CENTER FOR DEMOCRACY & TECHNOLOGY

CDT's Federal Privacy Legislation
Section-by-Section Analysis and Explanation

Section 1: Definitions

- Includes definitions for terms in the bill, most notably:
  - **Defines "personal information" broadly** to include any information linked or reasonably linkable by the covered entity to a specific covered person or consumer device, but excludes employee information from coverage. The individual rights in Section 2 do not require companies to re-identify information or convert non-personal information to personal information.
  - **Defines "covered entities" broadly** as any person or business that processes personal information in or affecting interstate commerce. Covered entities do not include government entities or natural persons, except for natural persons acting in a non-de-minimis commercial capacity.
  - **Defines "health information" to include three types of different data:** (1) information related to health conditions or the provision of health care, (2) information processed in the course of providing health or wellness services, or (3) information derived from a testing or examination of the body. Empowers the Federal Trade Commission (FTC) to further define "health information."
  - **Defines third parties to include corporate affiliates** if they hold themselves out as a separate entity such that reasonable individuals would not expect the two companies to be related.

Section 2: Individual Rights with Respect to Personal Information

- **Establishes affirmative rights for individuals** with respect to personal information.
  - **Right to Access and Correction:** Permits individuals to access both their personal information and the names of third parties to which personal information is sold or licensed. Allows individuals to dispute the accuracy of their personal information in certain circumstances such as where it is being used for an eligibility determination for credit, insurance, housing, employment or educational opportunity, or is health information.
  - **Right to Data Portability:** Permits individuals to transmit or transfer their personal information from a business, where appropriate, or lets individuals download personal information for their own use. Calls for the National Institute of Standards and Technology (NIST) to convene a working group to advance data portability.
  - **Right to Deletion:** Permits individuals to delete their personal information, which businesses may not make unreasonably difficult to do.
- **Provides reasonable exceptions for businesses** to deny these affirmative rights where individuals cannot confirm their identity, other legal limits are in place, or a covered entity makes a determination that exercising these rights creates a legitimate risk to another individual. Deletion and correction rights are also limited where a covered entity must retain

information for traditional business and security purposes, or deletion would interfere with ongoing research in the public interest.
- **Clarifies that de-identified data need not be re-identified** or "converted" back to personal information in order to affect these rights.

Section 3: Obligations of Covered Entities with Respect to Personal Information

- **Requires companies to put in place complaint mechanisms** for individuals to inquire about their privacy rights and to respond within 30 days.
- **Establishes clear rules for data security** by granting authority to the FTC to enact rules that are tailored to the business's practices, the type of personal information, and current state of the art in safeguards.
- **Requires companies to certify their privacy oversight policies** and disclose any material data security of privacy incidents. Requires companies to provide clear notice to individuals of their rights under this framework.
- **Addresses third-party data sharing** by requiring companies that license or sell personal information to third parties to contractually bind the third parties to the same privacy commitments as the company that collected the information. Companies are also required to exercise reasonable oversight of these contracts, take action against any company that violates these rules, and disclose those violations.
- **Addresses the lack of data broker transparency** by directing the FTC to create a centralized opt-out registry of data brokers.

Section 4: Deceptive Data Processing Practices

- **Codifies existing FTC enforcement precedent** by prohibiting misleading statements and material omissions regarding a company's privacy practices.

Section 5: Unfair Data Processing Practices

- **Identifies certain data practices as presumptively unfair** to individuals when those activities are **not required** for or **do not add to the functionality** of products, services, or specific features unless a limited exception applies or the FTC has reviewed the practice. For example, a flashlight application could no longer collect and use an individual's precise geolocation.
    - **Limits all processing of biometric information**, including facial recognition templates, for identifying an individual or verifying their identity.
    - **Limits all processing of precise location information** that is generated by consumer devices. Location information is defined to include precise geospatial data that generates latitude-longitude coordinates with an accuracy level below 1,500 feet.
    - **Limits "cross-device tracking,"** which is the use probabilistic methods like usage patterns to attribute specific consumer devices to specific individuals. Covered entities may still link devices through a common account or login.

    - **Limits the disclosure to third parties of information collected from children under the age of 13** and its use for targeted marketing.
    - **Limits the licensing or sale of personal information relating to the contents of communications or the parties to communications.** Contents are defined to have the same meaning as they do under the Electronic Communications Privacy Act. Parties to communications include the sender and recipient or destination of a communication. The definition of parties excludes subscriber information, such as contact information disclosed for the purpose of setting up an account.
    - **Limits the retention, use, or disclosure of information collected from microphones and cameras** of consumer devices.
    - **Limits processing of health information.** Recognizing that the line where information becomes "health" information varies, several collection- and use-based definitions are provided, and the FTC is afforded the flexibility to further define health information.
- **Provides a limited set of exceptions** to this broad prohibition, including (1) security and fraud, (2) imminent danger, (3) repairing errors in intended functionality, (4) research in the public interest, and (5) legal compliance. Importantly, providing a consent checkbox does not serve to get around the general prohibitions.
- **Directs the FTC to write rules within two years to create a process by which a company can seek an exception to these prohibitions**.

Section 6: Unfair Targeted Advertising Practices

- **Addresses unlawful discrimination in targeted advertising** by giving the FTC the authority to issue rules that restrict harmful targeted advertising practices that are likely to result in unlawful discrimination, including under existing civil rights laws. This provision encourages further research and investigation into the effects of algorithms and tools provided by social media services, ad networks, and data brokers to microtarget advertising online.

Section 7: Enforcement

- **Provides for joint enforcement by the FTC and state Attorneys General,** with the FTC having the ability to preempt action by states.
- Creates new civil penalties against companies that violate this framework.

Section 8: Additional Personnel in the Bureau of Consumer Protection

- **Boosts legal, privacy, and technical expertise within government** by requiring the FTC to hire additional personnel in the Bureau of Consumer Protection to police corporate privacy violations.

Section 9: Effective Date

- **Gives companies a two-year window** to provide sufficient lead time to meet the framework's requirements.

Section 10: Relation to Other Privacy & Security Laws

- **Preempts state laws that are focused primarily on data privacy** such as the **California Consumer Privacy Act** and the **Illinois Biometric Information Privacy Act**. Does not preempt state data breach notification requirements or consumer protection laws of general applicability, such as state unfair and deceptive acts or practices (UDAP) statutes that permit actions against fraud or other general consumer harms.
- **Affirms that this framework does not limit existing federal civil rights laws** but exists alongside most existing federal privacy laws.
- **Transfers privacy and security enforcement responsibilities** from the Federal Communications Commission (FCC) to the FTC for businesses regulated under the Communications Act of 1934. Brings nonprofits under the purview of the FTC for the purposes of this bill.
- **Requires regular reporting on how best to update or improve existing privacy laws** like the HIPAA Privacy Rule or the privacy provisions in GLBA. The Government Accountability Office (GAO) is assigned responsibility to undertake periodic studies to identify inconsistencies with the privacy protections in this framework.