

117TH CONGRESS  
1ST SESSION

**S.** \_\_\_\_\_

To establish data privacy and data security protections for consumers in  
the United States.

---

IN THE SENATE OF THE UNITED STATES

Mr. WICKER introduced the following bill; which was read twice and referred  
to the Committee on \_\_\_\_\_

---

## **A BILL**

To establish data privacy and data security protections for  
consumers in the United States.

1       *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE; TABLE OF CONTENTS.**

4       (a) **SHORT TITLE.**—This Act may be cited as the  
5 “Setting an American Framework to Ensure Data Access,  
6 Transparency, and Accountability Act” or the “SAFE  
7 DATA Act”.

8       (b) **TABLE OF CONTENTS.**—The table of contents for  
9 this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Definitions.
- Sec. 3. Effective date.

## TITLE I—INDIVIDUAL CONSUMER DATA RIGHTS

- Sec. 101. Consumer loyalty.
- Sec. 102. Transparency.
- Sec. 103. Individual control.
- Sec. 104. Rights to consent.
- Sec. 105. Minimizing data collection, processing, and retention.
- Sec. 106. Service providers and third parties.
- Sec. 107. Privacy impact assessments.
- Sec. 108. Scope of coverage.

## TITLE II—DATA TRANSPARENCY, INTEGRITY, AND SECURITY

- Sec. 201. Civil rights, algorithm bias, detection, and mitigation.
- Sec. 202. Data brokers.
- Sec. 203. Protection of covered data.

## TITLE III—CORPORATE ACCOUNTABILITY

- Sec. 301. Designation of data privacy officer and data security officer.
- Sec. 302. Internal controls.
- Sec. 303. Whistleblower protections.

## TITLE IV—ENFORCEMENT AUTHORITY AND NEW PROGRAMS

- Sec. 401. Enforcement by the Federal Trade Commission.
- Sec. 402. Enforcement by State attorneys general.
- Sec. 403. Approved certification programs.
- Sec. 404. Relationship between Federal and State law.
- Sec. 405. Constitutional avoidance.
- Sec. 406. Severability.

**1 SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **AFFIRMATIVE EXPRESS CONSENT.**—The  
4 term “affirmative express consent” means, upon  
5 being presented with a clear and conspicuous de-  
6 scription of an act or practice for which consent is  
7 sought, an affirmative act by the individual clearly  
8 communicating the individual’s authorization for the  
9 act or practice.

10 (2) **ALGORITHM.**—The term “algorithm” means  
11 a computational process derived from machine learn-  
12 ing, statistics, or other data processing or artificial

1 intelligence techniques, that processes covered data  
2 for the purpose of making a decision or facilitating  
3 human decision-making.

4 (3) COLLECTION.—The term “collection”  
5 means buying, renting, gathering, obtaining, receiv-  
6 ing, or accessing any covered data of an individual  
7 by any means.

8 (4) COMMISSION.—The term “Commission”  
9 means the Federal Trade Commission.

10 (5) COMMON BRANDING.—The term “common  
11 branding” means a shared name, servicemark, or  
12 trademark.

13 (6) COVERED DATA.—

14 (A) IN GENERAL.—The term “covered  
15 data” means information that identifies or is  
16 linked or reasonably linkable to an individual or  
17 a device that is linked or reasonably linkable to  
18 an individual.

19 (B) LINKED OR REASONABLY LINKABLE.—  
20 For purposes of subparagraph (A), information  
21 held by a covered entity is linked or reasonably  
22 linkable to an individual or a device if, as a  
23 practical matter, it can be used on its own or  
24 in combination with other information held by,

1 or readily accessible to, the covered entity to  
2 identify such individual or such device.

3 (C) EXCLUSIONS.—Such term does not in-  
4 clude—

5 (i) aggregated data;

6 (ii) de-identified data;

7 (iii) employee data; or

8 (iv) publicly available information.

9 (D) AGGREGATED DATA.—For purposes of  
10 subparagraph (C), the term “aggregated data”  
11 means information that relates to a group or  
12 category of individuals or devices that does not  
13 identify and is not linked or reasonably linkable  
14 to any individual or device.

15 (E) DE-IDENTIFIED DATA.—For purposes  
16 of subparagraph (C), the term “de-identified  
17 data” means information held by a covered en-  
18 tity that—

19 (i) does not identify, and is not linked  
20 or reasonably linkable to, an individual or  
21 device;

22 (ii) does not contain any persistent  
23 identifier or other information that could  
24 readily be used to reidentify the individual

1 to whom, or the device to which, the identi-  
2 fier or information pertains;

3 (iii) is subject to a public commitment  
4 by the covered entity—

5 (I) to refrain from attempting to  
6 use such information to identify any  
7 individual or device; and

8 (II) to adopt technical and orga-  
9 nizational measures to ensure that  
10 such information is not linked to any  
11 individual or device; and

12 (iv) is not disclosed by the covered en-  
13 tity to any other party unless the disclo-  
14 sure is subject to a contractually or other  
15 legally binding requirement that—

16 (I) the recipient of the informa-  
17 tion shall not use the information to  
18 identify any individual or device; and

19 (II) all onward disclosures of the  
20 information shall be subject to the re-  
21 quirement described in subclause (I).

22 (F) EMPLOYEE DATA.—For purposes of  
23 subparagraph (C), the term “employee data”  
24 means—

1 (i) information relating to an indi-  
2 vidual collected by a covered entity in the  
3 course of the individual acting as a job ap-  
4 plicant to, or employee (regardless of  
5 whether such employee is paid or unpaid,  
6 or employed on a temporary basis), owner,  
7 director, officer, staff member, trainee,  
8 vendor, visitor, volunteer, intern, or con-  
9 tractor of, the entity, provided that such  
10 information is collected, processed, or  
11 transferred by the covered entity solely for  
12 purposes related to the individual's status  
13 as a current or former job applicant to, or  
14 an employee, owner, director, officer, staff  
15 member, trainee, vendor, visitor, volunteer,  
16 intern, or contractor of, that covered enti-  
17 ty;

18 (ii) business contact information of an  
19 individual, including the individual's name,  
20 position or title, business telephone num-  
21 ber, business address, business email ad-  
22 dress, qualifications, and other similar in-  
23 formation, that is provided to a covered en-  
24 tity by an individual who is acting in a  
25 professional capacity, provided that such

1 information is collected, processed, or  
2 transferred solely for purposes related to  
3 such individual's professional activities;

4 (iii) emergency contact information  
5 collected by a covered entity that relates to  
6 an individual who is acting in a role de-  
7 scribed in clause (i) with respect to the  
8 covered entity, provided that such informa-  
9 tion is collected, processed, or transferred  
10 solely for the purpose of having an emer-  
11 gency contact on file for the individual; or

12 (iv) information relating to an indi-  
13 vidual (or a relative or beneficiary of such  
14 individual) that is necessary for the cov-  
15 ered entity to collect, process, or transfer  
16 for the purpose of administering benefits  
17 to which such individual (or relative or  
18 beneficiary of such individual) is entitled  
19 on the basis of the individual acting in a  
20 role described in clause (i) with respect to  
21 the entity, provided that such information  
22 is collected, processed, or transferred solely  
23 for the purpose of administering such ben-  
24 efits.

1 (G) PUBLICLY AVAILABLE INFORMA-  
2 TION.—

3 (i) IN GENERAL.—For the purposes of  
4 subparagraph (C), the term “publicly  
5 available information” means any informa-  
6 tion that a covered entity has a reasonable  
7 basis to believe—

8 (I) has been lawfully made avail-  
9 able to the general public from Fed-  
10 eral, State, or local government  
11 records;

12 (II) is widely available to the  
13 general public, including information  
14 from—

15 (aa) a telephone book or on-  
16 line directory;

17 (bb) television, internet, or  
18 radio content or programming; or

19 (cc) the news media or a  
20 website that is lawfully available  
21 to the general public on an unre-  
22 stricted basis (for purposes of  
23 this subclause a website is not re-  
24 stricted solely because there is a  
25 fee or log-in requirement associ-



1                   ated with accessing the website);

2                   or

3                   (III) is a disclosure to the gen-

4                   eral public that is required to be made

5                   by Federal, State, or local law.

6                   (ii) EXCLUSIONS.—Such term does

7                   not include an obscene visual depiction (as

8                   defined for purposes of section 1460 of

9                   title 18, United States Code).

10                  (7) COVERED ENTITY.—The term “covered en-

11                  tity” means any person that—

12                         (A) is subject to the Federal Trade Com-

13                         mission Act (15 U.S.C. 41 et seq.) or is—

14                                 (i) a common carrier described in sec-

15                                 tion 5(a)(2) of such Act (15 U.S.C.

16                                 45(a)(2)); or

17                                 (ii) an organization not organized to

18                                 carry on business for their own profit or

19                                 that of their members;

20                                 (B) collects, processes, or transfers covered

21                                 data; and

22                                 (C) determines the purposes and means of

23                                 such collection, processing, or transfer.

24                  (8) DATA BROKER.—

1 (A) IN GENERAL.—The term “data  
2 broker” means a covered entity whose principal  
3 source of revenue is derived from processing or  
4 transferring the covered data of individuals with  
5 whom the entity does not have a direct relation-  
6 ship on behalf of third parties for such third  
7 parties’ use.

8 (B) EXCLUSION.—Such term does not in-  
9 clude a service provider.

10 (9) DELETE.—The term “delete” means to re-  
11 move or destroy information such that it is not  
12 maintained in human or machine readable form and  
13 cannot be retrieved or utilized in such form in the  
14 normal course of business.

15 (10) EXECUTIVE AGENCY.—The term “Execu-  
16 tive agency” has the meaning set forth in section  
17 105 of title 5, United States Code.

18 (11) INDIVIDUAL.—The term “individual”  
19 means a natural person residing in the United  
20 States.

21 (12) LARGE DATA HOLDER.—The term “large  
22 data holder” means a covered entity that in the  
23 most recent calendar year—

24 (A) processed or transferred the covered  
25 data of more than 8,000,000 individuals; or

1 (B) processed or transferred the sensitive  
2 covered data of more than 300,000 individuals  
3 or devices that are linked or reasonably linkable  
4 to an individual (excluding any instance where  
5 the covered entity processes the log-in informa-  
6 tion of an individual or device to allow the indi-  
7 vidual or device to log in to an account adminis-  
8 tered by the covered entity).

9 (13) MATERIAL.—The term “material” means,  
10 with respect to an act, practice, or representation of  
11 a covered entity (including a representation made by  
12 the covered entity in a privacy policy or similar dis-  
13 closure to individuals), that such act, practice, or  
14 representation is likely to affect an individual’s deci-  
15 sion or conduct regarding a product or service.

16 (14) PROCESS.—The term “process” means  
17 any operation or set of operations performed on cov-  
18 ered data including analysis, organization, struc-  
19 turing, retaining, using, or otherwise handling cov-  
20 ered data.

21 (15) PROCESSING PURPOSE.—The term “proc-  
22 essing purpose” means a reason for which a covered  
23 entity processes covered data.

24 (16) RESEARCH.—The term “research” means  
25 the scientific analysis of information, including cov-

1       ered data, by a covered entity or those with whom  
2       the covered entity is cooperating or others acting at  
3       the direction or on behalf of the covered entity, that  
4       is conducted for the primary purpose of advancing  
5       scientific knowledge and may be for the commercial  
6       benefit of the covered entity.

7               (17) SENSITIVE COVERED DATA.—

8               (A) IN GENERAL.—The term “sensitive  
9       covered data” means any of the following forms  
10       of covered data of an individual:

11               (i) A unique, government-issued iden-  
12       tifier, such as a Social Security number,  
13       passport number, or driver’s license num-  
14       ber, that is not required to be displayed to  
15       the public.

16               (ii) Any covered data that describes or  
17       reveals the diagnosis or treatment of the  
18       past, present, or future physical health,  
19       mental health, or disability of an indi-  
20       vidual.

21               (iii) A financial account number, debit  
22       card number, credit card number, or any  
23       required security or access code, password,  
24       or credentials allowing access to any such  
25       account.

1 (iv) Covered data that is biometric in-  
2 formation.

3 (v) Precise geolocation information.

4 (vi) A persistent identifier.

5 (vii) The contents of an individual's  
6 private communications, such as emails,  
7 texts, direct messages, or mail, or the iden-  
8 tity of the parties subject to such commu-  
9 nications, unless the covered entity is the  
10 intended recipient of the communication.

11 (viii) Account log-in credentials such  
12 as a user name or email address, in com-  
13 bination with a password or security ques-  
14 tion and answer that would permit access  
15 to an online account.

16 (ix) Covered data revealing an individ-  
17 ual's racial or ethnic origin, or religion in  
18 a manner inconsistent with the individual's  
19 reasonable expectation regarding the proc-  
20 essing or transfer of such information.

21 (x) Covered data revealing the sexual  
22 orientation or sexual behavior of an indi-  
23 vidual in a manner inconsistent with the  
24 individual's reasonable expectation regard-

1 ing the processing or transfer of such in-  
2 formation.

3 (xi) Covered data about the online ac-  
4 tivities of an individual that addresses or  
5 reveals a category of covered data de-  
6 scribed in another clause of this subpara-  
7 graph.

8 (xii) Covered data that is calendar in-  
9 formation, address book information,  
10 phone or text logs, photos, or videos main-  
11 tained for private use on an individual's  
12 device.

13 (xiii) Any covered data collected or  
14 processed by a covered entity for the pur-  
15 pose of identifying covered data described  
16 in another clause of this subparagraph.

17 (xiv) Any other category of covered  
18 data designated by the Commission pursu-  
19 ant to a rulemaking under section 553 of  
20 title 5, United States Code.

21 (B) BIOMETRIC INFORMATION.—For pur-  
22 poses of subparagraph (A), the term “biometric  
23 information”—

24 (i) means the physiological or biologi-  
25 cal characteristics of an individual, includ-

1           ing deoxyribonucleic acid, that are used,  
2           singly or in combination with each other or  
3           with other identifying data, to establish the  
4           identity of an individual; and

5           (ii) includes—

6                   (I) imagery of the iris, retina,  
7                   fingerprint, face, hand, palm, vein  
8                   patterns, and voice recordings, from  
9                   which an identifier template, such as  
10                  a faceprint, a minutiae template, or a  
11                  voiceprint, can be extracted; and

12                  (II) keystroke patterns or  
13                  rhythms, gait patterns or rhythms,  
14                  and sleep, health, or exercise data  
15                  that contain identifying information.

16           (C) PERSISTENT IDENTIFIER.—For pur-  
17           poses of subparagraph (A), the term “persistent  
18           identifier” means a technologically derived iden-  
19           tifier that identifies an individual, or is linked  
20           or reasonably linkable to an individual over  
21           time and across services and platforms, which  
22           may include a customer number held in a cook-  
23           ie, a static Internet Protocol address, a proc-  
24           essor or device serial number, or another unique  
25           device identifier.

1 (D) PRECISE GEOLOCATION INFORMA-  
2 TION.—For purposes of subparagraph (A), the  
3 term “precise geolocation information” means  
4 technologically derived information capable of  
5 determining the past or present actual physical  
6 location of an individual or an individual’s de-  
7 vice at a specific point in time to within 1,750  
8 feet.

9 (18) SERVICE PROVIDER.—The term “service  
10 provider” means, with respect to a set of covered  
11 data, a covered entity that processes or transfers  
12 such covered data for the purpose of performing 1  
13 or more services or functions on behalf of, and at  
14 the direction of, a covered entity that—

15 (A) is not related to the covered entity pro-  
16 viding the service or function by common own-  
17 ership or corporate control; and

18 (B) does not share common branding with  
19 the covered entity providing the service or func-  
20 tion.

21 (19) SERVICE PROVIDER DATA.—The term  
22 “service provider data” means covered data that is  
23 collected by the service provider on behalf of a cov-  
24 ered entity or transferred to the service provider by  
25 a covered entity for the purpose of allowing the serv-



1 ice provider to perform a service or function on be-  
2 half of, and at the direction of, such covered entity.

3 (20) THIRD PARTY.—The term “third party”  
4 means, with respect to a set of covered data, a cov-  
5 ered entity—

6 (A) that is not a service provider with re-  
7 spect to such covered data; and

8 (B) that received such covered data from  
9 another covered entity—

10 (i) that is not related to the covered  
11 entity by common ownership or corporate  
12 control; and

13 (ii) that does not share common  
14 branding with the covered entity.

15 (21) THIRD PARTY DATA.—The term “third  
16 party data” means, with respect to a third party,  
17 covered data that has been transferred to the third  
18 party by a covered entity.

19 (22) TRANSFER.—The term “transfer” means  
20 to disclose, release, share, disseminate, make avail-  
21 able, or license in writing, electronically, or by any  
22 other means for consideration of any kind or for a  
23 commercial purpose.

1 **SEC. 3. EFFECTIVE DATE.**

2 Except as otherwise provided in this Act, this Act  
3 shall take effect 18 months after the date of enactment  
4 of this Act.

5 **TITLE I—INDIVIDUAL**  
6 **CONSUMER DATA RIGHTS**

7 **SEC. 101. CONSUMER LOYALTY.**

8 (a) PROHIBITION ON THE DENIAL OF PRODUCTS OR  
9 SERVICES.—

10 (1) IN GENERAL.—Subject to paragraph (2), a  
11 covered entity shall not deny products or services to  
12 an individual because the individual exercises a right  
13 established under subparagraph (A), (B), or (D) of  
14 section 103(a)(1).

15 (2) RULES OF APPLICATION.—A covered enti-  
16 ty—

17 (A) shall not be in violation of paragraph  
18 (1) with respect to a product or service and an  
19 individual if the exercise of a right described in  
20 such paragraph by the individual precludes the  
21 covered entity from providing such product or  
22 service to such individual; and

23 (B) may offer different types of pricing  
24 and functionalities with respect to a product or  
25 service based on an individual's exercise of a  
26 right described in such paragraph.

1 (b) NO WAIVER OF INDIVIDUAL CONTROLS.—The  
2 rights and obligations created under section 103 may not  
3 be waived in an agreement between a covered entity and  
4 an individual.

5 **SEC. 102. TRANSPARENCY.**

6 (a) IN GENERAL.—A covered entity that processes  
7 covered data shall, with respect to such data, publish a  
8 privacy policy that is—

9 (1) disclosed, in a clear and conspicuous man-  
10 ner, to an individual prior to or at the point of the  
11 collection of covered data from the individual; and

12 (2) made available, in a clear and conspicuous  
13 manner, to the public.

14 (b) CONTENT OF PRIVACY POLICY.—The privacy pol-  
15 icy required under subsection (a) shall include the fol-  
16 lowing:

17 (1) The identity and the contact information of  
18 the covered entity (including the covered entity's  
19 points of contact for privacy and data security in-  
20 quiries) and the identity of any affiliate to which  
21 covered data may be transferred by the covered enti-  
22 ty.

23 (2) The categories of covered data the covered  
24 entity collects.

1           (3) The processing purposes for each category  
2 of covered data the covered entity collects.

3           (4) Whether the covered entity transfers cov-  
4 ered data, the categories of recipients to whom the  
5 covered entity transfers covered data, and the pur-  
6 poses of the transfers.

7           (5) A general description of the covered entity's  
8 data retention practices for covered data and the  
9 purposes for such retention.

10          (6) How individuals can exercise their rights  
11 under section 103.

12          (7) A general description of the covered entity's  
13 data security practices.

14          (8) The effective date of the privacy policy.

15       (c) LANGUAGES.—A privacy policy required under  
16 subsection (a) shall be made available in all of the lan-  
17 guages in which the covered entity provides a product or  
18 service that is subject to the policy, or carries out activities  
19 related to such product or service.

20       (d) MATERIAL CHANGES.—If a covered entity makes  
21 a material change to its privacy policy, it shall notify the  
22 individuals affected before further processing or transfer-  
23 ring of previously collected covered data and, except as  
24 provided in section 108, provide an opportunity to with-  
25 draw consent to further processing or transferring of the

1 covered data under the changed policy. The covered entity  
2 shall provide direct notification, where possible, regarding  
3 a material change to the privacy policy to affected individ-  
4 uals, taking into account available technology and the na-  
5 ture of the relationship.

6 (e) APPLICATION TO INDIRECT TRANSFERS.—Where  
7 the ownership of an individual’s device is transferred di-  
8 rectly from one individual to another individual, a covered  
9 entity may satisfy its obligation to disclose a privacy policy  
10 prior to or at the point of collection of covered data by  
11 making the privacy policy available under subsection  
12 (a)(2).

13 **SEC. 103. INDIVIDUAL CONTROL.**

14 (a) ACCESS TO, AND CORRECTION, DELETION, AND  
15 PORTABILITY OF, COVERED DATA.—

16 (1) IN GENERAL.—Subject to paragraphs (2)  
17 and (3) and section 108, a covered entity shall pro-  
18 vide an individual, immediately or as quickly as pos-  
19 sible and in no case later than 90 days after receiv-  
20 ing a verified request from the individual, with the  
21 right to reasonably—

22 (A) access—

23 (i) the covered data of the individual,  
24 or an accurate representation of the cov-  
25 ered data of the individual, that is or has

1           been processed by the covered entity or any  
2           service provider on behalf of the covered  
3           entity;

4                 (ii) if applicable, a list of categories of  
5           third parties and service providers to whom  
6           the covered entity has transferred the cov-  
7           ered data of the individual; and

8                 (iii) if a covered entity transfers cov-  
9           ered data, a description of the purpose for  
10          which the covered entity transferred the  
11          covered data of the individual to a service  
12          provider or third party;

13          (B) request that the covered entity—

14                 (i) correct inaccuracies or incomplete  
15          information with respect to the covered  
16          data of the individual that is maintained  
17          by the covered entity; and

18                 (ii) notify any service provider or  
19          third party to which the covered entity  
20          transferred such covered data of the cor-  
21          rected information;

22          (C) request that the covered entity—

23                 (i) either delete or deidentify covered  
24          data of the individual that is or has been  
25          maintained by the covered entity; and

1                   (ii) notify any service provider or  
2                   third party to which the covered entity  
3                   transferred such covered data of the indi-  
4                   vidual's request under clause (i), unless the  
5                   transfer of such data to the third party  
6                   was made at the direction of the indi-  
7                   vidual; and

8                   (D) to the extent that is technically fea-  
9                   sible, provide covered data of the individual that  
10                  is or has been generated and submitted to the  
11                  covered entity by the individual and maintained  
12                  by the covered entity in a portable, structured,  
13                  and machine-readable format that is not subject  
14                  to licensing restrictions.

15                  (2) FREQUENCY AND COST OF ACCESS.—A cov-  
16                  ered entity shall—

17                         (A) provide an individual with the oppor-  
18                         tunity to exercise the rights described in para-  
19                         graph (1) not less than twice in any 12-month  
20                         period; and

21                         (B) with respect to the first 2 times that  
22                         an individual exercises the rights described in  
23                         paragraph (1) in any 12-month period, allow  
24                         the individual to exercise such rights free of  
25                         charge.

1 (3) EXCEPTIONS.—A covered entity—

2 (A) shall not comply with a request to ex-  
3 ercise the rights described in paragraph (1) if  
4 the covered entity cannot verify—

5 (i) that the individual making the re-  
6 quest is the individual to whom the covered  
7 data that is the subject of the request re-  
8 lates; or

9 (ii) the individual's assertion under  
10 paragraph (1)(B) that such information is  
11 inaccurate or incomplete;

12 (B) may decline to comply with a request  
13 that would—

14 (i) require the covered entity to retain  
15 any covered data for the sole purpose of  
16 fulfilling the request;

17 (ii) be impossible or demonstrably im-  
18 practicable to comply with;

19 (iii) require the covered entity to com-  
20 bine, relink, or otherwise reidentify covered  
21 data that has been deidentified;

22 (iv) result in the release of trade se-  
23 crets, or other proprietary or confidential  
24 data or business practices;



1 (v) interfere with law enforcement, ju-  
2 dicial proceedings, investigations, or rea-  
3 sonable efforts to guard against, detect, or  
4 investigate malicious or unlawful activity,  
5 or enforce contracts;

6 (vi) require disproportionate effort,  
7 taking into consideration available tech-  
8 nology, or would not be reasonably feasible  
9 on technical grounds;

10 (vii) compromise the privacy, security,  
11 or other rights of the covered data of an-  
12 other individual;

13 (viii) be excessive or abusive to an-  
14 other individual; or

15 (ix) violate Federal or State law or  
16 the rights and freedoms of another indi-  
17 vidual, including under the Constitution of  
18 the United States; and

19 (C) may delete covered data instead of pro-  
20 viding access and correction rights under sub-  
21 paragraphs (A) and (B) of paragraph (1) if  
22 such covered data—

23 (i) is not sensitive covered data; and

1                   (ii) is used only for the purposes of  
2                   contacting individuals with respect to mar-  
3                   keting communications.

4           (b) REGULATIONS.—Not later than 1 year after the  
5 date of enactment of this Act, the Commission shall pro-  
6 mulgate regulations under section 553 of title 5, United  
7 States Code, establishing processes by which covered enti-  
8 ties may verify requests to exercise rights described in sub-  
9 section (a)(1).

10 **SEC. 104. RIGHTS TO CONSENT.**

11           (a) CONSENT.—Except as provided in section 108, a  
12 covered entity shall not, without the prior, affirmative ex-  
13 press consent of an individual—

14                   (1) transfer sensitive covered data of the indi-  
15                   vidual to a third party; or

16                   (2) process sensitive covered data of the indi-  
17                   vidual.

18           (b) REQUIREMENTS FOR AFFIRMATIVE EXPRESS  
19 CONSENT.—In obtaining the affirmative express consent  
20 of an individual to process the sensitive covered data of  
21 the individual as required under subsection (a)(2), a cov-  
22 ered entity shall provide the individual with notice that  
23 shall—

1           (1) include a clear description of the processing  
2           purpose for which the sensitive covered data will be  
3           processed;

4           (2) clearly identify any processing purpose that  
5           is necessary to fulfill a request made by the indi-  
6           vidual;

7           (3) include a prominent heading that would en-  
8           able a reasonable individual to easily identify the  
9           processing purpose for which consent is sought; and

10          (4) clearly explain the individual's right to pro-  
11          vide or withhold consent.

12          (c) REQUIREMENTS RELATED TO MINORS.—A cov-  
13          ered entity shall not transfer the covered data of an indi-  
14          vidual to a third-party without affirmative express consent  
15          from the individual or the individual's parent or guardian  
16          if the covered entity has actual knowledge that the indi-  
17          vidual is between 13 and 16 years of age.

18          (d) RIGHT TO OPT OUT.—Except as provided in sec-  
19          tion 108, a covered entity shall provide an individual with  
20          the ability to opt out of the collection, processing, or trans-  
21          fer of such individual's covered data before such collection,  
22          processing, or transfer occurs.

23          (e) PROHIBITION ON INFERRED CONSENT.—A cov-  
24          ered entity shall not infer that an individual has provided  
25          affirmative express consent to a processing purpose from

1 the inaction of the individual or the individual's continued  
2 use of a service or product provided by the covered entity.

3 (f) **WITHDRAWAL OF CONSENT.**—A covered entity  
4 shall provide an individual with a clear and conspicuous  
5 means to withdraw affirmative express consent.

6 (g) **RULEMAKING.**—The Commission may promul-  
7 gate regulations under section 553 of title 5, United  
8 States Code, to establish clear and conspicuous procedures  
9 for allowing individuals to provide or withdraw affirmative  
10 express consent for the collection of sensitive covered data.

11 **SEC. 105. MINIMIZING DATA COLLECTION, PROCESSING,**  
12 **AND RETENTION.**

13 (a) **IN GENERAL.**—Except as provided in section 108,  
14 a covered entity shall not collect, process, or transfer cov-  
15 ered data beyond—

16 (1) what is reasonably necessary, proportionate,  
17 and limited to provide or improve a product, service,  
18 or a communication about a product or service, in-  
19 cluding what is reasonably necessary, proportionate,  
20 and limited to provide a product or service specifi-  
21 cally requested by an individual or reasonably antici-  
22 pated within the context of the covered entity's on-  
23 going relationship with an individual;

24 (2) what is reasonably necessary, proportionate,  
25 or limited to otherwise process or transfer covered

1 data in a manner that is described in the privacy  
2 policy that the covered entity is required to publish  
3 under section 102(a); or

4 (3) what is expressly permitted by this Act or  
5 any other applicable Federal law.

6 (b) BEST PRACTICES.—Not later than 1 year after  
7 the date of enactment of this Act, the Commission shall  
8 issue guidelines recommending best practices for covered  
9 entities to minimize the collection, processing, and trans-  
10 fer of covered data in accordance with this section.

11 (c) RULE OF CONSTRUCTION.—Notwithstanding sec-  
12 tion 404 of this Act, nothing in this section supersedes  
13 any other provision of this Act or other applicable Federal  
14 law.

15 **SEC. 106. SERVICE PROVIDERS AND THIRD PARTIES.**

16 (a) SERVICE PROVIDERS.—A service provider—

17 (1) shall not process service provider data for  
18 any processing purpose that is not performed on be-  
19 half of, and at the direction of, the covered entity  
20 that transferred the data to the service provider;

21 (2) shall not transfer service provider data to a  
22 third party for any purpose other than a purpose  
23 performed on behalf of, or at the direction of, the  
24 covered entity that transferred the data to the serv-  
25 ice provider;

1           (3) at the direction of the covered entity that  
2 transferred service provider data to the service pro-  
3 vider, shall delete or deidentify such data—

4           (A) as soon as practicable after the service  
5 provider has completed providing the service or  
6 function for which the data was transferred to  
7 the service provider; or

8           (B) as soon as practicable after the end of  
9 the period during which the service provider is  
10 to provide services with respect to such data, as  
11 agreed to by the service provider and the cov-  
12 ered entity that transferred the data;

13           (4) is exempt from the requirements of section  
14 103 with respect to service provider data, but shall,  
15 to the extent practicable—

16           (A) assist the covered entity from which it  
17 received the service provider data in fulfilling  
18 requests to exercise rights under section 103(a);  
19 and

20           (B) upon receiving notice from a covered  
21 entity of a verified request made under section  
22 103(a)(1) to delete, deidentify, or correct serv-  
23 ice provider data held by the service provider,  
24 delete, deidentify, or correct such data; and

1           (5) is exempt from the requirements of sections  
2           104 and 105.

3           (b) THIRD PARTIES.—A third party—

4           (1) shall not process third party data for a  
5           processing purpose inconsistent with the reasonable  
6           expectation of the individual to whom such data re-  
7           lates;

8           (2) for purposes of paragraph (1), may reason-  
9           ably rely on representations made by the covered en-  
10          tity that transferred third party data regarding the  
11          reasonable expectations of individuals to whom such  
12          data relates, provided that the third party conducts  
13          reasonable due diligence on the representations of  
14          the covered entity and finds those representations to  
15          be credible; and

16          (3) is exempt from the requirements of sections  
17          104 and 105.

18          (c) BANKRUPTCY.—In the event that a covered entity  
19          enters into a bankruptcy proceeding which would lead to  
20          the disclosure of covered data to a third party, the covered  
21          entity shall in a reasonable time prior to the disclosure—

22          (1) provide notice of the proposed disclosure of  
23          covered data, including the name of the third party  
24          and its policies and practices with respect to the cov-  
25          ered data, to all affected individuals; and

1           (2) provide each affected individual with the op-  
2           portunity to withdraw any previous affirmative ex-  
3           press consent related to the covered data of the indi-  
4           vidual or request the deletion or deidentification of  
5           the covered data of the individual.

6           (d) **ADDITIONAL OBLIGATIONS ON COVERED ENTI-**  
7 **TIES.—**

8           (1) **IN GENERAL.—**A covered entity shall exer-  
9           cise reasonable due diligence to ensure compliance  
10          with this section before—

11                   (A) selecting a service provider; or

12                   (B) deciding to transfer covered data to a  
13          third party.

14          (2) **GUIDANCE.—**Not later than 2 years after  
15          the effective date of this Act, the Commission shall  
16          publish guidance regarding compliance with this sub-  
17          section. Such guidance shall, to the extent prac-  
18          ticable, minimize unreasonable burdens on small-  
19          and medium-sized covered entities.

20 **SEC. 107. PRIVACY IMPACT ASSESSMENTS.**

21          (a) **PRIVACY IMPACT ASSESSMENTS OF NEW OR MA-**  
22 **TERIAL CHANGES TO PROCESSING OF COVERED DATA.—**

23           (1) **IN GENERAL.—**Not later than 1 year after  
24          the date of enactment of this Act (or, if later, not  
25          later than 1 year after a covered entity first meets



1 the definition of a large data holder (as defined in  
2 section 2)), each covered entity that is a large data  
3 holder shall conduct a privacy impact assessment of  
4 each of its processing activities involving covered  
5 data that present a heightened risk of harm to indi-  
6 viduals, and each such assessment shall weigh the  
7 benefits of the covered entity's covered data collec-  
8 tion, processing, and transfer practices against the  
9 potential adverse consequences to individual privacy  
10 of such practices.

11 (2) ASSESSMENT REQUIREMENTS.—A privacy  
12 impact assessment required under paragraph (1)—

13 (A) shall be reasonable and appropriate in  
14 scope given—

15 (i) the nature of the covered data col-  
16 lected, processed, or transferred by the  
17 covered entity;

18 (ii) the volume of the covered data  
19 collected, processed, or transferred by the  
20 covered entity;

21 (iii) the size of the covered entity; and

22 (iv) the potential risks posed to the  
23 privacy of individuals by the collection,  
24 processing, or transfer of covered data by  
25 the covered entity;

1 (B) shall be documented in written form  
2 and maintained by the covered entity unless  
3 rendered out of date by a subsequent assess-  
4 ment conducted under subsection (b); and

5 (C) shall be approved by the data privacy  
6 officer of the covered entity.

7 (b) ONGOING PRIVACY IMPACT ASSESSMENTS.—

8 (1) IN GENERAL.—A covered entity that is a  
9 large data holder shall, not less frequently than once  
10 every 2 years after the covered entity conducted the  
11 privacy impact assessment required under subsection  
12 (a), conduct a privacy impact assessment of the col-  
13 lection, processing, and transfer of covered data by  
14 the covered entity to assess the extent to which—

15 (A) the ongoing practices of the covered  
16 entity are consistent with the covered entity's  
17 published privacy policies;

18 (B) any customizable privacy settings in-  
19 cluded in a service or product offered by the  
20 covered entity are adequately accessible to indi-  
21 viduals who use the service or product and are  
22 effective in meeting the privacy preferences of  
23 such individuals;

1 (C) the practices and privacy settings de-  
2 scribed in subparagraphs (A) and (B), respec-  
3 tively—

4 (i) meet the expectations of a reason-  
5 able individual; and

6 (ii) provide an individual with ade-  
7 quate control over the individual's covered  
8 data;

9 (D) the covered entity could enhance the  
10 privacy and security of covered data through  
11 technical or operational safeguards such as  
12 encryption, deidentification, and other privacy-  
13 enhancing technologies; and

14 (E) the processing of covered data is com-  
15 patible with the stated purposes for which it  
16 was collected.

17 (2) APPROVAL BY DATA PRIVACY OFFICER.—

18 The data privacy officer of a covered entity shall ap-  
19 prove the findings of an assessment conducted by  
20 the covered entity under this subsection.

21 **SEC. 108. SCOPE OF COVERAGE.**

22 (a) GENERAL EXCEPTIONS.—Notwithstanding any  
23 provision of this title other than subsections (a) through  
24 (c) of section 102, a covered entity may collect, process  
25 or transfer covered data for any of the following purposes,

1 provided that the collection, processing, or transfer is rea-  
2 sonably necessary, proportionate, and limited to such pur-  
3 pose:

4 (1) To initiate or complete a transaction or to  
5 fulfill an order or provide a service specifically re-  
6 quired by an individual, including associated rou-  
7 tine administrative activities such as billing, ship-  
8 ping, financial reporting, and accounting.

9 (2) To perform internal system maintenance,  
10 diagnostics, product or service management, inven-  
11 tory management, and network management.

12 (3) To prevent, detect, or respond to a security  
13 incident or trespassing, provide a secure environ-  
14 ment, or maintain the safety and security of a prod-  
15 uct, service, network, or individual.

16 (4) To protect against malicious, deceptive,  
17 fraudulent, or illegal activity.

18 (5) To comply with a legal obligation or the es-  
19 tablishment, exercise, analysis, or defense of legal  
20 claims or rights, or as required or specifically au-  
21 thorized by law.

22 (6) To comply with a civil, criminal, or regu-  
23 latory inquiry, investigation, subpoena, or summons  
24 by an Executive agency.

1           (7) To cooperate with an Executive agency or  
2 a law enforcement official acting under the authority  
3 of an Executive or State agency concerning conduct  
4 or activity that the Executive agency or law enforce-  
5 ment official reasonably and in good faith believes  
6 may violate Federal, State, or local law, or pose a  
7 threat to public safety or national security.

8           (8) To address risks to the safety of an indi-  
9 vidual or group of individuals, or to ensure customer  
10 safety, including by authenticating individuals in  
11 order to provide access to large venues open to the  
12 public.

13           (9) To effectuate a product recall pursuant to  
14 Federal or State law.

15           (10) To conduct public or peer-reviewed sci-  
16 entific, historical, or statistical research that—

17                   (A) is in the public interest;

18                   (B) adheres to all applicable ethics and  
19 privacy laws; and

20                   (C) is approved, monitored, and governed  
21 by an institutional review board or other over-  
22 sight entity that meets standards promulgated  
23 by the Commission pursuant to section 553 of  
24 title 5, United States Code.

1           (11) To transfer covered data to a service pro-  
2           vider.

3           (12) For a purpose identified by the Commis-  
4           sion pursuant to a regulation promulgated under  
5           subsection (b).

6           (b) **ADDITIONAL PURPOSES.**—The Commission may  
7           promulgate regulations under section 553 of title 5,  
8           United States Code, identifying additional purposes for  
9           which a covered entity may collect, process or transfer cov-  
10          ered data.

11          (c) **SMALL BUSINESS EXCEPTION.**—Sections 103,  
12          105, and 301 shall not apply in the case of a covered enti-  
13          ty that can establish that, for the 3 preceding calendar  
14          years (or for the period during which the covered entity  
15          has been in existence if such period is less than 3 years)—

16                 (1) the covered entity's average annual gross  
17                 revenues did not exceed \$50,000,000;

18                 (2) on average, the covered entity annually  
19                 processed the covered data of less than 1,000,000  
20                 individuals;

21                 (3) the covered entity never employed more  
22                 than 500 individuals at any one time; and

23                 (4) the covered entity derived less than 50 per-  
24                 cent of its revenues from transferring covered data.

1 **TITLE II—DATA TRANSPARENCY,**  
2 **INTEGRITY, AND SECURITY**

3 **SEC. 201. CIVIL RIGHTS, ALGORITHM BIAS, DETECTION,**  
4 **AND MITIGATION.**

5 (a) CIVIL RIGHTS PROTECTIONS.—A covered entity,  
6 service provider, or third party may not collect, process,  
7 or transfer covered data in violation of Federal civil rights  
8 laws.

9 (b) FTC ENFORCEMENT ASSISTANCE.—

10 (1) IN GENERAL.—Whenever the Commission  
11 obtains information that a covered entity may have  
12 processed or transferred covered data in violation of  
13 Federal civil rights laws, the Commission shall  
14 transmit such information (excluding any such infor-  
15 mation that is a trade secret as defined by section  
16 1839 of title 18, United States Code) to the appro-  
17 priate Executive agency or State agency with au-  
18 thority to initiate proceedings relating to such viola-  
19 tion.

20 (2) ANNUAL REPORT.—Beginning in 2022, the  
21 Commission shall submit an annual report to Con-  
22 gress that includes—

23 (A) a summary of the types of information  
24 the Commission transmitted to Executive agen-

1           cies or State agencies during the preceding year  
2           pursuant to this subsection; and

3                   (B) a summary of how such information  
4           relates to Federal civil rights laws.

5           (3) COOPERATION WITH OTHER AGENCIES.—

6           The Commission may implement this subsection by  
7           executing agreements or memoranda of under-  
8           standing with the appropriate Executive agencies.

9                   (4) RELATIONSHIP TO OTHER LAWS.—Notwith-  
10          standing section 404, nothing in this subsection  
11          shall supersede any other provision of law.

12          (c) ALGORITHM TRANSPARENCY REPORTS.—

13                   (1) STUDY AND REPORT.—

14                           (A) STUDY.—The Commission shall con-  
15                           duct a study, using the Commission’s authority  
16                           under section 6(b) of the Federal Trade Com-  
17                           mission Act (15 U.S.C. 46(b)), examining the  
18                           use of algorithms to process covered data in a  
19                           manner that may violate Federal anti-discrimi-  
20                           nation laws.

21                                   (B) REPORT.—Not later than 3 years after  
22                                   the date of enactment of this Act, the Commis-  
23                                   sion shall publish a report containing the re-  
24                                   sults of the study required under subparagraph  
25                                   (A).



1           (C) GUIDANCE.—The Commission shall  
2           use the results of the study described in sub-  
3           paragraph (A) to develop guidance to assist  
4           covered entities in avoiding the use of algo-  
5           rithms to process covered data in a manner  
6           that violates Federal civil rights laws.

7           (2) UPDATED REPORT.—Not later than 5 years  
8           after the publication of the report required under  
9           paragraph (1), the Commission shall publish an up-  
10          dated report.

11 **SEC. 202. DATA BROKERS.**

12          (a) IN GENERAL.—Not later than January 31 of  
13          each calendar year that follows a calendar year during  
14          which a covered entity acted as a data broker, such cov-  
15          ered entity shall register with the Commission pursuant  
16          to the requirements of this section.

17          (b) REGISTRATION REQUIREMENTS.—In registering  
18          with the Commission as required under subsection (a), a  
19          data broker shall do the following:

20               (1) Pay to the Commission a registration fee of  
21               \$100.

22               (2) Provide the Commission with the following  
23               information:

24                       (A) The name and primary physical, email,  
25                       and internet addresses of the data broker.

1 (B) Any additional information or expla-  
2 nation the data broker chooses to provide con-  
3 cerning its data collection and processing prac-  
4 tices.

5 (c) PENALTIES.—A data broker that fails to register  
6 as required under subsection (a) shall be liable for—

7 (1) a civil penalty of \$50 for each day it fails  
8 to register, not to exceed a total of \$10,000 for each  
9 year; and

10 (2) an amount equal to the fees due under this  
11 section for each year that it failed to register as re-  
12 quired under subsection (a).

13 (d) PUBLICATION OF REGISTRATION INFORMA-  
14 TION.—The Commission shall publish on the internet  
15 website of the Commission the registration information  
16 provided by data brokers under this section.

17 **SEC. 203. PROTECTION OF COVERED DATA.**

18 (a) IN GENERAL.—A covered entity shall establish,  
19 implement, and maintain reasonable administrative, tech-  
20 nical, and physical data security policies and practices to  
21 protect against risks to the confidentiality, security, and  
22 integrity of covered data.

23 (b) DATA SECURITY REQUIREMENTS.—The data se-  
24 curity policies and practices required under subsection (a)  
25 shall be—

1           (1) appropriate to the size and complexity of  
2 the covered entity, the nature and scope of the cov-  
3 ered entity's collection or processing of covered data,  
4 the volume and nature of the covered data at issue,  
5 and the cost of available tools to improve security  
6 and reduce vulnerabilities; and

7           (2) designed to—

8                 (A) identify and assess vulnerabilities to  
9 covered data;

10                (B) take reasonable preventative and cor-  
11 rective action to address known vulnerabilities  
12 to covered data; and

13                (C) detect, respond to, and recover from  
14 cybersecurity incidents related to covered data.

15 (c) RULEMAKING AND GUIDANCE.—

16           (1) RULEMAKING AUTHORITY AND SCOPE.—

17                 (A) IN GENERAL.—The Commission may,  
18 pursuant to a proceeding in accordance with  
19 section 553 of title 5, United States Code, issue  
20 regulations to identify processes for receiving  
21 and assessing information regarding  
22 vulnerabilities to covered data that are reported  
23 to the covered entity.

24                 (B) CONSULTATION WITH NIST.—In pro-  
25 mulgating regulations under this paragraph, the

1 Commission shall consult with, and take into  
2 consideration guidance from, the National Insti-  
3 tute for Standards and Technology.

4 (2) GUIDANCE.—Not later than 1 year after  
5 the date of enactment of this Act, the Commission  
6 shall issue guidance to covered entities on how to—

7 (A) identify and assess vulnerabilities to  
8 covered data, including—

9 (i) the potential for unauthorized ac-  
10 cess to covered data;

11 (ii) vulnerabilities in the covered enti-  
12 ty's collection or processing of covered  
13 data;

14 (iii) the management of access rights;  
15 and

16 (iv) the use of service providers to  
17 process covered data;

18 (B) take reasonable preventative and cor-  
19 rective action to address vulnerabilities to cov-  
20 ered data; and

21 (C) detect, respond to, and recover from  
22 cybersecurity incidents and events.

23 (d) APPLICABILITY OF OTHER INFORMATION SECU-  
24 RITY LAWS.—A covered entity that is required to comply  
25 with title V of the Gramm-Leach-Bliley Act (15 U.S.C.

1 6801 et seq.) or the Health Information Technology for  
2 Economic and Clinical Health Act (42 U.S.C. 17931 et  
3 seq.), and is in compliance with the information security  
4 requirements of such Act, shall be deemed to be in compli-  
5 ance with the requirements of this section with respect to  
6 covered data that is subject to the requirements of such  
7 Act.

## 8 **TITLE III—CORPORATE** 9 **ACCOUNTABILITY**

### 10 **SEC. 301. DESIGNATION OF DATA PRIVACY OFFICER AND** 11 **DATA SECURITY OFFICER.**

12 (a) IN GENERAL.—A covered entity shall designate—

13 (1) 1 or more qualified employees or contrac-  
14 tors as a data privacy officer; and

15 (2) 1 or more qualified employees or contrac-  
16 tors (in addition to any employee or contractor des-  
17 igned under paragraph (1)) as a data security offi-  
18 cer.

19 (b) RESPONSIBILITIES OF DATA PRIVACY OFFICERS  
20 AND DATA SECURITY OFFICERS.—An employee or con-  
21 tractor who is designated by a covered entity as a data  
22 privacy officer or a data security officer shall be respon-  
23 sible for, at a minimum, coordinating the covered entity's  
24 policies and practices regarding—

1 (1) in the case of a data privacy officer, compli-  
2 ance with the privacy requirements with respect to  
3 covered data under this Act; and

4 (2) in the case of a data security officer, the se-  
5 curity requirements with respect to covered data  
6 under this Act.

7 **SEC. 302. INTERNAL CONTROLS.**

8 A covered entity shall maintain internal controls and  
9 reporting structures to ensure that appropriate senior  
10 management officials of the covered entity are involved in  
11 assessing risks and making decisions that implicate com-  
12 pliance with this Act.

13 **SEC. 303. WHISTLEBLOWER PROTECTIONS.**

14 (a) DEFINITIONS.—For purposes of this section:

15 (1) WHISTLEBLOWER.—The term “whistle-  
16 blower” means any employee or contractor of a cov-  
17 ered entity who voluntarily provides to the Commis-  
18 sion original information relating to non-compliance  
19 with, or any violation or alleged violation of, this Act  
20 or any regulation promulgated under this Act.

21 (2) ORIGINAL INFORMATION.—The term “origi-  
22 nal information” means information that is provided  
23 to the Commission by an individual and—

24 (A) is derived from the independent knowl-  
25 edge or analysis of an individual;

1           (B) is not known to the Commission from  
2           any other source at the time the individual pro-  
3           vides the information; and

4           (C) is not exclusively derived from an alle-  
5           gation made in a judicial or an administrative  
6           action, in a governmental report, a hearing, an  
7           audit, or an investigation, or from news media,  
8           unless the individual is a source of the allega-  
9           tion.

10       (b) EFFECT OF WHISTLEBLOWER RETALIATIONS ON  
11 PENALTIES.—In seeking penalties under section 401 for  
12 a violation of this Act or a regulation promulgated under  
13 this Act by a covered entity, the Commission shall consider  
14 whether the covered entity retaliated against an individual  
15 who was a whistleblower with respect to original informa-  
16 tion that led to the successful resolution of an administra-  
17 tive or judicial action brought by the Commission or the  
18 Attorney General of the United States on behalf of the  
19 Commission under this Act against such covered entity.

1 **TITLE IV—ENFORCEMENT AU-**  
2 **THORITY AND NEW PRO-**  
3 **GRAMS**

4 **SEC. 401. ENFORCEMENT BY THE FEDERAL TRADE COM-**  
5 **MISSION.**

6 (a) UNFAIR OR DECEPTIVE ACTS OR PRACTICES.—

7 A violation of this Act or a regulation promulgated under  
8 this Act shall be treated as a violation of a rule defining  
9 an unfair or deceptive act or practice prescribed under sec-  
10 tion 18(a)(1)(B) of the Federal Trade Commission Act  
11 (15 U.S.C. 57a(a)(1)(B)).

12 (b) POWERS OF COMMISSION.—

13 (1) IN GENERAL.—Except as provided in sub-  
14 sections (c) and (d), the Commission shall enforce  
15 this Act and the regulations promulgated under this  
16 Act in the same manner, by the same means, and  
17 with the same jurisdiction, powers, and duties as  
18 though all applicable terms and provisions of the  
19 Federal Trade Commission Act (15 U.S.C. 41 et  
20 seq.) were incorporated into and made a part of this  
21 Act.

22 (2) PRIVILEGES AND IMMUNITIES.—Any person  
23 who violates this Act or a regulation promulgated  
24 under this Act shall be subject to the penalties and  
25 entitled to the privileges and immunities provided in



1 the Federal Trade Commission Act (15 U.S.C. 41 et  
2 seq.).

3 (3) LIMITING CERTAIN ACTIONS UNRELATED  
4 TO THIS ACT; AUTHORITY PRESERVED.—The Com-  
5 mission shall not bring any action to enforce the  
6 prohibition in section 5 of the Federal Trade Com-  
7 mission Act (15 U.S.C. 45) on unfair or deceptive  
8 acts or practices with respect to the privacy or secu-  
9 rity of covered data, unless such alleged act of prac-  
10 tice violates this Act.

11 (c) COMMON CARRIERS AND NONPROFIT ORGANIZA-  
12 TIONS.—Notwithstanding section 4, 5(a)(2), or 6 of the  
13 Federal Trade Commission Act (15 U.S.C. 44, 45(a)(2),  
14 46) or any jurisdictional limitation of the Commission, the  
15 Commission shall also enforce this Act and the regulations  
16 promulgated under this Act, in the same manner provided  
17 in subsections (a) and (b) of this subsection, with respect  
18 to—

19 (1) common carriers subject to the Communica-  
20 tions Act of 1934 (47 U.S.C. 151 et seq.) and all  
21 Acts amendatory thereof and supplementary thereto;  
22 and

23 (2) organizations not organized to carry on  
24 business for their own profit or that of their mem-  
25 bers.

1 (d) DATA PRIVACY AND SECURITY FUND.—

2 (1) ESTABLISHMENT OF VICTIMS RELIEF  
3 FUND.—There is established in the Treasury of the  
4 United States a separate fund to be known as the  
5 “Data Privacy and Security Victims Relief Fund”  
6 (referred to in this paragraph as the “Victims Relief  
7 Fund”).

8 (2) DEPOSITS.—

9 (A) DEPOSITS FROM THE COMMISSION.—

10 The Commission shall deposit into the Victims  
11 Relief Fund the amount of any civil penalty ob-  
12 tained against any covered entity in any action  
13 the Commission commences to enforce this Act  
14 or a regulation promulgated under this Act.

15 (B) DEPOSITS FROM THE ATTORNEY GEN-

16 ERAL.—The Attorney General of the United  
17 States shall deposit into the Victims Relief  
18 Fund the amount of any civil penalty obtained  
19 against any covered entity in any action the At-  
20 torney General commences on behalf of the  
21 Commission to enforce this Act or a regulation  
22 promulgated under this Act.

23 (3) USE OF FUND AMOUNTS.—Amounts in the  
24 Victims Relief Fund shall be available to the Com-  
25 mission, without fiscal year limitation, to provide re-

1 dress, payments or compensation, or other monetary  
2 relief to individuals harmed by an act or practice for  
3 which civil penalties have been imposed under this  
4 Act. To the extent that individuals cannot be located  
5 or such redress, payments or compensation, or other  
6 monetary relief are otherwise not practicable, the  
7 Commission may use such funds for the purpose of  
8 consumer or business education relating to data pri-  
9 vacy and security or for the purpose of engaging in  
10 technological research that the Commission con-  
11 sidered necessary to enforce this Act.

12 (4) AMOUNTS NOT SUBJECT TO APPORTION-  
13 MENT.—Notwithstanding any other provision of law,  
14 amounts in the Victims Relief Fund shall not be  
15 subject to apportionment for purposes of chapter 15  
16 of title 31, United States Code, or under any other  
17 authority.

18 (e) AUTHORIZATION OF APPROPRIATIONS.—There is  
19 authorized to be appropriated to the Commission  
20 \$100,000,000 to carry out this Act.

21 **SEC. 402. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

22 (a) CIVIL ACTION.—In any case in which the attor-  
23 ney general of a State has reason to believe that an inter-  
24 est of the residents of that State has been or is adversely  
25 affected by the engagement of any covered entity in an

1 act or practice that violates this Act or a regulation pro-  
2 mulgated under this Act, the attorney general of the State,  
3 as *parens patriae*, may bring a civil action on behalf of  
4 the residents of the State in an appropriate district court  
5 of the United States to—

6 (1) enjoin that act or practice;

7 (2) enforce compliance with this Act or the reg-  
8 ulation;

9 (3) obtain damages, civil penalties, restitution,  
10 or other compensation on behalf of the residents of  
11 the State; or

12 (4) obtain such other relief as the court may  
13 consider to be appropriate.

14 (b) RIGHTS OF THE COMMISSION.—

15 (1) IN GENERAL.—Except where not feasible,  
16 the attorney general of a State shall notify the Com-  
17 mission in writing prior to initiating a civil action  
18 under subsection (a). Such notice shall include a  
19 copy of the complaint to be filed to initiate such ac-  
20 tion. Upon receiving such notice, the Commission  
21 may intervene in such action and, upon inter-  
22 vening—

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

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

3 (2) NOTIFICATION TIMELINE.—Where it is not  
4 feasible for the attorney general of a State to pro-  
5 vide the notification required by paragraph (2) be-  
6 fore initiating a civil action under paragraph (1), the  
7 attorney general shall notify the Commission imme-  
8 diately after initiating the civil action.

9 (c) CONSOLIDATION OF ACTIONS BROUGHT BY TWO  
10 OR MORE STATE ATTORNEYS GENERAL.—Whenever a  
11 civil action under subsection (a) is pending and another  
12 civil action or actions are commenced pursuant to such  
13 subsection in a different Federal district court or courts  
14 that involve 1 or more common questions of fact, a defend-  
15 ant in such action or actions may request that such action  
16 or actions be transferred for the purposes of consolidated  
17 pretrial proceedings and trial to the United States District  
18 Court for the District of Columbia; provided however, that  
19 no such action shall be transferred if pretrial proceedings  
20 in that action have been concluded before a subsequent  
21 action is filed by the attorney general of the State.

22 (d) ACTIONS BY COMMISSION.—In any case in which  
23 a civil action is instituted by or on behalf of the Commis-  
24 sion for violation of this Act or a regulation promulgated  
25 under this Act, no attorney general of a State may, during

1 the pendency of such action, institute a civil action against  
2 any defendant named in the complaint in the action insti-  
3 tuted by or on behalf of the Commission for violation of  
4 this Act or a regulation promulgated under this Act that  
5 is alleged in such complaint.

6 (e) INVESTIGATORY POWERS.—Nothing in this sec-  
7 tion shall be construed to prevent the attorney general of  
8 a State or another authorized official of a State from exer-  
9 cising the powers conferred on the attorney general or the  
10 State official by the laws of the State to conduct investiga-  
11 tions, to administer oaths or affirmations, or to compel  
12 the attendance of witnesses or the production of documen-  
13 tary or other evidence.

14 (f) VENUE; SERVICE OF PROCESS.—

15 (1) VENUE.—Any action brought under sub-  
16 section (a) may be brought in the district court of  
17 the United States that meets applicable require-  
18 ments relating to venue under section 1391 of title  
19 28, United States Code.

20 (2) SERVICE OF PROCESS.—In an action  
21 brought under subsection (a), process may be served  
22 in any district in which the defendant—

23 (A) is an inhabitant; or

24 (B) may be found.

1 (g) ACTIONS BY OTHER STATE OFFICIALS.—Any  
2 State official who is authorized by the State attorney gen-  
3 eral to be the exclusive authority in that State to enforce  
4 this Act may bring a civil action under subsection (a), sub-  
5 ject to the same requirements and limitations that apply  
6 under this section to civil actions brought under such sub-  
7 section by State attorneys general.

8 **SEC. 403. APPROVED CERTIFICATION PROGRAMS.**

9 (a) IN GENERAL.—The Commission shall establish a  
10 program in which the Commission shall approve voluntary  
11 consensus standards or certification programs that cov-  
12 ered entities may use to comply with 1 or more provisions  
13 in this Act.

14 (b) EFFECT OF APPROVAL.—A covered entity in com-  
15 pliance with a voluntary consensus standard approved by  
16 the Commission shall be deemed to be in compliance with  
17 the provisions of this Act.

18 (c) TIME FOR APPROVAL.—The Commission shall  
19 issue a decision regarding the approval of a proposed vol-  
20 untary consensus standard not later than 180 days after  
21 a request for approval is submitted.

22 (d) EFFECT OF NON-COMPLIANCE.—A covered entity  
23 that claims compliance with an approved voluntary con-  
24 sensus standard and is found not to be in compliance with

1 such program by the Commission or in any judicial pro-  
2 ceeding shall be considered to be in violation of this Act.

3 (e) RULEMAKING.—Not later than 120 days after the  
4 date of enactment of this Act, the Commission shall pro-  
5 mulgate regulations under section 553 of title 5, United  
6 States Code, establishing a process for review of requests  
7 for approval of proposed voluntary consensus standards  
8 under this section.

9 (f) REQUIREMENTS.—To be eligible for approval by  
10 the Commission, a voluntary consensus standard shall  
11 meet the requirements for voluntary consensus standards  
12 set forth in Office of Management and Budget Circular  
13 A–119, or other equivalent guidance document, ensuring  
14 that they are the result of due process procedures and ap-  
15 propriately balance the interests of all the stakeholders,  
16 including individuals, businesses, organizations, and other  
17 entities making lawful uses of the covered data covered  
18 by the standard, and—

19 (1) specify clear and enforceable requirements  
20 for covered entities participating in the program that  
21 provide an overall level of data privacy or data secu-  
22 rity protection that is equivalent to or greater than  
23 that provided in the relevant provisions in this Act;

24 (2) require each participating covered entity to  
25 post in a prominent place a clear and conspicuous



1 public attestation of compliance and a link to the  
2 website described in paragraph (4);

3 (3) include a process for an independent assess-  
4 ment of a participating covered entity's compliance  
5 with the voluntary consensus standard or certifi-  
6 cation program prior to certification and at reason-  
7 able intervals thereafter;

8 (4) create a website describing the voluntary  
9 consensus standard or certification program's goals  
10 and requirements, listing participating covered enti-  
11 ties, and providing a method for individuals to ask  
12 questions and file complaints about the program or  
13 any participating covered entity;

14 (5) take meaningful action for non-compliance  
15 with the relevant provisions of this Act by any par-  
16 ticipating covered entity, which shall depend on the  
17 severity of the non-compliance and may include—

18 (A) removing the covered entity from the  
19 program;

20 (B) referring the covered entity to the  
21 Commission or other appropriate Federal or  
22 State agencies for enforcement;

23 (C) publicly reporting the disciplinary ac-  
24 tion taken with respect to the covered entity;

1 (D) providing redress to individuals  
2 harmed by the non-compliance;

3 (E) making voluntary payments to the  
4 United States Treasury; and

5 (F) taking any other action or actions to  
6 ensure the compliance of the covered entity with  
7 respect to the relevant provisions of this Act;  
8 and

9 (6) issue annual reports to the Commission and  
10 to the public detailing the activities of the program  
11 and its effectiveness during the preceding year in en-  
12 suring compliance with the relevant provisions of  
13 this Act by participating covered entities and taking  
14 meaningful disciplinary action for non-compliance  
15 with such provisions by such entities.

16 **SEC. 404. RELATIONSHIP BETWEEN FEDERAL AND STATE**  
17 **LAW.**

18 (a) **RELATIONSHIP TO STATE LAW.**—No State or po-  
19 litical subdivision of a State may adopt, maintain, enforce,  
20 or continue in effect any law, regulation, rule, require-  
21 ment, or standard related to the data privacy or data secu-  
22 rity and associated activities of covered entities.

23 (b) **SAVINGS PROVISION.**—Subsection (a) may not be  
24 construed to preempt State laws that directly establish re-

1 requirements for the notification of consumers in the event  
2 of a data breach.

3 (c) RELATIONSHIP TO OTHER FEDERAL LAWS.—

4 (1) IN GENERAL.—Except as provided in para-  
5 graphs (2) and (3), the requirements of this Act  
6 shall supersede any other Federal law or regulation  
7 relating to the privacy or security of covered data or  
8 associated activities of covered entities.

9 (2) SAVINGS PROVISION.—This Act may not be  
10 construed to modify, limit, or supersede the oper-  
11 ation of the following:

12 (A) The Children’s Online Privacy Protec-  
13 tion Act (15 U.S.C. 6501 et seq.).

14 (B) The Communications Assistance for  
15 Law Enforcement Act (47 U.S.C. 1001 et seq.).

16 (C) Section 227 of the Communications  
17 Act of 1934 (47 U.S.C. 227).

18 (D) Title V of the Gramm-Leach-Bliley  
19 Act (15 U.S.C. 6801 et seq.).

20 (E) The Fair Credit Reporting Act (15  
21 U.S.C. 1681 et seq.).

22 (F) The Health Insurance Portability and  
23 Accountability Act (Public Law 104–191).

24 (G) The Electronic Communications Pri-  
25 vacy Act (18 U.S.C. 2510 et seq.).

1 (H) Section 444 of the General Education  
2 Provisions Act (20 U.S.C. 1232g) (commonly  
3 referred to as the “Family Educational Rights  
4 and Privacy Act of 1974”).

5 (I) The Driver’s Privacy Protection Act of  
6 1994 (18 U.S.C. 2721 et seq).

7 (J) The Federal Aviation Act of 1958 (49  
8 U.S.C. App. 1301 et seq.).

9 (K) The Health Information Technology  
10 for Economic and Clinical Health Act (42  
11 U.S.C. 17931 et seq).

12 (3) COMPLIANCE WITH SAVED FEDERAL  
13 LAWS.—To the extent that the data collection, proc-  
14 essing, or transfer activities of a covered entity are  
15 subject to a law listed in paragraph (2), such activi-  
16 ties of such entity shall not be subject to the re-  
17 quirements of this Act.

18 (4) NONAPPLICATION OF FCC LAWS AND REGU-  
19 LATIONS TO COVERED ENTITIES.—Notwithstanding  
20 any other provision of law, neither any provision of  
21 the Communications Act of 1934 (47 U.S.C. 151 et.  
22 seq.) and all Acts amendatory thereof and supple-  
23 mentary thereto nor any regulation promulgated by  
24 the Federal Communications Commission under  
25 such Acts shall apply to any covered entity with re-

1       spect to the collection, use, processing, transferring,  
2       or security of individual information, except to the  
3       extent that such provision or regulation pertains  
4       solely to “911” lines or other emergency line of a  
5       hospital, medical provider or service office, health  
6       care facility, poison control center, fire protection  
7       agency, or law enforcement agency.

8       **SEC. 405. CONSTITUTIONAL AVOIDANCE.**

9       The provisions of this Act shall be construed, to the  
10      greatest extent possible, to avoid conflicting with the Con-  
11      stitution of the United States, including the protections  
12      of free speech and freedom of the press established under  
13      the First Amendment to the Constitution of the United  
14      States.

15      **SEC. 406. SEVERABILITY.**

16      If any provision of this Act, or an amendment made  
17      by this Act, is determined to be unenforceable or invalid,  
18      the remaining provisions of this Act and the amendments  
19      made by this Act shall not be affected.