

117TH CONGRESS
1ST SESSION

H. R. 1816

To require the Federal Trade Commission to promulgate regulations related to sensitive personal information, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

MARCH 11, 2021

Ms. DELBENE introduced the following bill; which was referred to the Committee on Energy and Commerce

A BILL

To require the Federal Trade Commission to promulgate regulations related to sensitive personal information, and for other purposes.

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

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Information Trans-
5 parency & Personal Data Control Act”.

6 **SEC. 2. SENSE OF CONGRESS.**

7 It is the Sense of Congress that—

8 (1) the United States must develop a balanced,
9 high-standard digital privacy framework that com-
10 plements global standards;

1 (2) a key element of this framework is a strong
2 national standard that combats anti-consumer prac-
3 tices;

4 (3) it is critical that the Federal Government
5 provide guidance on the collection, processing, disclo-
6 sure, transmission and storage of sensitive data;

7 (4) it is important to provide the Nation with
8 fair and thoughtful digital consumer rights with re-
9 spect to such data;

10 (5) it is important to ensure that enforcement
11 authorities have the resources needed to protect con-
12 sumers from unlawful and deceptive acts of practices
13 in the data privacy and security space; and

14 (6) individuals have a right to—

15 (A) exercise control over the personal data
16 companies collect from them and how they use
17 it;

18 (B) easily understandable and accessible
19 information about privacy and security prac-
20 tices;

21 (C) expect that companies will collect, use,
22 and disclose personal data in ways that are con-
23 sistent with the context in which consumers
24 provide the data;

1 (D) secure and responsible handling of
2 sensitive personal information;

3 (E) access and correct persona data in us-
4 able formats, in a manner that is appropriate to
5 the sensitivity of the data and the risk of ad-
6 verse consequences to consumers if the data is
7 inaccurate; and

8 (F) reasonable limits on the personal data
9 that companies collect and retain.

10 **SEC. 3. REQUIREMENTS FOR SENSITIVE PERSONAL INFOR-**
11 **MATION.**

12 (a) REGULATIONS.—Not later than 18 months after
13 the date of enactment of this Act, the Federal Trade Com-
14 mission shall promulgate regulations under section 553 of
15 title 5, United States Code, to require, except as provided
16 in subsection (b), controllers, processors, and third parties
17 to make available to the public involving the collection,
18 transmission, storage, processing, sale, sharing of sensitive
19 personal information, or other use of sensitive personal in-
20 formation from persons operating in or persons located in
21 the United States when the sensitive personal information
22 is collected, transmitted, stored, processed, sold or shared
23 to meet the following requirements:

24 (1) AFFIRMATIVE, EXPRESS, AND OPT-IN CON-
25 SENT.—

1 (A) Any controller shall provide users
2 whose personal information is collected, trans-
3 mitted, stored, process, sold, or otherwise
4 shared with notice through a privacy and data
5 use policy of a specific request to collect, trans-
6 mit, sell, share or otherwise disclose their sen-
7 sitive personal information and require that
8 users provide affirmative, express consent to
9 any functionality that involves the sale, sharing,
10 or other disclosure of sensitive personal infor-
11 mation, including sharing sensitive personal in-
12 formation with third parties, if the sensitive
13 personal information is to be used by the third
14 party for purposes other than the purposes out-
15 lined in the notice.

16 (B) The documented instruction from a
17 controller to a processor or third party shall ad-
18 here to the limits of the consent granted in sub-
19 paragraph (A), and processors and third parties
20 shall not use or disclose the sensitive personal
21 information for any other purposes or in any
22 way that exceeds the limits of the consent
23 granted in subparagraph (A).

24 (C) Controllers and processors shall not be
25 liable for the failure of another processor or

1 third party to adhere to the limits of an opt-in
2 consent granted under subparagraph (A).

3 (2) PRIVACY AND DATA USE POLICY.—Control-
4 lers, processors, and third parties shall publicly
5 maintain an up-to-date, transparent privacy, secu-
6 rity, and data use policy that meets general require-
7 ments, including that such policy, presented in the
8 context where it applies—

9 (A) is concise, intelligible, and uses plain
10 language;

11 (B) is clear and conspicuous consistent
12 with the guidelines of the Federal Trade Com-
13 mission;

14 (C) uses visualizations, where appropriate
15 to make complex information understandable by
16 the ordinary user; and

17 (D) is provided free of charge.

18 (3) ADDITIONAL REQUIREMENTS FOR PRIVACY
19 AND DATA USE POLICY.—The privacy, security, and
20 data use policy required under paragraph (2) shall
21 include the following:

22 (A) Identity and contact information of the
23 entity collecting or processing the sensitive per-
24 sonal information.

1 (B) The purpose or use for collecting, stor-
2 ing, processing, selling, sharing, or otherwise
3 using the sensitive personal information.

4 (C) Categories of third parties with whom
5 the sensitive personal information will be shared
6 and for what general purposes.

7 (D) The process by which individuals may
8 withdraw consent to the collecting, storing,
9 processing, selling, sharing, or other use of the
10 sensitive personal information, including shar-
11 ing with third parties.

12 (E) How a user, controller, or processor
13 can view or obtain the sensitive personal infor-
14 mation that they have received or provided to a
15 controller or processor, including whether it can
16 be exported to other web-based platforms.

17 (F) The categories of sensitive personal in-
18 formation that is collected by the controller or
19 processor and shared with processors or third
20 parties.

21 (G) How sensitive personal information is
22 protected from unauthorized access or acquisi-
23 tion.

24 (4) OPT-OUT CONSENT.—

1 (A) For any collection, transmission, stor-
2 age, processing, selling, sharing, or other use of
3 non-sensitive personal information, including
4 sharing with third parties, controllers shall pro-
5 vide users with the ability to opt out at any
6 time.

7 (B) Controllers shall honor an opt out re-
8 quest from a user under subparagraph (A) to
9 the extent of its role in any collection, trans-
10 mission, storage, processing, selling, sharing, or
11 other use of non-sensitive personal information
12 and shall communicate an opt-out request to
13 the relevant processor or third party with which
14 the controller has shared information regarding
15 that user.

16 (C) Processors or third parties receiving an
17 opt out pursuant to subparagraph (A) and (B)
18 shall comply with such opt out to the extent of
19 their role in any collection, transmission, stor-
20 age, processing, selling, sharing, or other use of
21 non-sensitive personal information.

22 (D) Any controller that communicates an
23 opt out from a user as required by subpara-
24 graph (B) shall not be liable for the failure of

1 a service provider or third party to comply with
2 such opt out.

3 (5) RELATIONSHIP BETWEEN CONTROLLER
4 AND PROCESSOR.—

5 (A) Processing by a processor must be gov-
6 erned by a contract between the controller and
7 the processor that is binding on both parties
8 and that sets the processor to processes the
9 personal data only on documented instructions
10 from the controller.

11 (B) Processors shall share sensitive per-
12 sonal information with a subcontractor only for
13 purposes of providing services and only after
14 first providing the controller with an oppor-
15 tunity to object.

16 (C) In no event may any contract or docu-
17 mented instructions relieve a controller or a
18 processor from the obligations and liabilities im-
19 posed on them by this Act.

20 (6) PRIVACY AUDITS.—

21 (A) IN GENERAL.—Except as provided in
22 subparagraphs (C) and (D), at least once every
23 2 years, each controller, processor, or third
24 party that has collected, transmitted, stored,

1 processed, selling, shared, or otherwise used
2 sensitive personal information shall—

3 (i) obtain a privacy audit from a
4 qualified, objective, independent third-
5 party; and

6 (ii) shall make publicly available
7 whether or not the privacy audit found the
8 controller, processor, or third party compli-
9 ant.

10 (B) AUDIT REQUIREMENTS.—Each such
11 audit shall—

12 (i) set forth the privacy, security, and
13 data use controls that the controller, proc-
14 essor, or third party has implemented and
15 maintained during the reporting period;

16 (ii) describe whether such controls are
17 appropriate to the size and complexity of
18 the controller, processor, or third party,
19 the nature and scope of the activities of
20 the controller, processor, or third party,
21 and the nature of the sensitive personal in-
22 formation or behavioral data collected by
23 the controller, processor, or third party;

24 (iii) certify whether the privacy and
25 security controls operate with sufficient ef-

1 fectiveness to provide reasonable assurance
2 to protect the privacy and security of sen-
3 sitive personal information or behavioral
4 data, including with respect to data shared
5 with third parties, and that the controls
6 have so operated throughout the reporting
7 period;

8 (iv) be prepared and completed within
9 60 days after a substantial change to the
10 controller's privacy and data use policy de-
11 scribed in paragraph (2); and

12 (v) be provided—

13 (I) to the Federal Trade Com-
14 mission; and

15 (II) to any attorney general of a
16 State, or other authorized State offi-
17 cer, within 10 days of receiving writ-
18 ten request by the such attorney gen-
19 eral, or other authorized State officer
20 where such officer has presented to
21 the controller, processor, or third
22 party allegations that a violation of
23 this Act or any regulation issued
24 under this Act has been committed by

1 the controller, processor, or third
2 party.

3 (C) SMALL BUSINESS AUDIT EXEMP-
4 TION.—The audit requirements described in
5 this paragraph shall not apply to controllers
6 who collect, store, process, sell, share, or other-
7 wise use sensitive personal information relating
8 to 250,000 or fewer individuals per year.

9 (D) NON-SENSITIVE PERSONAL INFORMA-
10 TION EXEMPTION.—The audit requirements set
11 forth above shall not apply to controllers, proc-
12 essors or third parties who do not collect, store,
13 process, sell, share, or otherwise use sensitive
14 personal information.

15 (E) RULES THAT DO NOT INCENTIVIZE
16 SELLING INFORMATION.—The Commission shall
17 promulgate rules regarding qualifications and
18 requirements of third-party auditors such as a
19 duty to conduct an independent assessment that
20 does not incentivize the auditor to sell under
21 the guise of a potential violation by the con-
22 troller products or services when there is not a
23 violation of the Act.

24 (b) EXEMPTIONS.—

1 (1) NECESSARY OPERATIONS AND SECURITY
2 PURPOSES.—Subsection (a) shall not apply to the
3 processing, transmission, collecting, storing, sharing,
4 selling of sensitive and non-sensitive personal infor-
5 mation for the following purposes:

6 (A) Preventing or detecting fraud, identity
7 theft, unauthorized transactions, theft, shop-
8 lifting, or criminal activity including financial
9 crimes and money laundering.

10 (B) The use of such information to identify
11 errors that impair functionality or otherwise en-
12 hancing or maintaining the availability of the
13 services or information systems of the controller
14 for authorized access and use.

15 (C) Protecting the vital interests of the
16 consumer or another natural person.

17 (D) Responding in good faith to valid legal
18 process or providing information as otherwise
19 required or authorized by law.

20 (E) Monitoring or enforcing agreements
21 between the Controller, processor, or third
22 party and an individual, including but not lim-
23 ited to, terms of service, terms of use, user
24 agreements, or agreements concerning moni-
25 toring criminal activity.

1 (F) Protecting the property, services, or
2 information systems of the controller, processor,
3 or third party against unauthorized access or
4 use.

5 (G) Advancing a substantial public inter-
6 est, including archival purposes, scientific or
7 historical research, and public health, if such
8 processing does not create a significant risk of
9 harm to consumers.

10 (H) Uses authorized by the Fair Credit
11 Reporting Act or used by a commercial credit
12 reporting agency.

13 (I) Completing the transaction for which
14 the personal information was collected, provide
15 a good or service requested by the consumer
16 that is reasonably anticipated within the con-
17 text of a business' ongoing relationship with the
18 consumer, bill or collect for such good or service
19 or otherwise perform a contract between the
20 controller and a consumer.

21 (J) Complying with other Federal, State,
22 and local law.

23 (K) Conducting product recalls and serv-
24 icing warranties.

1 (2) REASONABLE EXPECTATION OF USERS.—

2 The regulations promulgated pursuant to subsection
3 (a) with respect to the requirement to provide opt-
4 in consent shall not apply to the processing, trans-
5 mission, storage, selling, sharing, or collection of
6 sensitive personal information in which such proc-
7 essing does not deviate from purposes consistent
8 with a controller’s relationship with users as under-
9 stood by the reasonable use, including but not lim-
10 ited to—

11 (A) carrying out the term of a contract or
12 service agreement, including elements of a cus-
13 tomer loyalty program, with a user;

14 (B) accepting and processing a payment
15 from a user;

16 (C) completing a transaction with a user
17 such as through delivering a good or service
18 even if such delivery is made by a processor or
19 third party;

20 (D) marking goods or services to a user as
21 long as the user is provided with the ability to
22 opt out of such marketing;

23 (E) taking steps to continue or extend an
24 existing business relationship with a user, or in-
25 viting a new user to participate in a customer

1 promotion, benefit or loyalty program, as long
2 as the user is provided with the ability to opt
3 out;

4 (F) conduct internal research to improve,
5 repair, or develop products, services, or tech-
6 nology; or

7 (G) municipal governments.

8 **SEC. 4. APPLICATION AND ENFORCEMENT BY THE FED-**
9 **ERAL TRADE COMMISSION.**

10 (a) COMMON CARRIERS.—Notwithstanding the limi-
11 tations in the Federal Trade Commission Act (15 U.S.C.
12 41 et seq.) on Commission authority with respect to com-
13 mon carriers, this Act applies, according to its terms, to
14 common carriers subject to the Communications Act of
15 (47 U.S.C. 151 et seq.) and all Acts amendatory thereof
16 and supplementary thereto. The Federal Trade Commis-
17 sion shall be the only Federal agency with authority to
18 enforce such common carriers' privacy practices.

19 (b) ENFORCEMENT.—

20 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
21 TICES.—A violation of this Act or a regulation pro-
22 mulgated under this Act shall be treated as a viola-
23 tion section 18(a)(1)(B) of the Federal Trade Com-
24 mission Act (15 U.S.C. 57(a)(1)(B)) regarding un-
25 fair or deceptive acts or practices.

1 (2) POWERS OF COMMISSION.—Except as pro-
2 vided in subsection (a), the Federal Trade Commis-
3 sion shall enforce this Act and the regulations pro-
4 mulgated under this Act in the same manner, by the
5 same means, and with the same jurisdiction, powers,
6 and duties as though all applicable terms and provi-
7 sions of the Federal Trade Commission Act (15
8 U.S.C. 41 et seq.) were incorporated into and made
9 a part of this Act. Any person who violates this Act
10 or a regulation promulgated under this Act shall be
11 subject to the penalties and entitled to the privileges
12 and immunities provided in the Federal Trade Com-
13 mission Act.

14 (c) CONSTRUCTION.—Nothing in this Act shall be
15 construed to limit the authority of the Federal Trade
16 Commission under any other provision of law.

17 (d) OPPORTUNITY TO COMPLY.—The Commission
18 shall notify a controller of alleged violations and provide
19 them with 30 days to cure a non-wilful violations of this
20 Act before the Commission shall commence and enforce-
21 ment action.

22 **SEC. 5. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

23 (a) RIGHT OF ACTION.—Except as provided in sub-
24 section (e), the attorney general of a State, alleging a vio-
25 lation of this Act or any regulation issued under this Act

1 that affects or may affect such State or its residents may
2 bring an action on behalf of the residents of the State in
3 any United States district court for the district in which
4 the defendant is found, resides, or transacts business, or
5 wherever venue is proper under section 1391 of title 28,
6 United States Code, to obtain appropriate injunctive relief.

7 (b) NOTICE TO COMMISSION REQUIRED.—A State
8 shall provide prior written notice to the Federal Trade
9 Commission of any civil action under subsection (a) to-
10 gether with a copy of its complaint, except that if it is
11 not feasible for the State to provide such prior notice, the
12 State shall provide such notice immediately upon insti-
13 tuting such action.

14 (c) INTERVENTION BY THE COMMISSION.—The Com-
15 mission may intervene in such civil action and upon inter-
16 vening—

17 (1) be heard on all matters arising in such civil
18 action; and

19 (2) file petitions for appeal of a decision in such
20 civil action.

21 (d) CONSTRUCTION.—Nothing in this section shall be
22 construed—

23 (1) to prevent the attorney general of a State,
24 or other authorized State officer, from exercising the
25 powers conferred on the attorney general, or other

1 authorized State officer, by the laws of such State;
2 or

3 (2) to prohibit the attorney general of a State,
4 or other authorized State officer, from proceeding in
5 State or Federal court on the basis of an alleged vio-
6 lation of any civil or criminal statute of that State.

7 (e) LIMITATION.—

8 (1) NO SEPARATE ACTION.—An action may not
9 be brought under subsection (a) if the same alleged
10 violation is the subject of a pending action by the
11 Commission or the United States.

12 (2) EXCLUSIVE PERIOD TO ACT BY COMMIS-
13 SION.—An action—

14 (A) may not be brought under subsection
15 (a) until the expiration of the 60-day period
16 that begins on the date on which a violation is
17 discovered by the Commission or the date on
18 which the Commission is notified of the viola-
19 tion; and

20 (B) may only be brought under subsection
21 (a) if the Commission does not bring an action
22 related to the violation during such period.

23 (f) OPPORTUNITY TO COMPLY.—Prior to bringing
24 any action under this section, the state attorney general
25 shall notify a controller of alleged violations and provide

1 them with 30 days to cure a non-wilful violations of this
 2 Act before commencing an enforcement action.

3 **SEC. 6. PRIVACY AND DATA SECURITY EMPLOYEES AND**
 4 **FUNDING FOR THE COMMISSION.**

5 (a) EMPLOYMENT AUTHORITY.—The Commission
 6 shall hire 500 new full-time employees to focus on privacy
 7 and data security, 50 of which shall have technology exper-
 8 tise.

9 (b) ADDITIONAL FUNDING FOR PRIVACY AND DATA
 10 SECURITY.—There is authorized to be appropriated to the
 11 Commission \$350,000,000 for issues related to privacy
 12 and data security.

13 **SEC. 7. DEFINITIONS.**

14 In this Act the following definitions apply:

15 (1) CALL DETAIL RECORD.—The term “call de-
 16 tail record”—

17 (A) means session-identifying information
 18 (including an originating or terminating tele-
 19 phone number, an International Mobile Sub-
 20 scriber Identity number, or an International
 21 Mobile Station Equipment Identity number), a
 22 telephone calling card number, or the time or
 23 duration of a call;

24 (B) does not include—

1 (i) the contents (as defined in section
2 (8) of title 18, United States Code) of any
3 communication;

4 (ii) the name, address, or financial in-
5 formation of a subscriber or customer;

6 (iii) cell site location or global posi-
7 tioning system information; or

8 (iv) business customers.

9 (2) CLEAR AND PROMINENT.—The term “clear
10 and prominent” means in any communication me-
11 dium, the required disclosure is—

12 (A) of a type, size, and location sufficiently
13 noticeable for an ordinary consumer to read
14 and comprehend the communication;

15 (B) provided in a manner such that an or-
16 dinary consumer is able to read and com-
17 prehend the communication;

18 (C) is presented in an understandable lan-
19 guage and syntax;

20 (D) includes nothing contrary to, incon-
21 sistent with, or that mitigates any statement
22 contained within the disclosure or within any
23 document linked to or referenced therein; and

24 (E) includes an option that is compliant
25 with applicable obligations of the controller

1 under title III of the Americans with Disabil-
2 ities Act of 1990 (42 U.S.C. 12181 et seq.).

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

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

9 (5) CONTROLLER.—The term “controller”
10 means a person that, on its own or jointly with other
11 entities, determines the purposes and means of proc-
12 essing sensitive personal information.

13 (6) DE-IDENTIFIED DATA.—The term “de-iden-
14 tified data” means information held that—

15 (A) does not identify, and is not linked or
16 reasonably linkable to, and individual or device;

17 (B) does not contain a persistent identifier
18 or other information that could readily be used
19 to de-identify the individual to whom, or the de-
20 vice to which, the identifier or information per-
21 tains;

22 (C) is subject to a public commitment by
23 the entity;

24 (D) to refrain from attempting to use such
25 information to identify any individual or device;

1 (E) to adopt technical and organizational
2 measures to ensure that such information is not
3 linked to any individual or device; and

4 (F) is not disclosed by the covered entity
5 to any other party unless the disclosure is sub-
6 ject to a contractually or other legally binding
7 requirement.

8 (7) EMPLOYEE DATA.—The term “employee
9 data” means—

10 (A) information relating to an individual
11 collected in the course of the individual acting
12 as a job applicant to, or employee (regardless of
13 whether such employee is paid or unpaid, or
14 employed on a temporary basis), owner, direc-
15 tor, officer, staff member, trainee, vendor, vis-
16 itor, volunteer, intern, or contractor;

17 (B) business contact information of an in-
18 dividual, including the individual’s name, posi-
19 tion or title, business telephone number, busi-
20 ness address, business email address, qualifica-
21 tions, and other similar information that is pro-
22 vided by an individual who is acting in a profes-
23 sional capacity, provided that such information
24 is collected, processed, or transferred solely for

1 purposes related to such individuals' profes-
2 sional activities; or

3 (C) emergency contact information col-
4 lected by a covered entity that relates to an in-
5 dividual who is acting in a role described in
6 subparagraph (A).

7 (8) PROCESSOR.—The term “processor” means
8 a person that processes data on behalf of a con-
9 troller or another processor according to and for the
10 purposes set forth in the documented instructions. If
11 a person processes data on its own behalf or for its
12 own purposes, then that person is not a processor
13 with respect to that data but is instead a controller.
14 Determining whether a person is acting as a con-
15 troller or processor with respect to a specific proc-
16 essing of data is a fact-based determination that de-
17 pends upon the controller’s documented instructions
18 and the context in which personal data is to be proc-
19 essed. A processor shall only remain a processor to
20 the extent that it continues to process data for the
21 sole purposes set forth in the documented instruc-
22 tions of the controller and adheres to those instruc-
23 tions and the limitations in the controller’s privacy
24 policy as communicated to the processor with respect
25 to a specific processing of personal information.

(9) SENSITIVE PERSONAL INFORMATION.—

(A) The term “sensitive personal information” means information relating to an identified or identifiable individual that is—

(i) financial account numbers;

(ii) health information;

(iii) genetic data;

(iv) any information pertaining to children under 13 years of age;

(v) Social Security numbers;

(vi) unique government-issued identifiers;

(vii) authentication credentials for a financial account, such as a username and password;

(viii) precise geolocation information;

(ix) content of a personal wire communication, oral communication, or electronic communication such as e-mail or direct messaging with respect to any entity that is not the intended recipient of the communication;

(x) call detail records for calls conducted in a personal and not a business capacity;

- 1 (xi) biometric information;
- 2 (xii) sexual orientation, gender iden-
- 3 tity, or intersex status;
- 4 (xiii) citizenship or immigration sta-
- 5 tus;
- 6 (xiv) mental or physical health diag-
- 7 nosis;
- 8 (xv) religious beliefs; or
- 9 (xvi) web browsing history, application
- 10 usage history, and the functional equiva-
- 11 lent of either that is data described in this
- 12 subparagraph that is not aggregated data.

13 (B) The term “sensitive personal informa-

14 tion” does not include—

- 15 (i) de-identified information (or the
- 16 measurement, analysis or process utilized
- 17 to transforming personal data so that it is
- 18 not directly relatable to an identified or
- 19 identifiable consumer);
- 20 (ii) information related to employ-
- 21 ment, including any employee data;
- 22 (iii) personal information reflecting a
- 23 written or verbal communication or a
- 24 transaction between a controller and the
- 25 user, where the user is a natural person

1 who is acting as an employee, owner, direc-
2 tor, officer, or contractor of a company,
3 partnership, sole proprietorship, non-profit,
4 or government agency and whose commu-
5 nications or transaction with the controller
6 occur solely within the context of the con-
7 troller conducting due diligence regarding,
8 or providing or receiving a product or serv-
9 ice to or from such company, partnership,
10 sole proprietorship, non-profit, or govern-
11 ment agency; or

12 (iv) publicly available information.

13 (10) STATE.—The term “State” means each
14 State of the United States, the District of Columbia,
15 and each commonwealth, territory, or possession of
16 the United States.

17 (11) THIRD PARTY.—The term “third party”
18 means an individual or entity that uses or receives
19 sensitive personal information obtained by or on be-
20 half of a controller, other than—

21 (A) a service provider of a controller to
22 whom the controller discloses the consumer’s
23 sensitive personal information for an oper-
24 ational purpose subject to section 3(a)(1)(B) of
25 this Act; and

1 (B) any entity that uses sensitive personal
2 information only as reasonably necessary—

3 (i) to comply with applicable law, reg-
4 ulation, or legal process;

5 (ii) to enforce the terms of use of a
6 controller;

7 (iii) to detect, prevent, or mitigate
8 fraud or security vulnerabilities; or

9 (iv) does not determine the purposes
10 and means of processing sensitive personal
11 information.

12 (12) TRANSFER.—The term “transfer” means
13 to disclose, release, share, disseminate, make avail-
14 able, or license in writing, electronically or by any
15 other means, for consideration of any kind for a
16 commercial purpose.

17 **SEC. 8. RULES OF CONSTRUCTION.**

18 (a) FEDERAL ACQUISITION.—Nothing in this Act
19 may be construed to preclude the acquisition by the Fed-
20 eral Government of—

21 (1) the contents of a wire or electronic commu-
22 nication pursuant to other lawful authorities, includ-
23 ing the authorities under chapter 119 of title 18,
24 United States Code (commonly known as the “Wire-
25 tap Act”), the Foreign Intelligence Surveillance Act

1 of 1978 (50 U.S.C. 1801 et seq.), or any other pro-
2 vision of Federal law not specifically amended by
3 this Act; or

4 (2) records or other information relating to a
5 subscriber or customer of any electronic communica-
6 tion service or remote computing service (not includ-
7 ing the content of such communications) pursuant to
8 the Foreign Intelligence Surveillance Act of 1978
9 (50 U.S.C. 1801 et seq.), chapter 119 of title 18,
10 United States Code (commonly known as the “Wire-
11 tap Act”), or any other provision of Federal law not
12 specifically amended by this Act.

13 (b) EFFECT ON OTHER LAWS.—Nothing in this Act
14 shall be construed to limit or substitute for the require-
15 ments under title V of the Gramm-Leach-Bliley Act (15
16 U.S.C. 6801 et seq.), section 264(c) of the Health Insur-
17 ance Portability and Accountability Act of 1996 (Public
18 Law 104–191), section 444 of the General Education Pro-
19 visions Act (commonly known as the Family Educational
20 Rights and Privacy Act of 1974) (20 U.S.C. 1232g), the
21 Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

22 **SEC. 9. NATIONAL STANDARD.**

23 (a) RELATIONSHIP TO STATE LAW.—No State or po-
24 litical subdivision of a State may adopt, maintain, enforce,
25 or continue in effect any law, regulation, rule, require-

1 ment, or standard related to the data privacy or associated
2 activities of covered entities.

3 (b) NONPREEMPTION.—Subsection (a) shall not be
4 construed to—

5 (1) preempt State laws that directly establish
6 requirements for the notification of consumers in the
7 event of a data breach;

8 (2) preempt State laws that directly establish
9 requirements regarding biometric laws;

10 (3) preempt State laws regarding wiretapping
11 laws; or

12 (4) preempt State laws like the Public Records
13 Act.

14 **SEC. 10. EFFECTIVE DATE.**

15 This Act shall take effect 180 days after the date of
16 the enactment of this Act.

○