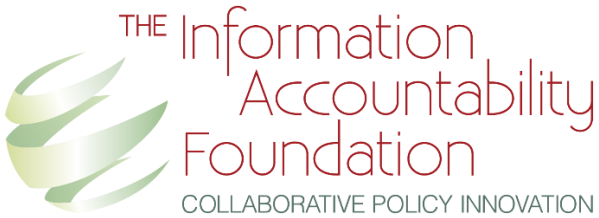

The FAIR and OPEN USE Act

A Demonstration of Accountability-Based Legislation To Assure the Fair Processing of Data Pertaining to People

May 25, 2021

May 25, 2021

The Information Accountability Foundation (IAF) is a non-profit global information policy think tank that works with regulatory authorities, policymakers, business leaders, civil society and other key stakeholders to promote responsible processing of data and help frame privacy and data protection policy. IAF believes that frameworks based on risk assessment and effective information governance will enable beneficial, data-driven innovation while protecting individuals and society from the myriad potential harms that may arise from data processing in the information age.

As part of these efforts, IAF drafted the FAIR and OPEN USE Act (Model Legislation) to demonstrate how accountability-based legislation can incentivize organizations to optimize beneficial uses of data while simultaneously minimizing adverse consequences for individuals and society as a whole. While the Model Legislation is intended to be educational, the IAF also hopes that it will inform the legislative process.

The IAF developed three principles to guide the drafting of the Model Legislation.

Accountable and Measurable
Organizations must be responsible for how data are used and be answerable to others for the means taken to be responsible. Decisions must be explainable to others based on objective measures. In sum, the Model Legislation provides organizations with flexibility to innovate but organizations are on the hook for any adverse outcomes their actions produce.

Informing and Empowering
Organizations have a proactive obligation to inform stakeholders about the data processed, the processes used to assess and mitigate risk, and an individual's ability to exert control and make choices. Although a risk-based framework shifts the burden from the individual to the organization to prevent adverse outcomes, individuals still participate and have some level of control.

Competency, Integrity and Enforcement
Organizations are evaluated by the competency they demonstrate in reaching decisions to process data, their honesty, disclosures and actions. A well-resourced and capable regulatory enforcement mechanism is necessary to help ensure trust and compliance Organizations are responsible for outcomes, but the Model Legislation contemplates that there is a difference between systematically bad decisions and anomalies.

Sections of the Model Legislation are color coded to highlight how the three principles are reflected and implemented in the text. Additional information about the principles may be found in Principles for Fair Processing Accountability.

A BILL[1]

To assure an innovative and fair digital future for all Americans by preserving America's innovation engine; protect individuals' interests in the fair, ethical, transparent, and responsible processing of personal data and other data that may impact an individual; mitigate risks of adverse impacts from the processing of personal data; and promote the benefits of the twenty-first century information age through an agile regulatory framework that contemplates that: (1) the sensitivity and value of data is 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.

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.—

[1] In order to help the reader understand the draft bill, all defined terms are capitalized throughout the document. We acknowledge that this is not legislative drafting convention.

[2] The IAF Model does not use the word "privacy." The term is imprecise and lacks a common definition. Even the International Association of Privacy Professionals website states, "What does privacy mean? Well, it depends on who you ask." It's difficult to craft a legislative solution to solve an undefined problem. In addition, traditional notions of "privacy" do not capture the full range of issues and risks presented by the processing of personal data in the information age. A future-oriented, legal framework should promote fair processing and broadly address how processing data can impact people in a highly observational digital ecosystem.

3) Section 6.03 Safe Harbor Programs for Responsible and Accountable Covered Entities
4) Section 6.04 Safe Harbor for Accountable Small Business and Non-Profit Organizations
5) Section 6.05 Accountability Reports and Assessments
6) Section. 6.06 Implementing Regulations to Support Accountability

(7) Article VII. Commission Education, Guidance, Outreach, and Reports
1) Section 7.01 Consumer Education
2) Section 7.02 Guidance and Outreach for Covered Entities
3) Section 7.03 International Cooperation for the Protection of Personal Data
4) Section 7.04 Report

(8) Article VIII. Commission Resources and Authorization of Appropriations
1) Section 8.01 Appointment of Additional Personnel
2) Section 8.02 Authority to Establish New Bureau or Office
3) Section 8.03 Authorization of Appropriations

(9) Article IX. Preemption
1) Section 9.01 Preemption
2) Section 9.02 Effect on Other Laws
3) Section 9.03 Government Accountability Office Study and Report

(10) Article X. Effective Date and Savings Clause
1) Section 10.01 Effective Date
2) Section 10.02 No Retroactive Applicability
3) Section 10.03 Savings Clause

Section 1.02 FINDINGS AND PURPOSE.

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

(b) The rapid evolution of lifechanging digital products, services, and consumer applications, however, has produced equally awesome challenges for individuals and society. Today, personal data[3] is not only collected directly from the individual but, rather, from a diverse range of sources without the individual's awareness of the personal data's origination and subsequent uses. In addition, a growing proportion of human activity is captured as data and groundbreaking technologies extract value from data to create new knowledge in ways once thought impossible.

(c) These complex, twenty-first century challenges cannot adequately be addressed by relying on twentieth century notions of notice, choice, and consent. Organizations that collect, create, use, and share data that may impact an individual must be responsible stewards of that data and be held accountable when their data practices create an unreasonable risk of harm to individuals or society.

(d) The rapid growth of innovative, data-driven technologies and the processing of data raises issues with respect to intrusion into seclusion, individual autonomy, fair use of an individual's data, the just use of that data, respect for civil rights, and individual freedom.

(e) The processing of data, including personal data, also raises issues with respect to societal interests including the protection of marginalized and vulnerable groups of individuals; the safeguarding of foundational values of the democracy of the United States, such as freedom of information, freedom of speech, justice, and human ingenuity and dignity; and the integrity of democratic institutions, including fair and open elections.

---

[3] Technically the terms "data" and "information" have distinct definitions. The National Institute of Standards and Technology (NIST), for example, defines "data" as "pieces of information from which 'understandable information' is derived" and defines "information" as the "meaningful interpretation or expression of data." NIST Guidelines for Media Sanitization, Publication 800-88 Rev. 1 In most contexts today, however, the two words are used interchangeably. Adding to the confusion, some privacy laws use the term "personal data" while others use "personal information." The IAF Model focuses on the term "data" but uses "information" in some contexts. For the purpose of interpretation, implementation, compliance, and enforcement, the two terms do not have a meaningful distinction.

(f) Data use must be—

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

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

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

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

(h) The benefits of the information age belong to everyone. Data should not just serve the interests of the organization that collected the data.

(i) 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.[4]

(j) Legal frameworks structured as a list of prohibitions are dated by the time they go into effect and may unnecessarily restrict beneficial uses of data.

(k) Legislative proposals that rely primarily on notice and consent are also ineffective. Given the complexity of the digital ecosystem and asymmetry of information, the burden of preventing harm from processing data should not fall upon the individual.

(l) In today's data-driven economy, organizations must be responsible stewards of data and accountable for their actions. Accountable

[4] IAF recognizes the appeal of simple solutions but difficult digital challenges that evolve in real time cannot be solved with a short, simple legislative solution. There is no quick, easy, overnight fix to the myriad challenges presented by processing personal data. IAF drafted the IAF Model with 2030 in mind, rather than focus on what many believe are the greatest challenges today. IAF contemplates that full implementation and compliance with the framework codified in the IAF Model will take years for most entities. This is intended to be a long-term solution to a rapidly evolving set of challenges that will grow more complicated over time.

organizations identify and avoid unacceptable levels of risk and are answerable for any misuse of data. Accountability also requires organizations to have policies that link to the law, mechanisms to put those policies in place, security safeguards, internal oversight, and documentation for basic processes.

(m) The United States needs a new twenty-first century paradigm for regulating the use of data that incentivizes organizations to optimize beneficial uses of data while simultaneously minimizing adverse consequences for individuals and society as a whole. A national framework based on accountability and risk assessment, backed by robust oversight and enforcement, meets this objective.[5]

Section 1.03 DEFINITIONS.

(a) ADVERSE PROCESSING IMPACT.— [6]The term "Adverse Processing Impact" means detrimental, deleterious, or disadvantageous consequences to an Individual arising from the Processing of that Individual's Personal Data or to society from the Processing of Personal Data, including—

(1) direct or indirect financial loss or economic harm;

(2) physical harm, harassment, or threat to an Individual or property;

---

[5] The first draft of the IAF Model was published in 2018. Dozens of stakeholders reviewed and commented on drafts of the IAF Model. International and state laws and regulations and proposed bills were reviewed and where appropriate were incorporated (some of these inclusions are reflected in the footnotes). IAF thanks the many individuals who provided their input. This draft of the IAF Model is significantly improved because of their contributions.

[6]The IAF Model does not use the terms "harm" or "injury." Instead, the IAF Model defines a broad concept of "Adverse Processing Impact." The definition of Adverse Processing Impact aligns with the approach to privacy risk and "privacy problems" codified in the National Institute of Standards and Technology's publication, NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0 2020 ("NIST Privacy Framework"). NIST defines privacy events as "potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal. NIST Privacy Framework at p, 3. NIST identifies the range of problems an individual can experience as a result of processing as ranging from dignity-type effects such as embarrassment or stigmas to more tangible harms such as discrimination, economic loss, or physical harm. Id. The definition of Adverse Processing Impact is also generally consistent with NIST's Catalog of Problematic Data Actions and Problems, which is a non-exhaustive, illustrative set of problematic data actions and problems that individuals could experience as the result of data processing.

(3) psychological harm, including anxiety, embarrassment, fear, and other mental trauma;

(4) inconvenience or expenditure of time;

(5) a negative outcome or decision with respect to an Individual's eligibility for a right, privilege, or benefit related to—

(A) employment, including hiring, firing, promotion, demotion, reassignment, or compensation;

(B) credit and insurance, including denial of an application, obtaining less favorable terms, cancellation, or an unfavorable change in terms of coverage;

(C) housing;

(D) education admissions;

(E) financial aid;

(F) professional certification;

(G) issuance of a license; or

(H) the provision of health care and related services.

(6) stigmatization or reputational injury;

(7) disruption and intrusion from unwanted commercial communications or contacts;

(8) discrimination in violation of Federal antidiscrimination laws or antidiscrimination laws of any State or political subdivision thereof;

(9) loss of autonomy [7]through acts or practices that are not reasonably foreseeable by an Individual and that are intended to materially—

(A) alter that Individual's experiences;

(B) limit that Individual's choices;

(C) influence that Individual's responses; or

[7] The concept of "loss of autonomy" is widely recognized in many bills and frameworks including the NIST Privacy Framework, which provides that, "[l]oss of autonomy includes losing control over determinations about information processing or interactions with systems/products/services, as well as needless changes in ordinary behavior, including self-imposed restrictions on expression or civic engagement." Catalog of Problematic Data Actions and Problems.

(D) predetermine results or outcomes for that Individual; or[8]

(10) other detrimental or negative consequences that affect an Individual's private life, privacy affairs, private family matters or similar concerns, including 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 or other data will not be collected, observed, or used.

(b) AFFIRMATIVE EXPRESS CONSENT.—The term "Affirmative Express Consent" means a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of the Individual's agreement to the Processing of Personal Data relating to the Individual.

(c) AUTOMATED DECISION MAKING.—The term "Automated Decision Making" means the use of algorithms, machine learning, artificial intelligence, predictive analytics, or other automated methods to make or facilitate decisions affecting Individuals. Automated Decision Making—

(1) includes techniques—

(A) performed by or in computer software, physical hardware, or any other digital context; and

(B) designed to learn to approximate a cognitive task, solve complex problems, make predictions, define or identify correlations, approve or deny transactions, grant or decline permissions, adapt to changing circumstances, or improve performance when exposed to new or existing data sets; and

(2) may operate with varying levels of autonomy or human intervention.

(d) BENEFIT TO INDIVIDUALS AND COMPETITION.—The term "Benefit to Individuals and Competition" means a material, objective, and identifiable positive effect or advantageous outcome—

[8] The IAF Model applies the well accepted drafting convention that "or" means "either or both", or if there is a series of items, "anyone item or combination of items".

(1) to Individuals or the marketplace as a result of the Processing of Personal Data; and

(2) which is 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.

(e) BIOMETRIC DATA.—The term "Biometric Data" means an Individual's physiological, biological, or behavioral characteristics, including an Individual's deoxyribonucleic acid (DNA), that can be used, alone or in combination with each other or with other Personal Data, to establish Individual identity.[9]

(f) COMMISSION.—The term "Commission" means the Federal Trade Commission.

(g) CONSISTENT WITH THE CONTEXT.—The term "Consistent with The Context" means Processing which is consistent with the context of the relationship between the Individual and the Covered Entity and within the reasonable expectation of similarly situated Individuals. To determine whether Processing is within the reasonable expectation of similarly situated Individuals, a Covered Entity shall consider—

(1) the source of the Personal Data and the method of collection, including whether the Personal Data was collected directly from the Individual;

(2) whether the specific use is necessary to provide the specific good or service that was affirmatively and unambiguously requested by the Individual;

(3) the extent to which an Individual engaged in one or more transactions directly with the Covered Entity, including whether—

(A) the Individual intended to interact with the Covered Entity; or

[9] Biometric data includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted as well as keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data containing identifying information. A bill could incorporate these examples as well as specific exceptions.

(B) the Individual and Covered Entity maintain an ongoing commercial or other relationship;

(4) whether the specific use of the Personal Data would be obvious to an Individual under the circumstances;

(5) with respect to Observed Data, the extent to which an Individual is likely to be aware of the observation occurring as a result of the presence of sensors or other devices, is likely to be aware that such sensors or devices are creating or Processing Observed Data about the Individual, or otherwise has knowledge of the Processing;

(6) the extent to which Processing may produce unanticipated revelations about an Individual;

(7) the extent to which the Processing involves Sensitive Personal Data;

(8) the extent to which the Processing, a Processing Activity, Processing Action, business practice, or use of technology is new, novel, or not yet widely deployed in a commercial context;

(9) the age and sophistication of similarly situated Individuals who use the Covered Entity's products or services, including whether a product or service is directed toward or significantly used by a vulnerable population identified in Section 5.02(j) of this Act;

(10) the level of Processing Risk associated with the specific Processing Activity; and

(11) the specific Adverse Processing Impact that may arise from the Processing considered from the perspective of the Individual and taking into account the full range of potential Adverse Processing Impacts identified in Section 1.03(a) of this Act.

(h) COVERED ENTITY.—[10]

[10] The definition of Covered Entity is consistent with most draft privacy bills. It closes the gap in FTC jurisdiction over common carriers and non-profit organizations, as a comprehensive framework must be equally applicable to every sector of our global, digital economy. The IAF Model does not exempt small businesses from the law entirely, following the approach taken in the Brookings Institution's proposed legislation, the Information Privacy Act – June 3, 2020. Rather, the IAF Model takes into account the unique compliance and implementation challenges small businesses may face by providing different standards and less severe penalties in certain contexts. The IAF Model is scalable to organizations of all sizes and complexities.

(1) The term "Covered Entity" means—

(A) any person subject to the authority of the Commission pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2));

(B) notwithstanding section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 45(a)(2)), a common carrier subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); or

(C) notwithstanding sections 4 and 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. 44 and 45(a)(2)), any non-profit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of the Internal Revenue Code of 1986;[11] and

(D) such person, common carrier, or non-profit organization is or has engaged in Processing Personal Data.

(2) Such term does not include—

(A) the Federal Government or any instrumentality of the Federal Government;[12]

(B) the government of any State or political subdivision of any State; or

(C) an Individual Processing Personal Data—

(i) in the context of purely personal or household activities; or

(ii) acting in a de minimis commercial capacity.

(i) 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 one or more factors specific to the physical,

[11] As with small business, accommodations have been made to take into account the potential challenges for non-profits. Non-profits, for example, are not subject to certain provisions in the Act including civil penalties or regulatory reviews as provided for in Section 6.04 of the Act. Moreover, there is a safe harbor for certain non-profits and FTC rulemakings must consider the impact of any new regulations on both non-profits and small business.

[12] As with other draft Federal privacy laws, the IAF Model does not address Processing by government entities. Therefore, the IAF Model does not address head on the core privacy and surveillance concerns raised in Case C-311/18, Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems, judgment of 16 July 2020 ("Schrems II"). Accountable organizations can take steps to limit government access, but commercial privacy legislation alone likely will not provide a "quick fix" to the concerns raised by the Schrems II decision.

physiological, genetic, mental, economic, cultural, or social identity of that Individual.

(j) INDIVIDUAL.—The term "Individual" means a living natural person or an agent, trustee, or representative acting on behalf of a living natural person.

(k) INFERRED DATA.—[13]The term "Inferred Data" means Personal Data created or derived through the analysis or interpretation of input data, features of data, assumptions, and generalizations that is probabilistic in nature. Uses of Inferred Data include, but are not limited to predictive purposes, classifying, categorizing, segmenting, profiling, personalization, customization, decision-making, risk or eligibility assessment, or other scoring.

(l) 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—

(1) static or video images collected from cameras;

(2) voice or other audible data collected from microphones;

(3) data regarding an Individual's real-time location, location history over time, or movements collected through global positioning systems (GPS), a device's proximity to Wi-Fi hotspots, cell tower triangulation, or other similar automated method;

(4) data about an Individual's movements, behavior, or health collected from connected device sensors, such as a gyroscope, accelerometer,

---

[13] The IAF Model defines four broad categories of Personal Data based on how the data originates: Provided by the Individual; Provided by a Third-Party; Observed; and Inferred. IAF believes that to get governance and risk assessment right, a Covered Entity must understand where data comes from, how it is created, and how aware and involved the Individual is in its creation. In the IAF Model, different obligations apply to different categories of data. A detailed explanation of the different categories may be found in IAF's paper, "The Origins of Personal Data and its Implications for Governance." Many other proposed bills draw similar distinctions between different categories of data based on the source of the data.

magnetometer, proximity sensor, ambient light sensor, touchscreen sensor, pedometer, barometer, heart rate sensor, or thermometer; and

(5) 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.

(m) PERSONAL DATA.—

(1) The term "Personal Data" means information that identifies, relates to, describes, is reasonably capable of being associated with, could reasonably be linked, directly or indirectly, with a particular Individual.

(2) Such term does not include information about employees or employment status collected or used by an employer pursuant to an employer-employee relationship.[14]

(n) PRECISE GEOLOCATION DATA.—The term "Precise Geolocation Data" means data obtained from a device about the physical location of that device that is sufficiently precise to locate a specific Individual or device with reasonable specificity.[15]

(o) 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, duplication, disclosure,

[14] Unlike most other proposed frameworks today, this definition of "Personal Data" does not carve out public information or publicly available information. Rather, the extent to which data is publicly available or public is a factor to be considered in a risk assessment. This is in line with laws such as the Privacy Act of 1974, 5 U.S.C. § 552a et seq., which recognizes that publicly available information, such as newspaper clippings or press releases, take on a different value when incorporated in government systems. Data, including public data, takes on a different value when maintained in the context of information about an individual rather than when maintained in a library - not in a file tied to a person. Sources and context also matter. Some "public data" may be "observed data" if it's scraped from a website without authorization or an agreement with the operator of the website. How the personal data is used or intended to be used is relevant to the analysis. Broad exceptions for public data may make compliance easier, but the distinction is becoming increasingly irrelevant and inconsistent with the policy objectives of limiting harmful uses of data.

[15] Unlike some proposed definitions, this definition does not refer to a specific radius. Any radius selected would be arbitrary and will become outdated as technology quickly evolves. In the context of a risk-based framework, it is more important to understand the accuracy and intended use of the data. Ease of compliance today should not trump sound policy objectives designed to promote a robust and trustworthy data-driven marketplace for tomorrow.

dissemination, Transfer, deletion, disposal, or destruction. Processing includes an operation or set of operations performed on data that results in the creation of Personal Data.

(p) PROCESSING ACTION.— [16]The term "Processing Action" means a single, discrete Processing operation performed on Personal Data, often characterized as one stage of the information lifecycle, including collection, creation, recording, structuring, storage, analysis, adaptation or alteration, retrieval, consultation, use, retention, duplication, disclosure, dissemination, Transfer, deletion, disposal, or destruction.

(q) PROCESSING ACTIVITY.— The term "Processing Activity" means a discrete set of resources organized for Processing or a specific set of Processing Actions performed on Personal Data that define the context and circumstances under which Personal Data is Processed in order to provide a logical and consistent frame of reference for assessing Processing Risk.

(1) Such circumstances may include the purpose of the Processing; legal or regulatory requirements; contractual obligations; boundaries of an information technology system or platform; accountable organization within a Covered Entity; stages within the lifecycle of Personal Data; or the Individual, Covered Entity, and other stakeholders directly or indirectly served or affected by the Processing.

(2) A Processing Activity may be identified with reference to a specific system, product, service, technology, method of Processing, business model, business function, or other item or activity as determined by a Covered Entity pursuant to a documented policy.

(r) PROCESSING RISK.—[17]The term "Processing Risk" means the level of Adverse Processing Impact potentially created as a result of or caused

---

[16] The NIST Privacy Framework describes these data operations in the singular as a data action and collectively as data processing. NIST Privacy Framework at p.3.

[17] This tracks NIST's definition of "privacy risk" in the NIST Privacy Framework, which is "[t]he likelihood that individuals will experience problems resulting from data processing, and the impact should they occur." NIST Privacy Framework, Appendix B: Glossary, at p. 30. This maps to the generally accepted concept of risk as a function of likelihood and severity. As defined by NIST, risk is a "measure of the extent to which an entity is

by Processing, a specific Processing Activity, or a specific Processing Action assessed as a function of—

(1) the likelihood Adverse Processing Impact will occur as a result of Processing, a specific Processing Activity, or a specific Processing Action; and

(2) the degree, magnitude, or potential severity of the Adverse Processing Impact should it occur.

(s) 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.

(1) Provided Data includes Personal Data provided by the Individual to the Covered Entity, such as—

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

(B) account or event registration information;

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

(D) password and answers to security questions entered to authenticate a user;

(E) response to a survey, questionnaire, contest, feedback form, comment field, or other inquiry or communication from the Covered Entity; or

(F) information submitted by an Individual as part of an application process or inquiry.

(2) Such term does not include Observed Data, Inferred Data, or Third-Party Provided Data.

(t) SENSITIVE PERSONAL DATA.—[18]The term "Sensitive Personal Data" means Personal Data that objectively and regardless of context, alone or

---

threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." NIST SP 800-12, Rev. 1, An Introduction to Information Security, Appendix B: Glossary, at p 30.

[18]The IAF Model's definition of "Sensitive Data" is designed for a future-oriented, risk based legal framework. While it may be desirable to define some data as being more sensitive than other data, it is important to recognize

in combination with other data, presents a higher-than-average Processing Risk for an average Individual acting reasonably.

(1) Evidence of higher-than-average Processing Risk includes—

(A) USE.—There are numerous uses for the Personal Data, alone or in combination with other data, including unlawful or nefarious uses by a malicious actor, that may cause substantial Adverse Processing Impact.

(B) IDENTIFIABILITY AND LINKABILITY.—The Personal Data itself identifies an Individual or is directly linked or linkable to an Identifiable Individual.[19]

(C) AUTHENTICATION AND VERIFICATION.—The Personal Data is routinely used for identification, authentication, and verification of identity for commercial transactions, travel, employment, medical treatment, public benefits, education, and physical and logical access.

(D) LEGAL OBLIGATIONS.—The Personal Data is subject to statutory, regulatory, and other legal obligations or restrictions.

(E) PERMANENCE.—The Personal Data remains useful and relevant over time and cannot easily be replaced or substituted or is immutable.[20]

---

that it is more often than not the context in which data are used that creates real risks of inappropriate consequences. Unlike other bills which provide a finite list of categories of sensitive data, this definition focuses on the criteria and risk factors that make a given category of data "sensitive." The model also provides an illustrative list of rebuttable presumptions that can be overcome in appropriate contexts. The criteria and risk factors are based, in part, on the criteria set forth in Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum M-17-12, January 3, 2017 .

[19] The IAF Model does not define "de-identified data," "aggregate data," "anonymous data," or "pseudonymous data." The focus of the analysis should be on the potential impact of the use of the data. Accordingly, the IAF Model does not exclude any of these categories of data from the definition of Personal Data or the coverage of the proposed law. Rather, the extent to which a given data set is identifiable is incorporated in the risk assessment. It is well understood today that even de-identified can and does have significant impacts on individuals, and therefore, de-identified data should not be excluded from a risk-based legal framework intended to promote beneficial innovation while limiting harmful outcomes. De-identification is a risk mitigation tool that should be part of an accountability and risk management program. Depending on the context, de-identified data and pseudonymous data can be Personal Data. This is consistent with the requirements in the General Data Protection Regulation (EU) 2016/679 (GDPR), and the current state of technology.

[20] This requirement includes an assessment of the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy or utility as it ages, while other information is likely to apply to an individual throughout his or her life. For example, an individual's health

(F) PRIVACY EXPECTATION.—The Personal Data is reasonably considered highly personal, private, or of an intimate nature, and the average Individual takes steps to maintain the confidentiality of the Personal Data.

(2) A rebuttable presumption exists that the following Personal Data presents a higher-than-average Processing Risk for an average Individual acting reasonably—

(A) Biometric Data;

(B) social security numbers, passport numbers, driver's license numbers, or any other unique government-issued identification number linked to a form of identification commonly used to identify, authenticate, or verify the identity of an Individual;

(C) unique account numbers together with any required security code, access code, or security question or password necessary to access an Individual's account;

(D) Precise Geolocation Data;

(E) Personal Data related to an Individual's physical, mental or behavioral health, including the provision of health care services;

(F) genetic data;[21]

(G) Personal Data related to an Individual's sexual life, including sexual activity, sexual orientation, and/or sexual behavior;

---

insurance ID number can be replaced. However, information about an individual's health, such as family health history or chronic illness, may remain relevant for an individual's entire life, as well as the lives of his or her family members. Special consideration is warranted with biometric information including fingerprints, hand geometry, retina or iris scans, and DNA or other genetic information. When considering the nature and sensitivity of biometric information, a Covered Entity should factor in the known current uses of the information and consider that, with future advancements in science and technology, biometric information could have many additional uses not yet contemplated.

[21] Under the IAF Model, human biological material is not necessarily Personal Data. The analysis will depend on the context, including the intended use of the biological material. Consideration of context plays a central role in the IAF Model.

(H) calendar information, address book information, phone or text logs, photos or videos maintained in an Individual's non-public account, whether on an Individual's device or otherwise; and

(I) the content or metadata of an Individuals' private communications and the identity of the parties to such communications, unless the Covered Entity is an intended party to a communication.

(u) SERVICE PROVIDER.—The term "Service Provider" means a person that—

(1) Processes Personal Data on behalf of and at the sole direction of a Covered Entity;

(2) may not Process such Personal Data except on instructions from the Covered Entity, unless otherwise required to do so by law; and

(3) 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.

(v) THIRD PARTY.—The term "Third Party" means, with respect to any Covered Entity, a person that—

(1) is not a Service Provider; and

(2) is not related to the Covered Entity by common ownership or corporate control.

(w) THIRD-PARTY PROVIDED DATA.—The term "Third-Party Provided Data" means Personal Data provided to a Covered Entity from—

(1) an Individual other than the Individual who is the subject of the Personal Data;

(2) a Third Party;

(3) a government or any instrumentality of a government; or

(4) any other person.

(x) TRANSFER.—The term "transfer" means to disclose, release, share, disseminate, make available, sell, license, or otherwise communicate Personal Data by any means to a Third Party—

(1) in exchange for consideration; or

(2) for a commercial purpose.[22]

Article II. FAIR PROCESSING OF PERSONAL DATA

Section 2.01 LAWFUL, RESPONSIBLE, AND FAIR PROCESSING.

(a) PERMISSIBLE PROCESSING.—A Covered Entity may Process Personal Data when—

(1) the purpose of the Processing is for a specified legitimate use;

(2) the Processing is reasonably necessary and proportionate in relation to the purpose;

(3) the Covered Entity has performed a processing impact assessment as required by Article V of this Act and concluded that the Processing does not present an unacceptable level of Processing Risk; and

(4) the Covered Entity has developed, documented, and implemented reasonable and appropriate policies, processes, and procedures taking into account the specific purpose of the Processing and the level of Processing Risk.

(b) LEGITIMATE USE.—The Processing of an Individual's Personal Data is legitimate only if and to the extent that a Covered Entity can demonstrate that one or more of the following applies—

(1) COMPLIANCE WITH LEGAL OBLIGATIONS.—The Individual's Personal Data is Processed to—

(A) comply with a Federal, State, or local law, rule, or other applicable legal requirement; or

(B) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, civil investigative demand, or summons by Federal, State, or local authorities.

(2) INFORMATION SECURITY.—The Individual's Personal Data is Processed to—

[22] This text is based on the definition of "transfer" in Brookings Institution's proposed legislation, the Information Privacy Act – June 3, 2020. This definition does not include transfers to Service Providers or affiliates of the Covered Entity. Certain transfers by non-profit organizations may also be excluded.

(A) protect the confidentiality, integrity, and availability of data and the security of devices, networks, products, services, systems, data sources, or facilities against malicious and illegal activity, including to prevent, detect, or respond to cybersecurity incidents; or

(B) verify and authenticate the identity of an Individual, provided that Personal Data collected to verify and authenticate the identity of an Individual shall not be used for any other purpose.

(3) ROUTINE BUSINESS PROCESSES.—The Individual's Personal Data is Processed to—

(A) support basic internal business functions that are necessary for a Covered Entity to operate, such as accounting, billing, payment processing, inventory and supply chain management, human resource management, quality assurance, and internal auditing;

(B) ensure correct and efficient operation of systems and processes, including to monitor, repair, and enhance performance, quality, or safety; or

(C) fulfill the terms of a written warranty or product recall conducted in accordance with Federal law.

(4) PROVIDE A REQUESTED PRODUCT OR SERVICE.—

(A) The Individual's Personal Data is Processed to provide goods or services requested by an Individual to that Individual. In order to rely upon Paragraph 2.01(b)(4) as the basis for the legitimate use, the use must be Consistent with the Context of the relationship between the Individual and the Covered Entity.

(B) The use of Personal Data to provide a requested product or service includes the use to—

(i) render or operate a specific product or service used, requested, or authorized by the Individual;

(ii) provide the Individual with ongoing customer service, assistance, and technical support;

(iii) perform a contract to which the Individual is a party or take steps at the request of the Individual prior to entering into a contract; or

(iv) complete the transaction for which the Personal Data was Processed.

(5) PROTECT AGAINST UNLAWFUL ACTIVITY.—The Individual's Personal Data is Processed to—

(A) 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;

(B) cooperate with law enforcement agencies concerning conduct or activity that the Covered Entity reasonably and in good faith believes may violate Federal, State, or local law; or

(C) exercise or defend legal claims.

(6) PUBLIC SAFETY AND HEALTH.—The Individual's Personal Data is Processed 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.

(7) AFFIRMATIVE EXPRESS CONSENT.—An Individual has provided Affirmative Express Consent for the specific use.

(A) In order to rely upon Affirmative Express Consent as the basis for the legitimate use for Processing a Covered Entity shall—

(i) obtain Affirmative Express Consent from the Individual for the specific use before the Covered Entity begins Processing the Individual's Personal Data; and

(ii) make available to the Individual a reasonable means to withdraw consent.

(B) To obtain Affirmative Express Consent, the description of the Processing for which consent is sought must be provided to the Individual in a standalone disclosure and must include a prominent heading identifying the Processing Activity or Activities for which consent is sought. Acceptance of a general or broad terms of use or

similar document that contains descriptions of Personal Data Processing along with other, unrelated information does not constitute Affirmative Express Consent.

(8) KNOWLEDGE DISCOVERY.[23]—The Individual's Personal Data is Processed for internal research, investigation, and analysis designed to acquire knowledge, generate predictions, detect patterns, extract insights, identify anomalies, avoid errors, increase efficiency, and facilitate product improvement or development. To rely upon knowledge discovery as the legitimate use for Processing—

(A) the purpose of the Processing must be reasonably Consistent with the Context of the relationship between the Individual and the Covered Entity; and

(B) the Covered Entity must—

(i) identify knowledge discovery as the purpose of the specific Processing;

(ii) be able to demonstrate that the specific knowledge discovery cannot reasonably be performed without Personal Data and that the Personal Data being Processed is relevant and necessary for the particular Processing;

(iii) maintain on an ongoing basis a complete, accurate, and appropriately detailed inventory of specific knowledge discovery activities conducted across the Covered Entity;

---

[23] "Knowledge Discovery" is a new but essential concept, which is distinct from the more traditional concept of research. Processing of Personal Data for Knowledge Discovery draws an important distinction between (1) learning from data and (2) applying what has been learned. Knowledge Discovery may involve gathering data to be analyzed, pre-processing it into a format that can be used, consolidating it for analysis, analyzing it to discover what it may reveal and interpreting it to understand the processes by which the data was analyzed and how conclusions were reached. The conclusions or new knowledge learned during the Processing may not be applied to an activity, business process, decision-making, etc. that will impact an Individual unless there is a separate legitimate use. Given this restriction, Processing for Knowledge Discovery presents a different set of risks and considerations than other Processing. P. Bruening, Advanced Data Analytic Processing – 2019 Update, at 4.

(iv) 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 use or application of the result or outcome of the Processing fully satisfies the requirements for a separate and independent legitimate use as otherwise required by this Section; and

(v) designate a qualified 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 Section 2.01(b)(8) of this Act. Such certification shall be maintained by the Covered Entity and be available to demonstrate compliance with this Act.

(9) RESEARCH.—The Individual's Personal Data is Processed for scientific analysis, systematic study, and observation, including basic research or applied research that is designed to develop or contribute to public or scientific knowledge and that adheres or otherwise conforms to all other applicable ethics and privacy laws, including but not limited to studies conducted in the public interest in the area of public health. In order to rely upon research as the legitimate use for Processing—

(A) the purpose of the Processing must be reasonably Consistent with the Context of the relationship between the Individual and the Covered Entity;

(B) the Covered Entity must be able to demonstrate that the research cannot reasonably be performed without Personal Data; and

(C) the Covered Entity must prohibit the use or application of the result or outcome of the research 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 use or application of the result or outcome of the research fully satisfies the requirements for a separate and independent legitimate use as otherwise required by this Section.

(10) ADVERTISING OR MARKETING PURPOSES.—The Individual's Personal Data is Processed to disseminate a communication in any medium intended to induce an Individual to obtain goods, services, or employment, provided that a Covered Entity obtains Affirmative Express Consent from an Individual before using the Individual's Sensitive Personal Data for Advertising or Marketing Purposes.[24]

(11) JOURNALISM.—The Individual's Personal Data is Processed for the investigation and publication of newsworthy information of legitimate public concern to the public.

(c) REASONABLE BASIS.—It is unlawful and an independent and separate violation of this Act for a Covered Entity to rely upon a specific legitimate use as set forth in Section 2.01(b) of this Act for the purpose of complying with Section 2.01(a) of this Act without having a reasonable basis for such reliance or claim. The failure to conduct and document an investigation or analysis prior to Processing shall be evidence that a Covered Entity did not have a reasonable basis.

Section 2.02 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, as defined in Section 5.03 of this Act, unless, at a minimum—

(1) the Processing is expressly authorized by Federal or State statute;

(2) the Covered Entity is in compliance with the applicable requirements of this Act; and

[24] Advertising and marketing, like other uses of personal data, are subject to a risk assessment. This is important given the increasingly diverse range of activities that often fall under the category of advertising or marketing in the information age. Moreover, as set forth in Article III, an individual may opt out of the sharing of personal data with third parties as well as the use of personal data for many, but not all, advertising and marketing purposes.

(3) the Covered Entity has obtained Affirmative Express Consent from the Individual before processing that Individual's Personal Data, unless otherwise prohibited by law.

(b) HIGH RISK.—Notwithstanding Section 2.01(a), a Covered Entity shall not rely on Sections 2.01(b)(8), (9), or (10) as the legitimate use for Processing when the Processing is reasonably likely to produce a high or greater level of Processing Risk.

(c) 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 3.01 of this Act.

Section 2.03 UNETHICAL AND RECKLESS PROCESSING.

(a) It is unlawful and an independent and separate violation of this Act for a Covered Entity to Process Personal Data with reckless disregard for Processing Risk or for Adverse Processing Impact to the Individual.

(b) When determining if a Covered Entity engaged in Processing with such reckless disregard in a given context in violation of this Act, the following factors shall be considered—

(1) the Covered Entity's intent to undertake the Processing that created the Processing Risk or caused the Adverse Processing Impact to the Individual;

(2) the foreseeability of the Processing Risk or the Adverse Processing Impact to the Individual;

(3) the closeness or proximity of the connection between the Processing and the severity of Adverse Processing Impact suffered by the Individual; and

(4) the extent to which the measures that could have been taken to mitigate Processing Risk were reasonably available or considered industry best practice at the time of the Processing.

(c) A Covered Entity may act with reckless disregard and thereby violate its legal duty to an Individual and this Act 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.[25]

(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 the following information—

(1) the identity of the Covered Entity, including any relevant affiliates, subsidiaries, or brands necessary to convey meaningful information to an Individual;

(2) the Covered Entity's guiding principles for accountability and data responsibility as required by Section 4.01(b) of this Act;

(3) a description of the categories of Provided Data, Third-Party Provided Data, Observed Data, and Inferred Data Processed by the Covered Entity;

(4) a description of the categories of Sensitive Data Processed by the Covered Entity;

(5) for each category of Personal Data identified pursuant to paragraphs (a)(3) and (a)(4) above, a description of the use of the Personal Data

[25] The IAF believes transparency is very important. There should be no secret data systems. Transparency also adds to the ability for the market and regulators to govern fair behavior. IAF further believes that transparency for individuals and regulators should be two different communications devices. Accordingly, and as required in many other model bills, a Covered Entity must publish two notices: (1) a comprehensive statement for regulators and others interested in the details around Processing and (2) a summary statement for Individuals. A similar approach is codified in the model bills circulated by The Brookings Institution (Information Privacy Act – June 3, 2020 -2020.) and Consumer Reports (Model State Privacy Bill).

and purpose for Processing, unless the Processing is reasonably likely to create a high or greater level of Processing Risk, in which case, the Covered Entity shall provide a clear and detailed explanation of the specific use of the Personal Data and purpose for Processing;

(6) a statement identifying new or novel Processing Activities, applications of technology, or uses of Personal Data that are not yet widely deployed in a commercial context;[26]

(7) the length of time the Covered Entity intends to retain each category of Personal Data or, if that is not possible, the criteria used to determine such period, provided that a Covered Entity shall not retain an Individual's Personal Data for longer than is reasonably necessary for the disclosed purpose for which the data was collected;[27]

(8) the specific purposes for which Personal Data may be Transferred to a Third Party and the categories of Third Parties who may receive such Personal Data;

(9) information regarding Automated Decision Making as required by Section 3.01(d) of this Act;

(10) an explanation of how an Individual may exercise each option available to the Individual with respect to the Processing of the Individual's Personal Data as required by Sections 3.02, 3.04, 3.05, and 3.07 of this Act;

(11) any material changes to the Covered Entity's Processing practices implemented in the preceding 12 months; and

(12) 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—

[26] A responsible and trustworthy organization affirmatively highlights new, novel, different or potentially surprising applications of technology or uses of personal data. An accountable organization should be transparent, truthful, and forthcoming with information about new or novel uses. This is not simply about deceptive omissions.

[27] This text is based on a similar provision in the California Consumer Privacy Act of 2018 ("CCPA").

(1) be drafted in a concise, intelligible, and easily accessible form using clear and plain language;

(2) be titled, "How We Process Your Personal Data;"

(3) identify the Covered Entity, including any relevant affiliates, subsidiaries, or brands necessary to convey meaningful information to an Individual;

(4) provide an Individual with a meaningful overview of the Processing of the Individual's Personal Data;

(5) be provided to an Individual at or before the point when the Individual begins a transaction, orders a product or service, or otherwise commences a relationship with the Covered Entity and at or before the point when the Covered Entity collects Personal Data from the Individual, taking into account the nature of the interaction and the technology; [28]

(6) 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

(7) link to the statement required in subsection (a) above.

(c) ADDITIONAL TRANSPARENCY AND ACCOUNTABILITY FOR HIGH RISK PROCESSING.—

(1) EXPLICIT NOTICE.—A Covered Entity shall provide explicit notice to an Individual prior to the collection from that Individual of Sensitive Personal Data or Personal Data that is reasonably likely to create a high or extreme level of Processing Risk under the circumstances.

(2) ENHANCED DISCLOSURES.—A Covered Entity shall conduct and document an analysis to determine if additional methods of notice and

[28] This requirement is similar to the requirement in the CCPA regulations, that a business provide both a comprehensive privacy policy and a notice at collection, The purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them and the purposes for which the personal information will be used.

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 processing impact assessment required by Section 5.04 of this Act and be conducted when—

(A) the Covered Entity launches a new Processing Activity or makes material modifications to a current Processing Activity; and

(B) the new or modified Processing Activity creates a high or extreme level of Processing Risk.

(d) TRANSPARENCY AND EXPLAINABILITY FOR AUTOMATED DECISION MAKING.—

(1) A Covered Entity shall establish one or more mechanisms to inform an Individual when Automated Decision Making may impact the Individual and the potential implications of such Automated Decision Making.

(2) The mechanism for providing the required information shall take into account the specific context of the Automated Decision Making and shall, to the extent practicable, provide the Individual with notice at the point of interaction.

(3) The notice shall, at a minimum, be designed to—

(A) make an Individual aware of the Individual's interaction with Automated Decision Making;

(B) enable an Individual to understand the purpose of the Automated Decision Making; and

(C) enable an Individual adversely affected by the use of or reliance on Automated Decision Making to challenge the Automated Decision Making pursuant to Section 3.05(b) of this Act.

Section 3.02 MEANINGFUL CONTROL.[29]

(a) DISCONTINUE THIRD-PARTY TRANSFERS.—

(1) A Covered Entity shall provide an Individual with a means to request that a Covered Entity that Transfers Personal Data about the Individual to Third Parties stop Transferring the Individual's Personal Data. A Covered Entity that has received a verified request from an Individual to stop Transfers of the Individual's Personal Data shall be prohibited from Transferring the Individual's Personal Data after its receipt of the Individual's request unless the Individual subsequently provides Affirmative Express Consent for the Transfer.

(2) RULEMAKING.—[30]

(A) IN GENERAL.—Not later than 18 months after the date of enactment of this Act, the Commission shall issue a rule under section 553 of title 5, United States Code, establishing one or more acceptable processes for Covered Entities to follow in allowing an Individual to discontinue Transfers of the Individual's Personal Data.

(B) REQUIREMENTS.—The processes established by the Commission pursuant to this subsection shall—

(i) be centralized, to the extent feasible, to minimize the number of requests of a similar type that an Individual must make;

---

[29] The IAF Model captures the controls that come from other regimes and proposals, evolves them for today's more complex data world, and merges them with the flexibility that has fostered innovation in the United States. The obligations on a Covered Entity and corresponding mechanisms for an Individual to exert control over data use and submit requests set forth in Article III must be read in conjunction with the specific and general exceptions in Article III. As with all proposed frameworks, there are reasonable limitations on an Individual's ability to access Personal Data and opt out of Processing. The exceptions in the IAF Model are generally consistent with most other draft bills and the CCPA.

[30] This text aligns with the opt-out and rulemaking provisions in Section 104(a) of the Brookings Institution's proposed legislation, the Information Privacy Act – June 3, 2020.

(ii) permit an Individual to authorize another person to submit a request on the Individual's behalf;

(iii) include clear and conspicuous discontinuation notices and consumer-friendly mechanisms to allow an Individual to discontinue Transfers of Personal Data;

(iv) allow an Individual who objects to a Transfer of Personal Data to view the status of such objection;

(v) allow an Individual who objects to a Transfer of Personal Data to withdraw or modify such objection; and

(vi) be informed by the Commission's experience developing and implementing the National Do Not Call Registry and researching technical mechanisms for expressing choice in other contexts.

(b) OPT OUT OF USE OF PERSONAL DATA.—

(1) A Covered Entity shall provide an Individual with a means to request that a Covered Entity that Processes Personal Data about the Individual stop using the Individual's Personal Data. A Covered Entity that has received a verified request from an Individual to stop using the Individual's Personal Data shall be prohibited from using the Individual's Personal Data after its receipt of the Individual's request unless the Individual subsequently provides Affirmative Express Consent.

(2) LIMITED EXCEPTION TO OPT OUT FOR CERTAIN ADVERTISING AND MARKETING.[31]—A Covered Entity may continue to use an Individual's Personal Data following a request pursuant to paragraph (b)(1) for advertising and marketing purposes on websites, applications, or services owned and operated by the Covered Entity to the extent that—

(A) the specific use is Consistent with the Context of the Relationship between the Individual and the Covered Entity; and

[31] The scope of this narrow exception is similar to the list of activities not considered to be targeted advertising under Virginia's new Consumer Data Protection Act .

(B) the advertising or marketing are not based on either—

(i) Processing the Individual's Personal Data over time and across unaffiliated websites, applications, or services; or

(ii) Sensitive Personal Data, unless the Covered Entity has obtained Affirmative Express Consent for the specific advertising or marketing use.

(c) DELETION OF PERSONAL DATA.—[32]A Covered Entity shall provide an Individual with a mechanism to request that the Covered Entity delete the Individual's Personal Data. In response to a verified request to delete Personal Data, the Covered Entity shall, to the extent practicable, delete such data from its records or the technical equivalent, and direct any Service Providers to delete the Individual's Personal Data from their records or the technical equivalent. A Covered Entity may satisfy this requirement by permanently disposing, deleting, destroying, purging, wiping or removing data elements from a data set such that the remaining data or data set no longer identifies, relates to, describes, is reasonably capable of being associated with, could reasonably be linked, directly or indirectly, with a particular Individual.

(d) EXCEPTIONS.—A Covered Entity shall not be required to comply with an Individual's request pursuant to this Section to the extent that—

(1) the Individual's Personal Data is necessary for the legitimate uses identified in Sections 2.01(b)(1)–2.01(b)(6); or

(2) the Individual's Personal Data is necessary to continue ongoing research as provided for in Section 2.01(b)(9) and honoring the Individual's request will render impossible or seriously impair the ability to complete such research.

[32] The opportunity for an Individual to request deletion of Personal Data under the IAF Model does not, and is not intended to, mirror the right to erasure ("right to be forgotten") under GDPR.

(e) SUBVERTING CHOICE AND MEANINGFUL CONTROL PROHIBITED.[33]—It is unlawful and a separate and independent violation of this Act for a Covered Entity to—

(1) knowingly design, modify, or manipulate a user interface with the purpose or substantial effect of obscuring, subverting, or impairing user autonomy, decision-making, or choice to obtain consent or Personal Data;

(2) impersonate any entity or Individual in order to collect Personal Data or obtain access to an Individual account or device, including but not limited to a financial, medical, email, internet, social media, or telecommunications account; or

(3) misrepresent or mischaracterize any product or service in order to induce the disclosure of Personal Data.

Section 3.03 DATA QUALITY, ACCURACY, AND RETENTION.

(a) A Covered Entity shall keep Personal Data Processed by the Covered Entity 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—

(1) the sensitivity of the Personal Data;

(2) the legitimate use of the Personal Data; and

(3) the level of Processing Risk.

(b) A Covered Entity shall implement reasonable procedures to track updates or changes to Personal Data over time.

(c) A Covered Entity shall not maintain Personal Data once the Personal Data is no longer reasonably necessary for a legitimate use. A Covered

[33] An ethical, trustworthy, and accountable organization should take proactive measures to make choices simple and straightforward for consumers. This text is based upon CPRA, which prohibits so-called "dark patterns." This was first addressed in the Deceptive Experiences to Online Users Reduction Act (DETOUR Act), introduced by Senators Mark Warner (D-VA) and Joni Ernst (R-IA). The SAFE DATA Act, and the Consumer Reports Model State Privacy Act include similar langauge.

Entity may satisfy this requirement by permanently disposing, deleting, destroying, purging, wiping, or removing data elements from a data set such that the remaining data or data set no longer identifies, relates to, describes, is reasonably capable of being associated with, could reasonably be linked, directly or indirectly, with a particular Individual.

Section 3.04 ACCESS AND DATA PORTABILITY.

(a) ACCESS TO PERSONAL DATA.—A Covered Entity shall provide an Individual with a mechanism to request access to the Individual's Personal Data. 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 and, when the response is in the affirmative, shall provide the Individual with reasonable access to the Individual's Personal Data retained by the Covered Entity as follows—

(1) Provided Data;

(2) Third-Party Provided Data, including information as to the source of the Personal Data, where practicable;

(3) with respect to Observed Data—

(A) a list of the specific categories of data that have been observed about the Individual;

(B) the specific purpose and legitimate use for Processing each of the specific categories of Observed Data; and

(C) the level of Processing Risk assigned to the Observed Data or relevant Processing Activity.

(4) with respect to Inferred Data—

(A) a list of the specific categories of Inferred Data about the Individual;

(B) the specific purpose and legitimate use for Processing each of the specific categories of Inferred Data;

(C) the reasonably anticipated consequences of such Processing and the level of Processing Risk assigned to the Inferred Data or relevant Processing Activity; and

(D) where the Processing of the Inferred Data creates a moderate or greater level of Processing Risk, meaningful information about the process or methodology employed to create the Inferred Data.

(b) STATEMENT OF ACCOUNTABILITY IN LIEU OF ACCESS.—

(1) Where a Covered Entity can demonstrate that it is unduly burdensome, technically infeasible, and not practicable to provide an Individual with access to all or a subset of the Individual's Personal Data as otherwise required by this Act and has determined with a high degree of certainty that the Processing does not create a high or extreme level of Processing Risk, a Covered Entity may provide an Individual with a written statement explaining the reasons that access cannot be provided and confirming that the Processing of the Individual's Personal Data is subject to internal policies, processes, and procedures 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.

(2) It shall be unlawful and a separate violation of this Act for a Covered Entity to rely upon Section 3.04(b) of this Act in bad faith or provide a statement as required in Section 3.04(b) of this Act that is false, misleading, or inaccurate.

(c) ACCESS TO INFORMATION ABOUT TRANSFERS TO THIRD PARTIES.—A Covered Entity shall provide an Individual with a mechanism to request a list identifying the Third Parties with whom the Covered Entity Transfers the Individual's Personal Data. Upon receiving a verified request from an Individual, a Covered Entity shall provide the Individual with a list identifying the specific category or categories of Third Parties with whom the Covered Entity Transfers the Individual's Personal Data, unless the Processing is reasonably likely to create a high or extreme level of Processing Risk, in which case the Covered Entity shall provide the Individual with a list identifying the specific Third Parties with whom the Covered Entity Transfers or has

Transferred the Individual's Personal Data and the purpose for such Transferring.

(d) DATA PORTABILITY.[34]

(1) A Covered Entity shall provide an Individual with a mechanism to request that the Covered Entity provide the Individual with copies of their Personal Data in a readily usable, portable format.

(2) PROVIDED DATA.—Upon receiving a verified request from an Individual, a Covered Entity shall, where technically feasible, make available a reasonable means for an Individual to transmit or Transfer Provided Data about the Individual retained by the Covered Entity to another Covered Entity in a structured, standardized, machine-readable, interoperable format, or otherwise download Personal Data in a readily usable format for the Individual's own use.

(3) THIRD-PARTY PROVIDED DATA, OBSERVED DATA, AND INFERRED 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(d), for Third-Party Provided Data, Observed Data or Inferred Data if the Transfer, transmission, or download of such data could—

(A) reasonably be expected to reveal confidential, proprietary or trade secret information, or other intellectual property; or

(B) provide a competitor with the benefit or value of Processing undertaken by the Covered Entity to the disadvantage of the Covered Entity.

---

[34] In contrast with access, correction, deletion, and other provisions in Article III, data portability is concerned primarily with competition. The Introduction to the Consumer Reports Model State Privacy Act, explains that data portability "requires companies to provide data in a format that could be easily transferred to a competing service, helping to improve competition among online services." Accordingly, different considerations and policy decisions inform the scope and desirability of the requirement. IAF has not conducted research regarding data portability or competition issues.

(e) BUSINESS CONTINUITY PLAN.—A Covered Entity shall identify those circumstances in which the inability of an Individual to access the Individual's Personal Data is reasonably likely to create a high or extreme level of Processing Risk. Where such Processing 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.

(f) EXCEPTIONS.—A Covered Entity shall not be required to make Personal Data available pursuant to this Section if—

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

(B) the Individual's Personal Data is—

(i) necessary for the legitimate uses identified in Sections 2.01(b)(2) or 2.01(b)(5); and

(ii) making the Personal Data available would be inconsistent with or undermine with such use; or

(C) the Personal Data—

(i) was previously deleted by the Covered Entity in compliance with documented data retention schedules;

(ii) constitutes confidential commercial information or trade secrets, including an algorithm used to make predictions, inferences, scores, or other decisions; or

(iii) a Covered Entity makes an individualized determination that fulfilling the request from the Individual would create Processing Risk or legitimate risk to the security, safety, free expression, or other rights of another Individual.

Section 3.05 RESPONSIBLE AND ACCESSIBLE REDRESS.

(a) CORRECTION OF PERSONAL DATA.—A Covered Entity shall, consistent with the requirements and exceptions in Section 3.04 of this Act, provide an Individual with a mechanism to dispute and resolve the accuracy or completeness of Personal Data. Upon receipt of a verifiable

request, a Covered Entity shall make commercially reasonable efforts to correct the inaccurate Personal Data.

(b) CHALLENGE AUTOMATED DECISION MAKING.—A Covered Entity shall provide an Individual with a mechanism to challenge Automated Decision Making when the Individual has reason to believe that the Individual suffered or is likely to suffer Adverse Processing Impact as a result of the Automated Decision Making.

(c) COMPLAINT PROCESS.—A Covered Entity shall provide an Individual with a mechanism to submit a complaint or inquiry regarding a Covered Entity's policies, processes, and procedures relating to the Processing of the Individual's Personal Data or compliance with this Act.

(d) ADDITIONAL REDRESS MECHANISMS FOR HIGH RISK PROCESSING.—A Covered Entity with annual revenue in excess of $100 million shall conduct and document an analysis before commencing any Processing Activity that creates a high or extreme 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 processing impact assessment required by Article V of this Act.

Section 3.06 DATA SECURITY.[35]

(a) A Covered Entity shall develop, document, and implement a comprehensive data security program that includes administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of Personal Data.[36] Such program shall be appropriate to the Covered Entity's size and complexity, the nature and scope of the Covered Entity's activities, the nature of Personal Data Processed by the Covered Entity, and the level of Processing Risk.

[35] The IAF Model does not address data breach notification.

[36] Like Article 32 of the GDPR, the IAF Model recognizes encryption as a security technique that may help keep personal data safe, but does not state that encrypted data is no longer personal data; nor does the IAF model state that encrypted data is not governed by the law.

(b) In order to develop, document, and implement a data security program, a Covered Entity shall—

(1) identify reasonably foreseeable internal and external risks to the confidentiality, integrity, and availability of Personal Data that could result in the unauthorized access, disclosure, use, alteration, destruction, or other compromise of such data, and assess the sufficiency of any safeguards in place to control these risks;

(2) maintain ongoing awareness of data security, vulnerabilities, threats, and incidents;

(3) develop, document, and implement incident management policies, processes, and procedures that address incident detection, response, and recovery;

(4) develop, document, and implement safeguards to control reasonably foreseeable risks through risk assessment and regularly test or otherwise monitor the effectiveness of the safeguards' key policies, processes, and procedures; and

(5) evaluate and adjust the Covered Entity's data 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 data security program.

Section 3.07 PROCEDURES, EXCEPTIONS, AND RULE OF CONSTRUCTION.

(a) REASONABLE PROCEDURES.—

(1) A Covered Entity shall make available a reasonably accessible, conspicuous, and easy-to-use means for an Individual to exercise, at no cost to the Individual, each option required by Article III of this Act.

(2) A Covered Entity shall honor an Individual's request pursuant to Sections 3.02(a) and 3.02(b) of this Act without undue delay and no later than 7 business days following the request.

(3) With respect to a request or complaint filed by an Individual pursuant to Sections 3.02(c), 3.04(a), 3.04(c), 3.04(d), 3.05(a), 3.05(b), and

3.05(c) of this Act, a Covered Entity shall respond to the Individual without undue delay and no later than 30 days after receiving the request or complaint. The Covered Entity shall provide the Individual with sufficient information to understand and act upon the response.

(4) A Covered Entity shall establish an internal process whereby Individuals may appeal a refusal to take action on a request made pursuant to Article III of this Act within a reasonable period of time after the Individual's receipt of the response sent by the Covered Entity as required by Section 3.07 of this Act. The appeal process must be conspicuously available and as easy to use as the process for submitting such a request under Section 3.07 of this Act.

(b) EXCEPTIONS.—

(1) A Covered Entity shall not be required to comply with Sections 3.01(d), 3.02(c), 3.04(a), 3.04(c), 3.04(d), 3.05(a), and 3.05(b) of this Act if the Covered Entity determines with a reasonable degree of certainty, after completing and documenting a processing impact assessment pursuant to Article V of this Act, that the Processing will create no more than a very low level of Processing Risk.

(2) A Covered Entity shall not be required to comply with a request from an Individual or to respond to an Individual's complaint or inquiry if the Covered Entity has reason to believe and can demonstrate that such request, complaint, or inquiry is frivolous, vexatious, and in bad faith.

(3) If a Covered Entity relies on an exception provided for in Title III of this Act, the Covered Entity bears the burden of demonstrating that the Covered Entity qualifies for the exception. It is unlawful and an independent and separate violation of this Act for a Covered Entity to rely upon a specific exception as set forth in this Section without having a reasonable basis for such reliance.

(4) Journalism Exception.—With the exception of Section 3.06, nothing in this Article shall apply to the publication of newsworthy

information of legitimate public concern to the public by a Covered Entity, or to the processing or Transfer of information by a Covered Entity for that purpose.[37]

(c) RULE OF CONSTRUCTION.—Nothing in this Act shall be construed to require a Covered Entity to—

(1) take an action that would convert information that is not Personal Data into Personal Data; or

(2) delete, destroy, or de-identify data that is retained for backup or archival purposes to the extent that such systems are not and cannot be accessed in the ordinary course.

(d) WAIVER.—The options available to Individuals and remedies provided under Article III of this Act may not be waived or limited by contract or otherwise.

(e) RULEMAKING.—The Commission shall, within 1 year of enactment of this Act and in accordance with section 553 of title 5, United States Code, promulgate regulations to—

(1) modify or add additional exceptions and limitations to the requirements set forth in Article III;

(2) identify the categories of Personal Data, Sensitive Personal Data, and Third Parties that Covered Entities must identify pursuant to Section 3.01 and 3.04; and

(3) establish reasonable requirements for a Covered Entity to verify the identity of an Individual when submitting a request to a Covered Entity pursuant to Article III of this Act.

Article IV. ACCOUNTABLE PROCESSING[38]

[37] The Journalism Exception is from the Brookings Institution's proposed legislation, the Information Privacy Act – June 3, 2020, All bills have a similar exception for freedom of the press and speech protected by the First Amendment of the Constitution .

[38] Interoperability of legal frameworks is one of the objectives of the IAF Model. To that end, it is relevant to highlight that the principle of accountability is one of the central pillars of the GDPR. GDPR Article 5(2), Like the IAF Model, the accountability requirements place responsibility firmly on the controller (Covered Entity) to take proactive action to achieve compliance and to be ready to demonstrate that compliance. The IAF Model, however, provides more detail to help organizations meet their obligations and to help regulators enforce the law in a

Section 4.01 ACCOUNTABLE PROCESSING MANAGEMENT PROGRAM.

(a) PURPOSE.—A Covered Entity shall develop, document, and implement an accountable processing management program to—

(1) comply with the requirements of this Act, other applicable legal or regulatory requirements, and recognized industry practices;

(2) promote structured, effective, and consistent management and oversight of Processing across the Covered Entity;

(3) evaluate Processing Risk and the impacts of Processing on Individuals and competition and consider the interests of all relevant stakeholders when making determinations about Processing;

(4) manage risk, including Processing Risk, on an ongoing basis; and

(5) demonstrate the Covered Entity's ongoing commitment to trustworthy, fair, responsible, and transparent Processing.

(b) GUIDING PRINCIPLES FOR ACCOUNTABILITY AND DATA RESPONSIBILITY.—

(1) ESTABLISH STRATEGIC VISION.—A Covered Entity shall define, document, and publish guiding principles regarding Processing that identify, 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.

(2) SENIOR MANAGEMENT REVIEW AND APPROVAL.—The Board of Directors or equivalent senior governing body of a Covered Entity shall review and approve the guiding principles on an annual basis and require all Processing across the Covered Entity to align with the Covered Entity's guiding principles for accountability and data responsibility.

---

consistent and predictable fashion. Similarities with the IAF Model may also be found in the Singapore Personal Data Protection Act 2012, which places a significant emphasis on accountability.

(c) PROGRAM DEVELOPMENT AND IMPLEMENTATION.—An accountable processing management program shall include—

(1) a qualified senior executive to oversee the development, documentation, and implementation of the program;

(2) strategic planning that considers across the Covered Entity both Personal Data itself and related resources, such as personnel, equipment, funds, and information technology;

(3) ongoing collaboration between designated senior executives across different functions and lines of business to ensure coordination of risk management, business operations, legal and regulatory compliance, security, and Processing Activities;

(4) documentation demonstrating that a Covered Entity has an accountable Processing management 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—

(A) management and structure of the program;

(B) resources dedicated to the program;

(C) role and authority of designated accountable officials and staff; and

(D) strategic goals and objectives of the program; and

(5) resources, staff, policies, processes, and procedures that are reasonable and appropriate to—

(A) a Covered Entity's size and complexity;

(B) the nature and scope of a Covered Entity's activities;

(C) legal requirements and obligations that apply to such activities;

(D) the scale of a Covered Entity's Processing operations; and

(E) the sensitivity of Personal Data Processed and the level of Processing Risk created by the Covered Entity's Processing Activities.

(d) RESPONSIBLE DATA GOVERNANCE.—As part of an accountable processing management program, a Covered Entity shall—

(1) establish policies, processes, and procedures to ensure that Personal Data is managed and maintained according to applicable laws, industry codes of conduct, recognized industry practices, and the requirements of the accountable management program;

(2) properly and consistently manage Personal Data as required by policies, processes, and procedures throughout its lifecycle, including all stages of Processing, such as creation, collection, use, analysis, storage, maintenance, dissemination, disclosure, Transfer, and disposition;

(3) identify, distinguish, and 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;

(4) classify Personal Data, including Sensitive Personal Data;

(5) designate an accountable employee who can reliably describe how Personal Data is Processed throughout each Processing Activity; and

(6) maintain a current, complete, and accurate inventory of the Covered Entity's information systems and information holdings, including the Covered Entity's information systems that Process Personal Data.

Section 4.02 ETHICAL, TRUSTWORTHY, AND PREVENTATIVE DESIGN.[39]

(a) PROGRAM OBJECTIVES.—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 analyses, design principles, and controls in order to build and deliver a more trustworthy Processing Activity and minimize adverse effects, including Processing Risk.

(b) CORE REQUIREMENTS.—A trustworthy Processing Activity shall seek to—

[39] This approach generally aligns with GDPR, Article 25, Data Protection by Design and By Default, and the new relevant guidance, EDPB 2020A: European Data Protection Board, Guidelines on Article 25 Data Protection by Design and by Default (Version 2.0, 20 October 2020),

(1) enable reliable assumptions by the Covered Entity, Individuals, and other entities about data and data Processing in a given Processing Activity; and

(2) meet the specific Processing requirements for each Processing Action such that the outcome or result of the Processing Activity is predictable and is capable of mitigating Processing Risk as anticipated and required.

(c) PLANNING FOR TRUSTWORTHY DESIGN.—A Covered Entity shall, during the initial stages of any development process and throughout the various stages of the Processing Activity development lifecycle—

(1) inventory, incorporate, and apply the legal rules, industry best practices, contractual obligations, and internal requirements for the Processing of Personal Data as well as for anticipating and facilitating implementation of controls that may be necessary to support compliance;

(2) identify discrete Processing Actions within a given Processing Activity and determine which data Processing Actions may create Processing Risk and assess the level of Processing Risk;

(3) develop, document, and implement a repeatable and measurable decision-making process that covers the life of each Processing Activity and includes explicit criteria for analyzing the benefits and risks, including information security and Processing Risk, associated with each stage in the lifecycle of both Personal Data and supporting technologies; and

(4) consider and document the impact of decisions and actions in each stage of the lifecycle.

(d) ASSESS AND IMPLEMENT REQUIREMENTS.—For each Processing Activity, a Covered Entity should—

(1) determine the need or desirability for the Covered Entity to have the capability to review, identify, access, Transfer, segregate, tag, track, retrieve, alter, delete, and otherwise manage Personal Data;

(2) integrate the required or desired capabilities into the design to the extent practicable;

(3) manage or administer Personal Data 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 an Individual's preferences about use and Transfer of their Personal Data are implemented and maintained;

(4) conduct technical, process, and risk analyses of alternative design implementations in order to reduce risk and increase accountability;

(5) 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;

(6) avoid the use of Personal Data for testing Processing Activities to the extent feasible and implement controls to mitigate Processing Risk if Personal Data must be used;

(7) enable the Processing of data without association to Individuals or devices beyond the operational requirements of the Processing Activity through technical methods such as de-identification and rule-based restrictions on Processing; and

(8) develop public facing mechanisms for an Individual to interact with the Processing Activity or exercise choices as required by Article III of this Act that—

(A) are clear and easy-to-use;

(B) are designed to reduce the burden on an Individual;

(C) would meet the expectations of a reasonable Individual; and

(D) do not have the substantial effect of subverting or impairing user autonomy, decision-making, or choice.

Section 4.03 ACCOUNTABILITY FOR AUTOMATED DECISION MAKING

(a) GENERAL OBLIGATIONS FOR THE TRUSTWORTHY AND ACCOUNTABLE USE OF AUTOMATED DECISION MAKING.—A Covered Entity that

relies upon or uses Automated Decision Making to make or inform a decision or incorporates Automated Decision Making at any point in a decision making process shall—

(1) understand the reasoning behind the Automated Decision Making;

(2) exercise judgment in deciding whether to accept the results of Automated Decision Making;

(3) implement mechanisms and safeguards, such as capacity for human determination, that are appropriate to the use or application of the specific Automated Decision Making given the context and purpose of the use; and

(4) achieve overall fairness of making predictions about an Individual from group-level data in a given context and comply with this Section before such predictions are relied upon or used in anyway.

(b) SPECIFIC REQUIREMENTS FOR TRUSTWORTHY AND ACCOUNTABLE AUTOMATED DECISION MAKING.[40]—A Covered Entity engaged in Automated Decision Making shall develop, document, and implement policies, processes, and procedures to ensure that—

(1) Personal Data used in or for Automated Decision Making is labeled or traceable to enable analysis of the Automated Decision Making and to enable responses to an inquiry, appropriate to the context, including the level of Processing Risk;

(2) Automated Decision Making that makes predictions includes indications of reliability to assist decision makers with giving the prediction appropriate weight;

(3) Automated Decision Making tools are designed and built to mitigate bias in both the model and data and that proper protocols are in place

[40] Although the scope of the IAF Model with respect to Automated Decision Making and the recently released draft EU Regulation for High Risk AI Systems, are different, the goals and obligations set forth in the two documents generally line up, including requirements concerning the quality of data sets used, technical documentation and record-keeping, transparency and the provision of information to users, data governance, and defined risk assessments.

to promote transparency and accountability. Such protocols shall address, as appropriate the—

(A) validity of the Automated Decision Making, taking into account the context around how the Personal Data was collected and what kind of inference is being drawn;

(B) accuracy of the Automated Decision Making, taking into account the Automated Decision Making model's performance; and

(C) bias of the Automated Decision Making including examination of potential bias at different stages of Automated Decision Making, imperfect data quality, missing data, sampling bias, or other relevant factors.

(c) Policies, processes, and procedures to implement the requirements of this Section shall be documented in order to achieve consistent application across the Covered Entity and shall identify by name and title the Individual authorized to approve the use of Automated Decision Making.

Section 4.04 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—

(1) 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;

(2) require the Service Provider by contract to develop, document, and implement appropriate measures designed to meet the objectives and requirements of this Act;

(3) 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 Transferred such Personal Data to the Service Provider;

(4) require, as appropriate, managers and staff of the Service Provider to complete education, awareness, and training programs related to Processing; and

(5) exercise reasonable oversight and take reasonable actions to be in 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, 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 Transfer 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 a Third Party's 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 to or support for 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.

(d) ADDITIONAL REQUIREMENTS.—

(1) A Covered Entity shall designate a qualified employee to be responsible and accountable for each Service Provider or Third Party and to ensure compliance with this Section of the Act.

(2) A Covered Entity shall take reasonable actions to advise a Third Party or Service Provider that relies upon or uses Automated Decision Making created by the Covered Entity of the intended and appropriate use of the Automated Decision Making and determine whether that Third Party or Service Provider complies with or has policies, processes, and procedures in place to help comply with Section 4.03.

Section 4.05 WORKFORCE ACCOUNTABILITY.

(a) DESIGNATION OF RESPONSIBLE AND ACCOUNTABLE EMPLOYEES.—A Covered Entity shall designate one or more qualified employees who have organization-wide responsibility and accountability for developing, documenting, and implementing policies, processes, and procedures to ensure compliance with this Act. Designated employees shall exercise judgment whether their skills or expertise are sufficient to support the demands of this section and, if these skills or expertise are not sufficient, they shall decline to serve or obtain relevant education and training.

(b) AWARENESS AND TRAINING PROGRAMS.—A Covered Entity shall develop, document, and implement an appropriate education, awareness, and training program for all personnel, including employees and independent contractors.

(c) NEEDS ASSESSMENT.—A Covered Entity shall establish policies, processes, and procedures to assess and address the hiring, training, continuing education, and professional development needs of personnel, including employees and independent contractors, with roles and responsibilities related to compliance with this Act.

(d) INTERNAL ENFORCEMENT.—A Covered Entity shall develop, document, and implement policies, processes, and procedures to ensure

that all personnel, including employees and independent contractors, are held accountable for complying with organization-wide information security and Personal Data Processing requirements and policies, including processes and procedures for internal enforcement of the Covered Entity's policies and discipline for non-compliance.

Section 4.06 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 systematically—

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

(2) monitor compliance with internal policies, processes, and procedures and alignment with public representations;

(3) confirm that the Covered Entity's Processing Activities are conducted as planned;

(4) evaluate the effectiveness of the Covered Entity's compliance with this Act; and

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

(b) POTENTIAL CONFLICTS OF INTEREST.—A Covered Entity shall develop, document, and implement reasonable and appropriate policies, processes, and procedures to ensure that—

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

(2) an accountable official responsible for approving a processing impact assessment or approving a specific Processing Activity does 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

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

(c) HIGH RISK PROCESSING ACTIVITY.—A Covered Entity engaged in Processing that is likely to create a high or greater level of Processing Risk shall—

(1) create an internal data Processing review board to evaluate and approve new Processing Activities, including Automated Decision Making, that is reasonably likely to create 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

(2) seek external review and validation, including external audits and certifications of policies, processes, and procedures to ensure compliance with relevant laws, industry best practices, internal procedures, and the requirements of this Act.

(d) EVIDENCE OF OVERSIGHT.—A Covered Entity shall document the internal review, audit, and assurance programs in order to demonstrate how oversight was conducted and that, in fact, it was conducted.

(e) SENIOR MANAGEMENT ENGAGEMENT.—A Covered Entity shall maintain internal controls and reporting structures to ensure that appropriate senior management officials of the Covered Entity are involved in assessing risks, ensuring ongoing accountability, and making decisions that implicate compliance with this Act.

Article V. PROCESSING RISK MANAGEMENT

Section 5.01 RISK MANAGEMENT STRATEGY.[41]

(a) A Covered Entity shall develop, document, and implement a comprehensive Processing Risk management strategy to—

(1) manage reasonably foreseeable Processing Risk;

(2) identify and avoid unacceptable levels of Processing Risk; and

[41] As explained in the NIST Cybersecurity and Privacy Program, a well-defined risk management strategy supports a Covered Entity's comprehensive Accountable Processing Management Program.

(3) approve and authorize Processing or material modifications in Processing.

(b) The Processing Risk management strategy shall, at a minimum, include policies, processes, and procedures designed to enable a Covered Entity to—

(1) identify, assess, and document the level of Processing Risk created by a Processing Activity;

(2) mitigate Processing Risk;

(3) make and document an informed determination that the Processing Risk remaining after taking steps to mitigate such risk presents an acceptable level of Processing Risk;[42]

(4) monitor Processing Risk; and

(5) ensure the measures put in place to mitigate Processing Risk over time are—

(A) implemented correctly;

(B) operating as intended; and

(C) sufficient to ensure ongoing compliance with applicable requirements and to manage identified and evolving Processing Risk on a continual basis.

(c) Processing Risk management shall be conducted as an entity-wide activity to ensure that risk-based decision-making is applied consistently across the Covered Entity and integrated into each aspect of the Covered Entity's planning and operations related to Processing.[43]

Section 5.02 ASSESSMENT OF PROCESSING RISK.[44]

---

[42] "[P]rivacy risk assessments help organizations distinguish between privacy risk and compliance risk. Identifying if data processing could create problems for individuals, even when an organization may be fully compliant with applicable laws or regulations, can help with ethical decision-making in system, product, and service design or deployment. . . . This facilitates optimizing beneficial uses of data while minimizing adverse consequences for individuals' privacy and society as a whole, as well as avoiding losses of trust that damage organizations' reputations, slow adoption, or cause abandonment of products and services." NIST Privacy Framework at p. 5.

[43] The NIST Privacy Framework recommends that the process of framing risk be conducted at an enterprise level. This process identifies executive level assumptions affecting risk assessments, risk responses, and risk monitoring; Priorities and trade-offs considered by the organization for managing risk; and organizational risk tolerance. NIST Privacy Framework, Appendix D,

[44] The GDPR, and Virginia's new Consumer Data Protection Act, also require Data Protection Assessments or Privacy Impact Assessments, which require a risk/benefit analysis of a processing activity. However, those laws fail

To assess the likelihood that Adverse Processing Impact will occur as a result of Processing, a Processing Activity, or a Processing Action and the degree, magnitude, or potential severity of the Adverse Processing Impact, should it occur,[45] a Covered Entity shall identify and inventory each piece of data to be Processed and evaluate, at a minimum, the following 13[46] factors—

(a) USE AND UTILITY.—A Covered Entity shall evaluate the use and utility of the Personal Data alone or in combination with other data, including—

(1) the specific, intended purpose and use for Processing;

(2) other potential and likely uses of the Personal Data; and

(3) potential unlawful uses and the likelihood of such uses.

(b) ADVERSE PROCESSING IMPACT.—A Covered Entity shall evaluate the Adverse Processing Impact that may be caused by Processing Personal Data alone or in combination with other data, considered from the perspective of the Individual and taking into account the full range of potential Adverse Processing Impacts identified in Section 1.03(a) of this Act.

---

to adequately explain the risk to be evaluated and the factors to be considered when assessing risk, creating uncertainly for companies and consumers alike. The detail included here is intended to promote consistency for risk assessments and build confidence in the process. This in turn will help Covered Entities effectively and efficiently mitigate risk and meet compliance obligations. It should also promote predictable enforcement by regulators.

[45] The NIST Privacy Framework approach to privacy risk is to consider "*privacy events* as potential problems individuals could experience arising from system, product, or service operations with data, whether in digital or non-digital form, through a complete life cycle from data collection through disposal." NIST Privacy Framework, at p. 3. Once an organization can identify the likelihood of any given problem arising from the data processing, which the Privacy Framework refers to as a *problematic data action* it can assess the impact should the problematic data action occur.

[46] Nothing in Section 5.02 is new. Indeed, IAF identified an even more comprehensive set of issues and risk factors in IAF's efforts to help companies conduct ethical data impact sssessmens. See, Ethical Data Impact Assessments and Oversight Models January 2019.

(c) INDIVIDUAL MITIGATION.—A Covered Entity shall evaluate the extent to which an Individual—

(1) is dependent on the outcome of the Processing or Processing Activity, in particular because, for practical or legal reasons, it is not reasonably possible to opt-out from that outcome; and

(2) would be able to discover, mitigate, and fully resolve any Adverse Processing Impact caused by Processing, taking into account the resources that would be required for an Individual to resolve any Adverse Processing Impact and obtain full redress.

(d) VOLUME AND SENSITIVITY OF PERSONAL DATA.—A Covered Entity shall evaluate the volume and sensitivity of Personal Data, including—

(1) the extent to which the Processing involves Sensitive Personal Data;

(2) the number of Individuals whose Personal Data is or may be Processed; and

(3) the amount of Personal Data Processed about each Individual.

(e) IDENTIFIABILITY AND LINKABILITY.—A Covered Entity shall evaluate identifiability and linkability of the Personal Data, including—

(1) the extent to which a given data set is linked or linkable to an Identifiable Individual or an Individual can be identified from a given data set; and

(2) the extent to which a given data set is intended to be linked to an Identifiable Individual at a future date or by another person.

(f) SOURCES AND ACCURACY OF PERSONAL DATA.—A Covered Entity shall evaluate the sources and accuracy of Personal Data, including—

(1) the number of distinct sources of Personal Data;

(2) whether the Personal Data includes Provided Data, Third-Party Provided Data, Observed Data, and Inferred Data;

(3) for Provided Data, the circumstances in which an Individual provided the Personal Data;

(4) for Third-Party Provided Data, Observed Data, or Inferred Data, whether the Individual was or could have been aware of the Personal Data or the Processing;

(5) the extent to which new Personal Data is created; and

(6) the reliability of sources and the verifiability of the accuracy of the Personal Data for the intended purpose.

(g) DURATION OF PROCESSING.—A Covered Entity shall evaluate the duration of Processing, including—

(1) the duration, period of time, or frequency of the Processing Activity, ranging from a one-time use or single transaction to ongoing, persistent, and systemic Processing; and

(2) the duration and methods for which Personal Data or the results of Processing Personal Data are stored.

(h) REASONABLE PRIVACY EXPECTATIONS.—A Covered Entity shall evaluate the extent to which the Personal Data—

(1) would reasonably be considered personal, private, or of an intimate nature under the circumstances; and

(2) is related to activities or communications 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, mobile home, or interior cabin of an Individual's personal automobile.

(i) EXTENT OF ACCESS, SHARING, DISCLOSURE, OR TRANSFER.—A Covered Entity shall evaluate the extent of access, sharing, disclosure, or Transfer, including—

(1) the intended scope of authorized access;

(2) the extent to which Personal Data will be Transferred to one or more Third Parties and the category or categories of such Third Parties, including whether the Personal Data will be Transferred to local, state, or federal government agencies and the purpose for which such government agency will use the Personal Data;

(3) intended public disclosure of Personal Data or widespread dissemination; and

(4) the extent to which Personal Data will be Transferred to one or more jurisdictions outside the United States.[47]

(j) VULNERABLE POPULATIONS.—A Covered Entity shall evaluate the extent to which the Processing targets or otherwise involves an identifiable or inferred vulnerability or potentially vulnerable population or the Adverse Processing Impact arising from Processing disproportionally affects a vulnerable population. For the purpose of this Act, vulnerable populations include children[48]; the elderly; Individuals with a serious health condition, impairment, cognitive deficiency, or disability; victims of certain crimes; deployed members of the military and their families; communities recovering from crisis or disaster; or groups facing undue economic hardship.

(k) RELIANCE ON AUTOMATED DECISION MAKING.—A Covered Entity shall evaluate the extent to which a Covered Entity uses or relies upon Automated Decision Making and the level of confidence that the Automated Decision Making is sufficiently accurate and appropriate for the intended use.

(l) CONSISTENT WITH THE CONTEXT.—A Covered Entity shall evaluate the extent to which the Processing is Consistent with the Context of the relationship between the Individual and the Covered Entity.

---

[47] In contrast with EU law, Covered Entities are not expected to verify, on a case-by-case basis, whether the law of the third country of destination ensures an adequate level of protection for Personal Data. See, e.g., GDPR Article 45(1). On the other hand, a Covered Entity should assess the potential risk of adverse processing impact to Individuals or specific categories of Individuals when Transferring Personal Data outside of the United States. For example, in some jurisdictions simply being a member of a particular minority group or expressing certain opinions could create a significant risk of harm. A Covered Entity should consider this type of risk before transferring Personal Data to such a jurisdiction. Here again, context is highly relevant, and a general rule cannot be applied to all circumstances. This provision should not in any way be interpreted as a data localization requirement.

[48] IAF believes that children's privacy is a critically important issue but chose not to address this issue in the IAF Model. There are many ongoing initiatives related to children's privacy. IAF has not conducted research in this area and does not have any particular expertise with respect to processing data about children. IAF anticipates that children's privacy would be addressed in a separate law or be incorporated into a law based on the framework codified in the IAF Model.

(m) LEGAL OBLIGATIONS.—A Covered Entity shall evaluate all statutory, regulatory, contractual, and other legal obligations or restrictions that may apply to the Processing.

Section 5.03 CATEGORIZATION OF PROCESSING RISK.

(a) LEVELS OF RISK.—When conducting a processing impact assessment, a Covered Entity shall categorize the level of Processing Risk as very low, low, moderate, high, or extreme.

(b) For the purpose of this Act, the term "extreme" refers to a severe, dire or catastrophic Adverse Processing Impact that results in—

(1) loss of life;

(2) life threatening or incapacitating injury, illness, or health condition;

(3) restriction of freedom, including incarceration, quarantine, involuntary commitment, limitations on travel or movement, or forced relocation;

(4) separation or isolation from family members; or

(5) infringement of a right guaranteed by the Constitution of the United States.

(c) 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.

(d) No Covered Entity shall be held liable for a violation of this Act solely for incorrectly categorizing the level of risk for a particular Processing Activity if the Covered Entity establishes by a preponderance of the evidence that the Covered Entity maintained reasonable policies, processes, and procedures to identify, assess, document, and mitigate risk as required by Article V of this Act.

Section 5.04 PROCESSING IMPACT ASSESSMENTS.[49]

[49] The IAF believes that a decision is not risk-based unless there is a measurement of the risks and benefits at issue and the integrity of the assessment is demonstrable to others. Risk/benefit decisions are not always intuitive. They require assessments that identify: the parties that might be impacted by the use of data, how they might be impacted, and whether the risks and benefits are mapped to the people, groups of people and society. Decisions must be explainable to others based on objective measures.

(a) WHEN TO CONDUCT.—A Covered Entity shall conduct and document a processing impact assessment when, at a minimum, Processing or a Processing Activity—

(1) is reasonably likely to create a moderate or greater level of Processing Risk;

(2) involves new or novel methods of Automated Decision Making or an application of Automated Decision Making that is not widely in use in commerce; or

(3) is conducted for a legitimate use as defined in Sections 2.01(b)(8), 2.01(b)(9), or 2.01(b)(10) of this Act unless the Covered Entity determines with a reasonable degree of certainty that the Processing or Processing Activity will create no more than a very low level of Processing Risk.

(b) REQUIRED ANALYSIS.— At a minimum, a processing impact assessment shall analyze and explain—

(1) the purpose, mission, business needs, and objectives of the Processing Activity;

(2) the functional needs or capabilities of the Processing Activity;

(3) the Adverse Processing Impact that may be created by the Processing Activity, taking into account the full range of potential Adverse Processing Impact identified in Section 1.03(a) of this Act;

(4) the level of Processing Risk that may be created by the Processing Activity, taking into account the 13 factors identified in Section 5.02;[50]

(5) the administrative, technical, and physical controls, safeguards, and other measures implemented to mitigate Processing Risk and other

[50] NIST explains that a risk assessment should "[d]etermin[e] the likelihood and impact of adverse effects on individuals arising from the processing of [personal data]." NIST Security and Privacy Controls for Information Systems and Organizations, 800-53, Revision 5 (September 2020), at p. 240.

risk throughout the lifecycle of the Personal Data and Processing Activity;

(6) the level of Processing Risk remaining after all practicable and reasonable measures are taken to mitigate Processing Risk;

(7) the Covered Entity's decision that the Processing Risk remaining presents an acceptable level of Processing Risk;

(8) the Benefits to Individuals or Competition; and

(9) the Covered Entity's decision to authorize and approve Processing and the basis for that decision, including the factors that support Processing despite the designated level of Processing Risk.

(c) TIMING.—

(1) A processing impact assessment shall be completed and documented before a Covered Entity begins Processing.

(2) Processing impact assessments shall be 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.

(d) ACCOUNTABLE OFFICIAL. —A Covered Entity shall designate one or more qualified employees who are authorized to accept risk. A processing impact assessment shall identify the employee who approved the level of Processing Risk and authorized Processing.

Section 5.05 ENHANCED PROCESSING IMPACT ASSESSMENT TO ASSESS IMPLICATIONS OF AUTOMATED DECISION MAKING.

(a) A Covered Entity shall conduct an enhanced processing impact assessment before the Covered Entity relies on Automated Decision Making unless the Covered Entity concludes with a reasonable degree of certainty that the any Processing which relies upon Automated Decision Making is unlikely to create a moderate or greater level of Processing Risk.

(b) An enhanced processing impact assessment shall, in addition to the requirements set forth in Section 5.04 of this Act—

(1) enable a relevant employee or other person to see how and why an Automated Decision Making model produced the specific outcome;

(2) provide attestation that Automated Decision Making models and insights have been tested, to the extent practicable, for accuracy and predictability;

(3) identify the specific Individual or body who has ultimate decision-making authority for the use of Automated Decision Making or reliance upon Automated Decision Making;

(4) identify potentially biased data sets and assess the desirability of modifying or not using the data set;

(5) detect and proactively mitigate bias, including potential bias that may develop or evolve as models learn or adapt to new experiences or stimuli;

(6) detect and proactively mitigate discrimination;

(7) determine the useful life of each Automated Decision Making output;

(8) explain how the Covered Entity considered and implemented the requirements set forth in Sections 4.03 and 4.04 of this Act; and

(9) confirm that an appropriate mechanism has been established to enable an Individual to challenge an adverse outcome created by the use or application of Automated Decision Making as required by Section 3.05(b) 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 and separate violation of this Act to—

(a) misrepresent, expressly or by implication, that a processing impact assessment or enhanced processing impact assessment was completed before the commencement of Processing;

(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; or

(c) omit material facts from a privacy impact assessment that are likely to impact or influence the analysis required by Sections 5.04 or 5.05 of this Act.

Section 5.07 RULEMAKING.

The Commission shall, within 18 months of enactment of this Act and in accordance with section 553 of title 5, United States Code, promulgate regulations with respect to the assessment and categorization of Processing Risk consistent with the purposes of this Act.

Article VI. ENFORCEMENT BY COMMISSION AND STATE ATTORNEYS GENERAL

Section 6.01 ENFORCEMENT BY COMMISSION.[51]

(a) IN GENERAL.—A violation of this Act or any regulation prescribed under this Act shall be treated as a violation of a rule under section 18 of the Federal Trade Commission Act (15 U.S.C. 57a) regarding unfair or deceptive acts or practices. Except where the Commission has been expressly granted additional authority under this Act, the Commission shall enforce this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act.

(b) CIVIL PENALTIES.—

(1) Any Covered Entity, other than a non-profit organization as defined in Section 1.03(h)(1)(C) of this Act, who violates the specific provisions of this Act as set forth in Section 6.01(b)(3) below or any regulation prescribed under this Act shall be subject to the penalties and entitled

[51] Strong, consistent, and flexible enforcement is essential to make sure that Covered Entities comply. There is bipartisan consensus that the limited tools available to the FTC today are inadequate to address the evolving consumer protection, privacy and data security challenges of the digital economy.

to the privileges and immunities provided in the Federal Trade Commission Act as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of this Act.

(2) In considering whether a civil penalty is in the public interest, the Commission shall consider—

(A) 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;

(B) the severity of Adverse Processing Impact to Individuals resulting either directly or indirectly from such act or omission;

(C) the level of Processing Risk created by the relevant Processing Activity and the extent to which the Covered Entity took reasonable steps to mitigate the Processing Risk;

(D) the history of previous violations or unlawful conduct;

(E) the size, financial resources, and good faith of the Covered Entity charged;

(F) the need to deter such Covered Entity from committing such acts or omissions; and

(G) such other matters as justice may require.

(3) VIOLATIONS SUBJECT TO CIVIL PENALTIES.—

(A) Upon the effective date of this Act, a Covered Entity may be subject to civil penalties for violations of Sections 2.01(a), 2.01(c), 2.02(a), 2.02(c), 2.03, 3.01(a), 3.01(b), 3.02, 3.04(a)3.04(b), 3.04(c), 3.05(a), 3.06,4.01(b), 4.02(c), 4.03, 4.04, 4.05, and 4.06(d).

(B) Upon the effective date of this Act, a Covered Entity engaged in Processing that creates a high or extreme level of Processing Risk may be subject to civil penalties for violations of Sections 4.01(c), 4.01(d), 4.02(d), and 5.06.

(C) In addition to the civil penalties provided for in 6.02(b)(1) and 6.02(b)(3) above, beginning 2 years after the effective date of this Act, a Covered Entity may be subject to civil penalties for violations of each Section in Articles III, IV, and IV.

(4) CIVIL PENALTY CAP.—

(A) Notwithstanding Sections 6.01(b)(1) and (3) above, no civil penalty shall be imposed under this Act in excess of $1,000,000,000 arising out of the same acts or omissions.

(B) The civil penalty cap set forth in this Section does not apply to—

(i) civil penalties related to a violation of a Commission order or otherwise imposed pursuant to statutes or regulations enforced by the Commission; and

(ii) acts or omissions that constitute independent and separate violations of this Act as set forth in Sections 2.03, 3.02(e), 3.04(b)(2), 3.07(b)(3), 4.04(c), and 5.06 of this Act.

(c) EQUITABLE RELIEF.—In any action or proceeding brought or instituted by the Commission under this Act, the Commission may seek, and any Federal court using its full equitable powers may grant, such equitable relief that may be appropriate or necessary to obtain monetary or other relief for past harm or injury, to prevent further violations of this Act, or as otherwise may be in the public interest. Such equitable remedies may include—

(1) temporary restraining order;

(2) preliminary or permanent injunction;

(3) cease-and-desist order;

(4) rescission or reformation of contracts;

(5) refund of money or return of property;

(6) redress, restitution, or disgorgement of profits;

(7) public notification requiring that a Covered Entity make accurate information available through disclosures, direct notification or

education, or publish educational information reasonably related to the violations;

(8) other remedies reasonably related to the unlawful practices conducted by the Covered Entity, as may be necessary to provide complete relief in light of the purposes of this Act or prevent future violations of this Act; and

(9) such other and further equitable relief as the court deems appropriate.[52]

(d) LIABILITY AND ACCOUNTABILITY FOR INDIVIDUALS IN POSITIONS OF AUTHORITY.—

(1) An Individual may be liable for a violation of this Act upon a showing that the Individual—

(A) had authority to direct or control the Covered Entity's acts or practices; and

(B) had actual knowledge of the Covered Entity's improper acts or practices; or

(C) exercised reckless, sustained, and systematic failure to exercise oversight.

(2) An Individual shall not be liable for civil penalties under this Act unless—

(A) the Individual knowingly violated this Act; and

(B) the Individual's unlawful conduct created a high or extreme level of Processing Risk and caused significant Adverse Processing Impact.

(e) ENFORCEMENT AUTHORITY PRESERVED.—Nothing in this Section shall be construed to affect any authority of the Commission under any other provision of this Act or other law. Remedies provided in this Section are in addition to, and not in lieu of, any other remedy or right of action otherwise provided by this Act or any other provision of law.

[52] This provision explicitly provides the FTC with the authority to seek equitable remedies, including monetary relief. Among other things, this provision restores the FTC with the authorities struck down by the US Supreme Court in AMG Capital Management, LLC v. FTC, and eliminates any further ambiguities in the FTC Act, 15 U.S.C. § 45 et seq., with respect to the FTC's authority to seek equitable remedies.

(f) STAY OF ENFORCEMENT.—The Commission may stay enforcement of one or more specific provisions of this Act for no more than 1 year after the effective date upon finding that such stay is in the public interest. The stay shall apply to all entities that are authorized to enforce this Act.[53]

(g) JURISDICTION OVER COMMON CARRIERS AND NON-PROFIT ORGANIZATIONS.—Notwithstanding Sections 4, 5(a)(2), or 6 of the Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2), 46) or any jurisdictional limitation of the Commission, the Commission shall enforce this Act with respect to—

(1) common carriers subject to the Communications Act of 1934 (47 U.S.C. 151 et seq.); and

(2) organizations not organized to carry on business for their own profit or that of their members, as defined in Section 1.03(h)(1)(C) of this Act.

(h) INDEPENDENT LITIGATING AUTHORITY.—The Commission is authorized to litigate cases, by its own attorneys, before any federal court or tribunal within the judicial branch of the United States in order to enforce the provisions of this Act and rules thereunder, and includes authority to commence, defend, intervene in, or appeal any action, suit, or proceeding to which the Commission is a party; enter and enforce orders issued for violations of this Act; litigate court orders related to proceedings to enforce this Act; and argue appeals of such orders or court decisions related to enforcement of this Act.

Section 6.02 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

[53] This provision authorizes the FTC to extend the enforcement grace period from 2 years to 3 years in the event the FTC does not complete the rulemaking on time or for other reasons in the public interest.

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—

(1) enjoin further violation of this Act by the defendant;

(2) compel compliance with this Act;

(3) obtain damages, restitution, or other compensation on behalf of the residents of the State;

(4) obtain civil penalties in the amount determined and consistent with the requirements under Section 6.01(b) above; and

(5) obtain such other relief as the court using its full equitable powers deems appropriate.

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

(1) intervene in such action; and

(2) upon intervening—

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

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

(c) PREEMPTIVE ACTION BY COMMISSION.—If the Commission institutes a civil action for violation of this Act or a regulation promulgated under this Act, no attorney general of a State may bring a civil action against any defendant named in the complaint of the Commission for the violations of this Act or a regulation promulgated pursuant to this Act alleged in the complaint.

Section 6.03 SAFE HARBOR PROGRAMS FOR RESPONSIBLE AND ACCOUNTABLE COVERED ENTITIES.

(a) IN GENERAL.—Industry groups or other persons may apply to the Commission for approval of self-regulatory programs (‘‘safe harbor programs’’) that provide guidance to Covered Entities on how to comply with requirements and obligations of this Act in the context of

specific industries, subsectors, technologies, or Processing Activities. A safe harbor program may address compliance with the entire Act or may be narrowly tailored to address compliance with one or more specified provisions of the Act.

(b) CRITERIA FOR APPROVAL OF PROGRAM GUIDELINES.—To be eligible for approval by the Commission, a safe harbor program shall, at a minimum—

(1) specify clear and enforceable requirements for a Covered Entity participating in the safe harbor program that provide substantially the same or greater protections as those contained in the relevant provisions of this Act;

(2) require each participating Covered Entity to post in a prominent place a clear and conspicuous public attestation of compliance;

(3) require a process for the independent assessment of a participating Covered Entity's compliance with the safe harbor program prior to attestation and on an annual basis; and

(4) take meaningful action for non-compliance with the safe harbor program or with relevant provisions of this Act by any participating Covered Entity.

(c) EFFECT OF APPROVAL.—A Covered Entity that complies with a safe harbor program approved by the Commission shall be deemed to be in compliance with the provisions of this Act addressed by such program.

(d) EFFECT OF NON-COMPLIANCE.— A Covered Entity that has certified compliance with an approved safe harbor program and is found not to be in compliance with such program by the Commission shall be considered to be in violation of the section 5 of the Federal Trade Commission Act (15 U.S.C. § 45) prohibition on unfair or deceptive acts or practices.

(e) RULEMAKING.—The Commission shall, within 1 year of enactment of this Act and in accordance with section 553 of title 5, United States Code, promulgate regulations to implement this Section of the Act. The

regulations by the Commission shall, at a minimum, identify the procedures for such safe harbor programs to be submitted to the Commission for approval and the criteria by which the Commission shall review, reject, or approve the proposed program in whole or in part.

Section 6.04 SAFE HARBOR FOR ACCOUNTABLE SMALL BUSINESS AND NON-PROFIT ORGANIZATIONS.

(a) A Covered Entity shall not be subject to enforcement as set forth in Article VI of this Act where the Covered Entity—

(1) is engaged in interstate commerce and independently owned and operated; or

(2) operates across states and meets the definition of non-profit set forth in section 501 of title 26, United States Code; and

(3) Processes Personal Data of fewer than 50,000 Individuals in any 12-month period;

(4) does not derive 50% or more of its annual revenue from selling or licensing Personal Data; and

(5) engages only in Processing that is likely to create no more than a moderate level of Processing Risk.

(b) MINIMUM REQUIREMENTS.—In order to be subject to the safe harbor, a Covered Entity shall make a legally enforceable public representation that the Covered Entity meets the criteria of Section 6.04(a) and has taken reasonable steps to confirm that the representation is and remains true as long as the Covered Entity relies on the safe harbor.

Section 6.05 ACCOUNTABILITY REPORTS AND ASSESSMENTS.

(a) AUTHORITY TO OBTAIN INFORMATION AND DOCUMENTS.—

(1) In addition to its existing authority pursuant to the Federal Trade Commission Act and other laws enforced by the Commission, including this Act, the Commission shall have the authority to require, by special orders, a Covered Entity, other than a non-profit

organization as defined in Section 1.03(h)(1)(C) of this Act, to file with the Commission, in such form as the Commission may prescribe, reports or answers in writing to specific questions, furnishing to the Commission such information as it may require as to the Covered Entity's—

(A) business operations;

(B) Processing Activities; and

(C) policies, processes, and procedures developed, documented, and implemented by the Covered Entity to meet the requirements of this Act.

(2) The Commission may seek such information, as it deems necessary to ensure that commercial practices are consistent with the requirements of this Act, assess compliance, determine whether a violation of law exists, gather information necessary to support the report to Congress as required by Section 7.04 of this Act, or for other reports to Congress or the Executive Branch. Information sought must be reasonably relevant to the Commission's mission, the purposes of this Act, and in the public interest. Special orders issued pursuant to this Section shall be reasonable and shall not impose an undue burden on a Covered Entity.

(3) Reports and answers shall be made under oath, or otherwise, as the Commission may prescribe, and shall be filed with the Commission within such reasonable period as the Commission may prescribe.

(4) The Commission's authority to obtain information pursuant to this Section shall not be subject to the Paperwork Reduction Act (44 U.S.C. 3501-3520).

(b) REVIEW OF RECORDS.—All final records, documents, or assessments 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 review by representatives of the Commission as the Commission deems necessary or appropriate in the public

interest, for the protection of Individuals, or otherwise in furtherance of the purposes of this Act.

(1) PROCEDURES.—A Covered Entity shall have the same right to challenge an order issued pursuant to this Section and seek judicial review of a decision by the Commission as provided for Commission orders issued pursuant to Section 6(b) of the Federal Trade Commission Act (15 U.S.C. 46(b)).

Section 6.06 IMPLEMENTING REGULATIONS TO SUPPORT ACCOUNTABILITY.

(a) AUTHORITY.—The Commission 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 Commission may implement such additional exclusions from this Act as the Commission considers consistent with the purposes of this Act and in the public interest.

(c) CRITERIA FOR ISSUANCE OF RULES.—

(1) In promulgating regulations, the Commission shall consider—

(A) the potential Processing Risk to Individuals and society arising from a particular act or practice;

(B) the potential benefits to Individuals and competition arising from the particular act or practice; and

(C) that compliance with such regulations must allow for flexibility in implementation and be reasonable and appropriate for a Covered Entity taking into account—

(i) the size, resources, and complexity of the Covered Entity;

(ii) the nature and scope of the Covered Entity's Processing Activities;

(iii) the potential level of Processing Risk created by such Processing; and

(iv) the burden on a Covered Entity that is a non-profit organization as defined in Section 1.03(h)(1)(C) of this Act.

(d) TECHNOLOGY NEUTRAL.—In promulgating such regulations, the Commission 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.

(e) MANDATORY REVIEW.—The Commission shall evaluate the need for modifications to the regulations promulgated to implement this Act as warranted and, at a minimum, every 3 years.

Article VII. COMMISSION EDUCATION, GUIDANCE, OUTREACH, AND REPORTS

Section 7.01 CONSUMER EDUCATION.

In order to protect Individuals' personal information and to ensure that Individuals have the confidence to take advantage of the many benefits of products offered in the marketplace, the Commission 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 provided for by this Act.

Section 7.02 GUIDANCE AND OUTREACH FOR COVERED ENTITIES.

(a) GUIDANCE.—The Commission shall publish guidance, training materials, proposed best practices, and other resources designed to assist Covered Entities with coming into compliance with 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) SMALL BUSINESS SUPPORT.—Recognizing that small businesses make up a large and vital segment of the U.S. economy, the Commission shall develop and implement guidance and resources specifically designed to help small businesses meet their obligations under this Act and shall undertake outreach efforts to ensure that small businesses are aware of their obligations under the Act and the resources available to support small businesses.

(c) The Commission shall establish a mechanism for a Covered Entity to submit an inquiry to the Commission regarding compliance with this Act. To the extent practicable and in the public interest, the Commission shall make available to the public the Commission's responses to such inquiries and shall take such inquiries into account when developing guidance and educational materials for Covered Entities. Responses may take the form of a Commission staff opinion letter or such other form as the Commission determines meets the objectives of this Section and purposes of this Act.

Section 7.03 INTERNATIONAL COOPERATION FOR THE PROTECTION OF PERSONAL DATA.[54]

The Commission shall, consistent with its current authorities, endeavor to cooperate and coordinate with foreign agencies and provide such agencies with information regarding this Act to foster—

(a) understanding of the protections for Personal Data and Individuals under this Act;[55]

[54] In an effort to develop a framework that will be interoperable with legal regimes around the world, IAF looked to principles published by non-governmental organizations such as the OECD and APEC, as well as legal frameworks in the EU, Canada, Australia and Asia. Many concepts have been ported from GDPR, including the definitions of personal data and processing.

[55] Accountability is a basic tenet of 21st century data protection law and governance across the globe. It is referenced explicitly GDPR, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA, the APEC Privacy Framework, Advisory Guidelines on Key Concepts in the new Singaporean Personal Data

(b) consistency in the interpretation and enforcement for the protection of Personal Data;

(c) cooperation and convergence toward best practices with respect to Processing covered by this Act; and

(d) timely evaluation of complaints with respect to alleged violations of this Act, subject to rules and restrictions as the Commission may determine, from Individuals regardless of country of residency.

Section 7.04 REPORT.

Not later than 3 years after the date of enactment of this Act, the Commission shall transmit to Congress a report describing the Commission's use of and experience with the authority granted by this Act, along with any recommendations for revisions to the Act or additional legislation. The report shall include—

(a) the number of complaints related to the Processing of Personal Data or alleged violations of this Act received by the Commission;

(b) the number of investigations initiated by the Commission related to the Processing of Personal Data and suspected violations of this Act;

(c) the number of enforcement actions initiated by the Commission for alleged violations of this Act and a summary of such enforcement actions;

(d) the Commission's efforts to coordinate with State Attorneys General regarding enforcement of this Act;

(e) the status of any rulemaking proceedings undertaken pursuant to this Act;

(f) the Commission's efforts to provide guidance to Covered Entities, including small sized Covered Entities as provided for in Section 7.02(b) of this Act;

(g) the Commission's efforts to provide education to Individuals as provided for in Section 7.01 of this Act;

Protection Act, and draft legislation introduced in Canada, An Act to Enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act, as an update to PIPEDA.

(h) the Commission's efforts to support the effective implementation and application of the safe harbor provisions of this Act, including approval of codes of conduct, as provided for in Section 6.03 of this Act;

(i) the Commission's exercise of its authority under Section 6.04 of this Act to undertake assessment reviews; and

(j) Commission resources allocated to the implementation and enforcement of this Act and an assessment of the adequacy of such resources.

Article VIII. COMMISSION RESOURCES AND AUTHORIZATION OF APPROPRIATIONS

Section 8.01 APPOINTMENT OF ADDITIONAL PERSONNEL.

(a) Notwithstanding any other provision of law, the Chair of the Commission may, without regard to the civil service laws (including regulations), appoint additional personnel for the purpose of enforcing this Act and otherwise meeting the Commission's obligations under this Act, including—

(1) 250 additional personnel in attorney positions; and

(2) 250 additional personnel in project management, technical, and administrative support positions.

(b) COMPENSATION.[56]—Notwithstanding any otherwise applicable provision of title 5, United States Code, concerning compensation, including the provisions of chapter 51 and chapter 53, the following provisions shall apply with respect to employees appointed pursuant to this Act or employed by the Commission for the purpose of enforcing this Act and otherwise meeting the obligations under this Act—

[56] This provision would bring the salaries of FTC staff in line with equivalent staff at financial regulators, which is approximately 30% more than other federal government employees. This is necessary for the FTC to be able to compete for resources with technology companies and law firms. This provision is based on a proposal by former FTC Chairman William E. Kavocic, Jones, Alison and Kovacic, William E., The Institutions of U.S. Antitrust Enforcement: Comments for the U.S. House Judiciary Committee on Possible Competition Policy Reforms (June 4, 2020).

(1) the rates of basic pay for all employees hired pursuant to paragraph (a) may be set and adjusted by the Chair of the Commission;

(2) the Chair of the Commission shall at all times provide compensation (including benefits) to each class of employees that, at a minimum, are comparable to the compensation and benefits then being provided by the Board of Governors for the corresponding class of employees; and

(3) all such employees shall be compensated (including benefits) on terms and conditions that are consistent with the terms and conditions set forth in section 11(l) of the Federal Reserve Act (12 U.S.C. 248(l)).

Section 8.02 AUTHORITY TO ESTABLISH NEW BUREAU OR OFFICE.

The attorneys and support personnel appointed pursuant to Section 8.01 of this Act shall be assigned to the Bureau of Consumer Protection or such other bureau or office as the Chair may create, taking into account—

(a) the efficient and effective application of Commission resources;

(b) avoidance of duplicative functions;

(c) impact on the Commission's ability to carry out its dual mission of protecting consumers and promoting competition; and

(d) the public interest.

Section 8.03 AUTHORIZATION OF APPROPRIATIONS.

There is authorized to be appropriated to the Commission such sums as may be necessary to carry out this Act.

Article IX. PREEMPTION[57]

Section 9.01 PREEMPTION.

For a Covered Entity subject to this Act, the provisions of this Act shall preempt any civil provisions of the law of any State or political subdivision

[57] IAF generally supports the concept of preemption. Consistent national privacy standards would benefit both individuals and industry. Article IX provides an example of language that may help policymakers address this complex issue but should not necessarily be interpreted as language endorsed by IAF. IAF believes that the substantive provisions of any framework should be addressed first so that the scope of the bill can inform discussions regarding preemption and related matters.

of a State to the degree they are focused on the reduction of Processing Risk through the regulation of Personal Data Processing Activities.

Section 9.02 EFFECT ON OTHER LAWS.

(a) CONSUMER PROTECTION LAWS.—Except as provided in Section 9.01, this Act shall not be construed to limit the enforcement or the bringing of a claim pursuant to any State consumer protection law by an attorney general of a State, other than to the extent to which those laws regulate Personal Data collection and Processing.

(b) PROTECTION OF CERTAIN STATE LAW.—Nothing in this Act shall be construed to preempt the applicability of—

(1) the constitutional, trespass, contract, data breach notification, or tort law of any state, other than to the degree such laws are substantially intended to govern Personal Data collection and Processing;

(2) any other state law to the extent that the law relates to acts of fraud, wiretapping, or the protection of social security numbers;

(3) any state law to the extent it provides additional provisions to specifically regulate the Covered Entities as defined in the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–91), the Family Educational Rights and Privacy Act (Public Law 93–380), the Fair Credit Reporting Act (Public Law 91–508) or the Financial Services Modernization Act of 1999 (Public Law 106–102); or

(4) private contracts based on any state law that require a party to provide additional or greater protections to an Individual than does this Act.

(c) PRESERVATION OF COMMISSION AUTHORITY.—Nothing in this Act shall be construed to in any way limit the authority of the Commission under any other provision of law.

(d) FCC AUTHORITY.—Insofar as any provision of the Communications Act of 1934 (47 U.S.C. 151 et seq.), including section 222 of the Communications Act of 1934 (47 U.S.C. 222), or any regulations promulgated under such Act, apply to any person subject to this Act

with respect to privacy policies, terms of service, and practices covered by this Act, such provision of the Communications Act of 1934 or such regulations shall have no force or effect, unless such regulations pertain to emergency services.

(e) TREATMENT OF COVERED ENTITIES GOVERNED BY OTHER FEDERAL LAW.—Covered entities subject to the Health Insurance Portability and Accountability Act of 1996 (Public Law 104–91), the Family Educational Rights and Privacy Act (Public Law 93–380), the Fair Credit Reporting Act (Public Law 91–508), or the Financial Services Modernization Act of 1999 (Public Law 106–102), are excluded from the provisions of this Act to the degree specific uses of Personal Data are covered by the relevant provisions of those laws.

Section 9.03 GOVERNMENT ACCOUNTABILITY OFFICE STUDY AND REPORT.

Not later than 3 years after the effective date of this Act, the Comptroller General of the United States shall submit to the President and Congress a report that surveys federal privacy and security laws that—

(a) identifies inconsistencies between this Act and other federal privacy and security laws; and

(b) provides recommendations to modify, amend, or rescind provisions of this Act or provisions of other federal laws in order to avoid or eliminate inconsistent, contradictory, duplicative, or outdated legal requirements that may no longer be relevant or necessary to protect consumers in light of this Act, rules thereunder, and changing technological and economic trends.

Article X. EFFECTIVE DATE AND SAVINGS CLAUSE.

Section 10.01 EFFECTIVE DATE.[58]

[58] Timeline for Implementation:
Year 0: Date of Enactment
18 months: FTC completes mandatory rulemaking regarding risk assessments
18 months: FTC completes mandatory rulemaking regarding the opt out of transfers of personal data
Year 2: FTC completes mandatory rulemaking regarding codes of conduct

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 10.02 NO RETROACTIVE APPLICABILITY.

This Act shall not apply to—

(a) any conduct that occurred before the effective date under Section 10.01; or

(b) any Personal Data collected or created before the date of enactment of this Act.

Section 10.03 SAVINGS CLAUSE.

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.

Year 2: FTC completes mandatory rulemaking regarding for Article III
Year 2: FTC completes mandatory rulemaking regarding categories of data to be disclosed
Year 3: Effective Date - law in effect and enforceable by FTC with limitations on civil penalties
Year 4: Expiration of optional 1 year stay of enforcement by FTC.
Year 5: All civil penalty provisions in effect (non-profits remain exempt)
Year 6: GAO Study regarding conflicts among federal privacy laws
Year 6: First FTC study regarding enforcement and compliance with Act
Year 6: First mandatory rule review by FTC