A BILL

To preserve America’s innovation engine; protect individuals’ interests in the fair, ethical, transparent, and responsible processing of their personal data; mitigate risks of adverse impacts from the processing of personal data; and promote the benefits of the 21st century information age through an agile regulatory framework which contemplates that:

(1) the sensitivity and value of data are increasingly difficult to understand and predict
and (2) the majority of data about individuals is collected passively and observed through machine-to-machine transactions or computationally inferred about them.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

Article I. SHORT TITLE AND TABLE OF CONTENTS

Section 1.01 SHORT TITLE AND TABLE OF CONTENTS

(a) SHORT TITLE.—This Act may be cited as the “Fair Accountable Innovative Responsible and Open Processing Enabling New Uses that are Secure and Ethical Act” or the “FAIR and OPEN USE Act.”

(b) TABLE OF CONTENTS.—

(i) Article I. Short Title and Table of Contents

1) Section 1.01 Short Title and Table of Contents
2) Section 102 Findings and Purpose
3) Section 1.03 Definitions

(ii) Article II. Fair And Trustworthy Use of Personal Data

1) Section 2.01 Lawful, Responsible and Fair Processing For A Legitimate Use
2) Section 2.02 Restrictions on Processing
3) Section 2.03 Bad Faith Claims Of Legitimate Use
4) Section 2.04 Duty of Care

(iii) Article III. Responsibilities of Accountable Covered Entities

1) Section 3.01 Open and Transparent Processing
2) Section 3.02 Data Quality, Accuracy and Retention
3) Section 3.03 Access
4) Section 3.04 Data Portability
5) Section 3.05 Redress
6) Section 3.06 Information Security
7) Section 3.07 Rule of Construction

(iv) Article IV. Accountable Processing

1) Section 4.01 Implementing an Accountable Processing Management and Governance Program

2) Section 4.02 Responsible Data Governance

3) Section 4.03 Ethical, Trustworthy and Preventative Design

4) Section 4.04 Responsible Stewardship Of Trustworthy and Accountable Automated Processing

5) Section 4.05 Accountability For Processing By Service Providers And Third Parties

6) Section 4.06 Employee Accountability

7) Section 4.07 Oversight: Demonstrating Trustworthy Compliance and Ongoing Commitment To Responsible Processing

(v) Article V. Risk Management

1) Section 5.01 Risk Management Program

2) Section 5.02 Risk Assessment

3) Section 5.03 Categorization of Processing Risk

4) Section 5.04 Processing Impact Assessments

5) Section 5.05 Enhanced Processing Impact Assessment To Assess Implications Of Automated Processing

6) Section 5.06 Bath Faith

7) Section 5.07 Rulemaking

(vi) Article VI. Individual Engagement

1) Section 6.01 Access

2) Section 6.02 Engagement and Appropriate Control

3) Section 6.03 Personal Data Shared With Third Parties

4) Section 6.04 Redress

(vii) Article VII. Enforcement, Oversight and Rulemaking

1) Section 7.01 Implementing Regulations to Promote Accountability

2) Section 7.02 Civil Enforcement By Agency

3) Section 7.03 Compliance Examinations and Inspections
Draft June 16, 2019

4) Section 7.04 Enforcement By State Attorneys General
5) Section 7.05 Safe Harbor

(viii) Article VIII. Education and Outreach
1) Section 8.01 Consumer Education
2) Section 8.02 Education Initiatives For Older Americans
3) Section 8.03 Collecting and Tracking Complaints
4) Section 8.04 Guidance for Covered Entities

(ix) Article IX. Savings Clause and Effective Date

(x) Article X. Placeholder for Effect on Other Laws

Section 1.02 FINDINGS AND PURPOSE

(a) The information ecosystem in the United States is the world’s most innovative. It has not just driven economic growth; it has facilitated positive changes in all sectors.

(b) Data, including personal data about an individual, constitutes the lifeblood of the information age by forming the basic building blocks of all business, government and social processes. Data provides unprecedented opportunities to drive information-based innovation in healthcare, public safety, education, transportation and almost every human endeavor.

(c) Sensors, artificial intelligence, machine learning and advanced analytics are now mainstays of our digital environment. These groundbreaking technologies extract value from data beyond that of the initial use and create new knowledge in ways once thought impossible.

(d) These technologies, however, can have an inappropriate or adverse impact on individuals and cause negative impact on societal goals and values. The rapid growth of innovative, data-driven technologies have increased angst in individuals and a sense that they may be harmed by the misuse of information from them or about them. This concern is justified. Uses of personal data create risk to both individuals and society unless effective governance is in place and organizations are accountable for their actions.
Increasingly personal data is not collected directly from the individual but, rather, from a diverse range of sources without the individual’s awareness of its origination and subsequent uses. In a world of artificial intelligence the systems themselves make decisions that impact people. The systems make decisions, based on human set objectives, but the direct human accountability has been lost.

The benefits of the information age belong to everyone. Individuals justifiably expect that organizations will process their data in a manner that creates benefits for the individual, or if not for the individual, for a broader community of people. Data should not just serve the interests of the organization that collected the data.

Data use should support the value of human dignity – that an individual has an innate right to be valued, respected and to receive ethical treatment. An individual should not be subjected to secret processing of data that pertains to or will have an impact on the individual.

Personal data must be kept secure. Too many organizations fail to protect sensitive personal data, undermining trust and confidence in the digital economy.

The United States needs a new national framework to address the processing of personal data that maintains the ability to think and learn from data while also protecting individuals in a highly observational digital ecosystem.

Many legal frameworks today are structured as a list of prohibitions. This approach may lead to legal certainty by creating white lists and black lists of activities. Since data use is dynamic, however, lists of prohibited activities leads to legal structures that are often dated when they go into effect. Moreover, such an approach may be unnecessarily restrictive while providing limited benefit or safeguards to individuals.

We live in a complex, data-driven world with diverse business models and infinite possibilities for innovation. This reality requires an equally complex, nuanced, innovative and agile policy and regulatory response. We cannot pretend that difficult digital challenges that evolve in real time can be solved with a short, simple legislative solution. We must embrace complexity, not run from it.
l) A future-oriented legal framework must take into account the rapid evolution of
data, technology and business processes. It must preserve the ability of all entities
to use data to pursue knowledge and should focus on flexible principles not rigid
prohibitions. It must be scalable to organizations of all sizes and complexities and
be equally applicable to every sector of our global, digital economy.

m) The use of data must be:

(i) Legal, the data used in a specific manner is specifically authorized or not
   prohibited;

(ii) Fair, data is used in a manner that maximizes stakeholder interests and mitigates
    risks to the extent possible; and

(iii) Just, inappropriate discrimination should be avoided even if the outcomes are
     maximized for many stakeholders.

n) In today’s data-driven economy, organizations must be responsible stewards of
   personal data and be accountable for their actions. Accountability requires
   organizations to be both responsible and answerable for any misuse of
   information.

(o) Accountability requires organizations to have policies that link to the law,
   mechanisms to put them in place, security safeguards, internal oversight and
   documentation for basic processes.

(p) Data should be collected, created, used and disclosed within the context of the
    relationship between the individual to whom the data pertains and the
    organization, based on the reasonable expectations of individuals as a group. It
    should be processed only for legitimate uses that have been disclosed or are in the
    context of those uses, and only the data necessary for those uses should be
    collected, created, used or disclosed.

(q) Individuals expect to know about data uses that may have a significant impact on
    them and to be able to control those uses through an appropriate level of consent.

(r) Individuals should always have the ability to question the use of data that impacts
    them and to challenge situations where use may create adverse consequences or
    have a negative impact.
Individuals should be able to access data they provided to an organization, to understand what observational data is created by the organization that pertains to them, and to be told what types of data are inferred by analytical algorithms.

A national framework based on risk assessment and accountability backed by robust oversight and enforcement will increase the confidence of individuals and organizations that their data will be protected wherever and by whomever it is stored or processed.
Section 1.03 DEFINITIONS

(a) ADVERSE PROCESSING IMPACT.—The term “adverse processing impact” means detrimental, deleterious, disadvantageous or harmful consequences to an individual arising from the processing of that individual’s personal data or to society from the processing of personal data including—

(i) direct or indirect financial loss or economic harm;
(ii) physical harm;
(iii) psychological harm, including anxiety, embarrassment, fear and other demonstrable mental trauma;
(iv) significant inconvenience or expenditure of time;
(v) negative outcomes or decisions with respect to an individual’s eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;
(vi) demonstrable stigmatization or reputational harm;
(vii) disruption and intrusion from unwanted commercial communications or contacts;
(viii) price discrimination;
(ix) effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relate, that are nevertheless reasonably foreseeable, contemplated by, or expected by the covered entity assessing adverse processing impact, that significantly—

1) alters that individual’s experiences;
2) limits that individual’s choices;
3) influences that individual’s responses; or
4) predetermines results or outcomes for the individual;
(x) other demonstrable detrimental or negative consequences that affect an individual’s private life, including private family matters, actions and communications within an individual’s home or similar physical, online, or
digital location, where an individual has a reasonable expectation that personal data will not be collected, observed or used; and

(xii) with respect to detrimental, deleterious, disadvantageous or harmful consequences to society arising from processing personal data, such other demonstrable consequences that may negatively impact a community or the public, taking into account factors such as national security, consumer confidence, the effective and efficient operation of government, effect on the public welfare, or ongoing or disproportionate allocation of risk on a particular population or community.

(b) **AUTOMATED PROCESSING**.—The term “automated processing” means processing through a machine-based system that can, for a given set of objectives, make predictions, recommendations or decisions influencing real or virtual environments. Automated processing—

(i) includes techniques such as machine learning, artificial intelligence, deep learning, analytics or the use of algorithms—

a) performed by or in computer software, physical hardware or other digital context; and

b) designed to learn to approximate a cognitive task, solve complex problems, make predictions, adapt to changing circumstances or improve performance when exposed to new or existing data sets;

(ii) may operate with varying levels of autonomy or human intervention;

(iii) may, but does not necessarily, involve human-like sensing, perception, cognition, reasoning, planning, learning, communication, decision-making or physical action; and

(iv) includes intelligent in-home assistants, computer vision systems, automated vehicles, unmanned aerial systems, voicemail transcription, advanced game-playing software, facial recognition systems, statistical models used to predict the probability of a particular future outcome or other processing activity that involves automation of analysis and decision making.

(c) **AGENCY**.—TBD but for the purpose of this draft the term “agency” should be read to mean a federal department or agency within the executive branch
designated by Congress to provide oversight, enforcement, rulemaking, guidance and other functions as set forth in this Act. It should be assumed that such agency shall have the requisite authority, jurisdiction and resources to provide such functions.

(d) **Covered Entity.**—The term “covered entity” means a legal person engaged in interstate commerce that processes personal data.

(i) Such term includes not-for-profit corporations, associations or other entities that operate across states and meet the definition of non-profit set forth in section 501 of title 26, United States Code.

(ii) Such term does not include—

1) the Federal Government or any instrumentality of the Federal Government, nor the government of any State or political subdivision of a State;

2) an individual processing personal data in the context of purely personal or household activities;

3) a legal person engaged in interstate commerce that—

   a) processes personal data on fewer than 100,000 individuals in any twelve-month period; and

   b) engages only in processing that is likely to create a low level of processing risk; and

4) a not-for-profit corporation, association or other entity that operates across states and meets the definition of non-profit set forth in section 501 of title 26, United States Code, if such entity—

   a) processes personal data on fewer than 100,000 individuals in any twelve-month period; and

   b) engages only in processing that is likely to create no more than a moderate level of processing risk.

(e) **Identifiable Individual.**—The term “identifiable individual” means an individual who can be identified, directly or indirectly, by an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual.
(f) **INDIVIDUAL.**—The term “individual” means a living natural person or an agent, trustee or representative acting on behalf of a living natural person.

(g) **INFERRED DATA.**—The term “inferred data” means personal data created or derived through the analysis or interpretation of input information, features of data and generalizations that is probabilistic in nature, often used for predictive purposes, classifying, profiling, personalization, customization, automated decisions, risk or eligibility assessment, or other scoring. Inferred data may be created or derived through processing or automated processing.

(h) **INFORMED CONSENT.**—The term “informed consent” means a clear affirmative act establishing a freely given, specific, and unambiguous indication of the individual’s agreement to the processing of personal data relating to him or her.

(i) **OBSERVED DATA.**—The term “observed data” means personal data captured by automatically recording the actions of an individual. Observed data includes data collected automatically by a covered entity such as:

   (i) Static or video images collected from cameras;

   (ii) Voice or other audible information collected from microphones;

   (iii) Data regarding an individual’s real-time location or location history over time collected through global positioning systems (GPS), a device’s proximity to WiFi hotspots, cell tower triangulation or other similar automated method;

   (iv) Information about an individual’s movements, behavior or health collected from connected device sensors such a gyroscope, accelerometer, magnetometer, proximity sensor, ambient light sensor, touchscreen sensor, pedometer, barometer, heart rate sensor, or thermometer; and

   (v) Data about an individual’s browser history, mobile application use, online posts, comments or similar digital communications, social media use or interactions with similar devices, platforms or applications.

(j) **PERSONAL DATA.**—The term “personal data” means any information relating to an identified or identifiable individual, in any medium, including paper and electronic information.
(i) The term “personal data” does not include information about employees or employment status collected or used by an employer pursuant to an employer-employee relationship.

(k) **PROCESSING.**—The term “processing” means any operation or set of operations which is performed on personal data such as collection, creation, recording, structuring, storage, analysis, adaptation or alteration, retrieval, consultation, use, retention, disclosure, dissemination or otherwise making available, deletion, disposal or destruction.

(l) **PROCESSING ACTIVITY.**—The term “processing activity” means a specific operation or set of operations performed on personal data that defines the circumstances under which personal data are processed including: the business or other context; legal or regulatory requirements; boundaries of an information technology system; stages within the life cycle of personal data; or the individual, covered entity and other stakeholders directly or indirectly served or affected by the processing. A processing activity may be identified with reference to a specific system, product, service, technology, method of processing, business model, or business function, among other things, as determined by a covered entity pursuant to a documented policy.

(m) **PROCESSING RISK.**—The term “processing risk” means the level of risk of adverse processing impact created by processing or a processing activity as follows:

(i) **LOW.**—Processing that could reasonably be expected to create no adverse processing impact or trivial, minor or de minimis adverse processing impact;

(ii) **MODERATE.**—Personal data processing that could reasonably be expected to create limited adverse processing impact;

(iii) **SIGNIFICANT.**—Personal data processing that could reasonably be expected to create serious adverse processing impact;

(iv) **HIGH.**—Personal data processing that could reasonably be expected to create severe or major adverse processing impact; and

(v) **EXTREME.**—Personal data processing that could reasonably be expected to create catastrophic adverse processing impact.
Provided Data.—The term “provided data” means personal data provided to a covered entity directly by the individual who is the subject of the personal data. Such term does not include observed data or inferred data. Provided data includes, but is not limited to, personal data provided by the individual to the covered entity such as—

(i) online or in-store transaction records, including credit or debit account information and contact information;

(ii) account or event registration information;

(iii) medical history given directly to a medical provider;

(iv) password and answers to security questions entered to authenticate a user,

(v) Response to a survey, questionnaire, contest, feedback form, comment field, or other inquiry or communication from the covered entity; or

(vi) Information submitted by an individual as part of an application process or inquiry.

Service Provider.—The term “service provider” means a legal person which.—

(i) processes personal data on behalf of and at the sole direction of a covered entity;

(ii) may not process such personal data except on instructions from the covered entity, unless otherwise required to do so by law; and

(iii) may not disclose the personal data received from or on behalf of the covered entity, or any personal data derived from such personal data, other than as directed by the covered entity.

Societal Benefit.—The term “societal benefit” means a material, objective and identifiable positive effect or advantageous outcome accruing to the public as a result of the processing of personal data. To meet the requirements of this Act, a societal benefit must—

(i) promote and enhance the well being of the general public; and

(ii) be separate and distinct from any positive outcome, advantageous impact or value that accrues to a covered entity, single person or individual, or a narrow or specific group of persons.
Examples of factors that may be considered include greater access to health care; better or lower cost health care; improvements to general wellness; improved education; environmental enhancements such as water conservation; energy cost reduction; protection of rights; and improved services or ease of use of services.

(q) **THIRD PARTY**.—The term “third party” means, with respect to any covered entity, a legal person that—

(i) is not a service provider; and

(ii) is not related to the covered entity by common ownership or corporate control.

(b) **THIRD-PARTY PROVIDED DATA**.—The term “third-party provided data” means personal data provided to a covered entity from—

(i) An individual other than the individual who is the subject of the personal data;

(ii) A third party;

(iii) A government or any instrumentality of a government; or

(iv) Any other person.

**Article II. FAIR PROCESSING OF PERSONAL DATA**

**Section 2.01 LAWFUL, RESPONSIBLE AND FAIR PROCESSING FOR A LEGITIMATE USE**

(a) **PERMISSIBLE PROCESSING**.—A covered entity may process personal data when—

(i) personal data is processed for a legitimate use;

(ii) the processing is necessary and proportionate in relation to the legitimate use; and

(iii) the covered entity has established, implemented, tested, revised and documented policies, procedures and other controls regarding processing to the extent necessary and appropriate given the specific legitimate use and the corresponding level of processing risk.

(b) **LEGITIMATE USE**.—The use of an individual’s personal data is legitimate for the purposes of this Act only when a covered entity can demonstrate one or more of the following:
(i) **COMPLIANCE WITH LEGAL OBLIGATIONS.**—The use is necessary to comply with a Federal, State, or local law, rule or other applicable legal requirement, including disclosures required by court order, subpoena, summons or other properly executed compulsory process.

(ii) **INFORMED CONSENT.**—The individual provided informed consent for the specific use.

(iii) **INFORMATION SECURITY.**—The use is necessary to detect security incidents, protect against malicious, deceptive, fraudulent or illegal activity or prosecute those responsible for that activity.

(iv) **ONGOING BUSINESS PROCESSES.**—The use is necessary to facilitate, improve or safeguard the logistical or technical ability of the covered entity to provide goods or services to the individual, manage its operations, or protect against risk and threats, including the use of personal data to—

1) provide, operate or improve a specific product or service used, requested or authorized by the individual, including the ongoing provision of customer service and support;

2) analyze the individual’s use of a product or service provided by the covered entity to improve the covered entity’s products, services or operations; or

3) support basic business functions that enable a covered entity to operate efficiently such as accounting, inventory and supply chain management, human resource management, quality assurance and internal auditing.

(v) **PROTECTION OF PROPERTY RIGHTS.**—The use is necessary to protect or defend the covered entity’s rights or property, including intellectual property, against actual or potential security threats, fraud, theft, unauthorized transactions or other illegal activities.

(vi) **PUBLIC SAFETY AND HEALTH.**—The use is necessary to protect the health or safety of the individual, a group of individuals or larger community, taking into account the totality of the circumstances pertaining to a particular threat.

(vii) **KNOWLEDGE DISCOVERY.**—The personal data is used to extract insights, acquire knowledge, generate accurate predictions, detect patterns, identify anomalies, pursue truth and avoid errors through research, investigation and
analysis. In order to rely upon knowledge discovery as the legitimate use for processing a covered entity must—
1) identify knowledge discovery as the purpose of the specific processing activity;
2) be able to demonstrate that the specific knowledge discovery activity cannot reasonably be performed without personal data and that the personal data being processed is relevant and necessary for the particular processing;
3) maintain on an ongoing basis a complete, accurate and appropriately detailed inventory of specific knowledge discovery activities conducted across the covered entity;
4) prohibit the use or application of the result or outcome of processing for knowledge discovery for any activities, measures, decisions, products or services that may impact or relate to an individual or group of individuals unless the covered entity can establish that the subsequent use or application of the knowledge discovered satisfies the requirements for a separate and independent legitimate use as otherwise required by this Section; and
5) designate an employee who shall—
   a) be responsible and accountable for the specific knowledge discovery processing activity; and
   b) certify in writing on an annual basis that the covered entity is in compliance with the requirements of this sub-section.
(viii) DEFINED AND DOCUMENTED BENEFITS.—After completing and documenting a processing impact assessment as required by Article V of this Act, the covered entity concludes with a high degree of certainly that—
1) the specific use of an individual’s personal data, alone or in combination with other data, produces a specific, objective, identifiable and measurable benefit for the individual or society; and
2) the use of the individual’s personal data—
   a) creates a low level of processing risk; or
   b) creates no more than a significant level of processing risk and—
   i) the risk is necessary and proportional to the benefit;
ii) the risk has been mitigated to the extent practicable; and

iii) the specific, objective, identifiable and measurable benefit is not outweighed or counterbalanced by the level of processing risk, after all practical controls to mitigate such risk have been identified and implemented.

(ix) RESPECT FOR CONTEXT.— The processing of an individual’s personal data is consistent with the context of the relationship between the individual and the covered entity. Processing of personal data of an individual is consistent with the context of the relationship between the individual and the covered entity if such processing is within the reasonable expectation of similarly situated individuals.

1) When assessing the reasonable expectation of similarly situated individuals a covered entity shall consider, at a minimum—

a) the source of the personal data, including whether the personal data was collected directly from the individual;

b) the method of collection;

c) for observed data, the extent to which an individual is aware of the observation occurring as a result of the presence of sensors or other devices, is aware that such sensors or devices are creating or processing observed data about the individual, or otherwise has knowledge of the processing;

d) the extent to which an individual engaged in one or more transactions directly with the covered entity, including whether the individual and covered entity maintain an ongoing commercial or other relationship;

e) the sensitivity of the personal data, considered from the perspective of the individual;

f) the specific use of the personal data, including whether the use would be obvious to an individual under the circumstances;

g) the application of automated processing and transparency of such processing; and

h) the level of processing risk associated with the specific processing activity.
2) fraud prevention, data security, authentication and identification shall be deemed to be consistent with the context of the relationship between the individual and the covered entity for the purposes of this Section.

Section 2.02 BAD FAITH CLAIMS OF LEGITIMATE USE.—

(a) It is unlawful and an independent violation of this Act for a covered entity to claim or represent that it processes personal data for a specific legitimate use or rely upon a specific legitimate use for processing without having a reasonable basis for such claim, representation or reliance. A covered entity’s failure to conduct and document an investigation or analysis before commencing processing shall be evidence of bad faith.

(b) It is unlawful and an independent violation of this Act for an employee of a covered entity or other individual acting on behalf of a covered entity to provide a certification as required by Section 2.01(b)(vii) without conducting an appropriate investigation and assessing the veracity of the statements in the certification. Such employee or other individual may be individually liable for violating this provision.

Section 2.03 RESTRICTIONS ON PROCESSING

(a) EXTREME RISK.—Notwithstanding Section 2.01, a covered entity shall not process personal data when the processing is reasonably likely to produce an extreme level of processing risk unless, at a minimum—

(i) the processing is expressly authorized by statute; and

(ii) the covered entity is in compliance with the applicable requirements of this Act.

(b) NO UNDISCLOSED PROCESSING.—A covered entity shall not process an individual’s personal data unless the covered entity makes available to the individual and the public the information required in Section 4.01 of this Act.

(c) EXCEPTIONS TO SECTIONS 2.01(B)(VII) AND (IX).—Notwithstanding Section 2.01 above, a covered entity may not rely on respect for context or defined and documented benefits as a legitimate use for processing if such processing is likely to create a high or extreme level of processing risk.
(d) **PROCESSING IN ABSENCE OF FAIR MUTUAL BENEFIT**

(i) **Benefit Of Processing**—

1) An individual should receive an objective, identifiable and measurable benefit, directly or indirectly, from the processing activities of a covered entity when the covered entity processes the personal data of the individual.

2) An individual may be the direct recipient of a benefit or may indirectly derive value from the benefit. A benefit in this context may include personalized services, the provision of a product or service at no or reduced cost, the provision of more efficient services, discounts related to loyalty programs, increased accuracy of data retrieval or other value.

3) A benefit for the purpose of this paragraph may not be purely speculative, presumed to exist or presumed to produce a positive impact.

4) A rebuttable presumption exists that an objective, identifiable and measurable societal benefit is considered a benefit to the individual for the purpose of this Section.

(ii) **Prohibition On Processing In Absence Of Benefit**.—Notwithstanding Section 2.01 of this Act—

1) A covered entity may not process an individual’s personal data if a covered entity exclusively or disproportionately derives the benefit from the processing such that any benefit which enures to the individual is grossly inequitable, cannot be assessed or identified with any degree of specificity, or is manifestly unreasonable under the circumstances.

2) **EXCEPTION.**—Notwithstanding paragraph (1) above, a covered entity may process an individual’s personal data if the covered entity concludes with a reasonable degree of certainly, after conducting a personal data processing impact assessment as set forth in Article V of this Act that the processing of the individual’s personal data presents a low risk of adverse processing impact.

(e) **BURDEN OF PROOF.**—A covered entity bears the burden of proving that the covered entity has satisfied each element required to process for a specific legitimate use as set forth in this Section.
Section 2.04  DUTY OF CARE.—Regardless of the legitimate use, when processing the personal data of an individual a covered entity has a legal duty to that individual to take measures to prevent reasonably foreseeable adverse processing impact to that individual. A covered entity violates its duty of care when the covered entity acts with reckless disregard for adverse processing impact to an individual arising out of the processing of the individual’s personal data.

(a) When determining if a covered entity violated its duty of care to an individual in a given context, the following factors shall be considered—

(i) the covered entity’s intent to undertake the processing that caused the adverse processing impact to the individual;

(ii) the foreseeability of adverse processing impact to the individual;

(iii) the closeness or proximity of the connection between the processing and the severity of adverse processing impact suffered by the individual; and

(iv) the extent to which the measures that could have been taken to mitigate the risk of adverse processing impact are considered industry best practice.

(b) A covered entity may act with reckless disregard and thereby violate the duty of care to an individual even if the covered entity does not intend to cause adverse processing impact. For the purposes of this Act, it is sufficient to establish that the covered entity intended to undertake the processing that caused the adverse processing impact to the individual.

Article III.  RESPONSIBILITIES OF ACCOUNTABLE COVERED ENTITIES

Section 3.01  OPEN AND TRANSPARENT PROCESSING

(a) COMPREHENSIVE PUBLIC STATEMENT OF POLICIES AND PRACTICES.—A covered entity shall publish and make readily available to the public on an ongoing basis a comprehensive statement about the covered entity’s processing and an individual’s options with regard to such processing, including, but not limited to, the following information—

(i) the identity of the covered entity, including any relevant affiliates, subsidiaries or brands necessary to convey meaningful information to an individual;
(ii) the covered entity’s guiding principles for accountability and data responsibility as required by Section 4.01(b);

(iii) a description of the provided data, third-party provided data, observed data and inferred data processed by the covered entity including the specific categories of such provided data, third-party provided data, observed data and inferred data;

(iv) a description of the purpose for which each category of personal data identified in paragraph (a)(iii) is processed. Such description shall—

1) be described clearly and specifically in relation to the intended use of the personal data by the covered entity;

2) disclose each legitimate use of personal data consistent with the requirements of Section 2.01; and

3) Identify the level of processing risk for the personal data or relevant processing activity.

(v) the specific purposes for which personal data may be disclosed to a third party and the categories of third parties who may receive such personal data;

(vi) an explanation of how an individual may—

1) obtain confirmation of whether the covered entity is processing the individual’s personal data;

2) access personal data that is processed about the individual as required by Section 3.03;

3) delete personal data as required by Section 3.05(a)(iii);

4) restrict the use of personal data as required by Section 6.02;

5) restrict the sharing of personal data with third parties as required by Section 6.03;

6) object to further processing of personal data as required by Section 6.04(a);

7) correct or supplement erroneous, incomplete or inaccurate personal data as required by Section 6.04(b);

8) request a statement confirming that a processing impact assessment was completed and the processing risk categorization for the personal data or processing activity;
9) challenge an adverse outcome created by automated processing as required by Section 3.05(a);
10) otherwise contact the covered entity with any inquiries or complaints regarding the covered entity’s processing as required by Section 3.05(b); and
11) submit a complaint with the Agency regarding the covered entity’s processing and compliance with this Act;
(vii) any material changes to the covered entity’s processing practices implemented in the preceding 12 months; and
(viii) the effective date of the statement.

(b) MEANINGFUL SUMMARY EXPLANATION OF PROCESSING DIRECTED TO THE INDIVIDUAL.—A covered entity shall publish and make readily available to the public on an ongoing basis a summary of the covered entity’s processing practices and activities. Such statement shall—
(i) be drafted in a concise, intelligible and easily accessible form, using clear and plain language;
(ii) identify the covered entity, including any relevant affiliates, subsidiaries or brands necessary to convey meaningful information to an individual;
(iii) provide an individual with a meaningful overview of the processing of the individual’s personal data;
(iv) provide an individual with a meaningful overview of the individual’s options with respect to the processing of the individual’s personal data;
(v) enable an individual to make a reasonably informed decision regarding the processing of the individual’s personal data and the options available to the individual; and
(vi) link to the statement required in Subsection (a).

(c) EXPLICIT NOTICE FOR HIGH RISK PROCESSING.—A covered entity shall provide explicit notice to an individual prior to the collection from that individual of personal data that is reasonably likely to create a high or greater level of processing risk.
(d) ADDITIONAL TRANSPARANCY AND ACCOUNTABILITY FOR HIGH RISK. — A covered entity shall conduct and document an analysis to determine if additional methods of notice and communication are necessary to provide an individual with clear, meaningful, relevant and timely information regarding the covered entity’s processing practices in a given context or circumstance. In conducting this analysis, a covered entity shall consider how an individual may obtain such information and assert their preferences, including the extent to which an individual has an opportunity to interact directly with information presented on a computer or mobile screen or similar mechanisms to configure preferences or exercise control over the way in which their personal data is processed. Such analysis shall be incorporated in the privacy impact assessment required by Section 5.04 of this Act and be conducted when—

(i) the covered entity launches a new processing activity or makes material modifications to a current processing activity; and

(ii) the new or modified processing activity creates a high or greater level of processing risk.

(e) NOTICE, TRANSPARANCY AND EXPLAINABILITY FOR AUTOMATED PROCESSING. —

(i) A covered entity shall establish mechanisms for informing an individual when automated processing is being used to make a decision about the individual and the potential implications of such decision on the individual unless the covered entity determines with a high degree of certainty that the use of automated processing in a particular context creates no more than a moderate level of processing risk.

(ii) The mechanism for providing an individual with the relevant information shall take into account the specific context and shall, to the extent practicable, provide information to the individual at the point of interaction.

(iii) The notice shall provide meaningful information to—

1) foster a general understanding of the specific automated processing;

2) make an individual aware of the individual’s interaction with automated processing;
3) enable an individual affected by automated processing to understand the outcome; and
4) enable an individual adversely affected by automated processing to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.

(f) EXCEPTION.—A covered entity shall not be required to comply with a specific provision in this Section to the extent the covered entity is prohibited by law from disclosing the information.

Section 3.02 DATA QUALITY, ACCURACY AND RETENTION.—
(a) A covered entity shall ensure that personal data processed by the covered entity is reasonably accurate, complete and current. In determining whether personal data is reasonably accurate, complete and current in a given context a covered entity shall consider, at a minimum—
(i) the legitimate use of the personal data; and
(ii) the level of processing risk.
(b) A covered entity shall not maintain personal data in identifiable form once the personal data is no longer necessary for a legitimate use.

Section 3.03 ACCESS.—
(a) Upon receiving a verified request from an individual, a covered entity shall provide the individual with confirmation as to whether or not the covered entity is processing personal data about the individual.
(b) Upon receiving a verifiable request from an individual, a covered entity shall disclose to the individual or provide the individual with access to the following:
(i) PROVIDED DATA.—
1) Provided data and, where practicable, third-party provided data about the individual.
2) With respect to third-party provided data, the covered entity shall provide to the individual information as to the source of the personal data, where practicable.
(ii) **OBSERVED DATA.**—
1) A list of the specific categories of data that have been observed about the individual;
2) The specific purpose and legitimate use for the processing of the specific categories of observed data; and
3) Confirmation that a personal data processing impact assessment was conducted pursuant to Article V of this Act and the level of processing risk assigned to the observed data or relevant processing activity.

(iii) **INFERRRED DATA.**—
1) A list of the specific categories of data that have been inferred about the individual;
2) The specific purpose and legitimate use for the processing of the specific categories of inferred data;
3) The reasonably anticipated consequences of such processing and the level of processing risk assigned to the inferred data or relevant processing activity; and
4) Where the processing of the inferred data creates a significant or greater level of processing risk, meaningful information about the process or methodology employed to create the inferred data.

(c) **EXCEPTIONS.**—A covered entity may not be required to make available to an individual personal data—
(i) collected by the covered entity for the exclusive purpose of preventing fraudulent, unlawful or potentially unlawful conduct by an individual;
(ii) previously deleted by the covered entity in compliance with documented data retention schedules;
(iii) that constitutes confidential commercial information, including an algorithm used to make predictions, inferences, scores or other decisions;
(iv) that is processed solely for a use that creates a low level of processing risk; or
(v) required to be kept confidential by any other provision of law;
(d) STATEMENT OF ACCOUNTABILITY.—

(i) Where a covered entity can demonstrate that it is not practicable to provide an
individual with access to the individual’s personal data as otherwise required by
this Section, a covered entity shall provide to an individual a statement
confirming that the processing of the individual’s personal data is subject to
internal policies, procedures and other controls for the processing of personal
data necessary to ensure lawful, responsible and accountable processing given
the intended uses of the data and the level of processing risk.

(ii) It shall be unlawful and a separate violation of this Act for a covered entity to
rely upon Section 3.03(d) in bad faith or provide a statement as required in
Section 3.03(d) that is false, misleading or inaccurate.

(e) VERIFICATION.—A covered entity shall provide the personal data and other
information specified in this Section to an individual only upon receipt of a
verifiable request from the individual.

(f) BUSINESS CONTINUITY PLAN.—

(i) A covered entity shall identify those circumstances in which the inability of an
individual to access the individual’s personal data may create a high or greater
level of processing risk.

(ii) Where such risk exists, a covered entity shall develop, document and implement
an appropriate business continuity plan in order to ensure services and access
can be reasonably maintained and restored as appropriate.

Section 3.04 DATA PORTABILITY.—

(a) PROVIDED DATA.—Where technically feasible, a covered entity shall make
available a reasonable means for an individual to transmit or transfer provided
data and third-party provided data about the individual retained by the covered
entity to another covered entity in a structured, standardized and machine-
readable interoperable format, or otherwise download personal data for the
individual’s own use.

(b) OBSERVED AND INFERRRED DATA.—A covered entity may decline to provide an
individual with the ability to transfer, transmit or download personal data as
specified in Section 3.04(a) for observed or inferred data if the transfer,
transmission or download of such data—
(i) could reasonably be expected to reveal confidential, proprietary or trade secret
information or other intellectual property; or
(ii) provide a competitor with the benefit or value of processing undertaken by the
covered entity to the disadvantage of the covered entity.

Section 3.05 REDRESS

(a) REDRESS MECHANISMS.—A covered entity shall make available a reasonably
accessible, conspicuous and easy-to-use means for an individual to exercise all of
the options available to an individual as required by this Act including the ability
to—
(i) access personal data consistent with the requirements of Section 3.03(b);
(ii) correct personal data consistent with the requirements of Section 6.04;
(iii) restrict processing consistent with the requirements of Section 6.02;
(iv) object to processing consistent with the requirements of Section 6.04
(v) obtain deletion to the extent practicable of personal data relating to the
individual, and any analysis or predictions based upon the processing of that
personal data;
(vi) challenge the outcome of automated processing when the individual has reason
to believe that the individual suffered adverse processing risk as a result of the
prediction, recommendation, decision or other outcome of the automated
processing; and
(vii) submit a complaint or inquiry regarding a covered entity’s policies and
procedures relating to the processing of the individual’s personal data or
compliance with this Act.

(b) COMPLAINT PROCESS.—A covered entity shall respond to an individual’s
complaint or inquiry according to policies and procedures developed and
documented by the covered entity provided, however, that a covered entity shall
respond to a complaint or inquiry within thirty days and provide an individual
with sufficient information to understand and act upon the response.
(c) ADDITIONAL REDRESS MECHANISMS FOR HIGH RISK PROCESSING.—A covered entity with more than 500 employees and annual revenue in excess of $25 million, shall conduct and document an analysis before commencing any processing activity that creates a high or greater level of processing risk in order to determine if additional or special redress mechanisms are warranted given the nature and scope of the covered entity’s activities and data holdings. Such analysis shall be incorporated in the privacy impact assessment required by Section 5.04 of this Act.

Section 3.06 INFORMATION SECURITY

(a) A covered entity shall develop, implement and maintain a comprehensive information security program that includes administrative, technical and physical safeguards that are appropriate to the covered entity’s size and complexity, the nature and scope of the covered entity’s activities, and the sensitivity of personal data processed by the covered entity. Such safeguards shall identify, assess and respond to risk arising from unauthorized activity related to the loss of confidentiality, integrity, or availability of personal data.

(b) In order to develop, implement, and maintain an information security program, a covered entity shall:

(i) Identify reasonably foreseeable internal and external risks to the confidentiality, integrity and availability of personal data that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such data, and assess the sufficiency of any safeguards in place to control these risks.

(ii) Maintain ongoing awareness of information security, vulnerabilities, threats and incidents.

(iii) Develop and implement incident management policies and procedures that address incident detection, response and recovery.

(iv) Design and implement safeguards to control reasonably foreseeable risks through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems and procedures.

(v) Evaluate and adjust the covered entity’s information security program in light of the results of the testing and monitoring; material changes to operations or
business arrangements; or other circumstances that may have a material impact
on the covered entity’s information security program.

Section 3.07 Rule of Construction.—Nothing in this Act shall be construed to
require a covered entity to take an action that would convert information that is not
personal data into personal data.

Article IV. Accountable Processing

Section 4.01 Implementing an Accountable Processing Management and
Governance Program

(a) General Obligations.—A covered entity shall implement a program to—
(i) ensure compliance with this Act and other applicable legal requirements;
(ii) promote effective management and oversight of processing across the covered
entity;
(iii) manage risk on an ongoing basis including risk of adverse processing impact;
(iv) evaluate adverse and beneficial impacts of processing on all relevant parties and
consider the interests of such parties when making determinations about
processing; and
(v) demonstrate the covered entity’s ongoing commitment to trustworthy, fair,
responsible and transparent processing.

(b) Guiding Principles for Accountability and Data Responsibility.
(i) Establish Strategic Vision.—A covered entity shall define, document and
publish guiding principles regarding processing which identifies, at a minimum,
a covered entity’s top-level goals and objectives, values and strategic vision with
respect to data stewardship, data ethics, responsible processing and
accountability. The guiding principles should extend beyond meeting minimum
regulatory requirements.
(ii) Senior Management Review and Approval.—The Board of Directors or
equivalent senior governing body of a covered entity shall—
1) review and approve the guiding principles on an annual basis; and
2) require all processing across the covered entity to align with the covered
entity’s guiding principles for accountability and data responsibility.
(c) PROGRAM DEVELOPMENT AND IMPLEMENTATION.— An accountable processing
management and governance program requires:

(i) Designation of a senior executive to oversee the development, implementation
and maintenance of the program.

(ii) Strategic planning that considers across the covered entity both personal data
itself and the related resources, such as personnel, equipment, funds and
information technology.

(iii) Mechanisms to ensure ongoing collaboration between designated senior
executives across different functions to ensure coordination of risk management,
business operations, legal and regulatory compliance, security and processing
activities.

(iv) Documentation to demonstrate that a covered entity has an accountable
processing management and governance program in place and the capacity to
comply with legal and program requirements on an ongoing basis. Such
documentation shall provide an overview of the program, including a
description of the—

1) structure of the program;
2) resources dedicated to the program;
3) role of designated accountable officials and staff; and
4) strategic goals and objectives of the program.

(v) Resources, staffing, policies and procedures that are appropriate to—

1) a covered entity’s size and complexity;
2) the nature and scope of a covered entity’s activities;
3) legal requirements and obligations that apply to such activities;
4) the scale of a covered entity’s processing operations taking into account factors
such as the:

a) number of individuals concerned;
b) volume of personal data processed by the covered entity;
c) variety and sources of personal data;
d) duration of processing; and

e) geographical extent of the processing;
5) the sensitivity of personal data processed and the level of processing risk of processing activities.

Section 4.02 RESPONSIBLE DATA GOVERNANCE.—

(a) DATA GOVERNANCE PROGRAM.—A covered entity shall establish a comprehensive, entity-wide program to oversee, manage and monitor personal data throughout the information lifecycle. As part of this program, a covered entity shall:

(i) Ensure that personal data is properly managed throughout its life cycle, including all stages of processing such as creation, collection, use, analysis, storage, maintenance, dissemination, disclosure and disposition.

(ii) Establish policies and procedures to ensure that personal data is managed and maintained according to applicable laws, industry codes of conduct, industry best practices and internal policies and procedures.

(iii) Be able to identify, distinguish and appropriately manage different categories of personal data and personal data obtained, collected, received or created from different sources including: provided data; third-party provided data; observed data; and inferred data.

(iv) Ensure that each processing activity has a designated accountable employee who can reliably describe how personal data is processed within a given system or across a specific business process or activity.

(b) INVENTORIES.—Effective management and oversight of personal data processing activities require that the covered entity have appropriate visibility across the covered entity of technology, systems and information. A covered entity shall—

(i) maintain a current, complete and accurate inventory of the covered entity’s information systems and information holdings;

(ii) maintain a current, complete and accurate inventory of the covered entity’s information systems that process personal data; and

(iii) identify within an information system provided data; third-party provided data; observed data; and inferred data.
Section 4.03 ETHICAL, TRUSTWORTHY AND PREVENTATIVE DESIGN.—

(a) GENERAL REQUIREMENTS.—When developing a new processing activity or updating an existing processing activity a covered entity shall consider, evaluate and integrate as appropriate technical and nontechnical processes, engineering analysis, design principles and controls in order to build and deliver a more trustworthy processing activity and minimize adverse effects, including adverse processing impact.

(b) SPECIFIC CONSIDERATIONS.—In implementing the requirements set forth in this section, a covered entity shall, during the initial stages of any development process and throughout the various stages of the life cycle—

(i) ensure close coordination between engineering teams and all relevant stakeholders;

(ii) inventory, incorporate and apply the legal rules, industry best practices and internal requirements for the processing of personal data;

(iii) identify discrete data processing actions within a given processing activity, and determine which of these data actions may create processing risk or other risk. Examples of data processing actions that should be considered include—

1) discrete and specific methods for a covered entity to ingest personal data from different sources;

2) de-identification and re-identification of personal data at different stages;

3) aggregation, merging or analysis of large or diverse datasets;

4) discrete and specific tracking, monitoring or other observation and personal data collection techniques; and

5) dissemination or sharing of personal data internally or externally as well as the need for and degree of connections to external systems or processing activities.

(iv) establish and document a decision-making process that covers the life of each processing activity and include explicit criteria for analyzing the benefits and risks, including information security and potential adverse processing impacts, associated with each stage in the life cycle of both personal data and supporting technologies; and
consider and document the impact of decisions and actions in each stage of the life cycle.

(c) **ASSESS AND IMPLEMENT REQUIREMENTS.**—For each processing activity a covered entity should:

(i) Determine the need or desirability for the covered entity to have the capability to identify, access, segregate, tag, track, retrieve, delete and otherwise manage personal data.

(ii) Ensure that the required or desired capabilities are integrated into the design to the extent practical.

(iii) Given the requirements identified in this Section, ensure that personal data can be managed or administered with sufficient granularity in order to provide confidence that inaccurate personal data can be identified and corrected, obsolete personal data is disposed of, personal data is processed only for legitimate uses, and that an individual’s preferences about use and sharing of their personal data are implemented and maintained.

(iv) Conduct technical, process and risk analyses of alternative design implementations in order to reduce risk and increase accountability.

(v) Consider how data retention and disposition requirements can be incorporated into personal data life cycle processes and stages, including the design, development, implementation, and decommissioning of a product, process, service or system.

(vi) Consider how a given system can be audited such that it is possible to trace any access to the information system, modifications made and any action carried out, in order to identify its author.

**Section 4.04 RESPONSIBLE STEWARDSHIP OF TRUSTWORTHY AND ACCOUNTABLE AUTOMATED PROCESSING**

(a) **GENERAL OBLIGATIONS FOR TRUSTWORTHY AND ACCOUNTABLE AUTOMATED PROCESSING.**—A covered entity engaged in automated processing is required to:

(i) understand the reasoning behind any decision or recommendation produced by automated processing;
(ii) exercise judgment in deciding whether to accept the decision or recommendation from automated processing;

(iii) implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the context of the specific automated processing and consistent with the state of art; and

(iv) ensure overall fairness of making predictions about an individual from group-level data in a given context.

(b) Specific Requirements for Trustworthy and Accountable Automated Processing.—A covered entity engaged in automated processing shall ensure that—

(i) personal data used in or for automated processing is labeled or traceable to enable analysis of the outcome or decisions from such automated processing and responses to an inquiry, appropriate to the context including the level of processing risk and consistent with the state of art;

(ii) reports including predictions include error bars, confidence intervals, or other similar indications of reliability to assist decision makers with giving the prediction appropriate weight;

(iii) automated processing tools are designed and built to mitigate bias at both the model and data layers, and that proper protocols are in place to promote transparency and accountability. Such protocols shall address as appropriate—

1) the validity of the outcome, taking into consideration the context around how the personal data was collected and what kind of inference is being drawn;

2) accuracy of the outcome, taking into consideration the automated processing model’s performance; and

3) bias of the outcome, including examination of potential bias at different stages of automated processing, imperfect data quality, missing data, sampling bias or other relevant factors.
Section 4.05 ACCOUNTABILITY FOR PROCESSING BY SERVICE PROVIDERS AND THIRD PARTIES

(a) SERVICE PROVIDERS.—When a covered entity engages a service provider to process personal data, the covered entity shall—

(i) exercise appropriate due diligence in the selection of the service provider and take reasonable steps to maintain appropriate controls for the processing and security of the personal data;

(ii) require the service provider by contract to implement and maintain appropriate measures designed to meet the objectives and requirements of this Act;

(iii) prohibit the service provider by contract from processing the personal data for any purpose other than the specific purposes and legitimate uses for which the covered entity shared such personal data with the service provider;

(iv) require as appropriate managers and staff of the service provider to complete education, awareness and training programs related to processing; and

(v) exercise reasonable oversight and take reasonable actions to ensure compliance with such contractual provisions, including the implementation of an assessment process to periodically determine whether the service provider has reasonable and appropriate procedures in place to comply with this Act. The assessment process shall reflect the particular circumstances of the covered entity including its size and complexity and the nature and scope of the covered entity’s data holdings and activities with respect to personal data and the relative level of processing risk.

(b) THIRD PARTIES.—A covered entity shall not sell or license personal data it holds to a third party unless that third party is contractually bound to meet the same processing 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.

(c) ASSISTANCE OR SUPPORT FOR VIOLATING THIS ACT.—It shall be unlawful and a separate violation of this Act for a covered entity to provide substantial assistance or support for or related to the processing of personal data to any person when
that covered entity knows or consciously avoids knowing that the person is engaged in ongoing or systemic acts or practices that violate this Act. Nothing in this section shall prohibit a covered entity from providing assistance or support to a person for the sole purpose of coming into compliance with the provisions of this Act.

Section 4.06 Employee Accountability

(a) Designation of Responsible and Accountable Employees.—A covered entity shall designate one or more employees who have organization-wide responsibility and accountability for developing, implementing and maintaining policies and procedures to ensure compliance with this Act.

(b) Awareness and Training Programs.—A covered entity shall develop, maintain and implement an appropriate education, awareness and training program for all employees. As part of such program a covered entity shall provide—

(i) foundational as well as more advanced levels of training;

(ii) role-based training to employees with assigned roles and responsibilities with respect to the processing of personal data and compliance with this Act; and

(iii) training and awareness for employees specifically on how to report and respond to incidents that may affect the confidentiality, availability or integrity of personal data.

(c) Needs Assessment.—A covered entity shall establish policies and procedures to assess and address the hiring, training, continuing education and professional development needs of employees with roles and responsibilities related to compliance with this Act.

(d) Internal Enforcement.—A covered entity shall document and implement policies and procedures to ensure that all employees are held accountable for complying with enterprise-wide information security and personal data processing requirements and policies, including procedures for internal enforcement of the covered entity’s policies and discipline for non-compliance.
Section 4.07 OVERSIGHT: DEMONSTRATING TRUSTWORTHINESS, COMPLIANCE AND ONGOING COMMITMENT TO RESPONSIBLE PROCESSING.—

(a) INTERNAL REVIEWS.—A covered entity shall establish an independent and objective internal review, audit and assurance program to—

(i) monitor compliance with legal obligations including statutory, regulatory and contractual obligations;

(ii) monitor compliance with internal policies and procedures and alignment with public commitments;

(iii) confirm that the covered entity’s processing activities are conducted as planned;

(iv) evaluate the effectiveness of the covered entity’s compliance with this Act; and

(v) assess whether risk assessments required by Article V of this Act have been conducted with integrity and competency.

(b) POTENTIAL CONFLICTS OF INTEREST.—A covered entity shall implement reasonable and appropriate procedures to ensure that—

(i) there is a clear separation of duties between different roles with respect to processing;

(ii) an accountable official responsible for approving a processing impact assessment or approving a specific processing activity shall not have a private, personal, professional, financial or other interest sufficient to appear to influence the objective exercise of his or her official duties; and

(iii) the oversight process is independent from the assessment process.

(c) HIGH RISK PROCESSING ACTIVITY.—

(i) A covered entity shall create an internal data processing review board to evaluate and approve new processing activities, including automated processing, that creates a high or extreme level of processing risk and assess whether the processing has been conducted with integrity and in full compliance with this Act; and

(ii) A covered entity shall seek external review and validation, including external audits and certifications of policies, procedures and practices to ensure compliance with relevant laws, industry best practices, internal procedures and the requirements of this Act.
Article V. PROCESSING RISK MANAGEMENT

Section 5.01 RISK MANAGEMENT PROGRAM.—

(a) PROGRAM OVERVIEW.—A covered entity shall establish a program to manage reasonably foreseeable processing risk. The program shall include processes and procedures to—

(i) identify processing risk;
(ii) assess the level of processing risk;
(iii) mitigate processing risk;
(iv) accept and document residual risk; and
(v) monitor processing risk over time.

(b) Risk management shall be conducted as an entity-wide activity to ensure that risk-based decision-making is integrated into every aspect of the covered entity’s planning and operations related to processing.

(c) The risk management strategy shall include strategic-level decisions by senior leaders and executives regarding the management of risk.

(d) A processing risk management program should be part of or aligned with a covered entity’s overall enterprise risk management strategy.

(e) As part of a covered entity’s risk management strategy, a covered entity should identify risk assumptions, risk tolerance, priorities and trade-offs.

(f) The risk management program shall assess and document a covered entity’s risk tolerance to help employees set priorities and manage risk consistently throughout the covered entity, unless risk tolerance is intended to vary across components of the covered entity, in which case the basis for that determination shall be documented and available to employees accountable for making risk decisions.

(g) Once controls are put in place to mitigate processing risk a covered entity shall conduct and document assessments of such controls to determine whether the controls are implemented correctly, operating as intended, and sufficient to ensure
compliance with applicable requirements and to manage identified risk including processing risk.

Section 5.02 PROCESSING RISK ASSESSMENT

(a) RISK OF ADVERSE PROCESSING IMPACT.—When assessing the level of adverse processing impact a covered entity shall take into account—

(i) the likelihood that adverse processing impact will occur; and

(ii) the potential severity of the adverse processing impact.

(b) CONSIDERATION OF CONTEXT.—When assessing the potential severity and likelihood of adverse processing impact a covered entity shall consider the context of the processing including:

(i) SENSITIVITY OF PERSONAL DATA.—The sensitivity of specific data elements processed as well as the sensitivity of the personal data when combined with other data elements, considered from the perspective of the individual and taking into account the full range of potential harmful consequences identified in Section 103(a).

(ii) IDENTIFIABILITY AND LINKABILITY.—The extent to which—

1) a given data set is linked or linkable to an identifiable individual; and

2) an individual can be identified from a given data set.

(iii) USE.—The specific purpose for which personal data is processed and the intended use of personal data or outcome from processing.

(iv) DATA SOURCES.—The sources and categories of personal data processed including provided data, third-party provided data, observed data and inferred data.

(v) PUBLICLY AVAILABLE INFORMATION.—The extent to which the source of the personal data is information in which—

1) an individual knowingly makes or permits to be made available to the public; or

2) is lawfully obtained, retrieved and accessed from government records that are available to the public, journalistic reports, or information required by law to be made available to the public.
DATA CREATION.—The extent to which a specific processing activity creates new personal data about an individual including inferences, scores or predictions.

REASONABLE EXPECTATIONS.—The extent to which an individual would reasonably expect the processing to occur.

LEGAL OBLIGATIONS.—All statutory, regulatory, contractual, and other legal obligations that may apply to the processing.

VULNERABLE POPULATIONS.—The extent to which the processing targets or otherwise involves a potentially vulnerable population such as children, the elderly, individuals with a disability, victims of certain crimes, or groups facing undue economic hardship.

PERMANENCE.—The relevance and utility of personal data or the outcome of processing over time.

DURATION.—The duration or frequency of the processing activity.

DISCLOSURE.—Intended public disclosure of personal data or widespread dissemination.

AUTOMATED DECISIONS.—The extent to which data-enabled decisions are being made without human intervention.

SOCIETAL RISK.—Such other factors as may be relevant to a community or the public in a given set of circumstances.

Section 5.03 Categorization Of Processing Risk.—

(a) LEVELS OF RISK.—When conducting a processing impact assessment as required by Sections 5.04 and 5.06 of this Act, a covered entity shall categorize the level of processing risk as one of the following:

(i) LOW.—Processing that could reasonably be expected to have no adverse processing impact or trivial, minor or de minimis adverse processing impact.

(ii) MODERATE.—Processing that could reasonably be expected to have a limited adverse processing impact.

(iii) SIGNIFICANT.—Processing that could reasonably be expected to have a serious adverse processing impact.
(iv) HIGH.—Processing that could reasonably be expected to have a severe adverse processing impact.

(v) EXTREME.—Processing that could reasonably be expected to have a catastrophic adverse processing impact.

(b) EFFECT OF RISK MITIGATION.—A covered entity shall categorize the level of risk of adverse processing impact after all practical steps have been implemented to mitigate the risk of adverse processing impact.

(c) LIMITED REBUTTABLE PRESUMPTIONS FOR RISK CATEGORIZATION.

(i) LOW—The risk categorization level for a processing activity shall be presumed to be low if the processing—

1) only involves provided data;

2) does not include any categories of personal data identified in Sections 5.03(c)(iii) or 5.03(c)(iv) of this Act; and

3) the provided data is not shared with a third party unless required for the legitimate uses set forth in Sections 2.01(b)(i) or 2.01(b)(vi) of this Act.

(ii) MODERATE—The risk categorization level for a processing activity shall be presumed to be no less than moderate if the processing involves—

1) matching or combining data sets;

2) the application of new technology or new methods of processing; or

3) sharing personal data with third parties.

(iii) SIGNIFICANT—The risk categorization level for a personal data processing activity shall be presumed to be no less than significant if processing activity involves any one of the following—

1) identification of geolocation;

2) biometric identification, including, but not limited to, facial recognition;

3) identification of racial or ethnic origin;

4) determination of an individual’s religion or religious practice;

5) analysis of physical and mental health data, including any past or present information regarding an individual’s medical history, mental or physical condition, medical treatment, or diagnosis by a health care professional;
6) analysis of sexual life, including sexual activity, sexual orientation, sexual preference, and/or sexual behavior;
7) analysis of DNA or genetic history;
8) analysis of activities inside an individual’s home or equivalent location where an individual has a reasonable expectation of privacy including a hotel room, rented room, locker room, dressing room, restroom, or mobile home;
9) inferred data;
10) observed data;
11) the processing of personal data is inconsistent with the context of the relationship between the individual and covered entity;
12) the processing occurs on a large scale;
13) the processing results in a decision being made without the intervention of an individual; or
14) the processing involves evaluation or scoring, including profiling and predicting.

(iv) HIGH.—The risk categorization level for a personal data processing activity shall be presumed to be no less than high if the processing—
1) creates a reasonable risk of physical harm;
2) creates a reasonable risk of financial or economic harm such as loss or theft of financial or other assets;
3) creates impacts an individual’s eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;
4) involves systemic observation or monitoring; or
5) creates personal data likely to be of interest to a government or military body outside the United States for uses or purposes inconsistent with the laws of the United States.
(v) EXTREME.— A personal data processing activity shall be presumed to have a risk categorization level of extreme if the processing involves risk of adverse processing impact such as:

1) loss of life or serious life threatening injuries;
2) restriction of freedom including incarceration, limitations on travel or movement, or forced relocation;
3) separation or isolation from family members; or
4) infringement of a right guaranteed by the Constitution of the United States.

(d) When classifying risk, a covered entity shall select the higher risk categorization if there is doubt as to the appropriate classification between two risk levels.

Section 5.04 PROCESSING IMPACT ASSESSMENTS.—

(a) A covered entity shall—

(i) develop, implement and document policies and procedures for conducting a processing impact assessment to—

(ii) ensure that processing conforms to applicable requirements;

(iii) determine the risks associated with a processing activity;

(iv) evaluate ways to mitigate such risks;

(v) conduct and document each processing impact assessment with sufficient clarity and specificity to demonstrate that the covered entity fully considered risk and incorporated appropriate controls to mitigate risk throughout the life cycle of the personal data and processing activity; and

(vi) ensure collaboration with program managers, information system owners, information technology experts, security officials, counsel, and other relevant officers and employees in order to produce a comprehensive and meaningful analysis.

(b) A processing impact assessment shall be conducted when, at a minimum, the processing of personal data—

(i) is reasonably likely to create a moderate or greater level of processing risk;

(ii) involves new processing for observed or inferred data, or a material change to such processing;
(iii) is conducted for a legitimate use as defined in Sections 2.01(b)(vii), 2.01(b)(viii) or 2.01(b)(ix) of this Act; or

(iv) does not produce a benefit to the individual as set forth in Section 2.03(d) of this Act.

(c) Threshold Assessment.—A covered entity may conduct and document a processing threshold assessment in order to determine the necessity of completing a full processing impact assessment consistent with the requirements of Section 5.04(b) of this Act. Such analysis shall estimate based on available information the risk of adverse processing impact and the level of processing risk for the relevant processing activity or activities.

(d) At a minimum a processing impact assessment shall analyze and explain—

(i) The purpose, mission, business needs and objectives of the processing activity;

(ii) The functional needs or capabilities of the processing activity;

(iii) The personal data processed;

(iv) The entity or entities, including third parties and services providers, involved with the processing;

(v) The category of individuals, groups or communities that may be impacted;

(vi) The assessment of the risk of adverse processing impact to an individual, including the level of processing risk, before measures are taken to mitigate risk;

(vii) The residual risk remaining after measures are taken to mitigate risk and the final determination of the level of processing risk;

(viii) The risk of adverse societal impact as appropriate; and

(ix) The covered entity’s decision to approve and authorize the processing as required by Section 5.04(e) of this Act.
(e) DECISION TO APPROVE AND AUTHORIZE PROCESSING.—

(i) In order to promote accountability and consistency a covered entity shall develop and document procedures to approve and authorize processing or material modifications in processing as part of the privacy impact assessment.

(ii) Such procedures shall include a documented framework to enable a covered entity to make an informed, explicit and justifiable decision to process after considering—

1) the level of processing risk, including an analysis of residual risk of adverse processing impact;

2) identifiable risk from forgoing a processing activity;

3) benefits to the individual; and

4) societal benefits.

(iii) To the extent a covered entity authorizes and approves the processing, a covered entity shall explain why the factors that support processing are not outweighed or counterbalanced by the residual processing risk.

(f) Processing impact assessments shall be—

(i) reviewed and updated on an ongoing basis to ensure they are accurate and current pursuant to a review schedule determined and documented by the covered entity as part of the covered entity’s risk management program; and

(ii) made available upon written request to the Agency, either in their entirety or a meaningful summary of the assessment.

Section 5.05 ENHANCED PROCESSING IMPACT ASSESSMENT TO ASSESS IMPlications OF AUTOMATED PROCESSING

(a) In addition to the other requirements in this Act, a covered entity shall conduct an enhanced processing impact assessment when the covered entity engages in automated processing that creates a significant or greater level of processing risk.

(b) An enhanced processing impact assessment shall examine the full range of interests of all parties potentially impacted by processing, including the risk of adverse processing impact to an individual or society, as well as potential benefits, including societal benefits.
At a minimum, an enhanced processing impact assessment shall, in addition to the requirements set forth in Section 5.05 of this Act—

(i) enable a relevant employee or other person to see how and why models make the recommendations they do;

(ii) provide attestation that analytic models and insights have been tested, to the extent practicable, for accuracy and predictability;

(iii) identify the specific individual or body who has ultimate-decision making authority for the automated processing activity;

(iv) detect and proactively mitigate bias, to ensure the performance of models is fair, including potential bias that may develop or evolve as models learn or adapt to new experiences or stimuli;

(v) determine the useful life of each insight generated by automated decisions;

(vi) explain how the covered entity considered and implemented the requirements set forth in Section 4.04 of this Act; and

(vii) confirm that an appropriate mechanism has been established to enable an individual to challenge an adverse outcome created by automated processing as required by Section 3.05(a) of this Act.

Section 5.06 BAD FAITH.—With respect to processing that begins after the effective date of this Act, it shall be unlawful and an independent violation of this Act to—

(a) falsely represent that a processing impact assessment or enhanced processing impact assessment was completed before the commencement of processing; or

(b) produce a processing impact assessment or enhanced processing impact assessment for the purpose of justifying and documenting a decision that was previously made without evaluating processing risk as required by this Act.

Section 5.07 RULEMAKING.—The Agency shall, within one year of enactment of this Act and in accordance with section 553 of title 5, United States Code, promulgate regulations to provide additional clarification with respect to categorization of processing risk consistent with the purposes of this Act.
Article VI. INDIVIDUAL ENGAGEMENT

Section 6.01 ACCESS.—An individual shall be entitled to request access to the individual’s personal data from a covered entity consistent with the requirements of Section 3.03 of this Act.

Section 6.02 ENGAGEMENT AND APPROPRIATE CONTROL.—

(a) An individual shall be able to restrict the use of the individual’s personal data where the use of the personal data presents risk to the individual of adverse processing impact as follows.—

(i) LOW RISK OF ADVERSE PROCESSING IMPACT.—Unless otherwise required by law, a covered entity is not required to provide an individual with the ability to restrict the use of personal data if the use of personal data creates no more than a low level of processing risk.

(ii) MODERATE RISK OF ADVERSE PROCESSING IMPACT.—An individual shall be provided with the ability to opt out of the use of the individual’s personal data where such use presents a moderate or greater level of processing risk.

(iii) HIGH RISK PROCESSING.—A covered entity should, where practicable, obtain consent from an individual before a covered entity processes that individual’s personal data where the processing is likely to create a high level of processing risk.

(iv) EXTREME RISK.—Unless otherwise provided by law, a covered entity must obtain informed consent from an individual before a covered entity processes that individual’s personal data where the processing is likely to create an extreme level of processing risk.
Section 6.03 Personal Data Shared With Third Parties

(a) Access.—An individual shall be able to request a list identifying those third parties with whom the covered entity shares the individual’s personal data if such sharing is—

(i) inconsistent with the context of the relationship between the individual and the covered entity; or

(ii) the processing otherwise produces a significant or greater risk of adverse processing impact.

(b) Discontinue Sharing.—An individual may request that the covered entity discontinue the sharing of the individual’s personal data.

Section 6.04 Redress.—

(a) Object to Processing.—

(i) An individual may object to the processing of the individual’s personal data when the individual has reason to believe that—

1) the individual’s personal data is inaccurate, and such inaccuracy may result in a significant or greater adverse processing impact to the individual;

2) the individual’s personal data is used for a purpose other than a purpose identified in the disclosures and statements required by Article IV of this Act;

or

3) a covered entity is processing the individual’s personal data and is in material noncompliance with the requirements set forth in this Act.

(b) Ensure Accuracy.—An individual may request changes or amendments to the individual’s personal data to ensure accuracy when the individual has reason to believe that the individual’s personal data is inaccurate, and such inaccuracy may result in a significant or greater adverse processing impact to the individual.

(c) Dispute Assessments.—An individual shall be afforded an opportunity to dispute the conclusion of a personal data processing impact assessment and categorization of risk of a processing activity if the individual presents a colorable argument that the assessment or conclusions in the assessment are inaccurate, incomplete or incorrect.
(d) **AUTOMATED PROCESSING.**—An individual shall be offered an opportunity to challenge the outcome of automated processing as required in Section 3.05 of this Act.

(e) **EXCEPTIONS.** A covered entity shall not be required to comply with Sections 6.02(a)(i), 6.02(a)(ii), 6.02(a)(iii), 6.03 and 6.04 if—

(i) the personal data is processed for a legitimate use as defined in Sections 2.01(b)(i),(iii),(v) or (vi) of this Act;

(ii) after conducting a privacy impact assessment, the covered entity determines with a high degree of certainty that the objective, identifiable and measurable benefits of the processing significantly outweigh the risk of adverse processing impact to the individual; or

(iii) as otherwise required by law.

### Article VII. **ENFORCEMENT, OVERSIGHT AND RULEMAKING**

**Section 7.01** **IMPLEMENTING REGULATIONS TO SUPPORT ACCOUNTABILITY**

(a) **AUTHORITY.**—The Agency shall, in accordance with section 553 of title 5, United States Code, promulgate regulations to carry out the purposes of this Act.

(b) **AUTHORITY TO GRANT EXCLUSIONS.**—In promulgating rules under this Act, the Agency may implement such additional exclusions from this Act as the Agency considers consistent with the purposes of this Act.

(c) **CRITERIA FOR ISSUANCE OF RULES.**—

(i) In promulgating regulations the Agency shall consider—

1) the potential benefits and costs to individuals and covered entities, including the potential reduction of access by individuals to products or services resulting from such regulations; and

2) that such regulations must be practical, reasonable and appropriate for a covered entity taking into account —

3) the size, resources, and complexity of the covered entity;

4) the nature and scope of the covered entity’s processing activities; and

5) the potential level of processing risk created by such processing.
(ii) In promulgating such regulations the Agency shall not require the deployment or use of any specific products or technologies, including any specific computer software or hardware, nor prescribe or otherwise require that computer software or hardware products or services be designed, developed, or manufactured in a particular manner.

**Section 7.02 CIVIL ENFORCEMENT BY AGENCY**

(a) **ENFORCEMENT AUTHORITY.**—Whenever it shall appear to the Agency that a covered entity has violated any provision of this Act, the rules or regulations thereunder, or a final order entered by the Agency, the Agency may bring an action through its own attorneys in a United States district court to seek, and the court shall have jurisdiction to impose, equitable and monetary relief including, upon a proper showing, a civil penalty to be paid by the covered entity or person who committed such violation.

(b) **REPRESENTATION.**—The Agency may act in its own name and through its own attorneys in enforcing any provision of this Act and rules thereunder, in any action, suit or proceeding to which the Agency is a party.

(c) **CIVIL PENALTIES.**—A violation of this Act shall be subject to a civil penalty in an amount that is not greater than $16,500 per individual for whom the covered entity processed personal data in violation of this Act.

(d) **DETERMINATION OF PUBLIC INTEREST.**—In considering under this section whether a civil penalty is in the public interest, the Agency shall consider—

(i) the gravity of the violation, including whether the act or omission for which such penalty is assessed involved fraud, deceit, manipulation, bad faith or deliberate or reckless disregard of a regulatory requirement;

(ii) the severity of adverse processing impact to individuals resulting either directly or indirectly from such act or omission;

(iii) the history of previous violations;

(iv) the size, financial resources and good faith of the covered entity charged;

(v) the need to deter such covered entity from committing such acts or omissions; and

(vi) such other matters as justice may require.
Draft June 16, 2019

(e) **Equitable Relief.**—In any action or proceeding brought or instituted by the Agency under this Act, the Agency may seek, and any Federal court may grant, any equitable relief that may be appropriate or necessary for the benefit of individuals impacted or in the public interest. Such equitable remedies may include:

(i) temporary and permanent injunctions;
(ii) cease-and-desist orders;
(iii) requirements that a covered entity make accurate information available through disclosures, direct notification or education;
(iv) restitution or disgorgement of profits; and
(v) such other equitable relief reasonably related to the unlawful practices conducted by the covered entity, as may be necessary to prevent future violations of this Act by the covered entity.

(f) **Liability and Accountability for Individuals in Positions Of Authority**

(i) An individual may be liable for a covered entity’s violation of this Act upon a showing that the individual had—

1) authority to direct or control the covered entity’s acts or practices; and
2) knowledge of the covered entity’s improper practices; or
3) sustained or systematic failure to exercise oversight.

(ii) An individual may not be subject to civil penalties for a violation of this Act unless—

1) the individual intended to violate a provision of this Act; and
2) the individual’s improper conduct created significant or greater processing risk and caused adverse processing impact.

(iii) Nothing in this Section shall alter the Agency’s ability to hold an individual liable under any other law enforced by the Agency.

Section 7.03 **Compliance Examinations and Inspections.**

(a) **Authority.**—The Agency is authorized to perform compliance inspections, conduct examinations and gather information regarding—

(i) a covered entity’s business operations;
(ii) a covered entity’s processing activities; and
(iii) the policies and procedures adopted and employed by a covered entity to meet
the requirements of this Act.

(b) REVIEW OF RECORDS.—All records required to be made and kept by a covered
entity pursuant to this Act are subject at any time, or from time to time, to such
reasonable periodic, special or other examinations by representatives of the
Agency as the Agency deems necessary or appropriate in the public interest, for
the protection of individuals or otherwise in furtherance of the purposes of this
Act.

(c) EXAMINATIONS OF LARGE-SCALE PROCESSING.—The Agency shall, pursuant to
reasonable schedules, policies and procedures to be published by the Agency,
conduct examinations to assess compliance with this Act by any covered entity
engaged in processing personal data of 50 million or more individuals where the
level of processing risk is reasonably believed to be significant or greater. Such
examinations shall be conducted to protect the public interest and further the
purposes of this Act.

Section 7.04 ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) 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 to—
(i) enjoin further violation of this Act by the defendant;
(ii) compel compliance with this Act;
(iii) obtain damages, restitution, or other compensation on behalf of the residents of
the State;
(iv) obtain civil penalties in the amount determined under section 702(d) above; and
(v) such other relief as the court deems appropriate.

(b) The attorney general of a State shall notify the Agency in writing of any civil
action prior to initiating such civil action. Upon receiving notice with respect to a
civil action, the Agency may—
(i) intervene in such action; and

(ii) upon intervening—

1) be heard on all matters arising in such civil action; and

2) file petitions for appeal of a decision in such action.

(iii) PREEMPTIVE ACTION BY AGENCY.—If the Agency 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 Agency for violation of this Act or a regulation promulgated pursuant to this Act.

Section 7.05  SAFE HARBOR

(a) Industry organizations and standards setting bodies may, pursuant to rules promulgated by the Agency, develop standardized risk assessment methodologies and enforceable codes of conduct to satisfy specific provisions under this Act.

(b) A covered entity that is in compliance with such standardized risk assessment methodologies and enforceable codes of conduct and has fully documented such compliance shall not be subject to civil penalties for violations of the specific provisions of this Act addressed by the standardized process or code implemented pursuant to this Section.

Article VIII.  EDUCATION AND OUTREACH

Section 8.01  CONSUMER EDUCATION.—The Agency shall publish resources to educate individuals with respect to—

(a) the various ways an individual may interact with processing as well as devices and technology that enable processing including the collection of personal data;

(b) the potential benefits and risks, including risk of adverse processing impact that may be associated with processing in order to help individuals make more informed decisions;

(c) helping individuals compare the processing activities of different digital products and services; and

(d) helping individuals understand their options with respect to processing by a covered entity afforded by this Act.
Section 8.02  Education Initiatives for Older Americans.—The Agency shall—

(a) engage in activities designed to facilitate the digital literacy of individuals who have attained the age of 62 years or more, including through the dissemination of materials to help such individuals protect and control their personal data, safely and effectively use new technology and devices necessary to engage in society, and understand their options with respect to processing by a covered entity;

(b) work with community organizations, non-profit organizations, and other entities that are involved with educating or assisting individuals who have attained the age of 62 years or more; and

(c) coordinate efforts to protect individuals who have attained the age of 62 years or more with other Federal agencies and State regulators, as appropriate, to promote consistent, effective, and efficient enforcement.

Section 8.03  Collecting and Tracking Complaints.—The Agency shall establish a mechanism to facilitate the centralized collection of, monitoring of, and response to complaints regarding processing of personal data and potential violations of this Act.

Section 8.04  Guidance for Covered Entities

(a) The Agency shall publish guidance, training materials, proposed best practices, and other resources designed to assist covered entities with compliance obligations under this Act, taking into account that the requirements of this Act are intended to be flexible and scalable to accommodate the range in types and sizes of covered entities that must comply with the provisions of this Act.

(b) The Agency shall, in particular, develop resources designed to assist small and medium-sized covered entities with compliance.

(c) The Agency shall establish a mechanism for a covered entity to submit inquiries to the Agency regarding compliance with this Act. To the extent practicable and in the public interest, the Agency shall make available to the public the Agency’s responses to such inquiries.
Article IX. SAVINGS CLAUSE AND EFFECTIVE DATE.—

Section 9.01 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.

Section 9.02 If any provision of this Act, an amendment made by this Act, or the application of such provision or amendment to any person or circumstance is held to be unconstitutional, the remainder of this Act, the amendments made by this Act, and the application of the provisions of such to any person or circumstance shall not be affected thereby.