

**AMENDMENT TO THE AMENDMENT IN THE
NATURE OF A SUBSTITUTE FOR H.R. 2668
OFFERED BY M . _____**

Before section 1 of the bill, insert the following:

1 **DIVISION A—CONSUMER**
2 **PROTECTION AND RECOVERY**

In section 1, strike “This Act” and insert “This division”.

At the end of the bill, insert the following:

3 **DIVISION B—SETTING AN AMER-**
4 **ICAN FRAMEWORK TO EN-**
5 **SURE DATA ACCESS, TRANS-**
6 **PARENCY, AND ACCOUNT-**
7 **ABILITY**

8 **SEC. 11. SHORT TITLE; TABLE OF CONTENTS.**

9 (a) **SHORT TITLE.**—This division may be cited as the
10 “Setting an American Framework to Ensure Data Access,
11 Transparency, and Accountability Act” or the “SAFE
12 DATA Act”.

13 (b) **TABLE OF CONTENTS.**—The table of contents for
14 this division is as follows:

Sec. 11. Short title; table of contents.

- Sec. 12. Definitions.
- Sec. 13. 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. Algorithm bias, detection, and mitigation.
- Sec. 202. Digital content forgeries.
- Sec. 203. Data brokers.
- Sec. 204. Protection of covered data.
- Sec. 205. Filter bubble transparency.
- Sec. 206. Unfair and deceptive acts and practices relating to the manipulation of user interfaces.

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. 12. DEFINITIONS.**

2 In this division:

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

1 communicating the individual’s authorization for the
2 act or practice.

3 (2) ALGORITHM.—The term “algorithm” means
4 a computational process derived from machine learn-
5 ing, statistics, or other data processing or artificial
6 intelligence techniques, that processes covered data
7 for the purpose of making a decision or facilitating
8 human decision making.

9 (3) ALGORITHMIC RANKING SYSTEM.—The
10 term “algorithmic ranking system” means a com-
11 putational process, including one derived from algo-
12 rithmic decision making, machine learning, statisti-
13 cal analysis, or other data processing or artificial
14 intelligence techniques, used to determine the order
15 or manner that a set of information is provided to
16 a user on a covered internet platform, including the
17 ranking of search results, the provision of content
18 recommendations, the display of social media posts,
19 or any other method of automated content selection.

20 (4) BEHAVIORAL OR PSYCHOLOGICAL EXPERI-
21 MENTS OR RESEARCH.—The term “behavioral or
22 psychological experiments or research” means the
23 study, including through human experimentation, of
24 overt or observable actions and mental phenomena
25 inferred from behavior, including interactions be-

1 tween and among individuals and the activities of so-
2 cial groups.

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

7 (6) COMMISSION.—The term “Commission”
8 means the Federal Trade Commission.

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

12 (8) COMPULSIVE USAGE.—The term “compul-
13 sive usage” means any response stimulated by exter-
14 nal factors that causes an individual to engage in re-
15 petitive, purposeful, and intentional behavior causing
16 psychological distress, loss of control, anxiety, de-
17 pression, or harmful stress responses.

18 (9) CONNECTED DEVICE.—For purposes of
19 paragraphs (20) and (37), the term “connected de-
20 vice” means a physical object that—

21 (A) is capable of connecting to the inter-
22 net, either directly or indirectly through a net-
23 work, to communicate information at the direc-
24 tion of an individual; and

1 (B) has computer processing capabilities
2 for collecting, sending, receiving, or analyzing
3 data.

4 (10) COVERED DATA.—

5 (A) IN GENERAL.—The term “covered
6 data” means information that identifies or is
7 linked or reasonably linkable to an individual or
8 a device that is linked or reasonably linkable to
9 an individual.

10 (B) LINKED OR REASONABLY LINKABLE.—
11 For purposes of subparagraph (A), information
12 held by a covered entity is linked or reasonably
13 linkable to an individual or a device if, as a
14 practical matter, it can be used on its own or
15 in combination with other information held by,
16 or readily accessible to, the covered entity to
17 identify such individual or such device.

18 (C) EXCLUSIONS.—Such term does not in-
19 clude—

20 (i) aggregated data;

21 (ii) de-identified data;

22 (iii) employee data; or

23 (iv) publicly available information.

24 (D) AGGREGATED DATA.—For purposes of
25 subparagraph (C), the term “aggregated data”

1 means information that relates to a group or
2 category of individuals or devices that does not
3 identify and is not linked or reasonably linkable
4 to any individual.

5 (E) DE-IDENTIFIED DATA.—For purposes
6 of subparagraph (C), the term “de-identified
7 data” means information held by a covered en-
8 tity that—

9 (i) does not identify, and is not linked
10 or reasonably linkable to, an individual or
11 device;

12 (ii) does not contain any persistent
13 identifier or other information that could
14 readily be used to re-identify the individual
15 to whom, or the device to which, the identi-
16 fier or information pertains;

17 (iii) is subject to a public commitment
18 by the covered entity—

19 (I) to refrain from attempting to
20 use such information to identify any
21 individual or device; and

22 (II) to adopt technical and orga-
23 nizational measures to ensure that
24 such information is not linked to any
25 individual or device; and

1 (iv) is not disclosed by the covered en-
2 tity to any other party unless the disclo-
3 sure is subject to a contractually or other
4 legally binding requirement that—

5 (I) the recipient of the informa-
6 tion shall not use the information to
7 identify any individual or device; and

8 (II) all onward disclosures of the
9 information shall be subject to the re-
10 quirement described in subclause (I).

11 (F) EMPLOYEE DATA.—For purposes of
12 subparagraph (C), the term “employee data”
13 means—

14 (i) information relating to an indi-
15 vidual collected by a covered entity in the
16 course of the individual acting as a job ap-
17 plicant to, or employee (regardless of
18 whether such employee is paid or unpaid,
19 or employed on a temporary basis), owner,
20 director, officer, staff member, trainee,
21 vendor, visitor, volunteer, intern, or con-
22 tractor of, the entity, provided that such
23 information is collected, processed, or
24 transferred by the covered entity solely for
25 purposes related to the individual’s status

1 as a current or former job applicant to, or
2 an employee, owner, director, officer, staff
3 member, trainee, vendor, visitor, volunteer,
4 intern, or contractor of, that covered enti-
5 ty;

6 (ii) business contact information of an
7 individual, including the individual's name,
8 position or title, business telephone num-
9 ber, business address, business email ad-
10 dress, qualifications, and other similar in-
11 formation, that is provided to a covered en-
12 tity by an individual who is acting in a
13 professional capacity, provided that such
14 information is collected, processed, or
15 transferred solely for purposes related to
16 such individual's professional activities;

17 (iii) emergency contact information
18 collected by a covered entity that relates to
19 an individual who is acting in a role de-
20 scribed in clause (i) with respect to the
21 covered entity, provided that such informa-
22 tion is collected, processed, or transferred
23 solely for the purpose of having an emer-
24 gency contact on file for the individual; or

1 (iv) information relating to an indi-
2 vidual (or a relative or beneficiary of such
3 individual) that is necessary for the cov-
4 ered entity to collect, process, or transfer
5 for the purpose of administering benefits
6 to which such individual (or relative or
7 beneficiary of such individual) is entitled
8 on the basis of the individual acting in a
9 role described in clause (i) with respect to
10 the entity, provided that such information
11 is collected, processed, or transferred solely
12 for the purpose of administering such ben-
13 efits.

14 (G) PUBLICLY AVAILABLE INFORMA-
15 TION.—

16 (i) IN GENERAL.—For the purposes of
17 subparagraph (C), the term “publicly
18 available information” means any informa-
19 tion that a covered entity has a reasonable
20 basis to believe—

21 (I) has been lawfully made avail-
22 able to the general public from Fed-
23 eral, State, or local government
24 records;

1 (II) is widely available to the
2 general public, including information
3 from—

4 (aa) a telephone book or on-
5 line directory;

6 (bb) television, internet, or
7 radio content or programming; or

8 (cc) the news media or a
9 website that is lawfully available
10 to the general public on an unre-
11 stricted basis (for purposes of
12 this subclause a website is not re-
13 stricted solely because there is a
14 fee or log-in requirement associ-
15 ated with accessing the website);
16 or

17 (III) is a disclosure to the gen-
18 eral public that is required to be made
19 by Federal, State, or local law.

20 (ii) EXCLUSIONS.—Such term does
21 not include an obscene visual depiction (as
22 defined for purposes of section 1460 of
23 title 18, United States Code).

24 (11) COVERED ENTITY.—The term “covered
25 entity” means any person that—

1 (A) is subject to the Federal Trade Com-
2 mission Act (15 U.S.C. 41 et seq.) or is—

3 (i) a common carrier described in sec-
4 tion 5(a)(2) of such Act (15 U.S.C.
5 45(a)(2)); or

6 (ii) an organization not organized to
7 carry on business for their own profit or
8 that of their members;

9 (B) collects, processes, or transfers covered
10 data; and

11 (C) determines the purposes and means of
12 such collection, processing, or transfer.

13 (12) COVERED INTERNET PLATFORM.—

14 (A) IN GENERAL.—The term “covered
15 internet platform” means any public-facing
16 website, internet application, or mobile applica-
17 tion, including a social network site, video shar-
18 ing service, search engine, or content aggrega-
19 tion service.

20 (B) EXCLUSIONS.—Such term shall not in-
21 clude a platform that—

22 (i) is wholly owned, controlled, and
23 operated by a person that—

1 (I) for the most recent 6-month
2 period, did not employ more than 500
3 employees;

4 (II) for the most recent 3-year
5 period, averaged less than
6 \$50,000,000 in annual gross receipts;
7 and

8 (III) collects or processes on an
9 annual basis the personal data of less
10 than 1,000,000 individuals; or

11 (ii) is operated for the sole purpose of
12 conducting research that is not made for
13 profit either directly or indirectly.

14 (13) DATA BROKER.—

15 (A) IN GENERAL.—The term “data
16 broker” means a covered entity whose principal
17 source of revenue is derived from processing or
18 transferring the covered data of individuals with
19 whom the entity does not have a direct relation-
20 ship on behalf of third parties for such third
21 parties’ use.

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

24 (14) DELETE.—The term “delete” means to re-
25 move or destroy information such that it is not

1 maintained in human or machine readable form and
2 cannot be retrieved or utilized in such form in the
3 normal course of business.

4 (15) EXECUTIVE AGENCY.—The term “Execu-
5 tive agency” has the meaning set forth in section
6 105 of title 5, United States Code.

7 (16) INDEPENDENT REVIEW BOARD.—The term
8 “independent review board” means a board, com-
9 mittee, or other group formally designated by a large
10 online operator to review, to approve the initiation
11 of, and to conduct periodic review of, any research
12 by, or at the direction or discretion of a large online
13 operator, involving human subjects.

14 (17) INDIVIDUAL.—The term “individual”
15 means a natural person residing in the United
16 States.

17 (18) INFERRED DATA.—The term “inferred
18 data” means information that is created by a cov-
19 ered entity through the derivation of information,
20 data, assumptions, or conclusions from facts, evi-
21 dence, or another source of information or data.

22 (19) INFORMED CONSENT.—For purposes of
23 section 206, the term “informed consent”—

24 (A) means a process by which a research
25 subject is provided adequate information prior

1 to being included in any experiment or study to
2 allow for an informed decision about voluntary
3 participation in a behavioral or psychological re-
4 search experiment or study, while ensuring the
5 understanding of the potential participant of
6 the furnished information and any associated
7 benefits, risks, or consequences of participation
8 prior to obtaining the voluntary agreement to
9 participate by the participant; and

10 (B) does not include—

11 (i) the consent of an individual under
12 the age of 13; or

13 (ii) the consent to a provision con-
14 tained in a general contract or service
15 agreement.

16 (20) INPUT-TRANSPARENT ALGORITHM.—

17 (A) IN GENERAL.—For purposes of section
18 205, the term “input-transparent algorithm”
19 means an algorithmic ranking system that does
20 not use the user-specific data of a user to deter-
21 mine the order or manner that information is
22 furnished to such user on a covered internet
23 platform, unless the user-specific data is ex-
24 pressly provided to the platform by the user for
25 such purpose.

1 (B) INCLUSION OF AGE-APPROPRIATE CON-
2 TENT FILTERS.—Such term shall include an al-
3 gorithmic ranking system that uses user-specific
4 data to determine whether a user is old enough
5 to access age-restricted content on a covered
6 internet platform, provided that the system oth-
7 erwise meets the requirements of subparagraph
8 (A).

9 (C) DATA PROVIDED FOR EXPRESS PUR-
10 POSE OF INTERACTION WITH PLATFORM.—For
11 purposes of subparagraph (A), user-specific
12 data that is provided by a user for the express
13 purpose of determining the order or manner
14 that information is furnished to a user on a
15 covered internet platform—

16 (i) shall include user-supplied search
17 terms, filters, speech patterns (if provided
18 for the purpose of enabling the platform to
19 accept spoken input or selecting the lan-
20 guage in which the user interacts with the
21 platform), saved preferences, and the
22 user's current geographical location;

23 (ii) shall include data supplied to the
24 platform by the user that expresses the
25 user's desire that information be furnished

1 to them, such as the social media profiles
2 the user follows, the video channels the
3 user subscribes to, or other sources of con-
4 tent on the platform the user follows;

5 (iii) shall not include the history of
6 the user's connected device, including the
7 user's history of web searches and brows-
8 ing, geographical locations, physical activ-
9 ity, device interaction, and financial trans-
10 actions; and

11 (iv) shall not include inferences about
12 the user or the user's connected device,
13 without regard to whether such inferences
14 are based on data described in clause (i).

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

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

20 (B) processed or transferred the sensitive
21 covered data of more than 300,000 individuals
22 or devices that are linked or reasonably linkable
23 to an individual (excluding any instance where
24 the covered entity processes the log-in informa-
25 tion of an individual or device to allow the indi-

1 vidual or device to log in to an account adminis-
2 tered by the covered entity).

3 (22) LARGE ONLINE OPERATOR.—For purposes
4 of section 206, the term “large online operator”
5 means any person that—

6 (A) provides an online service;

7 (B) has more than 100,000,000 authenti-
8 cated users of an online service in any 30-day
9 period; and

10 (C) is subject to the jurisdiction of the
11 Commission under the Federal Trade Commis-
12 sion Act (15 U.S.C. 41 et seq.).

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

20 (24) ONLINE SERVICE.—For purposes of sec-
21 tion 206, the term “online service” means a website
22 or a service, other than an internet access service,
23 that is made available to the public over the inter-
24 net, including a social network, a search engine, or
25 email service.

1 (25) OPAQUE ALGORITHM.—

2 (A) IN GENERAL.—The term “opaque al-
3 gorithm” means an algorithmic ranking system
4 that determines the order or manner that infor-
5 mation is furnished to a user on a covered
6 internet platform based, in whole or part, on
7 user-specific data that was not expressly pro-
8 vided by the user to the platform for such pur-
9 pose.

10 (B) EXCEPTION FOR AGE-APPROPRIATE
11 CONTENT FILTERS.—Such term shall not in-
12 clude an algorithmic ranking system used by a
13 covered internet platform if—

14 (i) the only user-specific data (includ-
15 ing inferences about the user) that the sys-
16 tem uses is information relating to the age
17 of the user; and

18 (ii) such information is only used to
19 restrict a user’s access to content on the
20 basis that the individual is not old enough
21 to access such content.

22 (26) PROCESS.—The term “process” means
23 any operation or set of operations performed on cov-
24 ered data including analysis, organization, struc-

1 turing, retaining, using, or otherwise handling cov-
2 ered data.

3 (27) PROCESSING PURPOSE.—The term “proc-
4 essing purpose” means a reason for which a covered
5 entity processes covered data.

6 (28) RESEARCH.—The term “research” means
7 the scientific analysis of information, including cov-
8 ered data, by a covered entity or those with whom
9 the covered entity is cooperating or others acting at
10 the direction or on behalf of the covered entity, that
11 is conducted for the primary purpose of advancing
12 scientific knowledge and may be for the commercial
13 benefit of the covered entity.

14 (29) SEARCH SYNDICATION CONTRACT; UP-
15 STREAM PROVIDER; DOWNSTREAM PROVIDER.—

16 (A) SEARCH SYNDICATION CONTRACT.—
17 The term “search syndication contract” means
18 a contract or subcontract for the sale, license,
19 or other right to access an index of web pages
20 on the internet for the purpose of operating an
21 internet search engine.

22 (B) UPSTREAM PROVIDER.—The term
23 “upstream provider” means, with respect to a
24 search syndication contract, the person that
25 grants access to an index of web pages on the

1 internet to a downstream provider under the
2 contract.

3 (C) DOWNSTREAM PROVIDER.—The term
4 “downstream provider” means, with respect to
5 a search syndication contract, the person that
6 receives access to an index of web pages on the
7 internet from an upstream provider under such
8 contract.

9 (30) SENSITIVE COVERED DATA.—

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

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

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

23 (iii) A financial account number, debit
24 card number, credit card number, or any
25 required security or access code, password,

1 or credentials allowing access to any such
2 account.

3 (iv) Covered data that is biometric in-
4 formation.

5 (v) A persistent identifier.

6 (vi) Precise geolocation information.

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

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

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

23 (x) Covered data revealing the sexual
24 orientation or sexual behavior of an indi-
25 vidual in a manner inconsistent with the

1 individual's reasonable expectation regard-
2 ing the processing or transfer of such in-
3 formation.

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

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

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

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

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

1 (i) means the physiological or biological
2 cal characteristics of an individual, including
3 deoxyribonucleic acid, that are used,
4 singly or in combination with each other or
5 with other identifying data, to establish the
6 identity of an individual; and

7 (ii) includes—

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

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

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

1 essor or device serial number, or another unique
2 device identifier.

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

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

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

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

23 (32) SERVICE PROVIDER DATA.—The term
24 “service provider data” means, with respect to a set
25 of covered data and a service provider, covered data

1 that is collected by the service provider on behalf of
2 a covered entity or transferred to the service pro-
3 vider by a covered entity for the purpose of allowing
4 the service provider to perform a service or function
5 on behalf of, and at the direction of, such covered
6 entity.

7 (33) **THIRD PARTY.**—The term “third party”
8 means, with respect to a set of covered data, a cov-
9 ered entity—

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

12 (B) that received such covered data from
13 another covered entity—

14 (i) that is not related to the covered
15 entity by common ownership or corporate
16 control; and

17 (ii) that does not share common
18 branding with the covered entity.

19 (34) **THIRD PARTY DATA.**—The term “third
20 party data” means, with respect to a third party,
21 covered data that has been transferred to the third
22 party by a covered entity.

23 (35) **TRANSFER.**—The term “transfer” means
24 to disclose, release, share, disseminate, make avail-
25 able, or license in writing, electronically, or by any

1 other means for consideration of any kind or for a
2 commercial purpose.

3 (36) USER DATA.—For purposes of section
4 206, the term “user data” means any information
5 relating to an identified or identifiable individual
6 user, whether directly submitted to the large online
7 operator by the user, or derived from the observed
8 activity of the user by the large online operator.

9 (37) USER-SPECIFIC DATA.—For purposes of
10 section 205, the term “user-specific data” means in-
11 formation relating to an individual or a specific con-
12 nected device that would not necessarily be true of
13 every individual or device.

14 **SEC. 13. EFFECTIVE DATE.**

15 Except as otherwise provided in this division, this di-
16 vision shall take effect 18 months after the date of enact-
17 ment of this Act.

18 **TITLE I—INDIVIDUAL**
19 **CONSUMER DATA RIGHTS**

20 **SEC. 101. CONSUMER LOYALTY.**

21 (a) PROHIBITION ON THE DENIAL OF PRODUCTS OR
22 SERVICES.—

23 (1) IN GENERAL.—Subject to paragraph (2), a
24 covered entity shall not deny products or services to
25 an individual because the individual exercises a right

1 established under subparagraph (A), (B), or (D) of
2 section 103(a)(1).

3 (2) RULES OF APPLICATION.—A covered enti-
4 ty—

5 (A) shall not be in violation of paragraph
6 (1) with respect to a product or service and an
7 individual if the exercise of a right described in
8 such paragraph by the individual precludes the
9 covered entity from providing such product or
10 service to such individual; and

11 (B) may offer different types of pricing
12 and functionalities with respect to a product or
13 service based on an individual's exercise of a
14 right described in such paragraph.

15 (b) NO WAIVER OF INDIVIDUAL CONTROLS.—The
16 rights and obligations created under section 103 may not
17 be waived in an agreement between a covered entity and
18 an individual.

19 **SEC. 102. TRANSPARENCY.**

20 (a) IN GENERAL.—A covered entity that processes
21 covered data shall, with respect to such data, publish a
22 privacy policy that is—

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

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

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

6 (1) The identity and the contact information of
7 the covered entity (including the covered entity's
8 points of contact for privacy and data security in-
9 quiries) and the identity of any affiliate to which
10 covered data may be transferred by the covered enti-
11 ty.

12 (2) The categories of covered data the covered
13 entity collects.

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

16 (4) Whether the covered entity transfers cov-
17 ered data, the categories of recipients to whom the
18 covered entity transfers covered data, and the pur-
19 poses of the transfers.

20 (5) A general description of the covered entity's
21 data retention practices for covered data and the
22 purposes for such retention.

23 (6) How individuals can exercise their rights
24 under section 103.

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

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

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

9 (d) MATERIAL CHANGES.—If a covered entity makes
10 a material change to its privacy policy, it shall notify the
11 individuals affected before further processing or transfer-
12 ring of previously collected covered data and provide an
13 opportunity to withdraw consent to further processing or
14 transferring of the covered data under the changed policy.
15 The covered entity shall provide direct notification, where
16 possible, regarding a material change to the privacy policy
17 to affected individuals, taking into account available tech-
18 nology and the nature of the relationship.

19 (e) APPLICATION TO INDIRECT TRANSFERS.—Where
20 the ownership of an individual's device is transferred di-
21 rectly from one individual to another individual, a covered
22 entity may satisfy its obligation to disclose a privacy policy
23 prior to or at the point of collection of covered data by
24 making the privacy policy available under subsection
25 (a)(2).

1 **SEC. 103. INDIVIDUAL CONTROL.**

2 (a) ACCESS TO, AND CORRECTION, DELETION, AND
3 PORTABILITY OF, COVERED DATA.—

4 (1) IN GENERAL.—Subject to paragraphs (2)
5 and (3), a covered entity shall provide an individual,
6 immediately or as quickly as possible and in no case
7 later than 90 days after receiving a verified request
8 from the individual, with the right to reasonably—

9 (A) access—

10 (i) the covered data of the individual,
11 or an accurate representation of the cov-
12 ered data of the individual, that is or has
13 been processed by the covered entity or any
14 service provider of the covered entity;

15 (ii) if applicable, a list of categories of
16 third parties and service providers to whom
17 the covered entity has transferred the cov-
18 ered data of the individual; and

19 (iii) if a covered entity transfers cov-
20 ered data, a description of the purpose for
21 which the covered entity transferred the
22 covered data of the individual to a service
23 provider or third party;

24 (B) request that the covered entity—

25 (i) correct material inaccuracies or
26 materially incomplete information with re-

1 spect to the covered data of the individual
2 that is maintained by the covered entity;
3 and

4 (ii) notify any service provider or
5 third party to which the covered entity
6 transferred such covered data of the cor-
7 rected information;

8 (C) request that the covered entity—

9 (i) either delete or de-identify covered
10 data of the individual that is or has been
11 maintained by the covered entity; and

12 (ii) notify any service provider or
13 third party to which the covered entity
14 transferred such covered data of the indi-
15 vidual's request, unless the transfer of
16 such data to the third party was made at
17 the direction of the individual; and

18 (D) to the extent that is technically fea-
19 sible, provide covered data of the individual that
20 is or has been generated and submitted to the
21 covered entity by the individual and maintained
22 by the covered entity in a portable, structured,
23 and machine-readable format that is not subject
24 to licensing restrictions.

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

3 (A) provide an individual with the oppor-
4 tunity to exercise the rights described in para-
5 graph (1) not less than twice in any 12-month
6 period; and

7 (B) with respect to the first 2 times that
8 an individual exercises the rights described in
9 paragraph (1) in any 12-month period, allow
10 the individual to exercise such rights free of
11 charge.

12 (3) EXCEPTIONS.—A covered entity—

13 (A) shall not comply with a request to ex-
14 ercise the rights described in paragraph (1) if
15 the covered entity cannot verify that the indi-
16 vidual making the request is the individual to
17 whom the covered data that is the subject of
18 the request relates;

19 (B) may decline to comply with a request
20 that would—

21 (i) require the covered entity to retain
22 any covered data for the sole purpose of
23 fulfilling the request;

24 (ii) be impossible or demonstrably im-
25 practicable to comply with; or

1 (iii) require the covered entity to com-
2 bine, relink, or otherwise re-identify cov-
3 ered data that has been de-identified;

4 (iv) result in the release of trade se-
5 crets, or other proprietary or confidential
6 data or business practices;

7 (v) interfere with law enforcement, ju-
8 dicial proceedings, investigations, or rea-
9 sonable efforts to guard against, detect, or
10 investigate malicious or unlawful activity,
11 or enforce contracts;

12 (vi) require disproportionate effort,
13 taking into consideration available tech-
14 nology, or would not be reasonably feasible
15 on technical grounds;

16 (vii) compromise the privacy, security,
17 or other rights of the covered data of an-
18 other individual;

19 (viii) be excessive or abusive to an-
20 other individual; or

21 (ix) violate Federal or State law or
22 the rights and freedoms of another indi-
23 vidual, including under the Constitution of
24 the United States; and

1 (C) may delete covered data instead of pro-
2 viding access and correction rights under sub-
3 paragraphs (A) and (B) of paragraph (1) if
4 such covered data—

5 (i) is not sensitive covered data; and
6 (ii) is used only for the purposes of
7 contacting individuals with respect to mar-
8 keting communications.

9 (b) REGULATIONS.—Not later than 1 year after the
10 date of enactment of this Act, the Commission shall pro-
11 mulgate regulations under section 553 of title 5, United
12 States Code, establishing requirements for covered entities
13 with respect to the verification of requests to exercise
14 rights described in subsection (a)(1).

15 **SEC. 104. RIGHTS TO CONSENT.**

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

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

21 (2) process sensitive covered data of the indi-
22 vidual.

23 (b) REQUIREMENTS FOR AFFIRMATIVE EXPRESS
24 CONSENT.—In obtaining the affirmative express consent
25 of an individual to process the sensitive covered data of

1 the individual as required under subsection (a)(2), a cov-
2 ered entity shall provide the individual with notice that
3 shall—

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

7 (2) clearly identify any processing purpose that
8 is necessary to fulfill a request made by the indi-
9 vidual;

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

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

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

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

1 (e) PROHIBITION ON INFERRED CONSENT.—A cov-
2 ered entity shall not infer that an individual has provided
3 affirmative express consent to a processing purpose from
4 the inaction of the individual or the individual’s continued
5 use of a service or product provided by the covered entity.

6 (f) WITHDRAWAL OF CONSENT.—A covered entity
7 shall provide an individual with a clear and conspicuous
8 means to withdraw affirmative express consent.

9 (g) RULEMAKING.—The Commission may promul-
10 gate regulations under section 553 of title 5, United
11 States Code, to establish requirements for covered entities
12 regarding clear and conspicuous procedures for allowing
13 individuals to provide or withdraw affirmative express con-
14 sent for the collection of sensitive covered data.

15 **SEC. 105. MINIMIZING DATA COLLECTION, PROCESSING,**
16 **AND RETENTION.**

17 (a) IN GENERAL.—A covered entity shall not collect,
18 process, or transfer covered data beyond—

19 (1) what is reasonably necessary, proportionate,
20 and limited to provide or improve a product, service,
21 or a communication about a product or service, in-
22 cluding what is reasonably necessary, proportionate,
23 and limited to provide a product or service specifi-
24 cally requested by an individual or reasonably antici-

1 pated within the context of the covered entity's on-
2 going relationship with an individual;

3 (2) what is reasonably necessary, proportionate,
4 or limited to otherwise process or transfer covered
5 data in a manner that is described in the privacy
6 policy that the covered entity is required to publish
7 under section 102(a); or

8 (3) what is expressly permitted by this division
9 or any other applicable Federal law.

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

15 (c) **RULE OF CONSTRUCTION.**—Notwithstanding sec-
16 tion 405 of this division, nothing in this section supersedes
17 any other provision of this division or other applicable
18 Federal law.

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

20 (a) **SERVICE PROVIDERS.**—A service provider—

21 (1) shall not process service provider data for
22 any processing purpose that is not performed on be-
23 half of, and at the direction of, the covered entity
24 that transferred the data to the service provider;

1 (2) shall not transfer service provider data to a
2 third party for any purpose other than a purpose
3 performed on behalf of, or at the direction of, the
4 covered entity that transferred the data to the serv-
5 ice provider without the affirmative express consent
6 of the individual to whom the service provider data
7 relates;

8 (3) at the direction of the covered entity that
9 transferred service provider data to the service pro-
10 vider, shall delete or de-identify such data—

11 (A) as soon as practicable after the service
12 provider has completed providing the service or
13 function for which the data was transferred to
14 the service provider; or

15 (B) as soon as practicable after the end of
16 the period during which the service provider is
17 to provide services with respect to such data, as
18 agreed to by the service provider and the cov-
19 ered entity that transferred the data;

20 (4) is exempt from the requirements of section
21 103 with respect to service provider data, but shall,
22 to the extent practicable—

23 (A) assist the covered entity from which it
24 received the service provider data in fulfilling

1 requests to exercise rights under section 103(a);
2 and

3 (B) upon receiving notice from a covered
4 entity of a verified request made under section
5 103(a)(1) to delete, de-identify, or correct serv-
6 ice provider data held by the service provider,
7 delete, de-identify, or correct such data; and

8 (5) is exempt from the requirements of sections
9 104 and 105.

10 (b) THIRD PARTIES.—A third party—

11 (1) shall not process third party data for a
12 processing purpose inconsistent with the reasonable
13 expectation of the individual to whom such data re-
14 lates;

15 (2) for purposes of paragraph (1), may reason-
16 ably rely on representations made by the covered en-
17 tity that transferred third party data regarding the
18 reasonable expectations of individuals to whom such
19 data relates, provided that the third party conducts
20 reasonable due diligence on the representations of
21 the covered entity and finds those representations to
22 be credible; and

23 (3) is exempt from the requirements of sections
24 104 and 105.

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

5 (1) provide notice of the proposed disclosure of
6 covered data, including the name of the third party
7 and their policies and practices with respect to the
8 covered data, to all affected individuals; and

9 (2) provide each affected individual with the op-
10 portunity to withdraw any previous affirmative ex-
11 press consent related to the covered data of the indi-
12 vidual or request the deletion or de-identification of
13 the covered data of the individual.

14 (d) ADDITIONAL OBLIGATIONS ON COVERED ENTI-
15 TIES.—

16 (1) IN GENERAL.—A covered entity shall exer-
17 cise reasonable due diligence to ensure compliance
18 with this section before—

19 (A) selecting a service provider; or

20 (B) deciding to transfer covered data to a
21 third party.

22 (2) GUIDANCE.—Not later than 2 years after
23 the effective date of this Act, the Commission shall
24 publish guidance regarding compliance with this sub-
25 section. Such guidance shall, to the extent prac-

1 ticable, minimize unreasonable burdens on small-
2 and medium-sized covered entities.

3 **SEC. 107. PRIVACY IMPACT ASSESSMENTS.**

4 (a) PRIVACY IMPACT ASSESSMENTS OF NEW OR MA-
5 TERIAL CHANGES TO PROCESSING OF COVERED DATA.—

6 (1) IN GENERAL.—Not later than 1 year after
7 the date of enactment of this Act (or, if later, not
8 later than 1 year after a covered entity first meets
9 the definition of a large data holder (as defined in
10 section 2)), each covered entity that is a large data
11 holder shall conduct a privacy impact assessment of
12 each of their processing activities involving covered
13 data that present a heightened risk of harm to indi-
14 viduals, and each such assessment shall weigh the
15 benefits of the covered entity's covered data collec-
16 tion, processing, and transfer practices against the
17 potential adverse consequences to individual privacy
18 of such practices.

19 (2) ASSESSMENT REQUIREMENTS.—A privacy
20 impact assessment required under paragraph (1)—

21 (A) shall be reasonable and appropriate in
22 scope given—

23 (i) the nature of the covered data col-
24 lected, processed, or transferred by the
25 covered entity;

1 (ii) the volume of the covered data
2 collected, processed, or transferred by the
3 covered entity;

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

5 (iv) the potential risks posed to the
6 privacy of individuals by the collection,
7 processing, or transfer of covered data by
8 the covered entity;

9 (B) shall be documented in written form
10 and maintained by the covered entity unless
11 rendered out of date by a subsequent assess-
12 ment conducted under subsection (b); and

13 (C) shall be approved by the data privacy
14 officer of the covered entity.

15 (b) ONGOING PRIVACY IMPACT ASSESSMENTS.—

16 (1) IN GENERAL.—A covered entity that is a
17 large data holder shall, not less frequently than once
18 every 2 years after the covered entity conducted the
19 privacy impact assessment required under subsection
20 (a), conduct a privacy impact assessment of the col-
21 lection, processing, and transfer of covered data by
22 the covered entity to assess the extent to which—

23 (A) the ongoing practices of the covered
24 entity are consistent with the covered entity's
25 published privacy policies and other representa-

1 tions that the covered entity makes to individ-
2 uals;

3 (B) any customizable privacy settings in-
4 cluded in a service or product offered by the
5 covered entity are adequately accessible to indi-
6 viduals who use the service or product and are
7 effective in meeting the privacy preferences of
8 such individuals;

9 (C) the practices and privacy settings de-
10 scribed in subparagraphs (A) and (B), respec-
11 tively—

12 (i) meet the expectations of a reason-
13 able individual; and

14 (ii) provide an individual with ade-
15 quate control over the individual's covered
16 data;

17 (D) the covered entity could enhance the
18 privacy and security of covered data through
19 technical or operational safeguards such as
20 encryption, de-identification, and other privacy-
21 enhancing technologies; and

22 (E) the processing of covered data is com-
23 patible with the stated purposes for which it
24 was collected.

1 (2) APPROVAL BY DATA PRIVACY OFFICER.—
2 The data privacy officer of a covered entity shall ap-
3 prove the findings of an assessment conducted by
4 the covered entity under this subsection.

5 **SEC. 108. SCOPE OF COVERAGE.**

6 (a) GENERAL EXCEPTIONS.—Notwithstanding any
7 provision of this title other than subsections (a) through
8 (c) of section 102, a covered entity may collect, process
9 or transfer covered data for any of the following purposes,
10 provided that the collection, processing, or transfer is rea-
11 sonably necessary, proportionate, and limited to such pur-
12 pose:

13 (1) To initiate or complete a transaction or to
14 fulfill an order or provide a service specifically re-
15 quested by an individual, including associated rou-
16 tine administrative activities such as billing, ship-
17 ping, financial reporting, and accounting.

18 (2) To perform internal system maintenance,
19 diagnostics, product or service management, inven-
20 tory management, and network management.

21 (3) To prevent, detect, or respond to a security
22 incident or trespassing, provide a secure environ-
23 ment, or maintain the safety and security of a prod-
24 uct, service, or individual.

1 (4) To protect against malicious, deceptive,
2 fraudulent, or illegal activity.

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

7 (6) To comply with a civil, criminal, or regu-
8 latory inquiry, investigation, subpoena, or summons
9 by an Executive agency.

10 (7) To cooperate with an Executive agency or
11 a law enforcement official acting under the authority
12 of an Executive or State agency concerning conduct
13 or activity that the Executive agency or law enforce-
14 ment official reasonably and in good faith believes
15 may violate Federal, State, or local law, or pose a
16 threat to public safety or national security.

17 (8) To address risks to the safety of an indi-
18 vidual or group of individuals, or to ensure customer
19 safety, including by authenticating individuals in
20 order to provide access to large venues open to the
21 public.

22 (9) To effectuate a product recall pursuant to
23 Federal or State law.

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

1 (A) is in the public interest;

2 (B) adheres to all applicable ethics and
3 privacy laws; and

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

9 (11) To transfer covered data to a service pro-
10 vider.

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

14 (b) **ADDITIONAL PURPOSES.**—The Commission may
15 promulgate regulations under section 553 of title 5,
16 United States Code, identifying additional purposes for
17 which a covered entity may collect, process or transfer cov-
18 ered data.

19 (c) **SMALL BUSINESS EXCEPTION.**—Sections 103,
20 105, and 301 shall not apply in the case of a covered enti-
21 ty that can establish that, for the 3 preceding calendar
22 years (or for the period during which the covered entity
23 has been in existence if such period is less than 3 years)—

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

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

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

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

8 **TITLE II—DATA TRANSPARENCY,**
9 **INTEGRITY, AND SECURITY**

10 **SEC. 201. ALGORITHM BIAS, DETECTION, AND MITIGATION.**

11 (a) FTC ENFORCEMENT ASSISTANCE.—

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

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

1 (A) a summary of the types of information
2 the Commission transmitted to Executive agen-
3 cies or State agencies during the preceding year
4 pursuant to this subsection; and

5 (B) a summary of how such information
6 relates to Federal anti-discrimination laws.

7 (3) COOPERATION WITH OTHER AGENCIES.—
8 The Commission may implement this subsection by
9 executing agreements or memoranda of under-
10 standing with the appropriate Executive agencies.

11 (4) RELATIONSHIP TO OTHER LAWS.—Notwith-
12 standing section 405, nothing in this subsection
13 shall supersede any other provision of law.

14 (b) ALGORITHM TRANSPARENCY REPORTS.—

15 (1) STUDY AND REPORT.—

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

23 (B) REPORT.—Not later than 3 years after
24 the date of enactment of this Act, the Commis-
25 sion shall publish a report containing the re-

1 sults of the study required under subparagraph
2 (A).

3 (C) GUIDANCE.—The Commission shall
4 use the results of the study described in para-
5 graph (A) to develop guidance to assist covered
6 entities in avoiding the discriminatory use of al-
7 gorithms.

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

12 **SEC. 202. DIGITAL CONTENT FORGERIES.**

13 (a) DEFINITION.—Not later than 6 months after the
14 date of enactment of this Act, the National Institute of
15 Standards and Technology shall develop and publish a def-
16 inition of “digital content forgery” and accompanying ex-
17 planatory materials.

18 (b) ELEMENTS OF DEFINITION.—In developing a
19 definition of “digital content forgery” under subsection
20 (a), the National Institute of Standards and Technology
21 shall consider the following factors:

22 (1) Whether the content is created with the in-
23 tent to deceive an individual into believing the con-
24 tent was genuine.

1 (2) Whether the content is genuine or manipu-
2 lated.

3 (3) The impression the content makes on a rea-
4 sonable individual that observes the content.

5 (4) Whether the production of the content was
6 substantially dependent upon technical means, rath-
7 er than the ability of another individual to physically
8 or verbally impersonate such individual.

9 (5) The scope of technologies that may be uti-
10 lized during the creation or publication of digital
11 content forgeries, including—

12 (A) video recording or film;

13 (B) sound recording;

14 (C) electronic image or photograph; or

15 (D) any digital representation of speech or
16 conduct.

17 (c) SCOPE OF DEFINITION.—The definition published
18 by the National Institute of Standards and Technology
19 under subsection (a) shall not supersede any other provi-
20 sion of law or be construed to limit the authority of any
21 Executive agency related to digital content forgeries.

22 (d) COMMISSION REPORTS.—

23 (1) INITIAL REPORT.—Not later than 1 year
24 after the National Institute of Standards and Tech-
25 nology publishes the definition and materials re-

1 required under subsection (a), the Commission shall
2 publish a report regarding the impact of digital con-
3 tent forgeries on individuals and competition.

4 (2) SUBSEQUENT REPORTS.—Not later than 2
5 years after the publication of the report required
6 under paragraph (1), and as often as the Commis-
7 sion shall deem necessary thereafter, the Commis-
8 sion shall publish an updated version of such report.

9 (3) CONTENT OF REPORTS.—Each report re-
10 required under this subsection shall include—

11 (A) a description of the types of digital
12 content forgeries, including those used to com-
13 mit fraud, cause adverse consequences, violate
14 any provision of law enforced by the Commis-
15 sion, or violate civil rights recognized under
16 Federal law;

17 (B) a description of the common sources in
18 the United States of digital content forgeries
19 and commercial sources of digital content for-
20 gery technologies;

21 (C) an assessment of the uses, applica-
22 tions, and adverse consequences of digital con-
23 tent forgeries, including the impact of digital
24 content forgeries on individuals, digital identity,
25 and competition;

1 (D) an analysis of the methods available to
2 individuals to identify digital content forgeries
3 as well as a description of commercial techno-
4 logical countermeasures that are, or could be,
5 used to address concerns with digital content
6 forgeries, which may include countermeasures
7 that warn individuals of suspect content;

8 (E) a description of any remedies available
9 to protect an individual's identity and reputa-
10 tion from adverse consequences caused by dig-
11 ital content forgeries, such as protections or
12 remedies available under the Federal Trade
13 Commission Act (15 U.S.C. 41 et seq.) or any
14 other law; and

15 (F) any additional information the Com-
16 mission determines appropriate.

17 (e) ESTABLISHMENT OF DIGITAL CONTENT FOR-
18 GERY PRIZE COMPETITION.—Not later than 1 year after
19 the date of enactment of this Act, the Director of the Na-
20 tional Institute of Standards and Technology, in coordina-
21 tion with the Commission, shall establish under section 24
22 of the Stevenson-Wydler Technology Innovation Act of
23 1980 (15 U.S.C. 3719) a prize competition to spur the
24 development of technical solutions to assist individuals and

1 the public in identifying digital content forgeries and re-
2 lated technologies.

3 **SEC. 203. DATA BROKERS.**

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

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

12 (1) Pay to the Commission a registration fee of
13 \$100.

14 (2) Provide the Commission with the following
15 information:

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

18 (B) Any additional information or expla-
19 nation the data broker chooses to provide con-
20 cerning its data collection and processing prac-
21 tices.

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

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

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

7 (d) PUBLICATION OF REGISTRATION INFORMA-
8 TION.—The Commission shall publish on the internet
9 website of the Commission the registration information
10 provided by data brokers under this section.

11 **SEC. 204. PROTECTION OF COVERED DATA.**

12 (a) IN GENERAL.—A covered entity shall establish,
13 implement, and maintain reasonable administrative, tech-
14 nical, and physical data security policies and practices to
15 protect against risks to the confidentiality, security, and
16 integrity of covered data.

17 (b) DATA SECURITY REQUIREMENTS.—The data se-
18 curity policies and practices required under subsection (a)
19 shall be—

20 (1) appropriate to the size and complexity of
21 the covered entity, the nature and scope of the cov-
22 ered entity's collection or processing of covered data,
23 the volume and nature of the covered data at issue,
24 and the cost of available tools to improve security
25 and reduce vulnerabilities; and

1 (2) designed to—

2 (A) identify and assess vulnerabilities to
3 covered data;

4 (B) take reasonable preventative and cor-
5 rective action to address known vulnerabilities
6 to covered data; and

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

9 (c) RULEMAKING AND GUIDANCE.—

10 (1) RULEMAKING AUTHORITY AND SCOPE.—

11 (A) IN GENERAL.—The Commission may,
12 pursuant to a proceeding in accordance with
13 section 553 of title 5, United States Code, issue
14 regulations to identify processes for receiving
15 and assessing information regarding vulnerabili-
16 ties to covered data that are reported to the
17 covered entity.

18 (B) CONSULTATION WITH NIST.—In pro-
19 mulgating regulations under this paragraph, the
20 Commission shall consult with, and take into
21 consideration guidance from, the National Insti-
22 tute for Standards and Technology

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

1 (A) identify and assess vulnerabilities to
2 covered data, including—

3 (i) the potential for unauthorized ac-
4 cess to covered data;

5 (ii) vulnerabilities in the covered enti-
6 ty's collection or processing of covered
7 data;

8 (iii) the management of access rights;
9 and

10 (iv) the use of service providers to
11 process covered data;

12 (B) take reasonable preventative and cor-
13 rective action to address vulnerabilities to cov-
14 ered data; and

15 (C) detect, respond to, and recover from
16 cybersecurity incidents and events.

17 (d) APPLICABILITY OF OTHER INFORMATION SECUR-
18 ITY LAWS.—A covered entity that is required to comply
19 with title V of the Gramm-Leach-Bliley Act (15 U.S.C.
20 6801 et seq.) or the Health Information Technology for
21 Economic and Clinical Health Act (42 U.S.C. 17931 et
22 seq.), and is in compliance with the information security
23 requirements of such Act, shall be deemed to be in compli-
24 ance with the requirements of this section with respect to

1 covered data that is subject to the requirements of such
2 Act.

3 **SEC. 205. FILTER BUBBLE TRANSPARENCY.**

4 (a) IN GENERAL.—Beginning on the date that is 1
5 year after the date of enactment of this Act, it shall be
6 unlawful—

7 (1) for any person to operate a covered internet
8 platform that uses an opaque algorithm unless the
9 person complies with the requirements of subsection
10 (b); or

11 (2) for any upstream provider to grant access
12 to an index of web pages on the internet under a
13 search syndication contract that does not comply
14 with the requirements of subsection (c).

15 (b) OPAQUE ALGORITHM REQUIREMENTS.—

16 (1) IN GENERAL.—The requirements of this
17 subsection with respect to a person that operates a
18 covered internet platform that uses an opaque algo-
19 rithm are the following:

20 (A) The person provides notice to users of
21 the platform that the platform uses an opaque
22 algorithm that makes inferences based on user-
23 specific data to select the content the user sees.
24 Such notice shall be presented in a clear, con-
25 spicuous manner on the platform whenever the

1 user interacts with an opaque algorithm for the
2 first time, and may be a one-time notice that
3 can be dismissed by the user.

4 (B) The person makes available a version
5 of the platform that uses an input-transparent
6 algorithm and enables users to easily switch be-
7 tween the version of the platform that uses an
8 opaque algorithm and the version of the plat-
9 form that uses the input-transparent algorithm
10 by selecting a prominently placed icon, which
11 shall be displayed wherever the user interacts
12 with an opaque algorithm.

13 (2) NONAPPLICATION TO CERTAIN DOWN-
14 STREAM PROVIDERS.—Paragraph (1) shall not apply
15 with respect to an internet search engine if—

16 (A) the search engine is operated by a
17 downstream provider with fewer than 1,000 em-
18 ployees; and

19 (B) the search engine uses an index of web
20 pages on the internet to which such provider re-
21 ceived access under a search syndication con-
22 tract.

23 (c) SEARCH SYNDICATION CONTRACT REQUIRE-
24 MENT.—The requirements of this subsection with respect
25 to a search syndication contract are that—

1 (1) as part of the contract, the upstream pro-
2 vider makes available to the downstream provider
3 the same input-transparent algorithm used by the
4 upstream provider for purposes of complying with
5 subsection (b)(1)(B); and

6 (2) the upstream provider does not impose any
7 additional costs, degraded quality, reduced speed, or
8 other constraint on the functioning of such algo-
9 rithm when used by the downstream provider to op-
10 erate an internet search engine relative to the per-
11 formance of such algorithm when used by the up-
12 stream provider to operate an internet search en-
13 gine.

14 **SEC. 206. UNFAIR AND DECEPTIVE ACTS AND PRACTICES**
15 **RELATING TO THE MANIPULATION OF USER**
16 **INTERFACES.**

17 (a) CONDUCT PROHIBITED.—

18 (1) IN GENERAL.—It shall be unlawful for any
19 large online operator—

20 (A) to design, modify, or manipulate a user
21 interface with the purpose or substantial effect
22 of obscuring, subverting, or impairing user au-
23 tonomy, decision making, or choice to obtain
24 consent or user data;

1 (B) to subdivide or segment consumers of
2 online services into groups for the purposes of
3 behavioral or psychological experiments or stud-
4 ies, except with the informed consent of each
5 user involved; or

6 (C) to design, modify, or manipulate a user
7 interface on a website or online service, or por-
8 tion thereof, that is directed to an individual
9 under the age of 13, with the purpose or sub-
10 stantial effect of cultivating compulsive usage,
11 including video auto-play functions initiated
12 without the consent of a user.

13 (b) DUTIES OF LARGE ONLINE OPERATORS.—Any
14 large online operator that engages in any form of behav-
15 ioral or psychological research based on the activity or
16 data of its users shall—

17 (1) disclose to its users on a routine basis, but
18 not less than once each 90 days, any experiments or
19 studies that a user was subjected to or enrolled in
20 with the purpose of promoting engagement or prod-
21 uct conversion;

22 (2) disclose to the public on a routine basis, but
23 not less than once each 90 days, any experiments or
24 studies with the purposes of promoting engagement

1 or product conversion being currently undertaken, or
2 concluded since the prior disclosure;

3 (3) shall present the disclosures in paragraphs
4 (1) and (2) in a manner that—

5 (A) is clear, conspicuous, context appro-
6 priate, and easily accessible; and

7 (B) is not deceptively obscured;

8 (4) establish an Independent Review Board for
9 any behavioral or psychological research, of any pur-
10 pose, conducted on users or on the basis of user ac-
11 tivity or data, which shall review and have authority
12 to approve, require modification in, or disapprove all
13 behavioral or psychological experiments or research;
14 and

15 (5) ensure that any Independent Review Board
16 established under paragraph (4) shall register with
17 the Commission, including providing to the Commis-
18 sion—

19 (A) the names and resumes of every board
20 member;

21 (B) the composition and reporting struc-
22 ture of the Board to the management of the op-
23 erator;

24 (C) the process by which the Board is to
25 be notified of proposed studies or modifications

1 along with the processes by which the Board is
2 capable of vetoing or amending such proposals;

3 (D) any compensation provided to board
4 members; and

5 (E) any conflict of interest that might
6 exist concerning a board member's participation
7 in the Board.

8 (c) REGISTERED PROFESSIONAL STANDARDS
9 BODY.—

10 (1) IN GENERAL.—An association of large on-
11 line operators may register as a professional stand-
12 ards body by filing with the Commission an applica-
13 tion for registration in such form as the Commis-
14 sion, by rule, may prescribe containing the rules of
15 the association and such other information and doc-
16 uments as the Commission, by rule, may prescribe
17 as necessary or appropriate in the public interest or
18 for protecting the welfare of users of large online op-
19 erators.

20 (2) PROFESSIONAL STANDARDS BODY.—An as-
21 sociation of large online operators may not register
22 as a professional standards body unless the Commis-
23 sion determines that—

24 (A) the association is so organized and has
25 the capacity to enforce compliance by its mem-

1 bers and persons associated with its members,
2 with the provisions of this division;

3 (B) the rules of the association provide
4 that any large online operator may become a
5 member of such association;

6 (C) the rules of the association ensure a
7 fair representation of its members in the selec-
8 tion of its directors and administration of its
9 affairs and provide that one or more directors
10 shall be representative of users and not be asso-
11 ciated with, or receive any direct or indirect
12 funding from, a member of the association or
13 any large online operator;

14 (D) the rules of the association are de-
15 signed to prevent exploitative and manipulative
16 acts or practices, to promote transparent and
17 fair principles of technology development and
18 design, to promote research in keeping with
19 best practices of study design and informed
20 consent, and to continually evaluate industry
21 practices and issue binding guidance consistent
22 with the objectives of this division;

23 (E) the rules of the association provide
24 that its members and persons associated with
25 its members shall be appropriately disciplined

1 for violation of any provision of this division,
2 the rules or regulations thereunder, or the rules
3 of the association, by expulsion, suspension,
4 limitation of activities, functions, fine, censure,
5 being suspended or barred from being associ-
6 ated with a member, or any other appropriate
7 sanction; and

8 (F) the rules of the association are in ac-
9 cordance with the provisions of this division,
10 and, in general, provide a fair procedure for the
11 disciplining of members and persons associated
12 with members, the denial of membership to any
13 person seeking membership therein, the barring
14 of any person from becoming associated with a
15 member thereof, and the prohibition or limita-
16 tion by the association of any person with re-
17 spect to access to services offered by the asso-
18 ciation or a member thereof.

19 (3) RESPONSIBILITIES AND ACTIVITIES.—

20 (A) BRIGHT-LINE RULES.—An association
21 shall develop, on a continuing basis, guidance
22 and bright-line rules for the development and
23 design of technology products of large online
24 operators consistent with subparagraph (B).

1 (B) SAFE HARBORS.—In formulating guid-
2 ance under subparagraph (A), the association
3 shall define conduct that does not have the pur-
4 pose or substantial effect of subverting or im-
5 pairing user autonomy, decision making, or
6 choice, or of cultivating compulsive usage for
7 children such as—

8 (i) de minimis user interface changes
9 derived from testing consumer preferences,
10 including different styles, layouts, or text,
11 where such changes are not done with the
12 purpose of obtaining user consent or user
13 data;

14 (ii) algorithms or data outputs outside
15 the control of a large online operator or its
16 affiliates; and

17 (iii) establishing default settings that
18 provide enhanced privacy protection to
19 users or otherwise enhance their autonomy
20 and decision-making ability.

21 (d) ENFORCEMENT BY THE COMMISSION.—

22 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
23 TICE.—A violation of subsection (a) or (b) shall be
24 treated as a violation of a rule defining an unfair or
25 deceptive act or practice under section 18(a)(1)(B)

1 of the Federal Trade Commission Act (15 U.S.C.
2 57a(a)(1)(B)).

3 (2) DETERMINATION.—For purposes of en-
4 forcement of this division, the Commission shall de-
5 termine an act or practice is unfair or deceptive if
6 the act or practice—

7 (A) has the purpose, or substantial effect,
8 of subverting or impairing user autonomy, deci-
9 sion making, or choice to obtain consent or user
10 data; or

11 (B) has the purpose, or substantial effect,
12 of cultivating compulsive usage by a child under
13 13.

14 (3) REGULATIONS.—Not later than 1 year after
15 the date of enactment of this Act, the Commission
16 shall promulgate regulations under section 553 of
17 title 5, United States Code, that—

18 (A) establish rules and procedures for ob-
19 taining the informed consent of users;

20 (B) establish rules for the registration, for-
21 mation, oversight, and management of the inde-
22 pendent review boards, including standards that
23 ensure effective independence of such entities
24 from improper or undue influence by a large
25 online operator;

1 (C) establish rules for the registration, for-
2 mation, oversight, and management of profes-
3 sional standards bodies, including procedures
4 for the regular oversight of such bodies and rev-
5 ocation of their designation; and

6 (D) in consultation with a professional
7 standards body established under subsection
8 (c), define conduct that does not have the pur-
9 pose or substantial effect of subverting or im-
10 pairing user autonomy, decision making, or
11 choice, or of cultivating compulsive usage for
12 children such as—

13 (i) de minimis user interface changes
14 derived from testing consumer preferences,
15 including different styles, layouts, or text,
16 where such changes are not done with the
17 purpose of obtaining user consent or user
18 data;

19 (ii) algorithms or data outputs outside
20 the control of a large online operator or its
21 affiliates; and

22 (iii) establishing default settings that
23 provide enhanced privacy protection to
24 users or otherwise enhance their autonomy
25 and decision-making ability.

1 (4) SAFE HARBOR.—The Commission may not
2 bring an enforcement action under this section
3 against any large online operator that relied in good
4 faith on the guidance of a professional standards
5 body.

6 **TITLE III—CORPORATE** 7 **ACCOUNTABILITY**

8 **SEC. 301. DESIGNATION OF DATA PRIVACY OFFICER AND** 9 **DATA SECURITY OFFICER.**

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

11 (1) one or more qualified employees or contrac-
12 tors as data privacy officers; and

13 (2) one or more qualified employees or contrac-
14 tors (in addition to any employee or contractor des-
15 igned under paragraph (1)) as data security offi-
16 cers.

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

23 (1) in the case of a data privacy officer, compli-
24 ance with the privacy requirements with respect to
25 covered data under this division; and

1 (2) in the case of a data security officer, the se-
2 curity requirements with respect to covered data
3 under this division.

4 **SEC. 302. INTERNAL CONTROLS.**

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

10 **SEC. 303. WHISTLEBLOWER PROTECTIONS.**

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

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

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

22 (A) is derived from the independent knowl-
23 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 division or a regulation promulgated
13 under this division by a covered entity, the Commission
14 shall consider whether the covered entity retaliated against
15 an individual who was a whistleblower with respect to
16 original information that led to the successful resolution
17 of an administrative or judicial action brought by the
18 Commission or the Attorney General of the United States
19 under this division 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) ENFORCEMENT BY THE FEDERAL TRADE COM-
7 MISSION.—

8 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
9 TICES.—A violation of this division or a regulation
10 promulgated under this division shall be treated as
11 a violation of a rule defining an unfair or deceptive
12 act or practice prescribed under section 18(a)(1)(B)
13 of the Federal Trade Commission Act (15 U.S.C.
14 57a(a)(1)(B)).

15 (2) POWERS OF COMMISSION.—

16 (A) IN GENERAL.—Except as provided in
17 paragraphs (3) and (4), the Commission shall
18 enforce this division and the regulations pro-
19 mulgated under this division in the same man-
20 ner, by the same means, and with the same ju-
21 risdiction, powers, and duties as though all ap-
22 plicable terms and provisions of the Federal
23 Trade Commission Act (15 U.S.C. 41 et seq.)
24 were incorporated into and made a part of this
25 division.

1 (B) PRIVILEGES AND IMMUNITIES.—Any
2 person who violates this division or a regulation
3 promulgated under this division shall be subject
4 to the penalties and entitled to the privileges
5 and immunities provided in the Federal Trade
6 Commission Act (15 U.S.C. 41 et seq.).

7 (C) LIMITING CERTAIN ACTIONS UNRE-
8 LATED TO THIS DIVISION; AUTHORITY PRE-
9 SERVED.—

10 (i) IN GENERAL.—The Commission
11 shall not bring any action to enforce the
12 prohibition in section 5 of the Federal
13 Trade Commission Act (15 U.S.C. 45) on
14 unfair or deceptive acts or practices with
15 respect to the privacy or security of cov-
16 ered data, unless such action is consistent
17 with this division.

18 (ii) RULE OF CONSTRUCTION.—Ex-
19 cept as provided in paragraph (1), nothing
20 in this division shall be construed to limit
21 the authority of the Commission under any
22 other provision of law, or to limit the Com-
23 mission's authority to bring actions under
24 section 5 of the Federal Trade Commission
25 Act (15 U.S.C. 45) relating to unfair or

1 deceptive acts or practices to enforce the
2 provisions of this division and regulations
3 promulgated thereunder, including to en-
4 sure that privacy policies required under
5 section 102 are truthful and non-mis-
6 leading.

7 (3) COMMON CARRIERS AND NONPROFIT ORGA-
8 NIZATIONS.—Notwithstanding section 4, 5(a)(2), or
9 6 of the Federal Trade Commission Act (15 U.S.C.
10 44, 45(a)(2), 46) or any jurisdictional limitation of
11 the Commission, the Commission shall also enforce
12 this division and the regulations promulgated under
13 this division, in the same manner provided in para-
14 graphs (1) and (2) of this subsection, with respect
15 to—

16 (A) common carriers subject to the Com-
17 munications Act of 1934 (47 U.S.C. 151 et
18 seq.) and all Acts amendatory thereof and sup-
19 plementary thereto; and

20 (B) organizations not organized to carry
21 on business for their own profit or that of their
22 members.

23 (4) DATA PRIVACY AND SECURITY FUND.—

24 (A) ESTABLISHMENT OF VICTIMS RELIEF
25 FUND.—There is established in the Treasury of

1 the United States a separate fund to be known
2 as the “Data Privacy and Security Victims Re-
3 lief Fund” (referred to in this paragraph as the
4 “Victims Relief Fund”).

5 (B) DEPOSITS.—

6 (i) DEPOSITS FROM THE COMMIS-
7 SION.—The Commission shall deposit into
8 the Victims Relief Fund the amount of any
9 civil penalty obtained against any covered
10 entity in any action the Commission com-
11 mences to enforce this division or a regula-
12 tion promulgated under this division.

13 (ii) DEPOSITS FROM THE ATTORNEY
14 GENERAL.—The Attorney General of the
15 United States shall deposit into the Vic-
16 tims Relief Fund the amount of any civil
17 penalty obtained against any covered entity
18 in any action the Attorney General com-
19 mences on behalf of the Commission to en-
20 force this division or a regulation promul-
21 gated under this division.

22 (C) USE OF FUND AMOUNTS.—Amounts in
23 the Victims Relief Fund shall be available to
24 the Commission, without fiscal year limitation,
25 to provide redress, payments or compensation,

1 or other monetary relief to individuals affected
2 by an act or practice for which civil penalties
3 have been imposed under this division. To the
4 extent that individuals cannot be located or
5 such redress, payments or compensation, or
6 other monetary relief are otherwise not prac-
7 ticable, the Commission may use such funds for
8 the purpose of consumer or business education
9 relating to data privacy and security or for the
10 purpose of engaging in technological research
11 that the Commission considers necessary to en-
12 force this division.

13 (D) AMOUNTS NOT SUBJECT TO APPOR-
14 TIONMENT.—Notwithstanding any other provi-
15 sion of law, amounts in the Victims Relief Fund
16 shall not be subject to apportionment for pur-
17 poses of chapter 15 of title 31, United States
18 Code, or under any other authority.

19 (5) AUTHORIZATION OF APPROPRIATIONS.—
20 There are authorized to be appropriated to the Com-
21 mission \$100,000,000 to carry out this division.

22 (b) ENFORCEMENT OF SECTION 206.—This section
23 shall not apply to a violation of section 206 or a regulation
24 promulgated under such section, and such section shall be
25 enforced under subsection (d) of such section.

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

2 (a) CIVIL ACTION.—Except as provided in subsection
3 (h), in any case in which the attorney general of a State
4 has reason to believe that an interest of the residents of
5 that State has been or is adversely affected by the engage-
6 ment of any covered entity in an act or practice that vio-
7 lates this division or a regulation promulgated under this
8 division, the attorney general of the State, as *parens*
9 *patriae*, may bring a civil action on behalf of the residents
10 of the State in an appropriate district court of the United
11 States to—

12 (1) enjoin that act or practice;

13 (2) enforce compliance with this division or the
14 regulation;

15 (3) obtain damages, civil penalties, restitution,
16 or other compensation on behalf of the residents of
17 the State; or

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

20 (b) RIGHTS OF THE COMMISSION.—

21 (1) IN GENERAL.—Except where not feasible,
22 the attorney general of a State shall notify the Com-
23 mission in writing prior to initiating a civil action
24 under subsection (a). Such notice shall include a
25 copy of the complaint to be filed to initiate such ac-
26 tion. Upon receiving such notice, the Commission

1 may intervene in such action and, upon inter-
2 vening—

3 (A) be heard on all matters arising in such
4 action; and

5 (B) file petitions for appeal of a decision in
6 such action.

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

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

1 (d) ACTIONS BY COMMISSION.—In any case in which
2 a civil action is instituted by or on behalf of the Commis-
3 sion for violation of this division or a regulation promul-
4 gated under this division, no attorney general of a State
5 may, during the pendency of such action, institute a civil
6 action against any defendant named in the complaint in
7 the action instituted by or on behalf of the Commission
8 for violation of this division or a regulation promulgated
9 under this division that is alleged in such complaint.

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

18 (f) VENUE; SERVICE OF PROCESS.—

19 (1) VENUE.—Any action brought under sub-
20 section (a) may be brought in the district court of
21 the United States that meets applicable require-
22 ments relating to venue under section 1391 of title
23 28, United States Code.

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

4 (A) is an inhabitant; or

5 (B) may be found.

6 (g) ACTIONS BY OTHER STATE OFFICIALS.—

7 (1) IN GENERAL.—Any State official who is au-
8 thorized by the State attorney general to be the ex-
9 clusive authority in that State to enforce this divi-
10 sion may bring a civil action under subsection (a),
11 subject to the same requirements and limitations
12 that apply under this section to civil actions brought
13 under such subsection by State attorneys general.

14 (2) AUTHORITY PRESERVED.—Nothing in this
15 section shall be construed to prohibit an authorized
16 official of a State from initiating or continuing any
17 proceeding in a court of the State for a violation of
18 any civil or criminal law of the State.

19 (h) EXCLUSION OF SECTION 206.—This section shall
20 not apply to a violation of section 206 or a regulation pro-
21 mulgated under such section.

22 **SEC. 403. APPROVED CERTIFICATION PROGRAMS.**

23 (a) IN GENERAL.—The Commission shall establish a
24 program in which the Commission shall approve voluntary
25 consensus standards or certification programs that cov-

1 ered entities may use to comply with one or more provi-
2 sions in this division.

3 (b) EFFECT OF APPROVAL.—A covered entity in com-
4 pliance with a voluntary consensus standard approved by
5 the Commission shall be deemed to be in compliance with
6 the provisions of this division.

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

11 (d) EFFECT OF NON-COMPLIANCE.—A covered entity
12 that claims compliance with an approved voluntary con-
13 sensus standard and is found not to be in compliance with
14 such program by the Commission or in any judicial pro-
15 ceeding shall be considered to be in violation of the section
16 5 of the Federal Trade Commission Act (15 U.S.C. 45)
17 prohibition on unfair or deceptive acts or practices.

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

24 (f) REQUIREMENTS.—To be eligible for approval by
25 the Commission, a voluntary consensus standard shall

1 meet the requirements for voluntary consensus standards
2 set forth in Office of Management and Budget Circular
3 A-119, or other equivalent guidance document, ensuring
4 that they are the result of due process procedures and ap-
5 propriately balance the interests of all the stakeholders,
6 including individuals, businesses, organizations, and other
7 entities making lawful uses of the covered data covered
8 by the standard, and—

9 (1) specify clear and enforceable requirements
10 for covered entities participating in the program that
11 provide an overall level of data privacy or data secu-
12 rity protection that is equivalent to or greater than
13 that provided in the relevant provisions in this divi-
14 sion;

15 (2) require each participating covered entity to
16 post in a prominent place a clear and conspicuous
17 public attestation of compliance and a link to the
18 website described in paragraph (4);

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

24 (4) create a website describing the voluntary
25 consensus standard or certification program's goals

1 and requirements, listing participating covered enti-
2 ties, and providing a method for individuals to ask
3 questions and file complaints about the program or
4 any participating covered entity;

5 (5) take meaningful action for non-compliance
6 with the relevant provisions of this division by any
7 participating covered entity, which shall depend on
8 the severity of the non-compliance and may in-
9 clude—

10 (A) removing the covered entity from the
11 program;

12 (B) referring the covered entity to the
13 Commission or other appropriate Federal or
14 State agencies for enforcement;

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

17 (D) providing redress to individuals
18 harmed by the non-compliance;

19 (E) making voluntary payments to the
20 United States Treasury; and

21 (F) taking any other action or actions to
22 ensure the compliance of the covered entity with
23 respect to the relevant provisions of this divi-
24 sion; and

1 (6) issue annual reports to the Commission and
2 to the public detailing the activities of the program
3 and its effectiveness during the preceding year in en-
4 suring compliance with the relevant provisions of
5 this division by participating covered entities and
6 taking meaningful disciplinary action for non-compli-
7 ance with such provisions by such entities.

8 **SEC. 404. RELATIONSHIP BETWEEN FEDERAL AND STATE**
9 **LAW.**

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

15 (b) **SAVINGS PROVISION.**—Subsection (a) may not be
16 construed to preempt State laws that directly establish re-
17 quirements for the notification of consumers in the event
18 of a data breach.

19 (c) **RELATIONSHIP TO OTHER FEDERAL LAWS.**—

20 (1) **IN GENERAL.**—Except as provided in para-
21 graphs (2) and (3), the requirements of this division
22 shall supersede any other Federal law or regulation
23 relating to the privacy or security of covered data or
24 associated activities of covered entities.

1 (2) SAVINGS PROVISION.—This division may
2 not be construed to modify, limit, or supersede the
3 operation of the following:

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

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

8 (C) Section 227 of the Communications
9 Act of 1934 (47 U.S.C. 227).

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

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

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

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

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

22 (I) The Driver’s Privacy Protection Act of
23 1994 (18 U.S.C. 2721 et seq.).

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

1 (K) The Health Information Technology
2 for Economic and Clinical Health Act (42
3 U.S.C. 17931 et seq.).

4 (3) COMPLIANCE WITH SAVED FEDERAL
5 LAWS.—To the extent that the data collection, proc-
6 essing, or transfer activities of a covered entity are
7 subject to a law listed in paragraph (2), such activi-
8 ties of such entity shall not be subject to the re-
9 quirements of this division.

10 (4) NONAPPLICATION OF FCC LAWS AND REGU-
11 LATIONS TO COVERED ENTITIES.—Notwithstanding
12 any other provision of law, neither any provision of
13 the Communications Act of 1934 (47 U.S.C. 151 et
14 seq.) and all Acts amendatory thereof and supple-
15 mentary thereto nor any regulation promulgated by
16 the Federal Communications Commission under
17 such Acts shall apply to any covered entity with re-
18 spect to the collection, use, processing, transferring,
19 or security of individual information, except to the
20 extent that such provision or regulation pertains
21 solely to “911” lines or other emergency line of a
22 hospital, medical provider or service office, health
23 care facility, poison control center, fire protection
24 agency, or law enforcement agency.

1 **SEC. 405. CONSTITUTIONAL AVOIDANCE.**

2 The provisions of this division shall be construed, to
3 the greatest extent possible, to avoid conflicting with the
4 Constitution of the United States, including the protec-
5 tions of free speech and freedom of the press established
6 under the First Amendment to the Constitution of the
7 United States.

8 **SEC. 406. SEVERABILITY.**

9 If any provision of this division, or an amendment
10 made by this division, is determined to be unenforceable
11 or invalid, the remaining provisions of this division and
12 the amendments made by this division shall not be af-
13 fected.

