

**Summary of Bipartisan Staff Draft  
As of December 18, 2019**

**Sec. 1. Short Title; Table of Contents**

This section is reserved for a short title and table of contents.

**Sec. 2. Sense of Congress**

This section is reserved for a Sense of Congress.

**Sec. 3. Transparency**

The draft directs the FTC to issue regulations to require covered entities to publish privacy policies in plain and concise English and other languages depending on targeted audiences. The policies must include specific information about the entity's privacy practices.

The draft also requires the largest companies to annually file more detailed privacy policies with the FTC, which the Commission must make public. If the Commission determines that some information should not be made public, it must publicly state the category of information withheld and why. Such large entities must also pay a filing fee.

In addition, the FTC is directed to conduct a study to determine the most effective short-form privacy statements, which describe how a covered entity collects covered information, the purposes for such collection and, if applicable, the category of third-parties such covered entity shares such information with. The FTC is to require such short-form statements based on the results of the study.

**Sec. 4. Privacy Program**

The draft directs the FTC to issue regulations that require covered entities to establish privacy programs appropriate for the size and nature of the covered entity's business, reasonably designed to address privacy and other risks resulting from the covered entity's processing of covered information.

Larger covered entities must designate a privacy protection officer who reports directly to the highest official at the company and is responsible for training employees about privacy, conducting audits, maintaining records of privacy and data security practices among other things. Other covered entities must designate an employee to oversee the privacy program.

**Sec. 5. Right to access covered information and request corrections and deletions of information**

The draft directs the FTC to issue regulations to establish affirmative rights of individuals to control their information through the rights to access, correct, and delete information held by covered entities, with limited exceptions. Exceptions include, among other things, retaining

covered information necessary to complete transactions requested by the individual, effectuate recalls, prevent security incidents, protect against fraud or other illegal activity, and if the covered information is publicly available. Covered entities will be required to make those rights easily exercisable and free of charge.

## **Sec. 6. Limitations on Processing Covered Information**

The draft prohibits the processing of covered information by a covered entity in a manner inconsistent with the framework established under the draft and directs the FTC to issue certain regulations. The framework sets forth a four-tier system of processing of information. The first tier allows processing of covered information within the reasonable consumer expectation within the context of the interactions (which the FTC is directed to issue guidance on) without consent, except for sensitive information, which requires affirmative consent before processing. The second tier allows covered entities to use covered information for first-party marketing but individuals may opt out. The third tier covers most other processing and requires specific and real-time notification and express, affirmative consent before processing. The fourth tier prohibits the use of certain types of highly sensitive data to the extent its use is beyond the scope of reasonable consumer expectations. Those prohibited uses include processing of biometric information to identify individuals, processing of precise geolocation information linkable to an individual, processing health information, among others.

The draft includes exceptions to the prohibited uses, including among other things, preventing security incidents, protecting against illegal activity, preventing imminent danger to personal safety, repairing errors that impair functionality, and complying with other law. The FTC is directed to promulgate regulations to allow covered entities to petition to the FTC for an exemption to practices prohibited in the draft.

## **Sec. 7. Data Retention**

The draft limits retention of covered information to only the time that is reasonably necessary for the purpose for which the covered information is processed as determined through FTC rulemaking. Covered entities may retain the data for other limited purposes including compliance with other laws, detecting and preventing security threats, preventing risks to health and safety, and debugging. The FTC may add to the list of exceptions to promote the public interest and protect the privacy of individuals.

## **Sec. 8. Limitation on Disclosing Covered Information to Third Parties**

Disclosure of covered information is limited unless certain conditions are met. Covered entities who want to disclose information to processors (entities who process data only on behalf of and at the direction of the covered entity) must have a contract with the processor that prohibits further processing of information and requires the processor to provide privacy and security protections, among other things. For covered entities to disclose information to any other entity, the covered entity must obtain prior express, affirmative consent for the disclosure for particular purposes and the parties must have a contract that restricts processing for any purpose for which consent was not given and requires privacy and security protections.

## **Sec. 9. Data Security**

The draft directs the FTC to issue regulations that require covered entities to establish reasonable data security measures consistent with the size, scope, nature, and complexity of the covered entity's business activities, and requires covered entities to conduct periodic assessments of those measures. The draft also requires covered entities to notify the FTC of a data breach and submit their security policies, which are to be treated as confidential, to the Commission at that time.

## **Sec. 10. Special Requirements on Information Brokers**

The draft requires additional obligations and prohibitions for data brokers, including maintenance of an audit log for covered information disclosed to third parties. It also requires the FTC to establish a centralized registry of information brokers where consumers can identify information brokers and get information about how to exercise their rights to access, correct, and delete information held about them. Data brokers would also be required to pay a fee when they register with the FTC.

## **Sec. 11. Prohibition on Discriminatory Use of Data**

The draft prohibits the processing of data in ways that discriminate on the basis of current protected classes under federal civil rights laws. The FTC is required to submit reports to Congress on a biennial basis on violations of this section, enforcement actions taken, enforcement priorities of the Commission, resources needed by the Commission, and developments in the technology to process covered information that may result in discrimination.

## **Sec. 12. Additional Prohibitions**

The draft prohibits take-it-or-leave-it terms in exchange for waiver of rights. It also prohibits offering financial incentives for an individual's agreement to waive rights guaranteed by this draft. It expressly protects loyalty programs provided that such programs comply with the draft.

## **Sec. 13. FTC Approved Compliance Guidelines**

The draft permits small businesses or a group of small businesses to apply to the FTC for approval of compliance guidelines. The FTC must seek public comments on proposed guidelines and approve guidelines that meet or exceed the requirements of the draft. A small business who is in compliance with approved guidelines will be deemed in compliance with the law. The FTC may withdraw approval if the guidelines no longer meet the requirements of the law (e.g., if the FTC updates regulations or the state of the technology changes, etc.), if after notice by the FTC, the guidelines are not updated within 90 days to meet the requirements of the draft.

## **Sec. 14. Bureau of Privacy**

The draft creates a new Bureau of Privacy within the FTC and includes new certified privacy professionals, including technologists. It also establishes an Office of Business Mentorship within the new bureau to consult with businesses, provide guidance, and help them comply with the law. Covered entities may petition the Office of Business Mentorship for tailored guidance as to how to comply with the requirements of the draft. In addition, it requires the FTC to dedicate employees to help small businesses.

#### **Sec. 15. Enforcement**

The draft gives the FTC civil penalty authority in the first instance. It also provides state attorneys general with authority to enforce the federal law in the same way as the FTC exclusively in federal court. No text at this time related to a private right of action.

In conducting rulemaking, the FTC is directed to ensure the rule is feasible, reasonable, flexible, risk-based, and privacy protective.

#### **Sec. 16. Relation to Other Federal and State Laws/Preemption**

No text at this time.

#### **Sec. 17. Definitions**

The draft defines covered entities to include non-profits and common carriers. The definition of covered information includes, among other things, information linked or reasonably linkable to an individual, but does not include employment data, de-identified data or data that is unreadable.

The draft specifies a subset of information as sensitive information, which includes, among other things, health information, biometric information, precise geolocation information, the contents and parties to communication, and financial information. Such information is entitled to greater protections.

The draft defines processing as including the collection, acquisition, recording, assembly, use, storage, disclosure, inference, analysis, deletion or modification of covered information.

#### **Sec. 18. Authorization of Appropriations**

The draft authorizes additional funding as needed to implement the Act.

#### **Sec. 19. Children's Privacy**

This section is reserved for children's privacy.

#### **Sec. 20. Effective Date**

This section is reserved for applicable effective dates for the sections of the Act and allows a grace period for consultation with the Commission to ensure compliance with the Act.

**Sec. 21. Relation to Communications Act**