Principles for Privacy Legislation

December 2019

Privacy for America®

Principles for Privacy Legislation

Contents

Summary

The Principles

Overview of Proposed New Framework for Legislation

Introduction

Privacy for America has developed a new framework for nationwide privacy legislation that would fundamentally change the way personal data is protected and secured in this country. This framework is intended to provide a new option to policy makers for their consideration as they address this important issue. Unlike existing domestic and international approaches to privacy regulation, the framework would not rely on burdensome "notice and choice" schemes to protect personal data. Rather, it would clearly define and prohibit practices that put personal data at risk or undermine accountability, while preserving the benefits to individuals and our economy that result from the responsible use of data.

Notably, the new framework would shift the burden away from individuals to read hundreds of lengthy privacy policies to protect themselves and toward a common set of data privacy and security norms. To ensure widespread compliance and rigorous enforcement, the framework would significantly expand federal and state oversight of data practices, including by creating a new data protection bureau at the Federal Trade Commission (FTC), authorizing FTC rulemaking in certain key areas, and providing civil penalty authority to both the FTC and State Attorneys General (AGs).

Scope of the Framework

The framework would apply to virtually all personal information collected and used in the United States and virtually all companies doing business here. It would give the FTC expanded authority over nonprofits and common carriers for purposes of the new law. In addition, the framework would apply broadly to all personal information, whether collected or inferred, that is linked or can reasonably be linked to a particular individual or device.

Prohibitions on Data Misuse

The framework would prohibit outright, rather than allow consent for, a range of practices that make personal data vulnerable to misuse. Many of these prohibitions would apply not only to companies that engage in these harmful practices directly, but to suppliers of data who have reason to know that the personal information will be used for these purposes.

- **Eligibility Determinations.** Determining whether individuals are eligible for benefits like a job or credit are among the most important decisions that companies make. Although many of these decisions are currently regulated by existing sectoral laws (e.g., the Fair Credit Reporting Act), companies can easily purchase data on the open market to evade compliance with these laws. The framework would prevent this abuse by banning the use of data to make eligibility decisions—about jobs, credit, insurance, healthcare, education, financial aid, or housing—outside these laws, thereby bolstering and clarifying the protections already in place. It also would provide new tools to regulators to cut off the suppliers of data that undermine these protections. To the extent that companies are unsure about whether a practice is permitted under existing law, they would be able to seek guidance from the FTC.
- **Discrimination.** The widespread availability of detailed personal information has increased concerns that this data will be used to discriminate against individuals. The new framework would supplement existing anti-discrimination laws by banning a particularly pernicious form of discrimination—using data to charge higher prices for goods or services based on personal traits such race, color, religion, national origin, sexual orientation, or gender identity. As discussed below, the framework also would allow individuals to opt out of data personalization, which can contribute to discrimination.
- **Fraud and Deception.** For decades, the FTC and the states have pursued cases against companies that engage in fraud and deception. The new framework would focus specifically on the use and supply of data for these purposes. Thus, it would ban a range of fraudulent practices designed to induce the disclosure of personal information and, more generally, material misrepresentations about data privacy and security.
- **Stalking.** In recent years, the proliferation of data has made it easier to track the location and activities of individuals for use in stalking. Of note, mobile apps designed for this very purpose have been identified in the marketplace. The framework would outlaw the use of personal information for stalking or other forms of substantial harassment, and would hold these types of apps accountable.
- **Use of Sensitive Data Without Express Consent.** Consumers care most about their sensitive data, and companies should have an obligation to protect it. The new framework would prohibit companies from obtaining a range of sensitive information—including health, financial, biometric, and geolocation information, as well as call records, private emails, and device recording and photos—without obtaining consumers' express consent.

- **Special Protections for Individuals Over 12 and Under 16 (Tweens).** The framework includes a robust set of safeguards for data collected from tweens, an age group that needs protection but is actively engaged online and not subject to constant parental oversight. Specifically, the framework would prohibit companies from transferring tween data to third parties when they have actual knowledge of age. It also would ban payment to tweens for personal data, except under a contract to which a parent or legal guardian is a party. Finally, companies would be required to implement data eraser requirements allowing individuals to delete data posted online when they were tweens.

Requirements to Ensure Accountability and Transparency

In addition to creating new prohibitions against data misuse, the framework would impose a series of requirements designed to enhance accountability, transparency, and consumer control with respect to individual's data

- **Privacy Compliance Plan.** The framework would require companies to develop and maintain a plan to ensure compliance with the privacy requirements of the law. The scope of the plan would depend on the privacy risks that any particular company faces—thus providing flexibility for both large and small businesses—but would require essential elements such as oversight by senior personnel, ongoing risk assessment, written policies, and employee training. Of particular importance, companies would be required to evaluate the risks created by the company's data collection and retention practices, as well as its reliance on automated processing and decision-making.
- **Privacy Policy.** Although the framework reduces the current emphasis on privacy policies as the means to protect consumers, privacy policies promote accountability and thus remain an important component of any privacy law. The framework would establish consistent criteria for what information must be included in a privacy policy, including a uniform summary of consumers' rights under the law, to be developed by the FTC, and details about a company's data practices and choices provided under the law. To ensure that individuals can compare privacy policies across different companies, the framework would give the FTC the authority to prescribe rules governing their format.
- **Vendor and Third-Party Oversight.** Ensuring protections for data when it is shared with different companies is critical to any effective privacy regime. The new framework would require companies that disclose personal data to vendors and third parties to conduct due diligence and enter into contracts with these parties to ensure that the data will be used

lawfully and consistent with promises made at collection. Of significance, the framework would require vendors and third parties to implement reasonable procedures to meet their contractual obligations. Thus, unlike other privacy frameworks and laws, the burden would not fall solely on the disclosing party to police downstream data use.

- **Access and Deletion.** The framework would give individuals the right to request access to, or request deletion of, the personal information that a company maintains about them, and to learn about the types of third parties with whom personal information has been shared. These requirements would apply to information that has been linked to the individual, thereby creating incentives to maintain information in a more protected form.
- **Portability.** Individuals have come to rely on companies as trusted custodians of personal information uploaded to personal accounts (e.g., family photos, digital address books, etc.). The framework would provide portability rights to individuals for this type of information—data uploaded by individuals to accounts that they created themselves.
- **Data Security.** The framework would require companies to implement a risk-based data security program, similar to the compliance plan required for privacy. Like the privacy compliance plan, this program would vary based on the risks faced by a particular company, but would require certain essential elements such as risk assessment, employee training, and incident response.
- **Data Personalization.** Many individuals welcome information about products, services, and content they find relevant, and companies offer this type of personalization by collecting and analyzing personal information. Individuals deserve a choice, however, about whether companies should be able to create and use detailed portfolios to infer or predict their behavior or interests. Accordingly, the framework would allow individuals to opt out of having companies create these types of detailed inferences and predictions ("data personalization"), except to enable companies to communicate with their customers. If an individual opts out, a company must cease engaging in data personalization, and must stop using or sharing with third parties any inferences or predictions already created.

FTC Rulemaking to Identify Additional Prohibitions and Requirements

With rapid changes in technology and business practices, it is inevitable that new data practices will emerge that present serious risks to consumers. The framework would thus provide the FTC with rulemaking authority to amend the law's prohibited practices and accountability requirements.

In any such rulemaking, the FTC would be required to weigh various factors to determine whether the costs to the privacy interests of individuals outweighs the countervailing benefits to consumers or competition. The factors to be weighed would include the harms and benefits to individuals, the impact on business practices, the reasonable expectations of individuals, and any risk mitigation measures included in the practice. For purposes of the framework, "harm" would include not only financial and physical harm, but also reputational harm and harassment, so long as it is real and concrete, and not speculative or trivial.

The framework would authorize the FTC to bring individual cases based on these same criteria, even in the absence of a rule.

Recognition of Data Practices that Are Reasonable and Permitted

Certain data practices are essential and expected in daily life—to protect individuals and property from harm, and to enable individuals to obtain products and service they have specifically requested. For this reason, the framework would provide exceptions to some of its requirements for practices that serve these beneficial purposes—exceptions that are narrowly tailored to prevent abuses. For example, a company would not need to obtain opt-in consent for the lawful collection or use of sensitive information to the extent necessary to respond to valid legal processes or prevent and detect security incidents. In addition, some of the framework's opt-in requirements include an exception for fulfillment—narrowly defined to mean data practices to the extent necessary to deliver a product or service requested by an individual, or to conduct related administrative activities like billing and shipping. The framework also contains exceptions for aggregated and de-identified information—both because this data presents fewer risks to individuals, and to provide incentives for companies to use this type of data.

FTC-Approved Certification Programs

To enhance compliance and provide flexibility where needed, the framework would encourage the development of certification programs by qualified organizations. If a program receives and maintains approval from the FTC, member companies that adhere the program's requirements would be presumed to be compliant with the law. To ensure robust consumer protections, these programs would be required to include rigorous standards and oversight of member companies, including clear rules of conduct, public attestations of compliance by the companies, mandatory audits, meaningful disciplinary action for non-compliance, and annual reports to the public.

Enforcement and Oversight

Strong enforcement is critical to ensure compliance, deterrence, and meaningful consumer protections. The framework would significantly strengthen enforcement and oversight in several key ways:

- **New FTC Bureau.** The FTC has led privacy efforts at the federal level for decades, but it currently lacks the resources needed to police the marketplace effectively. Therefore, in addition to giving the FTC new legal authority, the framework would create a new FTC Bureau to oversee privacy and data security issues. To build and staff the new bureau, the framework calls for appropriation of additional funds and 250 additional attorneys, technologists, and other personnel.
- **State AG Enforcement.** To ensure that there are multiple "cops on the beat," the framework would authorize enforcement by both the FTC and State AGs in federal court. To avoid duplicative actions, however, State AGs would be required to provide notice to the FTC, and could not bring an action against the same company for the same acts or practices addressed in an FTC action.
- **Civil Penalties.** The framework would authorize the FTC and State AGs to seek civil penalties for first-time violations. The amount of the civil penalty would be based on variety of factors, similar to those contained in the FTC Act. Although, as noted above, the framework would authorize the FTC to bring individual cases in certain circumstances even in the absence of a specific rule, civil penalties would not be available in these types of cases.

Comprehensive Legal Scheme

With dozens of federal sectoral privacy laws on the books, and the States rapidly moving to enact their own laws, consumers and companies alike are confused by the maze of legal requirements that conflict, leave gaps, and are difficult to understand. At the same time, it would not be realistic to repeal all of the privacy and data security laws that exist today, some of which work well and provide specific protections that consumers and companies have come to expect. The framework strikes the balance between these competing interests by preserving most federal sectoral laws, partially preempting State laws, and minimizing duplication overall. In brief, the framework would handle existing laws as follows:

- **Relationship to Federal Sectoral Laws.** The framework would exclude from coverage personal information covered by and collected and used in accordance with most of the existing

sectoral federal privacy laws. To the extent that a company collects personal information not subject to these other laws, the company would need to comply with the new law. In a few instances where the new law would conflict with existing laws, the new law would govern. The goal is to ensure robust protections while avoiding a dual regulatory or enforcement scheme for the same data.

- **Relationship to State Privacy Laws.** States have played an important role in creating and shaping privacy protections in this country. The framework does not intend to preempt state laws addressing traditional state issues such as K – 12 student privacy and state issued identifiers. It would, however, preempt State privacy laws that implicitly create national standards due to the nature of the internet and interstate commerce. The framework would thus provide the protections that consumers deserve while avoiding the pitfalls of competing efforts to regulate data privacy and security. As noted above, however, State AGs would be empowered to enforce the new federal law and obtain civil penalties in order to ensure rigorous enforcement and effective consumer protection.

Five-Year Reports to Congress

The framework would require the FTC to prepare and submit reports to Congress every five (5) years to address the effectiveness of the law in protecting individuals' privacy and security, the continued relevance of the law, the benefits and burdens of the law on companies that are subject to it, and any changes to the law that the FTC recommends. This requirement will enable Congress to exercise oversight and determine whether the law is working as intended or should be modified.

The Principles

Overview*

Goals:

- To provide strong and comprehensive data protections for individuals.
- To establish clear rules of the road for individuals, businesses, and law enforcers.
- To stop harmful and unexpected data practices while allowing beneficial practices to continue.
- To shift emphasis away from "notice and choice" and towards a common set of norms about what data practices should be prohibited and permitted.

Elements:

- Identifies data practices that are unreasonable and prohibited, including:
    - misusing data for eligibility, discriminatory pricing, stalking, and fraud;
    - sharing data with vendors or third parties without entering into enforceable contracts ensuring their lawful use of the data; and
    - failing to implement a data security program, obtain opt-in for sensitive information, and provide access, deletion, and portability rights.
- Permits data practices that are reasonable and beneficial, including:
    - using data to comply with the law, protect public safety, or prevent and detect security incidents; and
    - using data to deliver a product or service requested by an individual.
- Creates a new Data Protection Bureau within Federal Trade Commission (FTC), with additional staff and resources.
- Provides civil penalty authority to FTC and State Attorneys General for key violations.
- Creates a rigorous company certification program to be approved and overseen by the FTC.
- Authorizes FTC rulemaking to: (1) amend the prohibited practices, using defined regulatory criteria; (2) prescribe the format of disclosures and amend certain definitions; and (3) implement a process for overseeing company certification programs.
- Extends the FTC's jurisdiction under the new law to common carriers and nonprofits.
- Creates a consistent national standard that preserves most federal privacy laws, preempts certain state privacy laws, and reduces conflicting requirements.

**This document reflects discussions over the past year among members of the Privacy for America coalition but has not been specifically approved or endorsed by any participating individual company.*

Part I: Data Privacy and Security Protections

Section 1: Definitions

A. **Affiliate** means any entity related to a covered organization by common ownership or corporate control where such entity: (1) is treated as part of the covered organization for purposes of compliance with this law; (2) complies with the commitments made in the covered organization's privacy policy; and (3) is identified as part of the covered organization on an easily accessible affiliates page that is updated within ninety (90) days of adding or removing any affiliate.

B. **Affirmative Express Consent** means, upon being presented with a clear and conspicuous, specific description of each data practice for which consent is sought, an affirmative act by an individual clearly communicating authorization for each such practice. The description of the practice(s) for which consent is sought must be provided to the individual in a standalone disclosure, and must include a prominent heading identifying the practice(s) for which consent is sought.

C. **Aggregated Information** means information:

1. Pertaining to a group of individuals sufficiently large that it cannot reasonably be linked to a particular individual or particular device; and
2. Where the person or entity collecting, using, maintaining, or transferring the information: (a) publicly commits in any privacy policy required under Section 3.F to maintain and use the information only in aggregated form and not to re-identify it; and (b) contractually requires, in the applicable contracts required under Section 3.G, all vendors and third parties that will have access to the information to maintain and use it only in aggregated form, and not to re-identify it.

D. **Applicable Use Restriction** means any restriction on the collection, use, maintenance, or transfer of personal information created by: (1) a representation made to an individual at the time that the data was collected, or in the case of a material retroactive change, a data practice to which an individual has lawfully and properly provided affirmative express consent; or (2) a lawful privacy choice offered to and properly exercised by an individual through an opt-in, opt-out, privacy setting, or other choice mechanism. *Provided* that when the personal information at issue consists of public records, the applicable use restrictions shall be any restrictions or terms of use placed on the information by the relevant governmental entity.

E. **Automated Processing or Decision-Making** means the use of algorithms, machine learning, artificial intelligence, predictive analytics, or other automated methods that use personal information to make decisions affecting individuals.

F. **Call Detail Records** means any records that pertain to the transmission of a specific voice communication to or from specific telephone numbers, or other customer identifiers used for routing such voice communications, including telephone numbers or identifiers of the parties to the voice communication and the time, date, duration, and/or location of the voice communication. For purposes of this definition, a voice communication is the real-time, two-way transmission of the human voice through any "telecommunication service," interconnected VoIP service," "non-interconnected VoIP service," or "commercial mobile service" as those terms are defined in Sections 153 and 332 of Title 47 of the U.S. Code.

G. **Clear and Conspicuous** means that a disclosure or other statement is in a noticeable type, size, and location, using language and syntax comprehensible to reasonable individuals, is not combined with other text or information unrelated or immaterial to the subject matter of the disclosure, and is not contradicted by or inconsistent with other text or information.

H. **Collect** means to gather, obtain, receive, or access personal information, whether actively or passively.

I. **Covered Organization** means any person or entity over which the FTC has authority under the FTC Act; a common carrier subject to the Communications Act of 1934; or an entity not organized to carry on business for its own profit or that of its members. An affiliate within the meaning of Section 1.A is considered to be part of a covered organization.

J. **Customer Communication.** To communicate with an individual with whom the covered organization has a customer relationship, including for the purposes of providing support for a product or service, or providing advertising and marketing communications about the covered organization's new or existing products or services.

K. **Data Personalization** means the collection, use, maintenance, or transfer of personal information over time to infer or predict the behavior, characteristics, or interests associated with a particular individual or device.

L. **Deidentified Information** means that the person or entity collecting, using, maintaining, or transferring the information:

    1. Takes reasonable steps to prevent the information from being linked to a particular individual or device, including by: (a) removing all personal identifiers or other

information that could reasonably be used to re-identify the individual or device to whom the information pertains; and (b) taking reasonable steps to minimize the risk of re-identification, including through use of commonly accepted scientific and statistical methods;

2. Publicly commits in any privacy policy required under this law to maintain and use the information only in de-identified form and not to re-identify it; and

3. Contractually requires, in the applicable contracts required under this law, all vendors and third parties that will have access to the information to maintain and use it only in de-identified form and not to re-identify it.

M. **Device** means an electronic device that is used by individuals and that collects or generates information about individuals or individual behavior.

N. **FTC** means the Federal Trade Commission.

O. **Fulfillment** means the collection, use, maintenance, or transfer of personal information only as reasonably necessary to:

1. Deliver or provision a product or service requested by the individual to whom the information relates; or

2. Conduct administrative activities routinely associated with and necessary to perform the activity in Subsection (1), such as billing, shipping, and accounting.

P. **Genetic Information** means information derived from a test of an individual's deoxyribonucleic acid (DNA) (including mitochondrial DNA, complementary DNA, and DNA derived from ribonucleic acid), gene products, or chromosomes.

Q. **Individual** means a person acting in a personal or household capacity and does not include a person performing work, or acting in an ownership capacity, for a commercial or nonprofit entity, or a person performing professional services.

R. **Marketing Research.** The collection, use, maintenance, or transfer of personal information as reasonably necessary to investigate the market for or marketing of products, services, or ideas, where the information is not: (1) integrated into any product or service; (2) otherwise used to contact any particular individual or device; or (3) used to advertise or market to any particular individual or device.

S. **Online Health Service** means an online service or portion of an online service principally designed to provide information to individuals about physical or mental health, or to collect, use, maintain, or transfer personal information about the physical or mental health of individuals.

T. **Online Service** means: (1) any Internet website; (2) Internet connected software program; or (3) application connecting to the Internet or transmitting information over a wireless connection.

U. **Personal Information** means information, whether collected or inferred, that is linked or can reasonably be linked to a particular individual or particular device. For purposes of compliance with all provisions of this law except Section 3.N (data security), personal information does not include de-identified information or aggregated information.

V. **Personally Identified Information** means personal information that is or has been linked to a particular individual by or on behalf of the covered organization that maintains or controls the information.

W. **Precise Geolocation Information** means information 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.

X. **Public Records** means information that a covered organization has a reasonable basis to believe is lawfully made available from federal, state, or local government records, and that the covered organization collects, uses, maintains, and transfers in accordance with any restrictions or terms of use placed on the information by the relevant governmental entity. *Provided* that public records do not include information derived from public records or information that has been combined with data from non-public record sources.

Y. **Routine and Essential Data Practices** means the lawful collection and use of personal information only as reasonably necessary to: (1) respond to valid legal process or as required or specifically authorized by law; (2) protect public safety; (3) provide security for a product or service; (4) prevent and detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or take action against those responsible; (5) authenticate and verify the identity of an individual exercising one or more of the choices required under this law; or (6) provide an individual with notice of product recalls.

Z. **Third Party** means any person or entity other than an affiliate or a vendor of a covered organization that accesses, receives, maintains, processes, or uses personal information collected by another person or entity. *Provided* that a third party does not include: (1) any person or entity with whom the individual to whom the personal information relates has an independent customer relationship; or (2) a person or entity that transfers or receives personal information in the event of a merger, acquisition, bankruptcy, or similar transaction in which one person or entity assumes control or one or more operating units of another person or entity; the personal information pertains to customers of such operating unit(s);

and the person or entity receiving the personal information assumes the privacy policies, practices, and commitments of the person or entity transferring the personal information.

AA. **Transfer** means the sale, rental, provision of access to, release, or communication of personal information to any other person or entity.

AB. **Vendor** means any person or entity that accesses, receives, maintains, processes, or uses personal information solely for the purpose of supporting another person's or entity's business and operations.

Section 2: Prohibited Practices

Unreasonable data practices as defined under this law, or pursuant to a rulemaking authorized under this law, are declared unlawful and prohibited.

Section 3: *Per Se* Unreasonable Data Practices

This law designates as *per se* unreasonable the collection, use, maintenance, or transfer of personal information, in or affecting commerce, as follows:

Data Misuse

A. Eligibility.

1. Using personal information to determine that an individual is ineligible for any of the benefits listed below, or to impose adverse terms or conditions in granting such benefits, except as permitted under federal or state laws or regulations applicable to the covered organization:
    a. Employment;
    b. Credit;
    c. Insurance;
    d. Health care;
    e. Education admissions;
    f. Financial aid; or
    g. Housing.
2. Providing substantial assistance to another person or entity: (a) related to the collection, use, maintenance, or transfer of personal information; and (b) knowing or having reason to know that such personal information will be used for a purpose prohibited in Subsection (1).

3. *Provided* that a covered organization may submit a request to the FTC for a public opinion letter providing guidance as to whether a particular act or practice is permitted under this Section, to which the FTC must provide a timely response.

B. Discrimination.

1. Charging an individual a higher price for any product or service based in whole or in part on personal information relating to an individual's race, color, religion, national origin, sexual orientation, or gender identity.
2. Providing substantial assistance to another person or entity: (a) related to the collection, use, maintenance, or transfer of personal information; and (b) knowing or having reason to know that such personal information will be used for a purpose prohibited in Subsection (1).

C. Committing or Assisting Fraud.

1. Impersonating any entity or individual in order to collect personal information or obtain access to an individual account, including but not limited to a financial, medical, email, internet, social media, or telecommunications account.
2. Misrepresenting or mischaracterizing any product or service in order to induce the disclosure of personal information.
3. Using any personal information to defraud an individual.
4. Providing substantial assistance to another person or entity: (a) related to the collection, use, maintenance, or transfer of personal information; and (b) knowing or having reason to know that such personal information will be used for a purpose prohibited in Subsections (1) – (3).

D. Stalking.

1. Using personal information to intentionally engage in a course of conduct directed at a specific individual that (a) is likely to cause such individual to reasonably fear physical injury, the commission of a sex offense against, or the kidnapping, unlawful imprisonment, or death of such individual or a member of such individual's family; or (b) constitutes substantial harassment of such individual.
2. Providing substantial assistance to another person or entity: (a) related to the collection, use, maintenance, or transfer of personal information; and (b) knowing

or having reason to know that such personal information will be used for a purpose prohibited in Subsection (1).

Accountability

E. Privacy Compliance Plan. Failing to develop or implement a reasonable process to ensure compliance with the privacy provisions of this law, taking into account the nature and scope of the covered organization's business and operations and the privacy risks presented by its practices. Such process shall include:

1. Designating appropriate personnel to implement the compliance plan, who shall report to a senior-level person or persons responsible for compliance with this law.
2. Developing and maintaining written policies and procedures to govern compliance.
3. Providing training and guidance to employees regarding compliance.
4. Assessing whether the covered organization's data practices, including but not limited to its policies and practices governing data collection and retention and its reliance on automated processing or decision-making, comply with this law and minimize unreasonable privacy risks to individuals, based on an assessment of the criteria set forth in Section 4.B.
5. Adjusting and updating existing policies and procedures as needed to address the results of the assessment conducted in accordance with Subsection (4) and any other circumstances that could impact the sufficiency of the covered organization's compliance process.
6. *Provided* that within 180 days following the date of enactment of this law, the FTC shall issue guidance to facilitate compliance with this Section by covered organizations and to minimize burdens on small businesses. The FTC shall evaluate the need for changes to this guidance as warranted and, at a minimum, every two (2) years.

F. Privacy Disclosures and Commitments.

1. Privacy Policy. Failing to provide to individuals a clear and conspicuous privacy policy accurately describing the covered organization's privacy practices. Such privacy policy shall be posted in a prominent, easily accessible location on any online service(s) owned or operated by the covered organization, and also shall be provided to individuals through the covered organization's primary means of communication with its customers, if such primary means of communication is not

online. The information to be provided in the privacy policy shall include:

a. An FTC-developed summary of individuals' rights under this law ("Summary of Rights").
b. The name and contact information of the covered organization and either: (i) the names of any affiliate(s) within the meaning of this law; or (ii) a link to a separate "affiliates page" listing each such affiliate.
c. The categories of any personal information that the covered organization collects, and the categories of uses for that information.
d. The categories of any third parties to whom personal information will be transferred and for each such category, the categories of personal information to be transferred and the categories of uses for the information.
e. For any covered organization that owns or operates one or more online service(s) and that allows any person or entity other than a vendor or third party to collect personal information directly from individuals at or through such online service(s), an effective means for individuals to access, easily and in one place, the name, contact information, and privacy policy for each such person or entity.
f. For any covered organization required under this law to seek affirmative express consent for any data practice(s), a description of the personal information and data practice(s) for which affirmative express consent is sought, and a description of how and where an individual can provide or revoke such consent. *Provided* that a covered organization may elect instead to seek and obtain affirmative express consent at a particular point of collection or in connection with a "just-in-time" notice presented to the individual.
g. An explanation of the access, deletion, portability, and opt-out choices required to be offered under this law, and a description of how and where an individual can exercise such choices.
h. To the extent that the covered organization collects, uses, maintains, or transfers any aggregated and/or de-identified information, a statement explaining the covered organization's general practices regarding such collection, use, maintenance, or transfer and a commitment not to re-identify the information as required under Sections 1.C and 1.L.
i. The effective date of the policy.

2. Honoring Choices. Failing to implement any lawful privacy choice offered to and properly exercised by an individual through an opt-in, opt-out, privacy setting, or other mechanism.

3. Other Misrepresentations. Making any other material misrepresentation to an individual about the collection, use, maintenance, or transfer of personal information.

G. Vendor and Third-Party Oversight.

1. Failing to take the following actions when entering into any arrangement with a vendor or third party involving the collection, use, maintenance, or transfer of personal information:
    a. Conducting reasonable due diligence to ensure that the vendor or third party has the background and qualifications to collect, use, maintain, transfer, and secure personal information in accordance with this law and with the contract requirements in Subsection (1)(b).
    b. Entering into a written agreement with the vendor or third party:
        i. Restricting the vendor's or third party's collection, use, maintenance, and transfer of personal information to enumerated purposes that comply with this law and with any applicable use restrictions governing the information; and
        ii. Requiring the vendor or third party to develop, implement, and maintain a comprehensive data security program meeting the requirements of this law.
    c. For written agreements with vendors, conducting reasonable monitoring of the vendor to obtain assurance that it is complying with the written agreement in Subsection (1)(b).

2. Failing to take the following actions when serving as a vendor or third party to another person or entity:
    a. Collecting, using, maintaining, or transferring personal information only if there is a reasonable basis to believe that such practice complies with this law and with any applicable use restriction with respect to the information.
    b. Entering into a written agreement with the other person or entity:
        i. Agreeing to restrict the collection, use, maintenance, and transfer of personal information to enumerated purposes that comply with this law and with any applicable use restrictions governing the personal information; and

ii. Agreeing to develop, implement, and maintain a comprehensive data security program meeting the requirements of this law.

c. Implementing reasonable procedures to comply with the written agreement required by Subsection (1)(b), and, if serving as a vendor, to assist the other person or entity in monitoring vendor compliance pursuant to Subsection (1)(c).

3. When otherwise collecting, using, maintaining, or transferring personal information on behalf of another person or entity: The failure by either party to have a reasonable basis to believe that such use complies with this law and with any applicable use restrictions with respect to the information.

Individual Choices

H. Opt-In for Sensitive Information.

1. Collecting, using, maintaining, publicly posting, or transferring the following personal information without the prior, affirmative express consent of the individual to whom the information relates:

   a. Personal information relating to the physical or mental health of an individual, except and only as reasonably necessary for fulfillment, where the information: (i) was collected, created, or inferred by an online health service; (ii) relates to the provision of "health care" (as such term is defined in 45 C.F.R. § 160.103) to an individual; or (iii) was solicited from an individual or a member of the individual's family.

   b. Personal information relating to the physical or mental health of an individual that was inferred for a commercial purpose based on other personal information obtained from or about the individual, where such inference relates to a health condition that reasonable individuals would consider highly sensitive, such as depression, a sexually transmitted disease, or cancer.

   c. A financial account number, debit card number, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; or a government issued identifier such as Social Security number, passport number, or driver's license number, except and only as reasonably necessary for fulfillment. Provided that publicly posting such information is prohibited, regardless of consent.

d. A biometric identifier generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, a set of measurable characteristics of a human voice that uniquely identifies an individual, eye retinas, irises, face geometry, or other unique biological patterns or characteristics used to identify a specific individual, except and only as reasonably necessary for fulfillment. *Provided* that:
    i. A biometric identifier does not include a physical or digital photograph, or a video or audio recording, or data generated from a physical or digital photograph, or a video or audio recording, so long as such information cannot be used to identify an individual.
    ii. Affirmative express consent under this Subsection is not required when the sole purpose of collecting a biometric identifier is to verify that an individual has previously provided such consent to collection of the identifier, and any identifier for which such consent was not obtained is immediately and irrevocably destroyed.
e. Precise geolocation information, except and only as reasonably necessary for fulfillment.

2. Collecting, using, maintaining, publicly posting, or transferring the following personal information from an individual's device without the affirmative express consent of the owner or primary user of the device:
    a. The contents of an individual's private communications, unless the covered organization is the intended recipient of the communication.
    b. Call detail records, except and only as reasonably necessary for fulfillment.
    c. Personal information obtained through a microphone, camera, or sensor of the device, except and only as reasonably necessary for fulfillment.
    d. Calendar information, address book information, phone or text logs, or personal photos, videos, or audio files maintained on the device, except and only as reasonably necessary for fulfillment.
3. Collecting, using, maintaining, publicly posting, or transferring an intimate image of an identifiable individual, or of an identifiable individual engaging in sexually explicit conduct, without the affirmative express consent of that individual.
4. Failing to provide a clear and conspicuous means for an individual to revoke any

affirmative express consent previously provided, and to implement such revocation as soon as is practicable but not later than 45 days following its receipt.

5. *Provided* that:
    a. Obtaining affirmative express consent from an individual under this section cannot be used to override any provision of this law that does not itself include an affirmative express consent requirement.
    b. The requirements of this Section do not apply when personal information is collected, used, maintained, or transferred only as reasonably necessary for routine and essential data practices.

I. Data Access and Deletion.

1. Failing to provide to an individual through a clear and conspicuous mechanism an opportunity to request once per year:
    a. A copy of all personally identified information maintained about the individual by the covered organization at the time of the request.
    b. The categories of any third parties to which the covered organization transferred the individual's personally identified information during the prior 12-month period, the categories of information that were transferred, and the categories of uses for the information.
    c. Deletion of the personally identified information described in Subsection (1)(a).
2. Failing to implement any request received from an individual through the mechanism required in Subsection (1) as soon as reasonably practicable but not later than 45 days following receipt of the request.
    a. A covered organization may extend this period by an additional 45 days once for good cause, so long as it provides clear and conspicuous notice to the individual prior to the expiration of the initial 45-day period.
    b. The information to be provided to the individual shall include relevant information in the possession of the covered organization's vendors, and such vendors shall cooperate and assist in the response.
3. The mechanism required in Subsection 1 shall be included in any privacy policy required to be provided to individuals under this law.
4. For any covered organization that owns or operates one or more online service(s) and that allows any person or entity other than a vendor or third party to collect

personal information at or through such line service(s), an effective means enabling individuals to request access and/or deletion from each such other person or entity. Any such other person or entity must implement the request(s) in accordance with Subsections (1) – (3).

5. *Provided* that:
    a. To the extent that any covered organization serving as a vendor to another covered organization receives a request under this Section directly from an individual pertaining to personal information maintained in its vendor capacity, such vendor shall either refer the request to the covered organization or implement the request at the direction of the covered organization.
    b. This Section does not require a covered organization to:
        i. Provide access to or delete information that: (1) is not under its ownership or control; (2) was republished or reposted by an individual other than the registered user that originally posted the information; or (3) is collected, used, maintained, or transferred only as reasonably necessary for routine and essential data practices.
        ii. Delete information that: (1) consists of public records; (2) was posted by an individual that received monetary consideration for the posting pursuant to a written agreement, except as provided in Section 3.M; or (3) is collected, use, maintained, or transferred only as reasonably necessary for fulfillment or to protect the covered organization's legal rights or property.
    c. In granting access and deletion requests, a covered organization shall undertake reasonable procedures to ensure that the individual making the request is the individual to whom the relevant personally identified information relates. A covered organization shall not be held liable under any Federal or State law for any response to an access or deletion request made in good faith and following reasonable procedures.

J. Data Portability.

1. Failing to provide to an individual, through a clear and conspicuous mechanism on any online service owned and operated by the covered organization, an opportunity

to request once per year a copy of the personal information uploaded by an individual to an account created by that individual for his or her use, such as uploaded photos or contact information, in a format that allows the individual to transmit the information to another account in the individual's name at another entity using a commonly accepted method of transmission.

2. Failing to implement any request received from an individual through the mechanism required in Subsection (1) as soon as reasonably practicable but not later than 45 days following receipt of the request.
    a. A covered organization may extend this period by an additional 45 days once for good cause, so long as it provides clear and conspicuous notice to the individual prior to the expiration of the initial 45-day period.
    b. The information to be provided to the individual shall include relevant information in the possession of the covered organization's vendors, and such vendors shall cooperate and assist in the response.
3. *Provided* that:
    a. To the extent that any covered organization serving as a vendor to another covered organization receives a request under this Section directly from an individual pertaining to personal information maintained in its vendor capacity, such vendor shall either refer the request to the covered organization or implement the request at the direction of the covered organization.
    b. This Section does not require a covered organization to grant a portability request with respect to personal information no longer under its ownership or control.
    c. In granting portability requests, a covered organization must undertake reasonable procedures to ensure that the individual making the request is the individual to whom the relevant personal information relates. A covered organization shall not be held liable under any Federal or State law for any response to a portability request made in good faith and following reasonable procedures.

Privacy Protections for Individuals Over Age 12 and Under Age 16

K. Data Transfers to Third Parties. Transferring to a third party personal information obtained from an individual over age 12 and under age 16 with actual knowledge of such individual's age, except and only as reasonably necessary for routine and essential data practices,

fulfillment, or practices that fall within COPPA's "internal operations" exception (16 C.F.R Section 312.2).

L. Payment for Data. Providing any monetary consideration to an individual over age 12 and under age 16, with actual knowledge of the individual's age, in exchange for collecting, using, maintaining, transferring, or publicly posting the individual's personal information, without obtaining the individual's consent to such practices pursuant to a written agreement to which the individual's parent or legal guardian is a party.

M. Data Eraser. As to any covered organization that operates an online service, that allows registered users to post personal information in an online forum, and that has actual knowledge that a registered user is or was over age 12 and under age 16 when using such service:

1. Failing to provide the registered user, through a clear and conspicuous mechanism on the website, application, or online service, an opportunity to request deletion of any personally identified information posted by that registered user when over age 12 and under age 16.
2. Failing to implement a deletion request received through the above mechanism as soon as reasonably practicable but not later than 45 days following receipt of the request. The information to be deleted shall include relevant information in the possession of the covered organization's vendors, and such vendors shall cooperate and assist in the deletion.
3. *Provided* that:
    a. This Section does not apply to information that: (i) is not under the covered organization's ownership or control; (ii) was republished or reposted content by an individual other than the registered user that originally posted the information; (iii) was obtained in exchange for monetary consideration pursuant to a written agreement to which the individual's parent or guardian is a party; or (iv) is collected, used, maintained, or transferred only as reasonably necessary for routine and essential data practices.
    b. To the extent that any covered organization serving as a vendor to another covered organization receives a request under this Section directly from an individual pertaining to personal information maintained in its vendor capacity, such vendor shall either refer the request to the covered

organization or implement the request at the direction of the covered organization.

Data Security

N. Data Security Program. Failing to develop, implement, and maintain a comprehensive data security program that is written in one or more parts and that includes administrative, technical, and physical safeguards appropriate to the nature and scope of the covered organization's business and operations, the sensitivity of the personal information at issue, and the privacy risks and threats presented to the personal information. Such program shall include the following features:

1. Objectives. The data security program shall be reasonably designed to:
    a. Ensure the security, confidentiality, and integrity of personal information.
    b. Protect against unauthorized access to and use of personal information that would violate the prohibitions in this law or create a risk of harm to individuals within the meaning of Section 4.B of this law.
2. Elements. In developing, implementing, and maintaining its data security program, a covered organization shall:
    a. Risk Assessment.
        i. Identify reasonably foreseeable internal and external risks and threats that could result in the unauthorized access to, or the use, transfer, or alteration of personal information or systems containing personal information.
        ii. Assess the sufficiency of the policies, practices, technologies, and safeguards in place to control and minimize such risks.
    b. Risk Management and Control. Develop, implement, and maintain procedural and technical safeguards to control the risks identified under Subsection (2)(a) and regularly test the sufficiency and effectiveness of such safeguards.
    c. Incident Response. Develop, implement, and maintain an incident response program to promptly respond to and recover from any security event that materially affects the security, confidentiality, or integrity of personal information.
    d. Training. Provide periodic training and guidance to employees regarding the program's requirements.

e. Vendor and Third-Party Oversight. Conduct reasonable due diligence and oversight when entering into arrangements with vendors and third parties involving access to or handling of personal information, in accordance with the due diligence, contractual, and oversight requirements in Section 3.G.

f. Periodic Assessment. Regularly monitor, evaluate, and adjust as needed the data security program in light of any relevant changes in:

   i. Technology.

   ii. The sensitivity of the personal information that the covered organization handles or accesses.

   iii. Internal or external threats to the personal information.

   iv. The covered organization's business and operations, including new or changing business arrangements such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, bankruptcy, and changes to relevant information systems.

3. *Provided* that within 180 days following the date of enactment of this law, the FTC shall issue guidance to facilitate compliance with this Section by covered organizations and to minimize burdens on small businesses. The FTC shall evaluate the need for changes to this guidance as warranted and, at a minimum, every two (2) years.

O. *Provided* that nothing in Sections 3.A – N shall prevent a covered organization from engaging in customer communications or marketing research so long as the covered organization does not violate any provision in Sections 3.A – N.

Section 4: FTC Rulemaking to Amend *Per Se* Unreasonable Provisions

A. General Requirement. The FTC is authorized to promulgate regulations in accordance with Section 553 of Title 5 of the U.S. Code to add to or limit the *per se* unreasonable categories in Section 3, or to amend the *per se* unreasonable categories in Section 3.A – M. Any such rulemaking shall be governed by the criteria set forth below.

B. Criteria. Any rulemaking conducted pursuant to this Section must include an assessment of each of the following criteria to make a determination as to whether the costs to the privacy interests of individuals outweigh the countervailing benefits to individuals or to competition.

1. Harm to Individuals. The FTC must assess whether the practice has or is likely to substantially harm reasonable individuals targeted or affected by the conduct. The type of harm may be financial, physical, or reputational, or may involve substantial harassment or intrusion into private activity, but it must be real and concrete and not speculative or trivial.
2. Benefit to Individuals. The FTC must assess the benefits conferred by the practice, including the role of the practice in providing lower prices, greater availability and choice, improved functionality, and/or customer support for products or services.
3. Impact on Business Practices. The FTC must assess the role of the practice in enabling covered organizations to compete and innovate in the marketplace or otherwise offer products and services to the public.
4. Reasonable Expectations of Individuals. The FTC must assess the context surrounding the practice from the perspective of reasonable individuals, including relevant disclosures and choices, the relationship of individuals to the practice and the persons or entities engaged in it, the target audience for the practice, and the sensitivity of the personal information at issue.
5. Risk Mitigation. The FTC must assess whether the practice incorporates effective policies, practices, and/or technical measures to minimize the risk of individual harm and/or data practices contrary to reasonable individual expectations, and whether individuals can reasonably avoid such risks themselves.

Section 5: FTC Law Enforcement Against Practices Not Designated as *Per Se* Unreasonable

A. General Requirements. In circumstances where a data practice has not been determined under this law or FTC regulation to be *per se* unreasonable, the FTC may commence a civil action as provided in Part II, Section 3 against a covered organization when it has reason to believe such covered organization has engaged in an unreasonable data practice meeting the criteria below.

B. Criteria. Before commencing any civil action under Section 5.A, the FTC must assess each of the criteria set forth in Section 4.B above to make a determination as to whether the costs to the privacy interests of individuals outweigh the countervailing benefits to individuals and competition.

Section 6: Opt-Out for Data Personalization

A. Any covered organization engaged in data personalization shall provide an effective mechanism for an individual or user of a device to request that the covered organization stop data personalization with respect to that individual or device.

B. The opt-out mechanism described in Section 6.A shall be provided clearly and conspicuously in any privacy policy required to be provided to individuals under this law, and in a prominent location outside the privacy policy proximate to where data is collected for data personalization. The covered organization also must explain, in close proximity to any such mechanism, the right of individuals to make an opt-out request and what happens once such request is made.

C. A covered organization that receives an opt-out request from an individual or user of a device under this Section shall, as soon as is practicable but not later than 15 days following receipt of the request:

1. Stop engaging in data personalization with respect to that individual or device.
2. Stop using or transferring to any other party any inferences or predictions about that individual or device that were created based on data personalization prior to receipt of the request.

D. For any covered organization that owns or operates one or more online service(s) and that allows a person or entity other than a vendor or third party to collect personal information at or through such online service(s) for data personalization, the privacy policy shall, clearly and conspicuously and in close proximity to the opt-out mechanism required under this Section, provide access to an effective means enabling an individual or user of a device to opt out of data personalization for each such other person or entity, with an option to exercise a unified choice with respect to such other persons and entities.

E. Any opt-out request received under this Section shall be deemed to apply to any vendor engaged in data personalization on behalf of a covered organization, and such vendor shall assist in implementing the request. To the extent that a vendor performing such activity receives a request directly from an individual or user of a device, it shall either refer the individual to the covered organization for which it performed the activity or implement such request at the direction of the covered organization.

F. A covered organization that receives an opt-out request under this Section may engage in data personalization if it obtains affirmative express consent from the same individual or

user of a device that made the original request. *Provided* that the covered organization may not solicit such affirmative express consent until 30 days after the original request becomes effective.

G. *Provided* that:

1. Nothing in this Section shall prevent a covered organization from:
    a. Engaging in data personalization with respect to an individual or user of a device where: (i) the covered organization has a customer relationship with that individual or user of a device; (ii) the personal information collected and used for data personalization is obtained from or directly related to the covered organization's interaction with that individual or user of a device; and (iii) the inferences or predictions are used to deliver customer communications to that individual or user of a device related to a product or service owned and offered by the covered organization.
    b. Collecting, using, maintaining, or transferring personal information only as reasonably necessary to engage in contextual advertising, delivery of an advertisement, counting and limiting the number of advertising impressions, and validating and verifying positioning and quality of ad impressions, so long as such personal information is not used to otherwise contact, advertise or market to, or create or augment the ability to infer or predict the behavior, characteristics, or interests associated with a particular individual or device.
    c. Collecting, using, maintaining, or transferring personal information only as reasonably necessary for routine and essential data practices.

Part II: Administration and Enforcement

Section 1: New FTC Resources and Authority

A. FTC to Establish New Bureau. The FTC is directed to establish a new bureau, comparable in structure, organization, and authority to its existing Bureaus, the mission of which is to exercise the authorities and responsibilities delegated to the FTC under this law and other federal laws addressing privacy, data security, and related issues in or affecting commerce. Such Bureau shall be established, staffed, and fully operational within one (1) year of enactment of this law.

B. **Appointment of Personnel.** Notwithstanding any other provision of law, the FTC is authorized to appoint 250 additional personnel to fulfill the mission of the new Bureau, including attorneys, technologists, and support staff.

C. **Appropriations.** There are authorized to be appropriated such sums as may be necessary to carry out this law.

Section 2: Additional Rulemaking(s) by FTC

In addition to the rulemakings required or authorized under Part I of this law, the FTC is granted the following rulemaking authority, to be conducted in accordance with Section 553 of Title 5 of the U.S. Code:

A. **Required Disclosures.** Within 240 days following the date of enactment of this law, the FTC is directed to promulgate regulations prescribing the format of all information and choices required to be provided to individuals under this law. Such regulations shall be designed to enhance individual understanding of the data practices and choices described and to enable individuals to compare data practices across different covered organizations, whether operating online or offline.

B. **Definition of "Aggregated Information," "Deidentified Information," and "Precise Geolocation Information."** The FTC is authorized to promulgate regulations amending the definitions of aggregated information, de-identified information, and/or precise geolocation information contained in Part I to address relevant changes in the marketplace and in technology.

Section 3: Enforcement by FTC and States

A. **Action by FTC.** Compliance with this law shall be enforced by the FTC under the FTC Act. Notwithstanding Section 56(a)(1) of Title 15 of the U.S. Code, the FTC may commence an action in its own name to obtain civil penalties for violations of this law in a district court of the United States with appropriate jurisdiction.

B. **Action by States.** Compliance with the law's prohibitions against *per se* unreasonable practices, including as they may be amended by the FTC under Part I, Section 4 of this law, as well as with the law's opt-out requirement under Part I, Section 6, may be enforced by State Attorneys General on behalf of their residents in a district court of the United States with appropriate jurisdiction.

C. **Exclusive Authority to Enforce.** The FTC and the State Attorneys General shall have the exclusive authority to enforce compliance with this law. Any violation of this law shall not serve as the basis for, or be subject to, a private right of action under this law or under any other law.

D. Civil Penalties.

1. The FTC or a State Attorney General may seek civil penalties in any case where the covered organization had actual knowledge or knowledge fairly implied based on objective circumstances that its conduct violated the law's prohibitions against *per se* unreasonable practices, including as they may be amended by the FTC under Part I, Section 4 of this law, or the law's opt-out requirement under Part I, Section 6.
2. The amount of such civil penalties shall be the same as the amount prescribed for a violation of a rule defining an unfair or deceptive act or practice under Section 18(a)(1)(B) of the FTC Act.
3. When determining the amount of civil penalty, a court must assess the degree of culpability, history of prior such conduct, ability to pay, effect on ability to continue to do business, the extent of harm or risk of harm caused by the conduct, and other such matters as justice may require.
4. Any civil penalties obtained under this Section shall be placed into a Civil Penalty Fund and made available to the FTC for payment, without fiscal year limitations, to the victims of violations of this law. To the extent that such victims cannot be located or such payments are otherwise impracticable, the FTC may use such funds to provide consumer education or promote privacy and data security literacy.

E. Notice. Before filing an action under Section 3.B, any State Attorney General intending to file the action shall provide written notice to the FTC with a copy of the complaint.

F. Intervention. Upon receiving the notice under Section 3.E, the FTC shall have the right to intervene. If the FTC intervenes, it shall have the right to be heard with respect to any matter arising from the action and to file a petition for appeal.

G. Bar on Duplicative Actions. In any case in which the FTC has filed an action against a covered organization under Section 3.A, no State Attorney General may institute or maintain an action under Section 3.B against any defendant named in the FTC's complaint for law violations arising from the same acts or practices.

Section 4: FTC-Approved Certification Programs

A. Application for Approval. Accreditation or certification organizations may apply to the FTC for approval of certification programs meeting the criteria in Section 4.C below. A certification program may address some or all of the requirements in this law.

B. Effect of Approval. A covered organization that complies with the requirements of a valid, FTC-approved certification program shall be deemed to be in compliance with the part(s) of this law addressed by the program.

C. Criteria. To obtain and maintain approval, a certification program must:

1. Specify clear and enforceable rules for covered organizations participating in the program that provide an overall level of privacy protection that is equivalent to that provided in this law.
2. Require each participating covered organization to post in a prominent place, easily accessible online a clear and conspicuous public attestation of compliance and a link to the website described in Subsection (4) below.
3. Include an effective and mandatory process for the independent assessment, and certification or denial, of a participating covered organization's compliance with the program on an initial and annual basis.
    a. Such assessment shall be conducted by a qualified person or entity with a minimum of five (5) years of experience in privacy and data protection using standards and procedures generally accepted in the profession; and
    b. To ensure the independence of the assessments, the program must establish organizational, procedural, and reporting safeguards that the FTC determines are sufficient to ensure impartiality, objectivity, and integrity.
4. Provide a dedicated website describing the program's goals and requirements, listing participating covered organizations, and providing an effective method for individuals to ask questions and file complaints about any program and/or any participating covered organization.
5. Take meaningful disciplinary action for non-compliance by any participating covered organization, which shall depend on the severity of the non-compliance and shall include one or more of the following:
    a. Removal from the program.
    b. Referral to the FTC for enforcement.
    c. Public reporting of the disciplinary action.
    d. Redress to individuals.
    e. Voluntary payments to the U.S. Treasury.
    f. An equally effective action or actions to obtain compliance and deter non-compliance.

6. Issue annual reports to the FTC and to the public detailing the activities of the program and its effectiveness during the preceding year in obtaining compliance by participating covered organizations and taking meaningful disciplinary action for non-compliance.

D. Regulations Governing Approval Process. Within 180 days following the date of enactment of this law, the FTC shall promulgate regulations in accordance with Section 553 of Title 5 of the U.S. Code detailing the process it will use to approve and oversee certification programs. Such regulations shall include at a minimum:

1. Notice and comment to obtain public input on approval requests.
2. FTC decision on each request, with publication of the FTC's conclusions, within 180 days of filing the request.
3. Procedures for the FTC to review certification programs on an initial and annual basis, and to review and approve in advance proposed modifications to the program.
4. Procedures to revoke approval for certification programs no longer meeting the required criteria.
5. Recordkeeping and reporting requirements.

E. Reports to Congress. One (1) year following the effective date of this law and on an annual basis thereafter, the FTC shall submit a report to Congress describing the effectiveness of all certification programs in effect during the previous year in obtaining compliance by participating covered organizations and taking meaningful disciplinary action for non-compliance.

Section 5: Effective Dates

A. General Requirement. This law shall be effective immediately. Compliance shall be mandatory one (1) year from the effective date.

B. Vendor and Third-Party Oversight. Notwithstanding Section 5.A above, any covered organization shall be deemed in compliance with Part I, Section 3.G of this law if for eighteen (18) months following such effective date, it complies with a written agreement governing the collection, use, maintenance, or transfer of personal information by a vendor or third party that was executed prior to the effective date; *provided* that this provision does not apply where there is no vendor or third-party agreement in effect at the time of the effective date.

C. FTC Rulemaking(s). Notwithstanding Section 5.A above, any regulation issued by the FTC

under this law shall become effective six (6) months after final issuance of that regulation or at a later date as determined for good cause by the FTC.

Section 6: Five-Year FTC Reports to Congress

Not later than five (5) years after the effective date of this law and every five (5) years thereafter, the FTC shall, following public notice and comment, prepare and submit a report to Congress addressing the effectiveness of this law in protecting individual privacy and data security; the continued relevance of this law in light of changes in technology, business practices, and individual behavior; the benefits and burdens of this law on covered organizations; and any changes to the law that the FTC recommends.

Part III: Relationship to Other Federal and State Laws

Section 1: Relationship to Other Federal Laws

A. Except as stated in Section 1.C below, nothing in this law shall be construed to modify, impair, or supersede the authority of the FTC or any other federal agency or person under any other provision of federal law.

B. To the extent that personal information is covered by and collected, used, maintained, or transferred to third parties in compliance with the laws listed below, and their implementing rules and regulations, it shall be excluded from coverage of this law.

1. Fair Credit Reporting Act (FCRA).
2. Health Insurance Portability and Accountability Act (HIPAA).
3. Gramm-Leach-Bliley Act (GLBA).
4. Children's Online Privacy Protection Act (COPPA).
5. Fair Debt Collection Practices Act (FDCPA).
6. Driver's Privacy Protection Act.
7. Controlling Assault of Non-Solicited Pornography and Marketing Act.
8. Restore Online Shoppers' Confidence Act.
9. Telemarketing and Consumer Fraud and Abuse Prevention Act.
10. Telephone Consumer Protection Act (TCPA).
11. Family Educational Rights and Privacy Act (FERPA).

12. Genetic Information Nondiscrimination Act.

13. Section 222(b) of the Communications Act of 1934, as amended, and telecommunications carriers' authorization under Section 222 of Title 47 of the U.S. Code to provide information necessary for the provision of emergency services.

14. *Provided* that within 240 days following the date of enactment of this law, the FTC shall issue guidance to assist covered organizations in determining what personal information is covered by each of the laws listed above and subject to this Section. The FTC shall develop such guidance in consultation with the Consumer Financial Protection Bureau for GLBA, FCRA, and FDCPA; the Department of Health and Human Services for HIPAA; the Federal Communications Commission for TCPA and the portions of the Communications Act referenced in Subsection (13); and the Department of Education for FERPA.

C. To the extent that any covered organization subject to this law is also subject to the Communications Act of 1934, as amended (47 U.S.C. Section 151 et seq.), or 18 U.S.C. Section 2710, this law, including any enforcement mechanisms set forth herein, shall exclusively govern such covered organization's data privacy and security practices, except as provided in Subsection (13).

D. Nothing in this law shall be construed to infringe on any person's First Amendment rights, including but not limited to the protections of free speech and freedom of the press.

Section 2: Relationship to State Laws

A. State Privacy Laws.

1. This law supersedes any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law in any State or subdivision of a State (collectively "State laws"):
    a. Enacted after June 1, 2018; and
    b. To the extent that any such laws relate to the collection, use, maintenance, transfer, access, deletion, portability, or other handling or processing of personal information addressed by this law.

2. Notwithstanding the limitation in Subsection (1)(a), the following State laws shall be preempted regardless of their date of enactment:
    a. State laws specifically governing the collection or use of biometric information.

b. State laws requiring or prescribing content requirements for privacy notices.

c. State subdivision, municipality, or agency regulations, requirements, or ordinances relating to the collection, use, maintenance, transfer access, deletion, portability, or other handling or processing of personal information addressed by this law.

3. Subsection (1) shall not be interpreted to preempt enforcement of the following State laws, except to the extent that such enforcement would regulate the collection, use, maintenance, transfer, access, deletion, portability, or other handling or processing of personal information addressed by this law, or personal information, personally identifiable information, sensitive personal information, or any variation of these or similar terms as defined under State law.

   a. State consumer protection laws of general applicability.

   b. State laws prohibiting unfair or deceptive acts or practices.

   c. State laws protecting civil rights.

4. Subsection (1) shall not apply to:

   a. State tort law.

   b. State laws addressing the collection and use of social security numbers.

B. State Data Security Laws.

1. No State shall, with respect to a covered organization subject to this law, adopt, maintain, enforce, or impose or continue in effect any law, rule, regulation, duty, requirement, standard, or other provision having the force and effect of law requiring measures to protect personal information from unauthorized access, use, or disclosure.

2. Except as provided in Subsection (1), this Section shall not be construed to limit the enforcement of any State consumer protection laws by an Attorney General of a State.

3. Nothing in this law shall be construed to preempt the applicability of: (i) State breach notification laws; (ii) State trespass, contract, or tort law; or (iii) any other State laws to the extent those laws relate to acts of fraud.

Privacy for America

Privacy for America will work with Congress to support enactment of comprehensive federal consumer data privacy and security legislation. We have outlined a bold new paradigm for a national law that would make personal data less vulnerable to breach or misuse and set forth clear, enforceable, and nationwide consumer privacy protections for the first time.

Counsel:

Venable LLP

Stuart P. Ingis
Emilio W. Cividanes
Tara Sugiyama Potashnik
Patrick M. Kane
Rob Hartwell
Michael A. Signorelli

Consultant:

Jessica L. Rich

Provided advice and assistance in developing the proposed framework.