

116TH CONGRESS
1ST SESSION

H. R. 2013

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

IN THE HOUSE OF REPRESENTATIVES

APRIL 1, 2019

Ms. DELBENE (for herself, Miss RICE of New York, and Mr. SUOZZI) 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—

1 (1) the United States must develop a balanced,
2 high-standard digital framework that establishes
3 global standards;

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

7 (3) it is critical that the Federal Government
8 provide guidance on the collection and storage of
9 sensitive data;

10 (4) it is important to provide our country with
11 fair and thoughtful digital consumer rights; and

12 (5) it is important to ensure that our enforce-
13 ment authorities have the resources needed to pro-
14 tect consumers from bad actors in the privacy and
15 security space.

16 **SEC. 3. REQUIREMENTS FOR SENSITIVE PERSONAL INFOR-**
17 **MATION.**

18 (a) REGULATIONS.—Not later than 1 year after the
19 date of the enactment of this Act, the Federal Trade Com-
20 mission shall promulgate regulations under section 553 of
21 title 5, United States Code, to require, except as provided
22 in subsection (b), any controller that provides services to
23 the public involving the collection, storage, processing,
24 sale, sharing with third parties, or other use of sensitive
25 personal information from United States persons or per-

1 sons located in the United States when the data is col-
2 lected, to meet the following requirements:

3 (1) AFFIRMATIVE, EXPRESS, AND OPT-IN CON-
4 SENT.—Provide users with notice through a privacy
5 and data use policy of a specific request to use their
6 sensitive personal information and require that users
7 provide affirmative, express, and opt-in consent to
8 any functionality that involves the collection, stor-
9 age, processing, sale, sharing, or other use of sen-
10 sitive personal information, including sharing sen-
11 sitive personal information with third parties.

12 (2) PRIVACY AND DATA USE POLICY.—Provide
13 users with an up-to-date, transparent privacy, secu-
14 rity, and data use policy that meets general require-
15 ments, including that such policy, presented to users
16 in the context where it applies—

17 (A) is concise and intelligible;

18 (B) is clear and prominent in appearance;

19 (C) uses clear and plain language;

20 (D) uses visualizations where appropriate
21 to make complex information understandable by
22 the ordinary user; and

23 (E) is provided free of charge.

24 (3) ADDITIONAL REQUIREMENTS FOR PRIVACY
25 AND DATA USE POLICY.—The privacy, security, and

1 data use policy required under paragraph (2) shall
2 include the following:

3 (A) Identity and contact information of the
4 entity collecting the sensitive personal informa-
5 tion.

6 (B) The purpose or use for collecting, stor-
7 ing, processing, selling, sharing, or otherwise
8 using the sensitive personal information.

9 (C) Third parties with whom the sensitive
10 personal information will be shared and for
11 what purposes.

12 (D) The storage period for how long the
13 sensitive personal information will be retained
14 by the controller and any third party, as appli-
15 cable.

16 (E) How consent to collecting, storing,
17 processing, selling, sharing, or otherwise using
18 the sensitive personal information, including
19 sharing with third parties, may be withdrawn.

20 (F) How a user can view or obtain the sen-
21 sitive personal information that they have pro-
22 vided to a controller and whether it can be ex-
23 ported to other web-based platforms.

24 (G) What kind of sensitive personal infor-
25 mation is collected and shared.

1 (H) Whether the sensitive personal infor-
2 mation will be used to create profiles about
3 users and whether they will be integrated across
4 platforms.

5 (I) How sensitive personal information is
6 protected from unauthorized access or acquisi-
7 tion.

8 (4) OPT-OUT CONSENT.—For any collection,
9 storage, processing, selling, sharing, or other use of
10 non-sensitive personal information, including sharing
11 with third parties, controllers shall provide users
12 with the ability to opt out at any time.

13 (5) PRIVACY AUDITS.—

14 (A) IN GENERAL.—Except as provided in
15 subparagraphs (C) and (D), annually, each con-
16 troller collecting, storing, processing, selling,
17 sharing, or otherwise using sensitive personal
18 information shall—

19 (i) obtain a privacy audit from a
20 qualified, objective, independent third-
21 party; and

22 (ii) shall make public whether or not
23 the privacy audit found the controller com-
24 pliant.

1 (B) AUDIT REQUIREMENTS.—Each such
2 audit shall—

3 (i) set forth the privacy, security, and
4 data use controls that the controller has
5 implemented and maintained during the
6 reporting period;

7 (ii) describe whether such controls are
8 appropriate to the size and complexity of
9 the controller, the nature and scope of the
10 activities of the controller, and the nature
11 of the sensitive personal information or be-
12 havioral data collected by the controller;

13 (iii) certify whether the privacy and
14 security controls operate with sufficient ef-
15 fectiveness to provide reasonable assurance
16 to protect the privacy and security of sen-
17 sitive personal information or behavioral
18 data, including with respect to data shared
19 with third parties, and that the controls
20 have so operated throughout the reporting
21 period;

22 (iv) be prepared and completed within
23 60 days after the end of the reporting pe-
24 riod to which the audit applies; and

1 (v) be provided to the Federal Trade
2 Commission or to the attorney general of
3 a State, or other authorized State officer,
4 within 10 days of notification by the Com-
5 mission or the attorney general of a State,
6 or other authorized State officer where
7 such person has presented to the controller
8 allegations that a violation of this Act or
9 any regulation issued under this Act has
10 been committed by the controller.

11 (C) SMALL BUSINESS AUDIT EXEMP-
12 TION.—The audit requirements described in
13 this paragraph shall not apply to controllers
14 who collect, store, process, sell, share, or other-
15 wise use sensitive personal information relating
16 to 5,000 or fewer individuals.

17 (D) NON-SENSITIVE PERSONAL INFORMA-
18 TION EXEMPTION.—The audit requirements set
19 forth above shall not apply to controllers who
20 do not collect, store, process, sell, share, or oth-
21 erwise use sensitive personal information.

22 (b) EXEMPTIONS.—

23 (1) NECESSARY OPERATIONS AND SECURITY
24 PURPOSES.—Subsection (a) shall not apply to the
25 processing, collecting, storing, sharing, selling of

1 sensitive personal information for the following pur-
2 poses:

3 (A) Preventing or detecting fraud, identity
4 theft, or criminal activity.

5 (B) The use of such information to identify
6 errors that impair functionality or otherwise en-
7 hancing or maintaining the availability of the
8 services or information systems of the controller
9 for authorized access and use.

10 (C) Protecting the vital interests of the
11 consumer or another natural person.

12 (D) Responding in good faith to valid legal
13 process or providing information as otherwise
14 required or authorized by law.

15 (E) Monitoring or enforcing agreements
16 between the controller and an individual, includ-
17 ing but not limited to, terms of service, terms
18 of use, user agreements, or agreements concern-
19 ing monitoring criminal activity.

20 (F) Protecting the property, services, or
21 information systems of the controller against
22 unauthorized access or use.

23 (G) Advancing a substantial public inter-
24 est, including archival purposes, scientific or
25 historical research, and public health, if such

1 processing does not create a significant risk of
2 harm to consumers.

3 (2) REASONABLE EXPECTATION OF USERS.—

4 The regulations promulgated pursuant to subsection
5 (a) with respect to the requirement to provide opt-
6 in consent shall not apply to the processing, storage,
7 and collection of sensitive personal information or
8 behavioral data in which such processing does not
9 deviate from purposes consistent with a controller's
10 relationship with users as understood by the reason-
11 able user.

12 **SEC. 4. APPLICATION AND ENFORCEMENT BY THE FED-**
13 **ERAL TRADE COMMISSION.**

14 (a) COMMON CARRIERS.—Notwithstanding the limi-
15 tations in the Federal Trade Commission Act (15 U.S.C.
16 41 et seq.) on Commission authority with respect to com-
17 mon carriers, this Act applies, according to its terms, to
18 common carriers subject to the Communications Act of
19 1934 (47 U.S.C. 151 et seq.) and all Acts amendatory
20 thereof and supplementary thereto.

21 (b) ENFORCEMENT.—

22 (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-
23 TICES.—A violation of this Act or a regulation pro-
24 mulgated under this Act shall be treated as a viola-
25 tion of a rule under section 18(a)(1)(B) of the Fed-

1 eral Trade Commission Act (15 U.S.C.
2 57a(a)(1)(B)) regarding unfair or deceptive acts or
3 practices.

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

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

20 **SEC. 5. RIGHT OF ACTION.**

21 (a) RIGHT OF ACTION.—Except as provided in sub-
22 section (e), the attorney general of a State, or other au-
23 thorized State officer, alleging a violation of this Act or
24 any regulation issued under this Act that affects or may
25 affect such State or its residents may bring an action on

1 behalf of the residents of the State in any United States
2 district court for the district in which the defendant is
3 found, resides, or transacts business, or wherever venue
4 is proper under section 1391 of title 28, to obtain appro-
5 priate injunctive relief.

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

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

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

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

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

22 (1) to prevent the attorney general of a State,
23 or other authorized State officer, from exercising the
24 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.

1 **SEC. 6. PRIVACY AND DATA SECURITY EMPLOYEES AND**
2 **FUNDING FOR THE COMMISSION.**

3 (a) EMPLOYMENT AUTHORITY.—The Commission
4 shall hire 50 new full-time employees to focus on privacy
5 and data security, 15 of which shall have technology exper-
6 tise.

7 (b) ADDITIONAL FUNDING FOR PRIVACY AND DATA
8 SECURITY.—There is authorized to be appropriated to the
9 Commission \$35,000,000 for issues related to privacy and
10 data security.

11 **SEC. 7. DEFINITIONS.**

12 In this Act:

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

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

22 (B) does not include—

23 (i) the contents (as defined in section
24 2510(8) of title 18, United States Code) of
25 any communication;

- 1 (ii) the name, address, or financial in-
- 2 formation of a subscriber or customer;
- 3 (iii) cell site location or global posi-
- 4 tioning system information; or
- 5 (iv) business customers.

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

9 (A) of a type, size, and location sufficiently
10 noticeable for an ordinary consumer to read
11 and comprehend the communication;

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

15 (C) is presented in an understandable lan-
16 guage and syntax;

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

21 (E) includes an option that is compliant
22 with applicable obligations of the controller
23 under title III of the Americans with Disabil-
24 ities Act of 1990 (42 U.S.C. 12181 et seq.).

1 (3) COMMISSION.—The term “Commission”
2 means the Federal Trade Commission.

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

7 (5) PROCESSOR.—The term “processor” means
8 a person that processes data on behalf of the con-
9 troller.

10 (6) SENSITIVE PERSONAL INFORMATION.—

11 (A) The term “sensitive personal informa-
12 tion” means information relating to an identi-
13 fied or identifiable individual, including the fol-
14 lowing:

15 (i) Financial account information.

16 (ii) Health information.

17 (iii) Genetic data.

18 (iv) Information pertaining to children
19 under 13 years of age.

20 (v) Social Security numbers.

21 (vi) Unique government-issued identi-
22 fiers

23 (vii) Authentication credentials, such
24 as a username and password.

25 (viii) Precise geolocation information.

1 (ix) Content of a wire communication,
2 oral communication, or electronic commu-
3 nication with respect to any entity that is
4 not the intended recipient of the commu-
5 nication.

6 (x) Call detail records.

7 (xi) Web browsing history, application
8 usage history, and the functional equiva-
9 lent of either.

10 (xii) Biometric information.

11 (xiii) Sexual orientation.

12 (xiv) Religious beliefs.

13 (B) The term “sensitive personal informa-
14 tion” does not include—

15 (i) de-identified information (or the
16 process of transforming personal data so
17 that it is not directly relatable to an identi-
18 fied or identifiable consumer);

19 (ii) information related to employ-
20 ment; or

21 (iii) publicly available information.

22 (7) STATE.—The term “State” means each
23 State of the United States, the District of Columbia,
24 and each commonwealth, territory, or possession of
25 the United States.

1 (8) THIRD PARTY.—The term “third party”
2 means an individual or entity that uses or receives
3 sensitive personal information or behavioral data ob-
4 tained by or on behalf of a controller, other than—

5 (A) a service provider of a controller to
6 whom the controller discloses the consumer’s
7 sensitive personal information for an oper-
8 ational purpose pursuant to an agreement that
9 prohibits the service provider receiving the sen-
10 sitive personal information from using or dis-
11 closing the sensitive personal information for
12 the benefit of the provider; and

13 (B) any entity that uses sensitive personal
14 information only as reasonably necessary—

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

17 (ii) to enforce the terms of use of a
18 controller; or

19 (iii) to detect, prevent, or mitigate
20 fraud or security vulnerabilities.

21 **SEC. 8. RULE OF CONSTRUCTION.**

22 Nothing in this Act may be construed to preclude the
23 acquisition by the Federal Government of—

24 (1) the contents of a wire or electronic commu-
25 nication pursuant to other lawful authorities, includ-

1 ing the authorities under chapter 119 of title 18,
2 United States Code (commonly known as the “Wire-
3 tap Act”), the Foreign Intelligence Surveillance Act
4 of 1978 (50 U.S.C. 1801 et seq.), or any other pro-
5 vision of Federal law not specifically amended by
6 this Act; or

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

16 **SEC. 9. NATIONAL STANDARD.**

17 (a) PREEMPTION.—For a controller that is subject
18 to this Act, or any regulation promulgated pursuant to
19 this Act, the provisions of this Act, or any such regulation,
20 shall preempt any civil provision of the law of any State
21 or political subdivision of a State to the degree the law
22 is focused on the reduction of privacy risk through the
23 regulation of the collection of sensitive personal informa-
24 tion and the collection, storage, processing, sale, sharing
25 with third parties, or other use of such information.

1 (b) CONSUMER PROTECTION LAWS.—Except as pro-
2 vided in subsection (a), this section may not be construed
3 to limit the enforcement, or the bringing of a claim pursu-
4 ant to any State consumer protection law by an attorney
5 general of a State, other than the extent to which any
6 such law regulates the collection of sensitive personal in-
7 formation and the collection, storage, processing, sale,
8 sharing with third parties, or other use of such informa-
9 tion.

10 (c) PROTECTION OF CERTAIN STATE LAW.—Nothing
11 in this Act may be construed to preempt the applicability
12 of any of the following:

13 (1) State constitutional, trespass, contract, data
14 breach notification, or tort law, other than to the de-
15 gree such law is substantially intended to govern the
16 collection of sensitive personal information and the
17 collection, storage, processing, sale, sharing with
18 third parties, or other use of such information.

19 (2) Any other State law to the extent that the
20 law relates to acts of fraud, wiretapping, or the pro-
21 tection of social security numbers.

22 (3) Any State law to the extent the law pro-
23 vides additional provisions to specifically regulate the
24 covered entities as defined for purposes of the regu-
25 lations promulgated pursuant to section 264(c) of

1 the Health Insurance Portability and Accountability
2 Act of 1996 (Public Law 104–191), section 444 of
3 the General Education Provisions Act (commonly
4 known as the Family Educational Rights and Pri-
5 vacy Act of 1974) (20 U.S.C. 1232g), the Fair
6 Credit Reporting Act (15 U.S.C. 1681 et seq.), or
7 the Gramm-Leach-Bliley Act (15 U.S.C. 6701 et
8 seq.).

9 (4) Any private contract based on a State law
10 that requires a party to provide additional or greater
11 privacy for sensitive personal information or data se-
12 curity protections to an individual than this Act, or
13 any regulation promulgated pursuant to this Act.

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

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

○