

115TH CONGRESS  
2D SESSION

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

To amend the Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, or share personal information, to protect personal information, and for other purposes.

---

IN THE SENATE OF THE UNITED STATES

---

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

---

## **A BILL**

To amend the Federal Trade Commission Act to establish requirements and responsibilities for entities that use, store, or share personal information, to protect 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 “Consumer Data Pro-  
5       tection Act”.

6       **SEC. 2. DEFINITIONS.**

7       In this Act:

1           (1) AUTOMATED DECISION SYSTEM.—The term  
2           “automated decision system” means a computational  
3           process, including one derived from machine learn-  
4           ing, statistics, or other data processing or artificial  
5           intelligence techniques, that makes a decision or fa-  
6           cilitates human decision making, that impacts con-  
7           sumers.

8           (2) AUTOMATED DECISION SYSTEM IMPACT AS-  
9           SESSMENT.—The term “automated decision system  
10          impact assessment” means a study evaluating an  
11          automated decision system and the automated deci-  
12          sion system’s development process, including the de-  
13          sign and training data of the automated decision  
14          system, for impacts on accuracy, fairness, bias, dis-  
15          crimination, privacy, and security that includes, at a  
16          minimum—

17                 (A) a detailed description of the automated  
18                 decision system, its design, its training, data,  
19                 and its purpose;

20                 (B) an assessment of the relative benefits  
21                 and costs of the automated decision system in  
22                 light of its purpose, taking into account rel-  
23                 evant factors, including—

24                         (i) data minimization practices;

1 (ii) the duration for which personal  
2 information and the results of the auto-  
3 mated decision system are stored;

4 (iii) what information about the auto-  
5 mated decision system is available to con-  
6 sumers;

7 (iv) the extent to which consumers  
8 have access to the results of the automated  
9 decision system and may correct or object  
10 to its results; and

11 (v) the recipients of the results of the  
12 automated decision system;

13 (C) an assessment of the risks posed by  
14 the automated decision system to the privacy or  
15 security of personal information of consumers  
16 and the risks that the automated decision sys-  
17 tem may result in or contribute to inaccurate,  
18 unfair, biased, or discriminatory decisions im-  
19 pacting consumers; and

20 (D) the measures the covered entity will  
21 employ to minimize the risks described in sub-  
22 paragraph (C), including technological and  
23 physical safeguards.

24 (3) COMMISSION.—The term “Commission”  
25 means Federal Trade Commission.

1           (4) CONSUMER.—The term “consumer” means  
2           an individual.

3           (5) COVERED ENTITY.—The term “covered en-  
4           tity”—

5                   (A) means a person, partnership, or cor-  
6                   poration over which the Commission has juris-  
7                   diction under section 5(a)(2) of the Federal  
8                   Trade Commission Act (15 U.S.C. 45(a)(2);  
9                   and

10                   (B) does not include a person, partnership,  
11                   or corporation that—

12                           (i) with respect to the most recent fis-  
13                           cal year had—

14                                   (I) not greater than \$50,000,000  
15                                   in average annual gross receipts for  
16                                   the 3-taxable-year period preceding  
17                                   the fiscal year, as determined in ac-  
18                                   cordance with paragraphs (2) and (3)  
19                                   of section 448(c) of the Internal Rev-  
20                                   enue Code of 1986; and

21                                   (II) personal information on less  
22                                   than—

23   (aa) 1,000,000 consumers;  
24   and

1 (bb) 1,000,000 consumer de-  
2 vices;

3 (ii) is not substantially owned, oper-  
4 ated, or controlled by a person, partner-  
5 ship, or corporation that does not meet the  
6 requirements under clause (i); and

7 (iii) is not a data broker or other com-  
8 mercial entity that, as a substantial part of  
9 their business, collects, assembles, or main-  
10 tains personal information concerning an  
11 individual who is not a customer or an em-  
12 ployee of that entity in order to sell or  
13 trade the information or provide third-  
14 party access to the information.

15 (6) DATA PROTECTION IMPACT ASSESSMENT.—  
16 The term “data protection impact assessment”  
17 means a study evaluating the extent to which an in-  
18 formation system protects the privacy and security  
19 of personal information the system processes.

20 (7) EXECUTIVE CAPACITY.—The term “execu-  
21 tive capacity” means an assignment within an orga-  
22 nization in which the employee primarily—

23 (A) directs the management of the organi-  
24 zation or a major component or function of the  
25 organization;

1 (B) establishes the goals and policies of  
2 the organization, component, or function;

3 (C) exercises wide latitude in discretionary  
4 decision-making; and

5 (D) receives only general supervision or di-  
6 rection from higher level executives, the board  
7 of directors, or stockholders of the organization.

8 (8) HIGH-RISK AUTOMATED DECISION SYS-  
9 TEM.—The term “high-risk automated decision sys-  
10 tem” means an automated decision system that—

11 (A) taking into account the novelty of the  
12 technology used and the nature, scope, context,  
13 and purpose of the automated decision system,  
14 poses a significant risk—

15 (i) to the privacy or security of per-  
16 sonal information of consumers; or

17 (ii) of resulting in or contributing to  
18 inaccurate, unfair, biased, or discrimina-  
19 tory decisions impacting consumers;

20 (B) makes decisions, or facilitates human  
21 decision making, based on systematic and ex-  
22 tensive evaluations of consumers, including at-  
23 tempts to analyze or predict sensitive aspects of  
24 their lives, such as their work performance, eco-  
25 nomic situation, health, personal preferences,

1 interests, behavior, location, or movements,  
2 that—

3 (i) alter legal rights of consumers; or

4 (ii) otherwise significantly impact con-  
5 sumers;

6 (C) involves the personal information of a  
7 significant number of consumers regarding  
8 race, color, national origin, political opinions,  
9 religion, trade union membership, genetic data,  
10 biometric data, health, gender, gender identity,  
11 sexuality, sexual orientation, criminal convic-  
12 tions, or arrests;

13 (D) systematically monitors a large, pub-  
14 licly accessible physical place; or

15 (E) meets any other criteria established by  
16 the Commission in regulations issued under sec-  
17 tion 7(b)(1).

18 (9) HIGH-RISK INFORMATION SYSTEM.—The  
19 term “high-risk information system” means an in-  
20 formation system that—

21 (A) taking into account the novelty of the  
22 technology used and the nature, scope, context,  
23 and purpose of the information system, poses a  
24 significant risk to the privacy or security of per-  
25 sonal information of consumers;

1 (B) involves the personal information of a  
2 significant number of consumers regarding  
3 race, color, national origin, political opinions,  
4 religion, trade union membership, genetic data,  
5 biometric data, health, gender, gender identity,  
6 sexuality, sexual orientation, criminal convic-  
7 tions, or arrests;

8 (C) systematically monitors a large, pub-  
9 licly accessible physical place; or

10 (D) meets any other criteria established by  
11 the Commission in regulations issued under sec-  
12 tion 7(b)(1).

13 (10) INFORMATION SYSTEM.—The term “infor-  
14 mation system”—

15 (A) means a process, automated or not,  
16 that involves personal information, such as the  
17 collection, recording, organization, structuring,  
18 storage, alteration, retrieval, consultation, use,  
19 sharing, disclosure, dissemination, combination,  
20 restriction, erasure, or destruction of personal  
21 information; and

22 (B) does not include automated decision  
23 systems.

24 (11) JOURNALISM.—The term “journalism”  
25 means the gathering, preparing, collecting,

1       photographing, recording, writing, editing, reporting,  
2       or publishing of news or information that concerns  
3       local, national, or international events or other mat-  
4       ters of public interest for dissemination to the pub-  
5       lic.

6           (12) **PERSONAL INFORMATION.**—The term  
7       “personal information” means any information, re-  
8       gardless of how the information is collected, in-  
9       ferred, or obtained that is reasonably linkable to a  
10      specific consumer or consumer device.

11          (13) **SHARE.**—The term “share”—

12           (A) means the actions of a person, part-  
13      nership, or corporation transferring information  
14      to another person, partnership, or corporation;  
15      and

16           (B) includes actions to knowingly—

17           (i) share, exchange, transfer, sell,  
18      lease, rent, provide, disclose, or otherwise  
19      permit access to information; or

20           (ii) enable or facilitate the collection  
21      of personal information by a third party.

22          (14) **STORE.**—The term “store”—

23           (A) means the actions of a person, part-  
24      nership, or corporation to retain information;  
25      and

1 (B) includes actions to store, collect, as-  
2 semble, possess, control, or maintain informa-  
3 tion.

4 (15) THIRD PARTY.—The term “third party”  
5 means any person, partnership, or corporation that  
6 is not—

7 (A) the person, partnership, or corpora-  
8 tion, whether a covered entity or not, that is  
9 sharing the personal information;

10 (B) solely performing an outsourced func-  
11 tion of the person, partnership, or corporation  
12 sharing the personal information if—

13 (i) the person, partnership, or cor-  
14 poration is contractually or legally prohib-  
15 ited from using, storing, or sharing the  
16 personal information after the conclusion  
17 of the outsourced function; and

18 (ii) the person, partnership, or cor-  
19 poration is complying with regulations pro-  
20 mulgated under subparagraphs (A) and  
21 (B) of section 7(b)(1), regardless of wheth-  
22 er the person, partnership, or corporation  
23 is a covered entity; or

24 (C) a person, partnership, or corporation  
25 for whom the consumer gave opt-in consent for

1 the covered entity to disclose the personal infor-  
2 mation of the consumer.

3 (16) USE.—The term “use” means the actions  
4 of a person, partnership, or corporation in using in-  
5 formation, including actions to use, process, or ac-  
6 cess information.

7 **SEC. 3. NONECONOMIC INJURY.**

8 The first sentence of section 5(n) of the Federal  
9 Trade Commission Act (15 U.S.C. 45(n)) is amended by  
10 inserting “, including those involving noneconomic impacts  
11 and those creating a significant risk of unjustified expo-  
12 sure of personal information,” after “cause substantial in-  
13 jury”.

14 **SEC. 4. CIVIL PENALTY AUTHORITY.**

15 Section 5 of the Federal Trade Commission Act (15  
16 U.S.C. 45) is amended—

17 (1) in subsection (b)—

18 (A) in the fifth sentence, by inserting “,  
19 and it may, in its discretion depending on the  
20 nature and severity of the violation, include in  
21 the cease and desist order an assessment of a  
22 civil penalty, which shall be not more than an  
23 amount that is the greater of \$50,000 per viola-  
24 tion, taken as an aggregate sum of all viola-  
25 tions, and 4 percent of the total annual gross

1 revenue of the person, partnership, or corpora-  
2 tion for the prior fiscal year” before the period  
3 at the end;

4 (2) in subsection (l)—

5 (A) in the first sentence, by striking “of  
6 not more than \$10,000 for each violation” and  
7 inserting “, which shall be not more than an  
8 amount that is the greater of \$50,000 per viola-  
9 tion, taken as an aggregate sum of all viola-  
10 tions, and 4 percent of the total annual gross  
11 revenue of the person, partnership, or corpora-  
12 tion for the prior fiscal year”;

13 (3) in subsection (m)(1)—

14 (A) in subparagraph (A), in the second  
15 sentence, by striking “of not more than  
16 \$10,000 for each violation” and inserting “,  
17 which shall be not more than an amount that  
18 is the greater of \$50,000 per violation, taken as  
19 an aggregate sum of all violations, and 4 per-  
20 cent of the total annual gross revenue of the  
21 person, partnership, or corporation for the prior  
22 fiscal year”; and

23 (B) in subparagraph (B), in the matter  
24 following paragraph (2), by striking “of not  
25 more than \$10,000 for each violation” and in-

1           serting “, which shall be not more than an  
2           amount that is the greater of \$50,000 per viola-  
3           tion, taken as an aggregate sum of all viola-  
4           tions, and 4 percent of the total annual gross  
5           revenue of the person, partnership, or corpora-  
6           tion for the prior fiscal year”.

7 **SEC. 5. ANNUAL DATA PROTECTION REPORTS.**

8           (a) REPORTS.—

9           (1) IN GENERAL.—Each covered entity that has  
10          not less than \$1,000,000,000 per year in revenue  
11          and stores, shares, or uses personal information on  
12          more than 1,000,000 consumers or consumer devices  
13          or any covered entity that stores, shares, or uses  
14          personal information on more than 50,000,000 con-  
15          sumers or consumer devices shall submit to the  
16          Commission an annual data protection report de-  
17          scribing in detail whether, during the reporting pe-  
18          riod, the covered entity complied with the regula-  
19          tions promulgated in accordance with subparagraphs  
20          (A) and (B) of section 7(b)(1). To the extent that  
21          the covered entity did not comply with these regula-  
22          tions, this statement shall include a description of  
23          which regulations were violated and the number of  
24          consumers whose personal information was im-  
25          pacted.

1           (2) REGULATIONS.—Not later than 2 years  
2 after the date of enactment of this Act, the Federal  
3 Trade Commission shall promulgate regulations in  
4 accordance with section 553 of title 5, United States  
5 Code, carrying out this subsection.

6           (b) FAILURE OF CORPORATE OFFICERS TO CERTIFY  
7 PRIVACY AND DATA SECURITY REPORTS.—

8           (1) IN GENERAL.—Chapter 63 of title 18,  
9 United States Code, is amended by adding at the  
10 end the following:

11 **“§ 1352. Failure of corporate officers to certify data**  
12 **protection reports**

13           “(a) DEFINITION.—In this section, the term ‘covered  
14 entity’ has the meaning given the term in section 2 of the  
15 Consumer Data Protection Act.

16           “(b) CERTIFICATION OF ANNUAL DATA PROTECTION  
17 REPORTS.—Each annual report filed by a company with  
18 the Federal Trade Commission pursuant to section 5(a)  
19 of the Consumer Data Protection Act shall be accom-  
20 panied by a written statement by the chief executive offi-  
21 cer, chief privacy officer (or equivalent thereof), and chief  
22 information security officer (or equivalent thereof) of the  
23 company.

24           “(c) CONTENT.—The statement required under sub-  
25 section (b) shall certify that the annual report fully com-

1 plies with the requirements of section 5(a) of the Con-  
2 sumer Data Protection Act.

3 “(d) CRIMINAL PENALTIES.—Whoever—

4 “(1) certifies any statement as set forth in sub-  
5 sections (b) and (c) of this section knowing that the  
6 annual report accompanying the statement does not  
7 comport with all the requirements set forth in this  
8 section shall be fined not more than the greater of  
9 \$1,000,000 or 5 percent of the largest amount of  
10 annual compensation the person received during the  
11 previous 3-year period from the covered entity, im-  
12 prisoned not more than 10 years, or both; or

13 “(2) intentionally certifies any statement as set  
14 forth in subsections (b) and (c) of this section know-  
15 ing that the annual report accompanying the state-  
16 ment does not comport with all the requirements set  
17 forth in this section shall be fined not more than  
18 \$5,000,000 or 25 percent of the largest amount of  
19 annual compensation the person received during the  
20 previous 3-year period from the covered entity, im-  
21 prisoned not more than 20 years, or both.”.

22 (2) TECHNICAL AND CONFORMING AMEND-  
23 MENT.—The table of sections for chapter 63 of title  
24 18, United States Code, is amended by adding at  
25 the end the following:

“1352. Failure of corporate officers to certify data protection reports.”.

1 **SEC. 6. “DO NOT TRACK” DATA SHARING OPT OUT.**

2 (a) REGULATIONS.—Not later than 2 years after the  
3 date of enactment of this Act, the Commission shall pro-  
4 mulgate regulations, in accordance with section 553 of  
5 title 5, United States Code, to—

6 (1) implement and maintain a “Do Not Track”  
7 data sharing opt-out website—

8 (A) that allows consumers to opt-out of  
9 data sharing, view their opt-out status, and  
10 change their opt-out status;

11 (B) the effect of which opt-out is to pre-  
12 vent—

13 (i) covered entities from sharing the  
14 personal information of the consumer with  
15 third parties, including personal informa-  
16 tion shared with or stored by the covered  
17 entity prior to the opt-out unless—

18 (I) the sharing is necessary for  
19 the primary purpose for which the  
20 consumer provided the personal infor-  
21 mation; and

22 (II) the third party with whom  
23 the personal information was shared  
24 does not retain the personal informa-  
25 tion for secondary purposes; and

1 (ii) covered entities from storing or  
2 using personal information of the con-  
3 sumer that has been shared with them by  
4 non-covered entities, not including personal  
5 information shared with or stored by the  
6 covered entity prior to the opt-out;

7 (C) that is reasonably accessible and usa-  
8 ble by consumers; and

9 (D) that enables consumers to make use of  
10 the features described in subparagraph (A)  
11 through an Application Programming Interface;

12 (2) as part of the implementation of the opt-out  
13 website described in paragraph (1)—

14 (A) maintain a record of the opt-out status  
15 of consumers enrolled through the opt-out  
16 website, including the date and time when the  
17 consumer opted out;

18 (B) enable consumers to convey their opt-  
19 out status to covered entities in 1 or more pri-  
20 vacy-protecting ways through technological  
21 means determined by the Commission, such as  
22 through a consumer's web browser or operating  
23 system;

24 (C) enable covered entities to determine  
25 whether a particular consumer is enrolled in the

1 opt-out website in a privacy-preserving way that  
2 does not result in the disclosure of any personal  
3 information other than a consumer's opt-out  
4 status to that covered entity; and

5 (D) enable covered entities to make use of  
6 the mechanism described in subparagraph (C)  
7 through an Application Programming Interface,  
8 for which the Commission may charge a reason-  
9 able fee to cover the costs of operating the opt-  
10 out registry and access to the system;

11 (3) require that a covered entity be bound by  
12 the opt-out of a consumer when the opt-out is con-  
13 veyed through the opt-out website implemented and  
14 maintained by the Commission—

15 (A) immediately for new customers; and

16 (B) within 30 days for existing customers  
17 or consumers who are not customers, unless,  
18 after the consumer has opted out in the manner  
19 described in paragraph (1)(A), the covered enti-  
20 ty receives, in accordance with the procedures  
21 described in paragraph (10), consent from the  
22 consumer to not be bound by the consumer's  
23 opt-out;

24 (4) require covered entities that store or use  
25 personal data on consumers with which they—

1 (A) do not have a direct relationship; or

2 (B) otherwise do not have the ability to de-  
3 termine the consumer's opt-out preference  
4 through one of the technological means estab-  
5 lished pursuant to paragraph (2)(B);

6 to make a good-faith effort to determine the con-  
7 sumer's opt-out status at least as frequently as de-  
8 termined by the Commission, through the Applica-  
9 tion Programming Interface maintained by the Com-  
10 mission pursuant to paragraph (2)(D);

11 (5) permit covered entities to not be bound by  
12 the consumer's opt-out for—

13 (A) disclosures made to the government  
14 that are either required or permitted by law;

15 (B) disclosures made pursuant to an order  
16 of a court or administrative tribunal;

17 (C) disclosures made in response to a sub-  
18 poena, discovery request, or other lawful proc-  
19 ess provided that such process is accompanied  
20 by a protective order that—

21 (i) prohibits the parties from using or  
22 disclosing the personal information for any  
23 purpose other than the litigation or pro-  
24 ceeding for which such personal informa-  
25 tion was requested; and

1 (ii) requires the return to the covered  
2 entity or destruction of the personal infor-  
3 mation (including all copies made) at the  
4 end of the litigation or proceeding; or

5 (D) disclosures made to investigate, pro-  
6 tect themselves and their customers from, or re-  
7 cover from fraud, cyber attacks, or other unlaw-  
8 ful activity;

9 (6) establish standards and procedures, includ-  
10 ing through an Application Programming Interface,  
11 for a covered entity to request and obtain consent  
12 from a consumer who has opted-out in the manner  
13 described in paragraph (1)(A) for the covered entity  
14 to not be bound by the opt-out, provided such stand-  
15 ards and procedures—

16 (A) require the covered entity to provide  
17 the consumer, at the time the covered entity is  
18 seeking consent, in accordance with paragraph  
19 (10), and in a form that is understandable to  
20 a reasonable consumer—

21 (i) a list of each third party with  
22 whom the personal information of the con-  
23 sumer will or may be shared by the covered  
24 entity;

1 (ii) a description of the personal infor-  
2 mation of that consumer that will or may  
3 be shared; and

4 (iii) a description of the purposes for  
5 which the personal information of that con-  
6 sumer will or may be shared;

7 (B) if the covered entity requires consent  
8 as a condition for providing a product or serv-  
9 ice, require the covered entity to—

10 (i) notify the consumer that he or she  
11 can obtain a substantially similar product  
12 or service in exchange for monetary pay-  
13 ment or other compensation rather than by  
14 permitting the covered entity to share the  
15 consumer's personal information, as pro-  
16 vided in subsection (b)(1)(B); and

17 (ii) with respect to the notice de-  
18 scribed in clause (i)—

19 (I) make the notice in a clear  
20 and conspicuous manner; and

21 (II) include the cost of the fee, if  
22 any, and instructions for obtaining  
23 the substantially similar product or  
24 service described in clause (i);

1           (C) if the covered entity does not require  
2 consent as a condition for providing a product  
3 or service, require the covered entity to clearly  
4 and conspicuously notify the consumer that the  
5 consumer may refuse to provide consent but  
6 still obtain the product or service; and

7           (D) require the covered entity to notify the  
8 consumer of his or her right, and how to exer-  
9 cise that right, to later withdraw consent for  
10 the covered entity to not be bound by the con-  
11 sumer's opt-out;

12           (7) not less frequently than every 2 years, ex-  
13 amine the information that is presented to con-  
14 sumers in accordance with the procedures described  
15 in paragraph (6) to make sure that the information  
16 is useful, understandable, and to the extent possible,  
17 does not result in notification fatigue;

18           (8) establish standards and procedures requir-  
19 ing that when a non-covered entity that is not the  
20 consumer shares personal information about that  
21 consumer with a covered-entity, the covered entity  
22 shall make reasonable efforts to verify the opt-out  
23 status of the consumer whose personal information  
24 has been shared with the covered entity, after which

1 the covered entity may only store or use that per-  
2 sonal information—

3 (A) if the consumer has not opted-out in  
4 the manner described in paragraph (2)(A); or

5 (B)(i) if the non-covered entity knowingly  
6 enabled or facilitated the collection of personal  
7 information by the covered entity and the cov-  
8 ered entity itself receives consent from the con-  
9 sumer to store or use the consumer's personal  
10 information in accordance with paragraph (9);  
11 or

12 (ii) if the non-covered entity otherwise  
13 shares the information with the covered-entity  
14 and the consumer has given consent in accord-  
15 ance with paragraph (9) to the covered entity  
16 or non-covered entity for the non-covered entity  
17 to share the consumer's personal information  
18 with the specific covered entity;

19 (9) establish standards and procedures for a  
20 person, partnership, or corporation to request and  
21 obtain consent from a consumer, in accordance with  
22 paragraph (8)(B) that clearly identifies the covered  
23 entity that will be storing or using the personal in-  
24 formation and provides the consumer, at the time  
25 the person, partnership, or corporation is seeking

1 consent, in accordance with paragraph (10), and in  
2 a form that is understandable to a reasonable con-  
3 sumer—

4 (A) the name and contact information of  
5 the person, partnership, or corporation from  
6 whom the personal information of that con-  
7 sumer is to be obtained;

8 (B) a description of the personal informa-  
9 tion of that consumer that will be shared; and

10 (C) a description of the purposes for which  
11 the personal information of that consumer will  
12 be shared;

13 (10) detail the standardized form and manner  
14 in which certain information related to sharing shall  
15 be disclosed to consumers, which shall, to the extent  
16 that the Commission determines to be practicable  
17 and appropriate, be in the form of a table that—

18 (A) contains clear and concise headings for  
19 each item of such information; and

20 (B) provides a clear and concise form for  
21 stating each item of information required to be  
22 disclosed under each such heading; and

23 (11) permit a consumer to withdraw his or her  
24 consent to a covered entity to not be bound by the

1 consumer's opt-out at any time, including through  
2 an Application Programming Interface.

3 (b) ACTS PROHIBITED.—

4 (1) IN GENERAL.—It shall be unlawful for any  
5 covered entity to condition its products or services  
6 upon a requirement that consumers—

7 (A) change their opt-out status through  
8 the opt-out website maintained by the Commis-  
9 sion pursuant to subsection (a)(2); or

10 (B) give the covered entity consent to not  
11 be bound by the consumer's opt-out status, un-  
12 less the consumer is also given an option to pay  
13 a fee to use a substantially similar service that  
14 is not conditioned upon a requirement that the  
15 consumer give the covered entity consent to not  
16 be bound by the consumer's opt-out status.

17 (2) FEE.—The fee described in paragraph  
18 (1)(B) shall not be greater than the amount of mon-  
19 etary gain the covered entity would have earned had  
20 the average consumer not opted-out.

21 (c) ENFORCEMENT BY THE COMMISSION.—A viola-  
22 tion of subsection (b) shall be treated as a violation of  
23 a rule defining an unfair or deceptive act or practice under  
24 section 18(a)(1)(B) of the Federal Trade Commission Act  
25 (15 U.S.C. 57a(a)(1)(B)).

1 **SEC. 7. DATA PROTECTION AUTHORITY.**

2 (a) ACTS PROHIBITED.—It is unlawful for any cov-  
3 ered entity to—

4 (1) violate a regulation promulgated under sub-  
5 section (b); or

6 (2) knowingly provide substantial assistance to  
7 any person, partnership, or corporation whose ac-  
8 tions violate this Act.

9 (b) REGULATIONS.—

10 (1) IN GENERAL.—Not later than 2 years after  
11 the date of enactment of this section, the Commis-  
12 sion shall promulgate regulations, in accordance with  
13 section 553 of title 5, United States Code, that—

14 (A) require each covered entity to establish  
15 and implement reasonable cyber security and  
16 privacy policies, practices, and procedures to  
17 protect personal information used, stored, or  
18 shared by the covered entity from improper ac-  
19 cess, disclosure, exposure, or use;

20 (B) require each covered entity to imple-  
21 ment reasonable physical, technical, and organi-  
22 zational measures to ensure that technologies or  
23 products used, produced, sold, offered, or leased  
24 by the covered entity that the covered entity  
25 knows or has reason to believe store, process, or  
26 otherwise interact with personal information are

1 built and function consistently with reasonable  
2 data protection practices;

3 (C) require each covered entity to des-  
4 ignate at least 1 employee who reports directly  
5 to an employee acting in an executive capacity  
6 in the covered entity, to coordinate its efforts to  
7 comply with and carry out its responsibilities  
8 under this Act, including any request or chal-  
9 lenge related to the sharing of personal infor-  
10 mation;

11 (D) require each covered entity to provide,  
12 at no cost, not later than 30 business days after  
13 receiving a written request from a verified con-  
14 sumer about whom the covered entity stores  
15 personal information—

16 (i) a reasonable means to review any  
17 stored personal information of that verified  
18 consumer, including the manner in which  
19 the information was collected and the date  
20 of collection, in a form that is understand-  
21 able to a reasonable consumer;

22 (ii) a reasonable means to challenge  
23 the accuracy of any stored personal infor-  
24 mation of that verified consumer, includ-  
25 ing—

1 (I) by providing publicly acces-  
2 sible contact information for any em-  
3 ployee responsible for overseeing such  
4 a challenge; and

5 (II) implementing a reasonable  
6 process for responding to such chal-  
7 lenges, including the ability of the cov-  
8 ered entity to terminate an investiga-  
9 tion of information disputed by a con-  
10 sumer under this clause, and pro-  
11 viding notice to the consumer of such  
12 termination, if the covered entity rea-  
13 sonably determines that the dispute  
14 by the consumer is frivolous or irrele-  
15 vant, including by reason of a failure  
16 by a consumer to provide sufficient in-  
17 formation to investigate the disputed  
18 information;

19 (iii) a list of each person, partnership,  
20 or corporation with whom the personal in-  
21 formation of that verified consumer was  
22 shared by the covered entity that—

23 (I) does not include—

24 (aa) disclosures to govern-  
25 mental entities pursuant to a

1 court order or law that prohibits  
2 the covered entity from revealing  
3 that disclosure to the consumer;

4 (bb) disclosures of personal  
5 information to third parties when  
6 the personal information of the  
7 consumer was made available to  
8 and readily accessible by the gen-  
9 eral public with the consent of  
10 the verified consumer and shared  
11 with the third party through a  
12 mechanism available to any mem-  
13 ber of the general public; or

14 (cc) disclosures of informa-  
15 tion about the verified consumer  
16 that the covered entity did not  
17 obtain from that consumer, if re-  
18 vealing that disclosure of infor-  
19 mation would expose another  
20 consumer to likely harm; and

21 (II) except as provided in sub-  
22 paragraph (I), includes, at a min-  
23 imum—

24 (aa) the name and contact  
25 information of each person, part-

1                   nership, or corporation with  
2                   whom the personal information of  
3                   that verified consumer was  
4                   shared;

5                   (bb) a description of the per-  
6                   sonal information of that verified  
7                   consumer that was shared, in a  
8                   form that is understandable to a  
9                   reasonable consumer;

10                  (cc) a statement of the pur-  
11                  poses for which the personal in-  
12                  formation of that verified con-  
13                  sumer was shared;

14                  (dd) if the covered entity  
15                  claims consent from the con-  
16                  sumer as the basis for sharing, a  
17                  statement of the circumstances  
18                  surrounding that consumer con-  
19                  sent, specifically when, where,  
20                  and how the consent was ob-  
21                  tained and by whom the consent  
22                  was obtained; and

23                  (ee) a statement of when the  
24                  personal information of that

1 verified consumer was shared;

2 and

3 (iv) for any personal information  
4 about that verified consumer stored by the  
5 covered entity that the covered entity did  
6 not obtain directly from that verified con-  
7 sumer, a list identifying—

8 (I) the name and contact infor-  
9 mation of each person, partnership, or  
10 corporation from whom the personal  
11 information of that verified consumer  
12 was obtained;

13 (II) a description of the personal  
14 information, in a form that is under-  
15 standable to a reasonable consumer;

16 (III) a statement of the purposes  
17 for which the personal information of  
18 that verified consumer was obtained  
19 by the covered entity; and

20 (IV) a statement of the purposes  
21 for which the personal information of  
22 that verified consumer was shared  
23 with the covered entity;

24 (E) detail the standardized form and man-  
25 ner in which the information in subparagraph

1 (D) shall be disclosed to consumers which shall,  
2 to the extent the Commission determines to be  
3 practicable and appropriate, be in the form of  
4 a table that—

5 (i) contains clear and concise headings  
6 for each item of information; and

7 (ii) provides a clear and concise form  
8 for stating each item of information re-  
9 quired to be disclosed under each such  
10 heading;

11 (F) require each covered entity to correct  
12 the stored personal information of the verified  
13 consumer if, after investigating a challenge by  
14 a verified consumer under subparagraph (D),  
15 the covered entity determines that the personal  
16 information is inaccurate;

17 (G) require each covered entity to conduct  
18 automated decision system impact assessments  
19 of—

20 (i) existing high-risk automated deci-  
21 sion systems, as frequently as the Commis-  
22 sion determines is necessary; and

23 (ii) new high-risk automated decision  
24 systems, prior to implementation;

1 provided that a covered entity may evaluate  
2 similar high-risk automated decision systems  
3 that present similar risks in a single assess-  
4 ment;

5 (H) require each covered entity to conduct  
6 data protection impact assessments of—

7 (i) existing high-risk information sys-  
8 tems, as frequently as the Commission de-  
9 termines is necessary; and

10 (ii) new high-risk information sys-  
11 tems, prior to implementation;

12 provided that a covered entity may evaluate  
13 similar high-risk information systems that  
14 present similar risks in a single assessment;

15 (I) require each covered entity to conduct  
16 the impact assessments under subparagraphs  
17 (G) and (H), if reasonably possible, in consulta-  
18 tion with external third parties, including inde-  
19 pendent auditors and independent technology  
20 experts; and

21 (J) require each covered entity to reason-  
22 ably address in a timely manner the results of  
23 the impact assessments under subparagraphs  
24 (G) and (H).

1           (2) CONSULTATION.—The Commission shall  
2 promulgate regulations under subparagraphs (A)  
3 and (B) of paragraph (1) in consultation with the  
4 National Institute of Standards and Technology.

5           (3) OPTIONAL PUBLICATION OF IMPACT AS-  
6 SESSMENTS.—The impact assessments under sub-  
7 paragraphs (G) and (H) may be made public by the  
8 covered entity at its sole discretion.

9           (c) PREEMPTION OF PRIVATE CONTRACTS.—It shall  
10 be unlawful for any covered entity to commit the acts pro-  
11 hibited in subsection (a), regardless of specific agreements  
12 between entities or consumers.

13           (d) ENFORCEMENT BY THE COMMISSION.—

14           (1) UNFAIR OR DECEPTIVE ACTS OR PRAC-  
15 TICES.—A violation of subsection (a) shall be treated  
16 as a violation of a rule defining an unfair or decep-  
17 tive act or practice under section 18(a)(1)(B) of the  
18 Federal Trade Commission Act (15 U.S.C.  
19 57a(a)(1)(B)).

20           (2) POWERS OF THE COMMISSION.—

21           (A) IN GENERAL.—The Commission shall  
22 enforce this section in the same manner, by the  
23 same means, and with the same jurisdiction,  
24 powers, and duties as though all applicable  
25 terms and provisions of the Federal Trade

1 Commission Act (15 U.S.C. 41 et seq.) were in-  
2 corporated into and made a part of this section.

3 (B) PRIVILEGES AND IMMUNITIES.—Any  
4 person who violates subsection (a) shall be sub-  
5 ject to the penalties and entitled to the privi-  
6 leges and immunities provided in the Federal  
7 Trade Commission Act (15 U.S.C. 41 et seq.).

8 (C) AUTHORITY PRESERVED.—Nothing in  
9 this section shall be construed to limit the au-  
10 thority of the Commission under any other pro-  
11 vision of law.

12 **SEC. 8. BUREAU OF TECHNOLOGY.**

13 (a) ESTABLISHMENT.—There is established in the  
14 Federal Trade Commission a bureau to be known as the  
15 Bureau of Technology (referred to in this section as the  
16 “Bureau”).

17 (b) CHIEF TECHNOLOGIST.—The Bureau shall be  
18 headed by a chief technologist, who shall be appointed by  
19 the Chairman of the Commission.

20 (c) STAFF.—

21 (1) IN GENERAL.—Except as provided in para-  
22 graph (2), the Director of the Bureau may, without  
23 regard to the civil service laws (including regula-  
24 tions), appoint and terminate 50 additional per-  
25 sonnel with expertise in management, technology,

1 digital design, user experience, product management,  
2 software engineering, and other related fields to  
3 technologist and management positions to enable the  
4 Bureau to perform the duties of the Bureau.

5 (2) EXCEPTED SERVICE.—Not fewer than 40 of  
6 the additional personnel appointed under paragraph  
7 (1) shall be appointed to positions described in sec-  
8 tion 213.3102(r) of title 5, Code of Federal Regula-  
9 tions.

10 (d) AUTHORIZATION OF APPROPRIATIONS.—There is  
11 authorized to be appropriated to the Bureau such sums  
12 as are necessary to carry out this section.

13 **SEC. 9. ADDITIONAL PERSONNEL IN THE BUREAU OF CON-**  
14 **SUMER PROTECTION.**

15 (a) IN GENERAL.—Notwithstanding any other provi-  
16 sion of law, the Director of the Bureau of Consumer Pro-  
17 tection of the Federal Trade Commission may, without re-  
18 gard to the civil service laws (including regulations), ap-  
19 point—

20 (1) 100 additional personnel in the Division of  
21 Privacy and Identity Protection of the Bureau of  
22 Consumer Protection; and

23 (2) 25 additional personnel in the Division of  
24 Enforcement of the Bureau of Consumer Protection.

1 (b) AUTHORIZATION OF APPROPRIATIONS.—There is  
2 authorized to be appropriated to the Director of the Bu-  
3 reau of Consumer Protection such sums as may be nec-  
4 essary to carry out this section.

5 **SEC. 10. COMPLAINT RESOLUTION.**

6 The Commission shall create rules and guidance es-  
7 tablishing procedures for the resolution of complaints by  
8 consumers regarding covered entities that improperly use,  
9 store, or share the personal information of consumers, in-  
10 cluding procedures to—

11 (1) properly process and store complaints;

12 (2) provide a consumer with email updates re-  
13 garding the status of the consumer’s complaint;

14 (3) create an online portal that allows a con-  
15 sumer to log in and track the status of the con-  
16 sumer’s complaint;

17 (4) review and forward complaints to the cor-  
18 rect person, partnership, corporation, government  
19 agency, or other entity; and

20 (5) process and store each response from a per-  
21 son, partnership, corporation, government agency, or  
22 other entity to which a complaint was forwarded.

23 **SEC. 11. APPLICATION PROGRAMMING INTERFACES.**

24 The Commission shall, in consultation with the Na-  
25 tional Institute of Standards and Technology and relevant

1 stakeholders, including consumer advocates and inde-  
2 pendent technology experts—

3           (1) standardize Application Programming Inter-  
4 faces necessary to permit consumers and covered en-  
5 tities to programmatically avail themselves of the  
6 rights and responsibilities created by this Act;

7           (2) permit and enable consumers to securely  
8 delegate the ability to make requests on their behalf;  
9 and

10           (3) require covered entities to implement the  
11 Application Programming Interfaces, as appropriate.

12 **SEC. 12. NEWS MEDIA PROTECTIONS.**

13       Covered entities engaged in journalism shall not be  
14 subject to the obligations imposed under this Act to the  
15 extent that those obligations directly infringe on the jour-  
16 nalism, rather than the business practices, of the covered  
17 entity.