Section-by-Section Summary of the *Online Privacy Act*

Congresswomen Anna Eshoo and Zoe Lofgren

Section 1. Short Title; Table of Contents

Sec. 2. Definitions [Only select definitions are included here.]

1. **Agency—**The Digital Privacy Agency established under Section 301.
2. **Behavioral Personalization—**
    a. The processing of personal information using an algorithm built using that individual's (or similar individuals') personal information collected over time to: alter, influence or predict behavior; personalize a product of service; or filter content.
    b. Does not include the use of historical personal information to merely prevent the display of or provide additional information about previously accessed content.
3. **Covered Entity—**Any entity (including nonprofits and common carriers) that intentionally collects, processes, or maintains personal information AND transmits personal information over an electronic network. Does not include natural persons acting noncommercially.
4. **De-identify**—
    a. Performing actions on information such that the information cannot reasonably identify, relate to, describe, reference, or be associated with or linked to an individual or device; has been de-identified using best practices; cannot be re-identified because technical safeguards and business processes to prevent re-identification are in place; and no attempt is made to re-identify.
    b. The Agency may deem de-identification techniques are insufficient.
5. **Disclose—**Sell, release, transfer, share, disseminate, make available, or otherwise communicate personal information to a third party.
6. **Personal Information—**Any information that is linked or reasonably linkable to a specific individual or device, including de-identified personal information. Personal Information does <u>not</u> include:
    a. Publicly available information linked to an individual.
    b. Information derived or inferred from personal information that can't be linked back to an individual (e.g., a result or calculation from aggregate data).
7. **Privacy Harm—**Actual or potential adverse consequences from data collection, processing, maintenance, or disclosure of personal information, including: financial loss/economic harm; physical harm; psychological harm; adverse impact on rights or benefits like employment, housing, etc.; reputational harm; price discrimination; adverse consequences affecting the private life of an individual from collection or use of information that there was a reasonable expectation that it would not be collected; the chilling of free expression or action of an individual, a group of individuals, or society due to perceived or actual pervasive and excessive privacy violations; impairing the autonomy of an individual, a group of individuals, or society; and others as determined by the Agency.
8. **Privacy-Preserving Computing—**

   a. The collecting, processing, disclosing, or maintaining of personal information that has been encrypted or otherwise rendered unintelligible using a means that cannot be reversed by a covered entity, or a covered entity's service provider, such that processing can still occur on the personal information and a result returned that is only accessible to the requesting individual.

   b. The Agency may deem privacy-preserving computing techniques insufficient.

9. **Protected Class—**The actual or perceived race, color, ethnicity, national origin, religion, sex (including sexual orientation and gender identity or expression), familial status, or disability of an individual or group of individuals.

10. **Publicly Available Information—**

   a. includes lawfully available government records (as long as the documents are used for a compatible purpose); widely available information about public individuals and officials; and information made widely available by that individual.

   b. Does not include: biometric information collected without knowledge; information obtained from government records for the purpose of selling it; information used to contact or locate a private individual physically or electronically.

11. **Reasonable Mechanism—**A mechanism for exercising user rights or interacting with covered entities is "reasonable" if it is equivalent to the primary means the user uses for interacting with the covered entity. All user rights must have a "reasonable mechanism" available to exercise them.

12. **Sale—**The disclosure of personal information for monetary consideration or thing of value by a covered entity to a third party for the purposes of processing, maintaining, or disclosing such personal information at the third party's discretion. Does not include disclosures to: third parties with a relationship with the individual; affiliates/subsidiaries of covered entities; and mergers or other similar transactions where personal information is less than half the value of assets.

13. **Service Provider—**A covered entity that processes, discloses, or maintains personal information at the direction of and for the benefit of another covered entity.

   a. A service provider does not: directly collect personal information from an individual; earn revenue from personal information except through the offering of services to the covered entity providing the personal information; disclose personal information to a covered entity unless that covered entity originally disclosed it; offer services targeting individuals with personal information not provided by the covered entity; or link the personal information with from another source.

   b. A service provider must also assist the covered entity in its compliance with Title I

14. **Significant Privacy Harm—**A direct or indirect financial loss or economic harm; physical harm; or adverse impact on rights or benefits like employment, housing, etc.

15. **Small Business**—A covered entity that: does not earn revenue from the sale of personal information; earns less than half of annual revenues from processing personal information or targeted adverting; has not maintained the personal information of

250,000 individuals for 3 or more of the preceding 12 months; has less than 200 employees; and has annual revenue under $25 million.

Sec. 3. General Provisions

a. **Prohibition on Waivers**—No provision under this Act may be waived or modified, and any contract purporting to do so is void. No predispute arbitration agreement shall be valid or enforceable with respect to claims under this Act.

b. **Journalism Exception**—Covered entities shall not be subject to the obligations imposed under this Act that directly infringe on journalism (rather than other business practices), so long as there are safeguards against using the information for non-journalism purposes.

c. **Small Business Compliance Ramp**—A former small business has nine months to fully comply with this Act upon losing its small business status.

d. **Prohibition on the Collection or Maintenance of Personal Information**—A covered entity may not collect or maintain personal information using a channel of interstate commerce unless such covered entity is in compliance with all requirements of this Act.

Sec. 4. Limitation on Disclosing Non-Redacted Government Records

Prohibits government entities from disclosing personal information of an individual in records without prohibiting the recipient of such information from selling it without the express consent of the individual for each disclosure. Exception for government-to-government disclosures.

Sec. 5. Privacy Considerations for Legislative Branch Agencies

Directs the Director of the Government Publishing Office, the Librarian of Congress, the Secretary of the Board of Regents at the Smithsonian Institution, and the Chief Administrative Officer of the House of Representatives to assess risks related to privacy harms and personal information and implement measures appropriate to mitigate such risks.

Sec. 6. Criminal Prohibition on Doxxing

Criminal prohibition on disclosing personal information of an individual with the intent:

a. to threaten, intimidate, or harass such individual (i.e., doxxing); or

b. that others will threaten, intimidate, or harass such individual;

shall be fined under this title or imprisoned not more than five years, or both.

TITLE I - USER RIGHTS

Sec. 101. Right of Access

User must have access to:

a. all categories of personal information a company maintains about that user, even information received from third parties (portability rights grant ability to download specific data);

b. a list of third parties (includes affiliates/subsidiaries) the personal information has been disclosed to and where the entity has received the personal information from;

c. a concise and clear description of business purpose for collecting/ processing/ maintaining/ disclosing of personal information (does not apply to small businesses); and

d. a list of automated decision-making processes that an individual has a right to request human review of under Section 105 with descriptions of the implications and intended effects of such process.

Sec. 102. Right of Correction

a. User has the right to dispute the accuracy or completeness of personal information if improper use of that information creates or increases significant privacy harms.

b. Section does not apply to small businesses.

Sec. 103. Right of Deletion

User has the right to request deletion of personal information both directly collected by the covered entity and information received from third parties.

Sec. 104. Right of Portability

a. For covered entities determined by the Agency to be in a "portable category" (i.e., categories of services that: benefit from encouraging increased competition, have less than three competitors, or have a Herfindahl-Hirschman >= 2,000; and have more than 10 million users), they must provide two types of data portability:

i. ability to download in a machine-readable format all of the personal information that individual has provided to the service and

ii. an Application Programming Interface (API) that allows the direct transfer of all personal information about or related to that individual to another covered entity as long as that receiving entity has been "certified."

1. The process for certification is a self-certification framework that the entity is a covered entity, that the entity does and will continue to comply with this Act, can receive personal information under Sec. 204, and will only use the API at the individual's request.

2. An API provider can deny API access on a reasonable belief that the covered entity has failed to meet the self-certification requirements, but such denials are subject to Agency review and potential penalties.

[NOTE: data received through the API is intended to be substantially broader than data obtained through download and is intended to include information such as pictures the user has been tagged in, even if uploaded by a different user.]

b. Section does not apply to small businesses.

Sec. 105. Right to Human Review of Automated Decisions

User has the right to request a human review of any decision made solely by an automated process, where that decision creates or increases significant privacy harms to that user.

Sec. 106. Right to Individual Autonomy

a. A covered entity may not collect, process, disclose, or maintain personal information for the purpose of behavioral personalization without express affirmative ("opt-in") consent.

b. Where consent is denied, the covered entity must provide a de-personalized version of the product or service. Where that's infeasible, the covered entity must offer a core aspect of the product or service that can be provided de-personalized. Where no core aspect of the product or service can be offered de-personalized, the covered entity is not required to offer the service.

c. Usability Improvement Exception

   i. Exception to express affirmative consent requirement for behavioral processing that increases usability so long as the data is representative of the entire user base and the outputs/results of the processing are uniform and independent of a specific individual user's personal characteristics (e.g., age, sex, past user actions).

      [NOTE: Covered entity must still obtain consent from the standard process. This exception exists to allow companies to improve products and services for all users, using the standard consent process. Examples include using face recognition to find pictures of family on your phone, improving search results dependent only on the search term and independent of past search history.]

   ii. Usability does not mean increasing the addictiveness or amount of time spent on the product or service.

d. Section does not apply to small businesses.

Sec. 107. Right to be Informed

A covered entity that collects the personal information of an individual it does not have an existing relationship with must (if possible) notify the individual of that collection.

Sec. 108. Right to Impermanence

a. A covered entity may not maintain a category of personal information for longer than expressly consented to by the individual. When obtaining express affirmative consent, the covered entity must provide the following durations:

   i. no longer than necessary to complete the specific request/transaction (with a time estimate of this duration);

   ii. until consent is revoked; and

   iii. one or more additional durations based on reasonable expectations or norms for maintaining that category of data.

b. Exception for implied consent, where the need for a long storage of the personal information is obvious on its face and a core feature of the service or product at the request of the individual, and it is stored only to provide that product or service. [NOTE: This is intended to allow for a covered entity to permanently store an individual's documents, photos, contacts, messages, etc. by default, but the covered entity cannot use those for any other purpose than storage. For example, they cannot use your stored photos to improve facial recognition if they use this exception.]

Sec. 109. Exemptions and Exceptions

a. Title does not apply to personal information collected, processed, disclosed, or maintained for the following purposes (as long as technical safeguards and business processes limit collection, processing, disclosure, and maintenance to these purposes):

i. detecting, responding to, or preventing cybersecurity incidents;

ii. protecting against malicious, deceptive, fraudulent or illegal activity;

iii. a good faith response to, or compliance with, a valid subpoena, court order, or warrant or otherwise providing information as required by law;

iv. protecting a legally recognized privilege or other legal right;

v. protecting public safety;

vi. collecting, processing, or maintaining records about employees or employment status by an employer;

vii. preventing prospective abuses of a service by an individual whose account has been previously terminated;

viii. routing a communication through a communications network or resolving the location of a host or client on a communications network; and

ix. providing transparency in advertising or origination of user generated content.

b. Re-identification—Where compliance with this title would require the re-identification of de-identified personal information, and the covered entity does not already maintain the information necessary for such re-identification, the covered entity shall be exempt from such compliance, except for with Sec. 106. [NOTE: This is meant to encourage covered entities to delete personal information that could be used for re-identification. Additionally, without this exception a covered entity would be required to get personal information from a third party to comply with Title I.]

c. If a covered entity exercises the exemptions above, it must disclose in a privacy policy what information is collected, processed, maintained, and disclosed for that exempted purpose and what rights do not apply.

d. Exceptions for specific requests—covered entity may deny a request under this title if—

i. An individual's identity cannot be confirmed;

ii. A covered entity is prohibited by law from complying with the request, or denying the request is necessary to protect a legally recognized right or privilege;

iii. Granting the request would create a legitimate risk of privacy, security or safety of another;

iv. Granting the request would create a legitimate risk to free expression; or

v. For deletion or correction requests: personal information is necessary for the completion of a transaction or contract initiated before the request and collected specifically solely for that; or would undermine the integrity of a legally significant transaction.

e. If a covered entity denies a request under this Title, it shall, within 30 days, inform such individual of the reason for such denial.

f. Title I does not apply to service providers.

g. Except for Sections 101, 105, and 106, this Title does not apply to personal information secured using privacy-preserving computing. [NOTE: This is meant to encourage the adoption of privacy-preserving computing and to not undermine the protection it

provides. Individuals still have access to categories of data collected, the right to review automated decisions, the prohibition on behavioral personalization, and fee prohibitions.]

h. Fees—Covered entity may not charge a fee for exercising the above rights, except if a request is determined to be unfounded or excessive, then they can charge reasonable administrative costs.

TITLE II - PRIVACY AND SECURITY REQUIREMENTS

Sec. 201. Data Minimization

Collection, processing, disclosure, and maintenance of personal information shall have a reasonable, articulated basis that takes into account reasonable business needs of the covered entity and the minimum amount of personal information needed to provide the product or service balanced with the potential privacy harms and reasonable expectations of privacy.

a. **Minimization of Collection**—A covered entity may not collect more than is reasonably needed to provide the product or service the user has requested.

b. **Minimization of Processing**—A covered entity may not process personal information for a purpose other than the purpose it was originally collected for.

c. **Minimization of Disclosure**—A covered entity may not disclose personal information for a purpose other than the purpose for which such information was originally collected.

d. **Minimization of Maintenance**—A covered entity may not store personal information for longer than necessary for the original purpose of collection.

e. **Ancillary Collection, Processing, Disclosure, Maintenance**—Collection, processing, disclosure, and maintenance beyond the limitations of (a)–(d) may occur under the following conditions:

   i. No consent needed for collection, processing, or maintenance of personal information substantially similar to the original purposes of their collection, processing, or maintenance.

   ii. Notice is required for ancillary collection, processing, disclosure, or maintenance if it would either result in increased potential for privacy harms (but not significant privacy harms) or is not substantially similar to the original purpose (but not both).

   However, if using privacy-preserving computing collection, processing, maintenance, or disclosure can both result in increased potential for privacy harms (but not significant privacy harms) and not be substantially similar to the original purpose.

   iii. Notice and consent is required if ancillary collection, processing, disclosure, or maintenance is not substantially similar and would result in increased potential for privacy harms (Sec. 212 exceptions for implied consent and privacy-preserving computing do not apply to this category).

f. Substitution—Where personal information can be obscured or replaced with an equivalent substitution without substantially reducing its utility, a covered entity shall do so.

Sec. 202. Employee Access Minimization

a. Access to personal information by employees or contractors shall be restricted based on an articulated balance between potential for privacy harm, reasonable expectations of the employees, and reasonable business needs.

b. A covered entity (excluding small businesses) shall maintain records identifying each instance when an employee or a contractor accesses contents of communications or personal information if the disclosure or breach could result in increased privacy harms. Such records include employee, date/time, and fields of information accessed.

Sec. 203. Prohibitions on Disclosure of Personal Information

a. May not intentionally disclose personal information without notice and consent.

   i. Disclosures must include the original purpose the information was collected for.

   ii. Notice is sufficient for personal information that has been de-identified using best practices and where disclosure is limited to narrowest scope for intended benefits, and contractual obligations limit its processing.

   iii. Notice is sufficient if information is secured using privacy-preserving computing.

b. May not sell personal information without the express consent of the individual for each sale (does not apply to lead-generating and aggregation services requested by user).

c. Disclosures for advertisements:

   i. may not include personal information that would allow the linking of past or future disclosures; and

   ii. may include: truncated IP; truncated geolocation; general description of device/browser; and identifier that is unique to each disclosure.

Sec. 204. Disclosing to Entities Not Subject to U.S. Jurisdiction

a. May not disclose personal information to an entity not subject to this Act or to U.S. jurisdiction.

   i. Exception for personal information that is an identifier created primarily for sending/receiving communications at the request of the individual and solely disclosed for that purpose.

   ii. Safe Harbors—Allow for the disclosure of personal information to a foreign entity:

      1. Agency Contract

         A. Disclosing entity must have reasonable belief that the foreign entity is complying with this Act; is solvent enough to pay fines; agrees to follow this Act; and has an agreement with the Agency under (b).

         B. Foreign entity enters into an agreement with the Agency where it agrees to comply with this Act, voluntarily subject itself to U.S. jurisdiction for this Act, and agrees to pay fees if the Agency is required to enforce judgement in a foreign court.

      2. Private Contract

         A. Disclosing covered entity enters into a contract with a foreign entity where the foreign entity agrees to: comply with this Act, pay

damages for violations when the covered entity cannot; gives covered entity the right to audit and inspect compliance; assists covered entity in compliance; and not use information for non-contracted purposes.

B. Covered entity must: have knowledge of compliance and solvency of the foreign entity; have an auditing and compliance program for the foreign entity; and submit the above to the Agency for approval.

C. Covered entity must have an agreement with the Agency that it will be the point of contact for all individual requests, and agency and court orders intended for the third-party regarding data it disclosed.

3. If using safe harbor (2), the covered entity shall be jointly liable for all violations involving the disclosed personal information by the foreign entity, except where the covered entity is first to disclose a violation by the foreign entity, then it will be severally liable. Where a covered entity had reason to know there was a violation and did not report it, it will be considered a continuing violation for every day it fails to report.

b. Rule of construction against data localization— Nothing shall be construed to require the localization of personal information to within the United States, or limit internal disclosure of personal information within a covered entity regardless of the country in which the covered entity will process, disclose, or maintain personal information.

Sec. 205. Prohibition on Re-identification

a. A covered entity shall not use personal information or publicly available information to re-identify an individual.

b. Exception for qualified research entities.

Sec. 206. Restriction on Communications Content

a. May not collect, process, disclose, or maintain communications content for any purpose other than—

i. Transmission, storage, display for sender or recipient;

ii. Legitimate cybersecurity purposes that don't require disclosing encryption keys or forced decryption;

iii. Providing drafting assistance services (e.g., auto correct or grammar check);

iv. Processing that is expressly requested by the sending or receiving party, as long as consent can be withdrawn;

v. Filtering of commercial communications/spam;

vi. Detecting or enforcing an abuse or violation of the service's terms of service that would result in either a temporary or permanent ban from using the service; and

vii. A disclosure required by law.

b. Exception for publicly available communications— (a) shall not apply when the contents of communication are made publicly accessible by the sender without restrictions on accessibility, other than the general authorization to access the services used to make the

information accessible. [NOTE: This exception means publicly-broadcasted messages, like public tweets or comments on articles, are not protected]

c. Encryption Protection—A covered entity may not prevent encryption of a communication by an individual nor require an individual to decrypt or provide the means to decrypt a communication.

d. A service provider is not liable for a violation if it is acting at the direction of and on behalf of a covered entity.

Sec. 207. Prohibition on Discriminatory Processing

a. A covered entity shall not process personal information or contents of communication for employment, finance, healthcare, credit, insurance, housing, or education opportunities in a manner that discriminates on the basis of an individual's protected class status.

b. A covered entity shall not process personal information in a manner that segregates, discriminates, or otherwise makes unavailable the goods, services, or accommodations of any place of public accommodation on the basis of the protected class status of an individual or group of individuals.

Sec. 208 Requirements for Notice and Consent Process

a. The Agency shall establish minimum thresholds of the percentage of users who must read and understand a privacy policy and a notice and consent process.

b. A covered entity shall make available a reasonable mechanism to revoke consent.

c. A covered entity may submit their study/data to demonstrate (a) to the Agency. If approved, the entity will receive a safe harbor. Agency shall publish approved UX's.

d. A small business may freely use the approved consent/notice process of another entity.

e. A small business cannot be penalized for failure to objectively show compliance with (a), (b), and (c), where there is no approved consent/notice process that is reasonably applicable to its business.

Sec. 209 Prohibition on 'Dark Patterns' in Notice and Consent Processes and Privacy Policies

In providing notice, obtaining consent, or maintaining a privacy policy as required by this title, a covered entity may not intentionally take any action that substantially impairs, obscures, or subverts the ability of an individual to: understand the contents of such notice or such privacy policy; understand the process for granting such consent; make a decision regarding whether to grant or withdraw such consent; or act on any such decision.

Sec. 210 Notice and Consent Required

a. Must provide an individual with notice of the personal information it collects, processes, stores, and discloses through a process that is concise and clear and can be objectively shown to meet metrics established by the Agency under Sec. 208(a).

b. May not collect or process personal information that creates or increases the risk of foreseeable privacy harms without consent that is concise and clear and can be objectively shown to meet metrics established by the Agency under Sec. 208(a).

    i. Exception for "implied consent" where consent is obvious and necessary on its face for providing the service (e.g., car sharing app needs geolocation to send you a car, but doesn't need it to track you when not on a ride).

ii. Exemption for privacy-preserving computing— Except in section 106, express consent is not required for collection, processing, or maintenance of personal information secured using privacy-preserving computing. Nothing in this paragraph exempts the covered entity from the requirement to provide notice.

c. A service provider is not liable for a violation if it is acting at the direction of and on behalf of a covered entity.

Sec. 211. Privacy Policy

a. Covered entity shall make available its privacy policy in plain language that can be objectively shown to meet metrics established by the Agency under Sec. 208(a) and it shall contain:

   i. Practices of the entity regarding collection, processing, storage, and disclosure;

   ii. How users may exercise their Title I rights;

   iii. Categories of personal information collected;

   iv. List of third parties entity has received information from and to which it disclosed information; and

   v. Articulated basis for the collection, processing, disclosure, and maintenance of personal information, as required under section 201.

b. A service provider is not liable for a violation if it is acting at the direction of and on behalf of a covered entity.

Sec. 212. Information Security Requirements

The Agency, in consultation with NIST and CISA, shall promulgate regulations to require a covered entity to implement reasonable information security policies and procedures for the protection of personal information.

a. These policies shall consider the covered entity's activities, sensitivity of personal information, state of the art of safeguards, and costs.

b. The policies shall include a written security policy that is publicly available, a process to mitigate vulnerabilities, a process to discard unneeded personal information, employee training, and a data breach response plan.

c. The Director, in consultation with NIST, CISA, SBA, the Minority Business Development Agency, and small businesses, shall develop policy templates, toolkits, tip sheets, configuration guidelines for commonly used hardware and software, interactive tools, and other materials to assist small businesses with complying with this section.

Sec. 213. Notification of Data Breach or Data Sharing Abuse

In the case of a data breach or data sharing abuse with respect to personal information, a covered entity shall:

a. Notify the agency within 72 hours after becoming aware of such incident;

b. Notify covered entities if breached or abused personal information was obtained from another covered entity, unless the breach or abuse is unlikely to create or increase foreseeable privacy harms, within 72 hours; and

c. Notify an individual, if the covered entity has a relationship with the individual, within 14 days, unless the breach or abuse is unlikely to create or increase foreseeable privacy harms, using the same medium an individual routinely interacts with such covered entity and one additional medium, where possible.

TITLE III – DIGITAL PRIVACY AGENCY

Sec. 301. Establishment; Director and Deputy Director

Establishes the Digital Privacy Agency with both principal and field offices. The Director is appointed by the President and confirmed by the Senate that serves a six-year term. The Deputy Director shall be appointed by the Director.

Sec. 302. Agency Powers and Authority

a. The Agency has independence and has the authority to carry out its duties under this Act. This authority is largely vested in the Director.

b. The Director may prescribe rules and issue orders and guidance, as may be necessary or appropriate to enable the Agency to administer and carry out the purposes and objectives of this Act, and to prevent evasions thereof.

Sec. 303. Reporting and Audit Requirements

a. Not later than 6 months after the date of the enactment, and every 6 months thereafter, the Director shall submit a report to the President and to Congress, and to be published on the Agency's website containing: significant privacy and security problems individuals face; a justification of the Agency's budget request; significant Agency actions in the past 6 months; enforcement actions; and significant actions by non-federal government entites.

b. The Director shall order an annual independent audit of the operations and budget of the Agency

Sec. 304. Relation to Other Agencies

a. Other federal agencies shall coordinate with the Agency for enforcement of provisions federal privacy laws. Such agencies may recommend the Agency initiate enforcement.

b. Authorities granted to the FTC granted under federal privacy laws (and the FTC Act relating to privacy) are transferred to the Agency. Employees of the FTC shall be transferred if their office had primary responsibilities relating to privacy.

Sec. 305. Personnel

a. The Director may establish a compensation scale different from civil service requirements so long as the requirements are fair, transparent, and equitable manner.

b. The Agency shall employ privacy experts, technologists, computer scientists, user experience designers and researchers, data scientists, ethicists, attorneys, investigators, economists, civil rights experts, and other employees as may be deemed necessary.

c. Have a Chief Information Officer, Inspector General, and Ombud.

Sec. 306. Office of Civil Rights.

The Director shall establish an Office of Civil Rights to provide oversight and enforcement of this Act to data practices are fair, equitable, and non-discriminatory; develop and promote

practices for equal opportunity in civil rights contexts; coordinate the Agency's civil rights efforts with other government entities; work with civil rights groups; and other matters.

Sec. 307. Complaints of Individuals

a. The Agency shall have a unit dedicated to collecting, monitoring, and responding to individual's complaints.

b. The Agency will create a mechanism to electronically share complaints from its complaint system to the appropriate state agencies. The Agency must share complaints with the appropriate federal and state agencies.

c. The Agency will create and maintain a database to publish user complaints about privacy.

Sec. 308. Advisory Boards

a. "User Advisory Board" of experts in consumer protection, privacy, civil rights, and ethics.

b. "Research Advisory Board" of experts in privacy, cybersecurity, computer science, innovation, design, ethics, economics, law, and public policy.

c. "Startup Advisory Board" of small businesses and small business investors in.

d. d. "Product Advisory Board" of technologists, computer scientists, designers, product managers, attorneys, and other representatives of covered entities.

Sec. 309. Authorization of Appropriations

Appropriates $550,000,000 for each of the fiscal years 2022, 2023, 2024, 2025, and 2026. [NOTE: This amount was determined by first adding together the number of employees in the Data Protection Agencies that report employee figures across the EU needed to enforce their data privacy law (~1,600 employees), and then looking at the funding level of similarly sized U.S. federal agencies.]

TITLE IV – ENFORCEMENT

Sec. 401. Investigations and Administrative Discovery

The Agency may conduct joint investigations, where appropriate, with other federal agencies, State attorneys general, and State privacy regulators, subpoena for testimony or documents, and issue civil investigative demands, and must treat investigation documents confidentially.

Sec. 402. Hearings and Adjudication Proceedings

The Agency may conduct hearings and adjudication proceedings to ensure or enforce compliance of this Act. The Agency may issue cease-and-desist orders, and temporary cease-and-desist orders if continued actions during a proceeding may result in insolvency of an affected person or prejudice consumer interest.

Sec. 403. Litigation Authority

The Agency may commence a civil action to impose a civil penalty or to seek all appropriate legal and equitable relief, including permanent or temporary injunction.

Sec. 404. Enforcement by States

State attorneys general or State privacy regulators may bring civil action as parens patriae, on behalf of residents of the state. The State attorneys general and State privacy regulators must

notify the Agency of such action, and the Agency may intervene. Agency action shall preempt state action.

Sec. 405. Private Rights of Action

a. **Injunctive Relief**—A person who is aggrieved by a violation of this Act may bring a civil action in an appropriate district court for declaratory or injunctive relief with respect to the violation.

b. **Civil Action for Damages**—Except for claims under rule 23 of the Federal Rules of Civil Procedure or a similar judicial procedure authorizing an action to be brought by one or more representatives, a person who is aggrieved by a violation of this Act may bring a civil action for damages in any court of competent jurisdiction in any state or in an appropriate district court. [NOTE: (b) allows for a single person to bring a suit for damages, but not a class or collection action.]

c. **Non-Profit Collective Representation**—An individual shall have the right to appoint a non-profit organization (501(c)(3)s only) that has objectives which are in the public interest and is active in protecting individuals' privacy rights to lodge the complaint on his or her behalf to exercise the rights referred to in this Act.

   i. A non-profit may represent a class of aggrieved individuals.

   ii. A prevailing non-profit shall receive reasonable compensation for expenses, including attorneys' fees.

   iii. Individuals shall receive an equally divided share of the total damages.

   iv. **State Appointment**—A state may provide that any organization referred to in (c), independently of an individual's appointment, has the right to lodge, in that state, a complaint with the Agency and to exercise the rights referred to in this Act if it considers that the rights of an individual under this Act have been infringed.

Sec. 406. Relief Available

The court or the Agency has the authority to grant appropriate legal or equitable relief including: rescission or reformation of contracts; refund of moneys or return of real property; restitution; disgorgement or compensation for unjust enrichment; monetary relief; injunctive relief; civil money penalties (maximum of $43,792 per individual).

Sec. 407. Referral for Criminal Proceedings

The Agency shall transmit evidence of violations of federal crimes to the Attorney General.

Sec. 408. Whistleblower Protections

Any person who becomes aware, based on non-public information, that a covered entity has violated this Act may file a civil action for civil penalties, if prior to filing such action, the person files with the Director a written request for the Director to commence the action.

TITLE V - RELATION TO OTHER LAW

Sec. 501. Effective Date

The Act takes effect one year after enactment.

Sec. 502. Relation to Other Federal Law

This law does not impact or supersede the following laws: Privacy Act of 1974; Right to Financial Privacy Act of 1978; Fair Credit Reporting Act; Fair Debt Collection Practices Act; the Gramm-Leach-Bliley Act; Children's Online Privacy Protection Act of 1998; chapters 119, 123, and 206 of title 18, United States Code; General Education Provisions Act; Privacy Protection Act of 1980; Health Insurance Portability and Accountability Act of 1996; Communications Assistance for Law Enforcement Act; sections 222, 227, 338, or 631 of the Communications Act of 1934; E-Government Act of 2002; Paperwork Reduction Act of 1995; Federal Information Security Management Act of 2002; Currency and Foreign Transactions Reporting Act of 1970; National Security Act of 1947; Foreign Intelligence Surveillance Act of 1978; Civil Rights Act of 1964; Americans with Disabilities Act; Fair Housing Act Consumer Financial Protection Act of 2010; Equal Credit Opportunity Act; Age Discrimination in Employment Act; Genetic Information Nondiscrimination Act; subpart A of part 46 of title 45, Code of Federal Regulations; Driver's Privacy Protection Act of 1994; Video Privacy Protection Act; chapters 61, 68, 75, and 76 of the Internal Revenue Code of 1986; section 1106 of the Social Security Act; Stored Communications Act; and any other privacy or information security provision of Federal law.

Sec. 503. Relation to State Law

This Act, and any amendment, standard, rule, requirement, assessment, or regulation promulgated under this Act, does not annul, alter, affect, or exempt any person subject to the provisions of this Act from complying with the laws of any State or political subdivision of a State with respect to privacy or consumer protection, except to the extent that those laws are inconsistent with any provisions of this Act, and then only to the extent of the inconsistency.

Sec. 504. Severability

If any provisions or amendments of this Act are held unconstitutional or otherwise invalid, the validity of the remainder of the Act shall not be affected.

TITLE VI—NIST AND NSF ACTIVITIES

Sec. 601. National Institute of Standards and Technology Privacy Research and Development

Amends Section 2 of the NIST Act (15 U.S.C. 272) to authorize the agency to create a voluntary privacy risk management framework to help organizations address privacy risks.

Sec. 602. National Privacy Awareness and Education Initiative

Directs NIST to carry out a privacy-related education, standardization, and public awareness activities to support the development of the privacy workforce.

Sec. 601. National Science Foundation Privacy Research

Directs NSF to support multidisciplinary and transdisciplinary research on privacy enhancing technologies and other privacy-related topics across a range of modalities.