination that fulfilling this request would create a legitimate risk to the privacy,

security, safety, free expression or other rights of an individual other than the covered person or the covered entity.

(B) A covered entity shall not be required to correct or delete personal information under subsections (1) and (3) respectively if:

(i) A covered person cannot reasonably document or confirm his or her identity to the covered entity;

(ii) Such correction or deletion request is limited by law, legally recognized privilege, or other legal obligation;

(iii) A covered entity makes an individualized determination that fulfilling such request would create a legitimate risk to the privacy, security, safety, free expression or other rights of an individual other than the covered person or the covered entity;

(iv) Retention of the information is necessary to:

(a) Complete the transaction for which the personal information was collected, provide a product or service affirmatively requested by a covered person, or otherwise necessary to perform a contract, including billing, financial reporting, and accounting;

(b) Detect or prevent security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for such activity;

(c) Identify and repair errors that impair existing intended functionality, or to ensure a product or service functions as intended; or

(v) Personal information is used in public or peer-reviewed scientific, medical, historical, or statistical research in the public interest that adheres to commonly accepted ethical standards or laws, with informed consent. In order to preempt a deletion request, the research must already be in progress at the time when deletion is requested.

(5) DENIAL OF REQUEST TO EXERCISE AN INDIVIDUAL RIGHT. -- If a covered entity denies a request by a covered person to exercise that person's right to access, correction, or deletion, the covered entity shall inform the covered person without undue delay, but no longer than 30 days, of the reasons for not fulfilling such request and any rights the covered individual may have to appeal the decision of the covered entity.

(6) FEES TO EXERCISE AN INDIVIDUAL RIGHT. -- A covered entity may not charge a fee to a covered person for exercising a right under Section 2 of this Act, unless such request is unfounded or excessive in which case a covered entity may

charge a reasonable fee for the administrative costs of complying with the request.

(7) RULE OF CONSTRUCTION. -- Nothing in this section shall be interpreted to require a covered entity to take an action that would convert information that is not personal information into personal information.

SEC. 3: OBLIGATIONS OF COVERED ENTITIES WITH RESPECT TO PERSONAL INFORMATION

(1) REDRESS. --

(A) A covered entity shall provide a reasonably accessible, conspicuous, and easy-to-use means for a covered person to make a complaint or inquiry regarding a covered entity's policies and procedures required by this Act. A covered entity shall be required to respond to a covered person's complaint or inquiry submitted via the established process without undue delay, but no longer than 30 days, to provide a response explaining what the outcome of that complaint or inquiry is, and to provide information about how to contact state Attorneys General and the Commission.

(2) SECURITY. --

(A) A covered entity shall establish and implement reasonable policies, practices, and procedures regarding information security practices for the protection of personal information taking into consideration --

(i) the nature, scope, and complexity of the activities engaged in by such covered entity;

(ii) the sensitivity of any personal information at issue;

(iii) the current state of the art in administrative, technical, and physical safeguards for protecting such information; and

(iv) the cost of implementing such administrative, technical, and physical safeguards.

(B) REQUIREMENTS. -- The policies, practices, and procedures required in subpart (A) of this section must include the following:

(i) A written security policy with respect to the processing of such personal information.

(ii) The identification of an officer or other individual as the point of contact with responsibility for the management of information security.

(iii) A process for identifying and assessing reasonably foreseeable security vulnerabilities in the system or systems maintained by such covered entity that contains such personal information, which shall

include regular monitoring for vulnerabilities and a breach of security of such system or systems.

(iv) A process for taking action designed to mitigate against vulnerabilities identified in the process required by subparagraph (iii), which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software, or for regularly testing or otherwise monitoring the effectiveness of the existing safeguards.

(v) A process for determining if personal information is no longer needed and disposing of personal information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such personal information permanently unreadable or indecipherable.

(vi) A process for overseeing persons who have access to personal information, including through network-connected devices.

(vii) A process for employee training and supervision for implementation of the policies, practices, and procedures required by this subsection.

(viii) A written plan or protocol for internal and public response in the event of a breach of security.

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

(3) LIMITS ON THIRD PARTIES AND SERVICE PROVIDERS. --

(A) THIRD PARTIES. -- A covered entity shall not sell or license personal information it holds to a third party unless that third party is contractually bound to meet the same privacy and security obligations as the covered entity under this Act and any additional obligations to which the covered entity has publicly committed. A covered entity shall exercise reasonable oversight and take reasonable actions to ensure compliance with such contractual provisions.

(i) A covered entity that sells or licenses access to personal information to third parties shall be obligated to limit access to and seek certification of destruction of personal information if it obtains actual knowledge that another covered entity has materially violated the requirements of this Act. Such violations must be disclosed in the disclosures required in subsection (4), subpart (B).

(B) SERVICE PROVIDERS. -- A covered entity may not share or disclose personal information to a service provider unless the covered entity enters into a contractual agreement with the service provider that prohibits the

service provider from processing the personal information for any purpose other than the purposes for which the covered entity shared such personal information with the service provider. A service provider may not sell or license personal information provided by a covered entity. A covered entity shall exercise reasonable oversight and take reasonable actions to ensure compliance with such contractual provisions.

(4) DISCLOSURES. --

(A) INFORMATION TO COVERED PERSONS. --

(i) A covered entity shall make available, in reasonably clear, easily understandable, timely and visually prominent machine-readable format, information about the following:

(a) The types of personal information that the covered entity collects and the names of the third parties, including affiliates to whom the covered entity sells or licenses personal information;

(b) The general purposes for which the covered entity collects and uses personal information, including disclosure as to whether and how the covered entity customizes products or services or changes the prices of products or services based, in whole or in part, on a covered person's personal information;

(c) A description of how the covered entity provides individual rights as enumerated in this Act;

(d) A description of the controls and mechanisms, including methods of de-identifying personal information, the covered entity uses or makes available to covered persons to limit the collection, use, disclosure, or other processing of personal information;

(e) A description of the process by which the covered entity will notify individuals of material changes to its data policies; and

(f) The effective date of the disclosure.

(B) PERIODIC PRIVACY PROTECTION DISCLOSURES. --

(i) A covered entity shall be required to publish a disclosure at least annually, and prior to any material change, that includes:

(a) a list of purposes for which the covered entity processes personal information, including disclosure as to whether and how the covered entity customizes products or services or changes the prices of products or services based, in whole or in part, on a covered person's personal information;

(b) an assessment of the covered entity's approach to mitigating privacy risks, including:
  i) the designation of an employee charged with monitoring the covered entity's privacy practices covered by this Act;
  ii) the processes by which employees of a covered entity are educated and trained on data processing obligations;
  iii) the processes and procedures by which a covered entity audits, monitors, and addresses privacy risks;
  iv) a data retention policy that details how long personal information is retained in days, months, or years, or a disclosure that such information is retained indefinitely or permanently; and
  v) a summary of the security policies, practices, and procedures adopted pursuant to subsection (2).

(c) any material changes to the covered entity's policies or practices related to data processing and privacy since prior disclosure; and

(d) any security incidents or violations of the company's security about which the covered entity was required by law to provide notice to any individual located within the United States and privacy programs, including violations by third parties, and a general description of the covered entity's response.

(ii) A corporate officer of the covered entity must certify the information contained in the annual reports. A corporate officer includes one of the named executive officers under Item 402 of Regulation S-K under the Securities Act of 1933, the chief privacy officer (or equivalent thereof), or the chief information security officers (or equivalent thereof) of the covered entity.

(iii) The corporate officer must certify that:

(a) They have reviewed the disclosures;

(b) Based on their knowledge, the disclosures do not contain any untrue statement of fact or omission of a material fact necessary in order to make the statements not misleading with respect to the policies or practices covered in the report;

(c) They are responsible for establishing, maintaining and regularly evaluating the effectiveness of the covered entity's internal information security and privacy controls; and

(d) They have included information in the disclosure sufficient to understand any significant changes in the covered entity's internal information security and privacy controls.

(iv) The disclosures required by this subsection may be used to supplement the information provided to covered persons pursuant to the previous subsection, but shall not be sufficient to satisfy that subsection.

(v) EXCEPTION. -- This section does not apply to covered entities that process the personal information of 50,000 or fewer covered persons a year.

(C) DATA BROKERS. --

(i) The Commission shall facilitate or create an accessible online mechanism for individuals to identify data brokers. A covered entity which is a data broker shall be required to register with the Commission and provide information into their sources of personal information and how individuals may exercise their individual rights with respect to data brokers.

SEC. 4: DECEPTIVE DATA PROCESSING PRACTICES

(1) It shall be an unlawful for covered entities to make material misrepresentations with respect to the processing of personal information.

(A) MATERIALITY. -- A representation is material if it is likely to affect a reasonable person's conduct or decision with regard to a product or service. Express statements are presumptively material.

(2) A misrepresentation with respect to the processing of personal information includes but is not limited to:

(A) Notices, settings, interfaces, or other representations likely to mislead consumers as to how their personal information is being collected, retained, used, repurposed, shared, sold, or otherwise processed;

(B) The use of false pretenses, fraudulent statements, or other misrepresentations to induce the disclosure of personal information; and

(C) Misleading omission of material information about the processing of personal information.

(i) A misleading omission occurs when qualifying information necessary to prevent a practice, claim, representation, or reasonable expectation or belief from being misleading is not disclosed.

(3) When evaluating whether a representation is misleading, the Commission shall consider the totality of the covered entity's relevant representations from the

perspective of a reasonable consumer under the circumstances. When representations are targeted to a specific audience, the Commission shall evaluate the representations from the perspective of a reasonable member of that group.

(4) RULE OF CONSTRUCTION. -- Nothing in this section shall be construed to limit the Commission's authority to enforce against unfair and deceptive practices or to limit the authority of any federal agency or state to enforce any civil rights law, regulation, or requirement.

SEC. 5: UNFAIR DATA PROCESSING PRACTICES

(1) It shall be unlawful for a covered entity to engage in the following data processing practices when those practices are not required to provide or add to the functionality of the product, service, or specific feature that a covered person has requested.

(A) EXCEPTIONS. -- Not later than 2 years after the date of enactment of this Act, the Commission shall promulgate regulations under section 553 of title 5, United States Code, to implement procedures by which covered entities may petition the Commission for an exception to these prohibitions.

(2) BIOMETRIC INFORMATION TRACKING. -- The processing of biometric information to identify a covered person, or to verify a covered person's identity.

(A) BIOMETRIC INFORMATION. -- “Biometric information” means any personal information generated from the measurement or specific technological processing of an individual’s unique biological, physical, or physiological characteristics. Biometric information includes measurements of, but is not limited to, fingerprints, voice prints, iris scans, facial characteristics, identifying DNA (deoxyribonucleic acid) information, or other unique biological characteristics, including any mathematical code or algorithmic model generated or extracted from measurements of these characteristics. Biometric information does not include writing samples, written signatures, photographs, demographic data or physical descriptions such as height, weight, hair color, or eye color.

(3) PRECISE GEOSPATIAL INFORMATION TRACKING. -- The processing of precise geospatial information generated by a consumer device.

(A) PRECISE GEOSPATIAL INFORMATION. -- “Precise Geospatial Information” means information derived from a consumer device through any technology that is capable of determining with specificity the spatial

location of a person or device, such as latitude-longitude coordinates with an accuracy level of below 1,750 feet provided by GPS, or triangulated location provided by network radios or beacons such as Wi-Fi, or other technologies and inferences, provided however that it does not include information that is or will be altered prior to subsequent processing such that it cannot be determined with specificity the physical location of an individual or device.

(4) PROBABILISTIC CROSS-DEVICE TRACKING. -- The use of probabilistic methods, such as algorithms and usage patterns, to attribute a consumer device to a specific covered person.

(A) Information derived from probabilistic cross-device tracking for security, fraud detection, or other permissible purposes enumerated in subsection (9) shall not be used for any other purpose not enumerated in subsection (9) or otherwise required or permitted by law.

(5) TRACKING OF CHILDREN UNDER THE AGE OF 13. -- The disclosure of personal information collected from a child under 13 to third parties, and the use of such personal information for targeted advertising purposes, where a covered entity has actual knowledge that it is collecting personal information from a child or such information is collected from services, products, or specific features directed to children under the age of 13.

(6) CONTENT OF AND PARTIES TO COMMUNICATIONS. -- The licensing or sale to third parties of personal information relating to the contents of communications or the parties to communications.

(A) CONTENTS OF COMMUNICATIONS. -- “Content of communications” includes any part of the substance, purport, or meaning of a communication. Examples of contents include the text of an email or instant message; the video, webpage, application, or other information viewed or requested by a covered person; and the contents of a voice command from a covered person to a consumer device.

(B) PARTIES TO COMMUNICATIONS. -- “Parties to communications” means records or logs revealing the sender and recipient or destination of an electronic communication or telephone call.

(i) EXCEPTION.-- This section does not include subscriber information, which is contact information provided by a covered person to the covered entity to establish or maintain an account or communication channel.

(7) AUDIO AND VISUAL RECORDING. -- The retention, use, or disclosure to a third party of personal information or communications collected through the microphone or camera of a consumer device.

(8) HEALTH INFORMATION. -- The processing of personal health information.

(D) The Commission may by regulation promulgated under section 553 of title 5, United States Code, further define "health information," taking into consideration the reasonable expectations of an covered person and the adverse effect that a covered person may experience if such information is processed.

(9) EXCEPTIONS. -- Nothing in this section shall limit covered entities from engaging in these practices when necessary and solely for purposes of

(E) detecting and preventing security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity; or prosecuting those responsible for that activity;

(F) preventing imminent danger to the personal safety of an individual or group of individuals;

(G) identifying or repairing errors that impair existing intended functionality;

(H) engaging in public or peer reviewed scientific, medical, historical, or statistical research in the public interest that adheres to commonly accepted ethical standards or laws, with informed consent;

(I) complying with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process; and

(J) any other exception specified by the Commission pursuant to Section 5(1)(A) of this Act.

(11) RULE OF CONSTRUCTION. -- Nothing in this section shall be construed to limit the Commission's authority to enforce against unfair and deceptive practices or to limit the authority of any federal agency or state to enforce any civil rights law, regulation, or requirement.

SEC. 6: UNFAIR TARGETED ADVERTISING PRACTICES

FEDERAL TRADE COMMISSION RULEMAKING ON UNFAIR TARGETED ADVERTISING PRACTICES. --

(1) The Commission shall promulgate rules under section 553 of title 5, United States Code, to define and prohibit unfair targeted advertising practices, including but

not limited to practices that are likely to result in unlawful discrimination. In promulgating these rules, the Commission shall consider:

(A) Established public policy, such as civil rights laws, that can guide the Commission's determinations of what constitutes an unfair targeted advertising practice;
(B) The tools made available to, developed by, or used by advertisers to target advertisements online;
(C) The actual targeted advertising practices engaged in by advertisers and other covered entities;
(D) The effects of algorithms on the audiences reached by targeted advertisements;
(E) Methodologies for measuring discriminatory effects of targeted advertising;
(F) any relevant results of studies measuring discrimination, including discriminatory effect, in targeted advertising; and
(G) The role of all actors in the digital advertising ecosystem, including advertisers; websites and applications that carry targeted advertisements, including but not limited to social media services; advertising networks; and data brokers.

(2) RULE OF CONSTRUCTION. -- Nothing in this section shall be construed to limit the Federal Trade Commission's authority to enforce against unfair and deceptive practices or to limit the authority of any federal agency or state to enforce any civil rights law, regulation, or requirement.

SEC. 7: ENFORCEMENT

(1) ENFORCEMENT BY THE FEDERAL TRADE COMMISSION. --
(A) UNFAIR OR DECEPTIVE ACTS OR PRACTICES. -- A violation of this Act shall be treated as an unfair and deceptive act or practice in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act.
(B) POWERS OF COMMISSION. -- The Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as through 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, except where granted rulemaking authority under section 553 of title 5, United States Code herein.
(C) COMMON CARRIERS AND NONPROFIT ORGANIZATIONS. -- Notwithstanding Sections 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall also enforce this Act with respect to:

(i) Common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); and
(ii) Organizations not organized to carry on business for their own profit or that of their members.

(2) ENFORCEMENT BY STATE ATTORNEYS GENERAL. --
(A) CIVIL ACTION. -- In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is adversely affected by any person who violates this Act, the attorney general of the State, as parens patriae, may bring a civil action on behalf of the residents of the State in an appropriate district court of the United States --
(i) to enjoin further violation of this Act by the defendant;
(ii) to compel compliance with this Act; or
(iii) for violations of subsections of this Act to obtain civil penalties in the amount determined under subsection (3).
(B) RIGHTS OF FEDERAL TRADE COMMISION. -- The attorney general of a State shall notify the Federal Trade Commission in writing of any civil action under subsection (2), subpart (A), prior to initiating such civil action. Upon receiving notice with respect to a civil action, the Federal Trade Commission may --
(i) intervene in such action; and
(ii) upon intervening --
(a) be heard on all matters arising in such civil action; and
(b) file petitions for appeal of a decision in such action.
(C) PREEMPTIVE ACTION BY FEDERAL TRADE COMMISSION. -- If the Federal Trade Commission institutes a civil action for violation of this Act or a regulation promulgated under this Act, no attorney general of a State may bring a civil action against any defendant named in the complaint of the Commission for violation of this Act or a regulation promulgated under this Act that is alleged in such complaint.

(3) CIVIL PENALTIES. -- The Commission or State Attorneys General may commence a civil action to recover a civil penalty in a district court of the United States against any covered entity or service provider that violates this Act.
(A) IN GENERAL. -- A violation of this Act shall be subject to a civil penalty in an amount that is not greater than $16,500 per covered person for whom the covered entity processed personal information in violation of this Act.
(B) DETERMINATION. -- Penalties shall be calculated based on the number of individuals whose personal information was affected by a violation;

however, penalties shall be proportionate to the severity of the violation as well as to the size and revenues of the covered entity.

SEC. 8: ADDITIONAL PERSONNEL IN THE BUREAU OF CONSUMER PROTECTION

(1) IN GENERAL. -- Notwithstanding any other provision of law, the Director of the Bureau of Consumer Protection of the Commission shall appoint--

(A) 100 additional personnel in the Division of Privacy and Identity Protection of the Bureau of Consumer Protection, of which no fewer than 25 personnel will be added to the Office of Technology Research and Investigation; and no fewer than 25 additional personnel in the Division of Enforcement of the Bureau of Consumer Protection.

(2) AUTHORIZATION OF APPROPRIATIONS. -- There is to be 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. 9: EFFECTIVE DATE

(1) The provisions of this Act that apply to covered entities shall apply beginning on or after the date that is 2 years from the date of enactment of this Act.

SEC. 10: RELATION TO OTHER PRIVACY & SECURITY LAWS

(1) SEVERABILITY. -- If any provision of this Act, or the application thereof to any covered entity or covered person, is held unconstitutional or otherwise invalid, the validity of the remainder of the Act and the application of such provision to other covered entities and covered persons shall not be affected thereby.

(2) PREEMPTION. -- This Act supersedes any provision of a statute, regulation, requirement, or rule of a State or political subdivision of a State, with respect to those entities covered by this Act, that requires covered entities to implement requirements with respect to the processing of personal information addressed in this Act.

(A) EXCEPTIONS.-- This law does not preempt laws that address the collection, use, or disclosure of health information covered by the Health Insurance Portability and Accountability Act or financial information covered by Gramm-Leach-Bliley Act.

(B) RULE OF CONSTRUCTION. -- This Act shall not be construed to preempt the applicability of the following laws, rules, regulations or requirements:
- (i) Consumer protection laws of general applicability unrelated to privacy or security;
- (ii) Civil rights laws;
- (iii) Laws that govern the privacy rights or other protections of employees and employee information;
- (iv) Laws that address notification requirements in the event of a data breach;
- (v) Trespass, contract, or tort law;
- (vi) Criminal laws governing fraud, unauthorized access to information, malicious behavior, and similar provisions, and laws of criminal procedure; and
- (vii) Public safety or sector specific laws unrelated to privacy or security.

(3) GOVERNMENT ACCOUNTABILITY OFFICE STUDY AND REPORT. --

(A) Not later than 3 years after the date of effective date of this Act, and every 3 years thereafter, the Comptroller General of the United States shall submit to the President and Congress a report that surveys federal privacy and security laws, including any legislative or executive recommendations, that:
- (i) Identifies inconsistencies between this Act and those enumerated laws in subsection (4);
- (ii) Provides recommendations for how to amend federal privacy and security laws in light of changing technological and economic trends; and
- (iii) Details the privacy and security enforcement activities of the Commission and other federal agencies.

(4) EFFECT ON OTHER FEDERAL LAWS. --

(A) Nothing in this Act may be construed to modify, limit, or supersede the operation of privacy or security provisions in the following Federal laws:
- (i) Section 552a of title 5, United States Code (commonly known as the Privacy Act of 1974);
- (ii) The Right to Financial Privacy Act of 1978 (12 U.S.C. § 3401 et seq.);
- (iii) The Fair Credit Reporting Act (15 U.S.C. § 1681 et seq.);
- (iv) The Fair Debt Collection Practices Act (15 U.S.C. § 1692 et seq.);
- (v) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 et seq.);
- (vi) Chapters 119, 123, 206, and 121 of Title 18, United States Code;
- (vii) Section 2710 of Title 18, United States Code;

(viii) Sections 444 and 445 of the General Education Provisions Act (20 U.S.C. §§ 1232g, 1232h), commonly known as the "Family Educational Rights and Privacy Act of 1974" and the "Protection of Pupil Rights Amendment," respectively;
(ix) Sections 5701 and 7332 of Title 38, United States Code;
(x) The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d-2 et seq.);
(xi) The Privacy Protection Act of 1980 (42 U.S.C. § 2000aa et seq.);
(xii) The provisions of part C of title XI of the Social Security Act, section 264 of the Health Insurance Portability and Accountability Act of 1996, and subtitle D of title IV of the Health Information Technology for Economic and Clinical Health Act, and regulations under such provisions;
(xiii) The E-Government Act of 2002 (44 U.S.C. § 101 et seq.);
(xiv) The Paperwork Reduction Act of 1995 (44 U.S.C. § 3501 et seq.);
(xv) Federal Information Security Management Act of 2002 (44 U.S.C. § 3541 et seq.);
(xvi) The Communications Assistance for Law Enforcement Act (47 U.S.C. § 1001 et seq.);
(xvii) The Currency and Foreign Transactions Reporting Act of 1970, as amended (commonly known as the Bank Secrecy Act) (12 U.S.C. §§ 1829b and 1951-1959, 31 U.S.C. §§ 5311-5314 and 5316-5332), including the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, Title III of P.L. 107-56, as amended;
(xviii) Executive Order 12333, as amended, "United States Intelligence Activities, July 30, 2008," and any successor orders;
(xix) National Security Act of 1947 (50 U.S.C. § 3001 et seq.);
(xx) Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. § 1801 et seq.);
(xxi) The Civil Rights Act of 1964 (Pub.L. 88–352, 78 Stat. 241);
(xxii) The Americans with Disabilities Act (42 U.S.C. § 12101 et seq.);
(xxiii) The Fair Housing Act (42 U.S.C. § 3601 et seq.);
(xxiv) The Dodd-Frank Wall Street Reform and Consumer Protection Act (Pub. L. 111–203, 124 Stat. 1376–2223);
(xxv) The Equal Credit Opportunity Act (15 U.S.C. § 1691 et seq.);
(xxvi) The Age Discrimination in Employment Act (29 U.S.C. § 621 et seq.); and
(xxvii) The Genetic Information Nondiscrimination Act (Pub. L. 110–233, 122 Stat. 881).

(B) CHILDREN'S PRIVACY. -- Nothing in this Act may be construed to modify, limit, or supersede the operation of the Children's Online Privacy Protection Act of 1998 (15 U.S.C. § 6501 et seq.), except for Section 5, subsection (5) of this Act.

(C) COMMUNICATIONS PRIVACY. -- If a covered entity is subject to a privacy or security requirement or provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.), including but not limited to section 201, 222, or 631, or any regulations promulgated under that Act, such requirement, provision, or regulation shall have no force or effect, unless such requirement, provision, or regulation pertains to emergency services.