

111TH CONGRESS
1ST SESSION

S. 1490

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

IN THE SENATE OF THE UNITED STATES

JULY 22, 2009

Mr. LEAHY introduced the following bill; which was read twice and referred to the Committee on the Judiciary

A BILL

To prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

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

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

4 (a) SHORT TITLE.—This Act may be cited as the
5 “Personal Data Privacy and Security Act of 2009”.

6 (b) TABLE OF CONTENTS.—The table of contents of
7 this Act is as follows:

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

TITLE I—ENHANCING PUNISHMENT FOR IDENTITY THEFT AND
OTHER VIOLATIONS OF DATA PRIVACY AND SECURITY

- Sec. 101. Organized criminal activity in connection with unauthorized access to personally identifiable information.
- Sec. 102. Concealment of security breaches involving sensitive personally identifiable information.
- Sec. 103. Review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information.
- Sec. 104. Effects of identity theft on bankruptcy proceedings.

TITLE II—DATA BROKERS

- Sec. 201. Transparency and accuracy of data collection.
- Sec. 202. Enforcement.
- Sec. 203. Relation to State laws.
- Sec. 204. Effective date.

TITLE III—PRIVACY AND SECURITY OF PERSONALLY
IDENTIFIABLE INFORMATION

Subtitle A—A Data Privacy and Security Program

- Sec. 301. Purpose and applicability of data privacy and security program.
- Sec. 302. Requirements for a personal data privacy and security program.
- Sec. 303. Enforcement.
- Sec. 304. Relation to other laws.

Subtitle B—Security Breach Notification

- Sec. 311. Notice to individuals.
- Sec. 312. Exemptions.
- Sec. 313. Methods of notice.
- Sec. 314. Content of notification.
- Sec. 315. Coordination of notification with credit reporting agencies.
- Sec. 316. Notice to law enforcement.
- Sec. 317. Enforcement.
- Sec. 318. Enforcement by State attorneys general.
- Sec. 319. Effect on Federal and State law.
- Sec. 320. Authorization of appropriations.
- Sec. 321. Reporting on risk assessment exemptions.
- Sec. 322. Effective date.

Subtitle C—Office of Federal Identity Protection

- Sec. 331. Office of Federal Identity Protection.

TITLE IV—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL
DATA

- Sec. 401. General services administration review of contracts.
- Sec. 402. Requirement to audit information security practices of contractors and third party business entities.

Sec. 403. Privacy impact assessment of government use of commercial information services containing personally identifiable information.

Sec. 404. Implementation of chief privacy officer requirements.

1 **SEC. 2. FINDINGS.**

2 Congress finds that—

3 (1) databases of personally identifiable informa-
4 tion are increasingly prime targets of hackers, iden-
5 tity thieves, rogue employees, and other criminals,
6 including organized and sophisticated criminal oper-
7 ations;

8 (2) identity theft is a serious threat to the Na-
9 tion's economic stability, homeland security, the de-
10 velopment of e-commerce, and the privacy rights of
11 Americans;

12 (3) over 9,300,000 individuals were victims of
13 identity theft in America last year;

14 (4) security breaches are a serious threat to
15 consumer confidence, homeland security, e-com-
16 merce, and economic stability;

17 (5) it is important for business entities that
18 own, use, or license personally identifiable informa-
19 tion to adopt reasonable procedures to ensure the se-
20 curity, privacy, and confidentiality of that personally
21 identifiable information;

22 (6) individuals whose personal information has
23 been compromised or who have been victims of iden-
24 tity theft should receive the necessary information

1 and assistance to mitigate their damages and to re-
2 store the integrity of their personal information and
3 identities;

4 (7) data brokers have assumed a significant
5 role in providing identification, authentication, and
6 screening services, and related data collection and
7 analyses for commercial, nonprofit, and government
8 operations;

9 (8) data misuse and use of inaccurate data have
10 the potential to cause serious or irreparable harm to
11 an individual's livelihood, privacy, and liberty and
12 undermine efficient and effective business and gov-
13 ernment operations;

14 (9) there is a need to ensure that data brokers
15 conduct their operations in a manner that prioritizes
16 fairness, transparency, accuracy, and respect for the
17 privacy of consumers;

18 (10) government access to commercial data can
19 potentially improve safety, law enforcement, and na-
20 tional security; and

21 (11) because government use of commercial
22 data containing personal information potentially af-
23 fects individual privacy, and law enforcement and
24 national security operations, there is a need for Con-

1 gress to exercise oversight over government use of
2 commercial data.

3 **SEC. 3. DEFINITIONS.**

4 In this Act, the following definitions shall apply:

5 (1) AGENCY.—The term “agency” has the same
6 meaning given such term in section 551 of title 5,
7 United States Code.

8 (2) AFFILIATE.—The term “affiliate” means
9 persons related by common ownership or by cor-
10 porate control.

11 (3) BUSINESS ENTITY.—The term “business
12 entity” means any organization, corporation, trust,
13 partnership, sole proprietorship, unincorporated as-
14 sociation, or venture established to make a profit, or
15 nonprofit.

16 (4) IDENTITY THEFT.—The term “identity
17 theft” means a violation of section 1028 of title 18,
18 United States Code.

19 (5) DATA BROKER.—The term “data broker”
20 means a business entity which for monetary fees or
21 dues regularly engages in the practice of collecting,
22 transmitting, or providing access to sensitive person-
23 ally identifiable information on more than 5,000 in-
24 dividuals who are not the customers or employees of
25 that business entity or affiliate primarily for the

1 purposes of providing such information to non-
2 affiliated third parties on an interstate basis.

3 (6) DATA FURNISHER.—The term “data fur-
4 nisher” means any agency, organization, corpora-
5 tion, trust, partnership, sole proprietorship, unincor-
6 porated association, or nonprofit that serves as a
7 source of information for a data broker.

8 (7) ENCRYPTION.—The term “encryption”—

9 (A) means the protection of data in elec-
10 tronic form, in storage or in transit, using an
11 encryption technology that has been adopted by
12 an established standards setting body which
13 renders such data indecipherable in the absence
14 of associated cryptographic keys necessary to
15 enable decryption of such data; and

16 (B) includes appropriate management and
17 safeguards of such cryptographic keys so as to
18 protect the integrity of the encryption.

19 (8) PERSONAL ELECTRONIC RECORD.—

20 (A) IN GENERAL.—The term “personal
21 electronic record” means data associated with
22 an individual contained in a database,
23 networked or integrated databases, or other
24 data system that is provided to nonaffiliated

1 third parties and includes sensitive personally
2 identifiable information about that individual.

3 (B) EXCLUSIONS.—The term “personal
4 electronic record” does not include—

5 (i) any data related to an individual’s
6 past purchases of consumer goods; or

7 (ii) any proprietary assessment or
8 evaluation of an individual or any propri-
9 etary assessment or evaluation of informa-
10 tion about an individual.

11 (9) PERSONALLY IDENTIFIABLE INFORMA-
12 TION.—The term “personally identifiable informa-
13 tion” means any information, or compilation of in-
14 formation, in electronic or digital form serving as a
15 means of identification, as defined by section
16 1028(d)(7) of title 18, United State Code.

17 (10) PUBLIC RECORD SOURCE.—The term
18 “public record source” means the Congress, any
19 agency, any State or local government agency, the
20 government of the District of Columbia and govern-
21 ments of the territories or possessions of the United
22 States, and Federal, State or local courts, courts
23 martial and military commissions, that maintain
24 personally identifiable information in records avail-
25 able to the public.

1 (11) SECURITY BREACH.—

2 (A) IN GENERAL.—The term “security
3 breach” means compromise of the security, con-
4 fidentiality, or integrity of computerized data
5 through misrepresentation or actions that result
6 in, or there is a reasonable basis to conclude
7 has resulted in, acquisition of or access to sen-
8 sitive personally identifiable information that is
9 unauthorized or in excess of authorization.

10 (B) EXCLUSION.—The term “security
11 breach” does not include—

12 (i) a good faith acquisition of sensitive
13 personally identifiable information by a
14 business entity or agency, or an employee
15 or agent of a business entity or agency, if
16 the sensitive personally identifiable infor-
17 mation is not subject to further unauthor-
18 ized disclosure; or

19 (ii) the release of a public record not
20 otherwise subject to confidentiality or non-
21 disclosure requirements.

22 (12) SENSITIVE PERSONALLY IDENTIFIABLE IN-
23 FORMATION.—The term “sensitive personally identi-
24 fiable information” means any information or com-

1 pilation of information, in electronic or digital form
2 that includes—

3 (A) an individual's first and last name or
4 first initial and last name in combination with
5 any 1 of the following data elements:

6 (i) A non-truncated social security
7 number, driver's license number, passport
8 number, or alien registration number.

9 (ii) Any 2 of the following:

10 (I) Home address or telephone
11 number.

12 (II) Mother's maiden name, if
13 identified as such.

14 (III) Month, day, and year of
15 birth.

16 (iii) Unique biometric data such as a
17 finger print, voice print, a retina or iris
18 image, or any other unique physical rep-
19 resentation.

20 (iv) A unique account identifier, elec-
21 tronic identification number, user name, or
22 routing code in combination with any asso-
23 ciated security code, access code, or pass-
24 word that is required for an individual to

1 obtain money, goods, services, or any other
2 thing of value; or

3 (B) a financial account number or credit
4 or debit card number in combination with any
5 security code, access code, or password that is
6 required for an individual to obtain credit, with-
7 draw funds, or engage in a financial trans-
8 action.

9 **TITLE I—ENHANCING PUNISH-**
10 **MENT FOR IDENTITY THEFT**
11 **AND OTHER VIOLATIONS OF**
12 **DATA PRIVACY AND SECU-**
13 **RITY**

14 **SEC. 101. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION**
15 **WITH UNAUTHORIZED ACCESS TO PERSON-**
16 **ALLY IDENTIFIABLE INFORMATION.**

17 Section 1961(1) of title 18, United States Code, is
18 amended by inserting “section 1030(a)(2)(D) (relating to
19 fraud and related activity in connection with unauthorized
20 access to sensitive personally identifiable information as
21 defined in the Personal Data Privacy and Security Act of
22 2009,” before “section 1084”.

1 **SEC. 102. CONCEALMENT OF SECURITY BREACHES INVOLV-**
2 **ING SENSITIVE PERSONALLY IDENTIFIABLE**
3 **INFORMATION.**

4 (a) IN GENERAL.—Chapter 47 of title 18, United
5 States Code, is amended by adding at the end the fol-
6 lowing:

7 **“§ 1041. Concealment of security breaches involving**
8 **sensitive personally identifiable informa-**
9 **tion**

10 “(a) Whoever, having knowledge of a security breach
11 and of the obligation to provide notice of such breach to
12 individuals under title III of the Personal Data Privacy
13 and Security Act of 2009, and having not otherwise quali-
14 fied for an exemption from providing notice under section
15 312 of such Act, intentionally and willfully conceals the
16 fact of such security breach and which breach causes eco-
17 nomic damage to 1 or more persons, shall be fined under
18 this title or imprisoned not more than 5 years, or both.

19 “(b) For purposes of subsection (a), the term ‘person’
20 has the same meaning as in section 1030(e)(12) of title
21 18, United States Code.

22 “(c) Any person seeking an exemption under section
23 312(b) of the Personal Data Privacy and Security Act of
24 2009 shall be immune from prosecution under this section
25 if the United States Secret Service does not indicate, in

1 writing, that such notice be given under section 312(b)(3)
 2 of such Act”.

3 (b) CONFORMING AND TECHNICAL AMENDMENTS.—

4 The table of sections for chapter 47 of title 18, United
 5 States Code, is amended by adding at the end the fol-
 6 lowing:

“1041. Concealment of security breaches involving personally identifiable infor-
 mation.”.

7 (c) ENFORCEMENT AUTHORITY.—

8 (1) IN GENERAL.—The United States Secret
 9 Service shall have the authority to investigate of-
 10 fenses under this section.

11 (2) NONEXCLUSIVITY.—The authority granted
 12 in paragraph (1) shall not be exclusive of any exist-
 13 ing authority held by any other Federal agency.

14 **SEC. 103. REVIEW AND AMENDMENT OF FEDERAL SEN-**
 15 **TENCING GUIDELINES RELATED TO FRAUDU-**
 16 **LENT ACCESS TO OR MISUSE OF DIGITIZED**
 17 **OR ELECTRONIC PERSONALLY IDENTIFIABLE**
 18 **INFORMATION.**

19 (a) REVIEW AND AMENDMENT.—The United States
 20 Sentencing Commission, pursuant to its authority under
 21 section 994 of title 28, United States Code, and in accord-
 22 ance with this section, shall review and, if appropriate,
 23 amend the Federal sentencing guidelines (including its
 24 policy statements) applicable to persons convicted of using

1 fraud to access, or misuse of, digitized or electronic per-
2 sonally identifiable information, including identity theft or
3 any offense under—

4 (1) sections 1028, 1028A, 1030, 1030A, 2511,
5 and 2701 of title 18, United States Code; and

6 (2) any other relevant provision.

7 (b) REQUIREMENTS.—In carrying out the require-
8 ments of this section, the United States Sentencing Com-
9 mission shall—

10 (1) ensure that the Federal sentencing guide-
11 lines (including its policy statements) reflect—

12 (A) the serious nature of the offenses and
13 penalties referred to in this Act;

14 (B) the growing incidences of theft and
15 misuse of digitized or electronic personally iden-
16 tifiable information, including identity theft;
17 and

18 (C) the need to deter, prevent, and punish
19 such offenses;

20 (2) consider the extent to which the Federal
21 sentencing guidelines (including its policy state-
22 ments) adequately address violations of the sections
23 amended by this Act to—

24 (A) sufficiently deter and punish such of-
25 fenses; and

1 (B) adequately reflect the enhanced pen-
2 alties established under this Act;

3 (3) maintain reasonable consistency with other
4 relevant directives and sentencing guidelines;

5 (4) account for any additional aggravating or
6 mitigating circumstances that might justify excep-
7 tions to the generally applicable sentencing ranges;

8 (5) consider whether to provide a sentencing en-
9 hancement for those convicted of the offenses de-
10 scribed in subsection (a), if the conduct involves—

11 (A) the online sale of fraudulently obtained
12 or stolen personally identifiable information;

13 (B) the sale of fraudulently obtained or
14 stolen personally identifiable information to an
15 individual who is engaged in terrorist activity or
16 aiding other individuals engaged in terrorist ac-
17 tivity; or

18 (C) the sale of fraudulently obtained or
19 stolen personally identifiable information to fi-
20 nance terrorist activity or other criminal activi-
21 ties;

22 (6) make any necessary conforming changes to
23 the Federal sentencing guidelines to ensure that
24 such guidelines (including its policy statements) as
25 described in subsection (a) are sufficiently stringent

1 to deter, and adequately reflect crimes related to
2 fraudulent access to, or misuse of, personally identi-
3 fiable information; and

4 (7) ensure that the Federal sentencing guide-
5 lines adequately meet the purposes of sentencing
6 under section 3553(a)(2) of title 18, United States
7 Code.

8 (c) EMERGENCY AUTHORITY TO SENTENCING COM-
9 MISSION.—The United States Sentencing Commission
10 may, as soon as practicable, promulgate amendments
11 under this section in accordance with procedures estab-
12 lished in section 21(a) of the Sentencing Act of 1987 (28
13 U.S.C. 994 note) as though the authority under that Act
14 had not expired.

15 **SEC. 104. EFFECTS OF IDENTITY THEFT ON BANKRUPTCY**
16 **PROCEEDINGS.**

17 (a) DEFINITIONS.—Section 101 of title 11, United
18 States Code, is amended—

19 (1) by redesignating paragraph (27B) as para-
20 graph (27D); and

21 (2) by inserting after paragraph (27A) the fol-
22 lowing:

23 “(27) The term ‘identity theft’ means a fraud
24 committed or attempted using the personally identi-
25 fiable information of another person.

1 “(28) The term ‘identity theft victim’ means a
2 debtor who, as a result of an identify theft in any
3 consecutive 12-month period during the 3-year pe-
4 riod before the date on which a petition is filed
5 under this title, had claims asserted against such
6 debtor in excess of the least of—

7 “(A) \$20,000;

8 “(B) 50 percent of all claims asserted
9 against such debtor; or

10 “(C) 25 percent of the debtor’s gross in-
11 come for such 12-month period.”.

12 (b) PROHIBITION.—Section 707(b) of title 11, United
13 States Code, is amended by adding at the end the fol-
14 lowing:

15 “(8) No judge, United States trustee (or bankruptcy
16 administrator, if any), trustee, or other party in interest
17 may file a motion under paragraph (2) if the debtor is
18 an identity theft victim.”.

19 **TITLE II—DATA BROKERS**

20 **SEC. 201. TRANSPARENCY AND ACCURACY OF DATA COL-** 21 **LECTION.**

22 (a) IN GENERAL.—Data brokers engaging in inter-
23 state commerce are subject to the requirements of this
24 title for any product or service offered to third parties that

1 allows access or use of sensitive personally identifiable in-
2 formation.

3 (b) LIMITATION.—Notwithstanding any other provi-
4 sion of this title, this section shall not apply to—

5 (1) any product or service offered by a data
6 broker engaging in interstate commerce where such
7 product or service is currently subject to, and in
8 compliance with, access and accuracy protections
9 similar to those under subsections (c) through (f) of
10 this section under the Fair Credit Reporting Act
11 (Public Law 91–508);

12 (2) any data broker that is subject to regulation
13 under the Gramm-Leach-Bliley Act (Public Law
14 106–102);

15 (3) any data broker currently subject to and in
16 compliance with the data security requirements for
17 such entities under the Health Insurance Portability
18 and Accountability Act (Public Law 104–191), and
19 its implementing regulations;

20 (4) information in a personal electronic record
21 that—

22 (A) the data broker has identified as inac-
23 curate, but maintains for the purpose of aiding
24 the data broker in preventing inaccurate infor-

1 mation from entering an individual's personal
2 electronic record; and

3 (B) is not maintained primarily for the
4 purpose of transmitting or otherwise providing
5 that information, or assessments based on that
6 information, to nonaffiliated third parties; and

7 (5) information concerning proprietary meth-
8 odologies, techniques, scores, or algorithms relating
9 to fraud prevention not normally provided to third
10 parties in the ordinary course of business.

11 (c) DISCLOSURES TO INDIVIDUALS.—

12 (1) IN GENERAL.—A data broker shall, upon
13 the request of an individual, disclose to such indi-
14 vidual for a reasonable fee all personal electronic
15 records pertaining to that individual maintained spe-
16 cifically for disclosure to third parties that request
17 information on that individual in the ordinary course
18 of business in the databases or systems of the data
19 broker at the time of such request.

20 (2) INFORMATION ON HOW TO CORRECT INAC-
21 CURACIES.—The disclosures required under para-
22 graph (1) shall also include guidance to individuals
23 on procedures for correcting inaccuracies.

24 (d) DISCLOSURE TO INDIVIDUALS OF ADVERSE AC-
25 TIONS TAKEN BY THIRD PARTIES.—

1 (1) IN GENERAL.—In addition to any other
2 rights established under this Act, if a person takes
3 any adverse action with respect to any individual
4 that is based, in whole or in part, on any informa-
5 tion contained in a personal electronic record that is
6 maintained, updated, or otherwise owned or pos-
7 sessed by a data broker, such person, at no cost to
8 the affected individual, shall provide—

9 (A) written or electronic notice of the ad-
10 verse action to the individual;

11 (B) to the individual, in writing or elec-
12 tronically, the name, address, and telephone
13 number of the data broker that furnished the
14 information to the person;

15 (C) a copy of the information such person
16 obtained from the data broker; and

17 (D) information to the individual on the
18 procedures for correcting any inaccuracies in
19 such information.

20 (2) ACCEPTED METHODS OF NOTICE.—A per-
21 son shall be in compliance with the notice require-
22 ments under paragraph (1) if such person provides
23 written or electronic notice in the same manner and
24 using the same methods as are required under sec-
25 tion 313(1) of this Act.

1 (e) ACCURACY RESOLUTION PROCESS.—

2 (1) INFORMATION FROM A PUBLIC RECORD OR
3 LICENSOR.—

4 (A) IN GENERAL.—If an individual notifies
5 a data broker of a dispute as to the complete-
6 ness or accuracy of information disclosed to
7 such individual under subsection (c) that is ob-
8 tained from a public record source or a license
9 agreement, such data broker shall determine
10 within 30 days whether the information in its
11 system accurately and completely records the
12 information available from the licensor or public
13 record source.

14 (B) DATA BROKER ACTIONS.—If a data
15 broker determines under subparagraph (A) that
16 the information in its systems does not accu-
17 rately and completely record the information
18 available from a public record source or licen-
19 sor, the data broker shall—

20 (i) correct any inaccuracies or incom-
21 pleteness, and provide to such individual
22 written notice of such changes; and

23 (ii) provide such individual with the
24 contact information of the public record or
25 licensor.

1 (2) INFORMATION NOT FROM A PUBLIC RECORD
2 SOURCE OR LICENSOR.—If an individual notifies a
3 data broker of a dispute as to the completeness or
4 accuracy of information not from a public record or
5 licensor that was disclosed to the individual under
6 subsection (c), the data broker shall, within 30 days
7 of receiving notice of such dispute—

8 (A) review and consider free of charge any
9 information submitted by such individual that is
10 relevant to the completeness or accuracy of the
11 disputed information; and

12 (B) correct any information found to be in-
13 complete or inaccurate and provide notice to
14 such individual of whether and what informa-
15 tion was corrected, if any.

16 (3) EXTENSION OF REVIEW PERIOD.—The 30-
17 day period described in paragraph (1) may be ex-
18 tended for not more than 30 additional days if a
19 data broker receives information from the individual
20 during the initial 30-day period that is relevant to
21 the completeness or accuracy of any disputed infor-
22 mation.

23 (4) NOTICE IDENTIFYING THE DATA FUR-
24 NISHER.—If the completeness or accuracy of any in-
25 formation not from a public record source or licensor

1 that was disclosed to an individual under subsection
2 (c) is disputed by such individual, the data broker
3 shall provide, upon the request of such individual,
4 the contact information of any data furnisher that
5 provided the disputed information.

6 (5) DETERMINATION THAT DISPUTE IS FRIVO-
7 LOUS OR IRRELEVANT.—

8 (A) IN GENERAL.—Notwithstanding para-
9 graphs (1) through (3), a data broker may de-
10 cline to investigate or terminate a review of in-
11 formation disputed by an individual under those
12 paragraphs if the data broker reasonably deter-
13 mines that the dispute by the individual is friv-
14 olous or intended to perpetrate fraud.

15 (B) NOTICE.—A data broker shall notify
16 an individual of a determination under subpara-
17 graph (A) within a reasonable time by any
18 means available to such data broker.

19 **SEC. 202. ENFORCEMENT.**

20 (a) CIVIL PENALTIES.—

21 (1) PENALTIES.—Any data broker that violates
22 the provisions of section 201 shall be subject to civil
23 penalties of not more than \$1,000 per violation per
24 day while such violations persist, up to a maximum
25 of \$250,000 per violation.

1 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
2 data broker that intentionally or willfully violates the
3 provisions of section 201 shall be subject to addi-
4 tional penalties in the amount of \$1,000 per viola-
5 tion per day, to a maximum of an additional
6 \$250,000 per violation, while such violations persist.

7 (3) EQUITABLE RELIEF.—A data broker en-
8 gaged in interstate commerce that violates this sec-
9 tion may be enjoined from further violations by a
10 court of competent jurisdiction.

11 (4) OTHER RIGHTS AND REMEDIES.—The
12 rights and remedies available under this subsection
13 are cumulative and shall not affect any other rights
14 and remedies available under law.

15 (b) FEDERAL TRADE COMMISSION AUTHORITY.—
16 Any data broker shall have the provisions of this title en-
17 forced against it by the Federal Trade Commission.

18 (c) STATE ENFORCEMENT.—

19 (1) CIVIL ACTIONS.—In any case in which the
20 attorney general of a State or any State or local law
21 enforcement agency authorized by the State attorney
22 general or by State statute to prosecute violations of
23 consumer protection law, has reason to believe that
24 an interest of the residents of that State has been
25 or is threatened or adversely affected by the acts or

1 practices of a data broker that violate this title, the
2 State may bring a civil action on behalf of the resi-
3 dents of that State in a district court of the United
4 States of appropriate jurisdiction, or any other court
5 of competent jurisdiction, to—

6 (A) enjoin that act or practice;

7 (B) enforce compliance with this title; or

8 (C) obtain civil penalties of not more than
9 \$1,000 per violation per day while such viola-
10 tions persist, up to a maximum of \$250,000 per
11 violation.

12 (2) NOTICE.—

13 (A) IN GENERAL.—Before filing an action
14 under this subsection, the attorney general of
15 the State involved shall provide to the Federal
16 Trade Commission—

17 (i) a written notice of that action; and

18 (ii) a copy of the complaint for that
19 action.

20 (B) EXCEPTION.—Subparagraph (A) shall
21 not apply with respect to the filing of an action
22 by an attorney general of a State under this
23 subsection, if the attorney general of a State
24 determines that it is not feasible to provide the

1 notice described in subparagraph (A) before the
2 filing of the action.

3 (C) NOTIFICATION WHEN PRACTICABLE.—

4 In an action described under subparagraph (B),
5 the attorney general of a State shall provide the
6 written notice and the copy of the complaint to
7 the Federal Trade Commission as soon after
8 the filing of the complaint as practicable.

9 (3) FEDERAL TRADE COMMISSION AUTHOR-
10 ITY.—Upon receiving notice under paragraph (2),
11 the Federal Trade Commission shall have the right
12 to—

13 (A) move to stay the action, pending the
14 final disposition of a pending Federal pro-
15 ceeding or action as described in paragraph (4);

16 (B) intervene in an action brought under
17 paragraph (1); and

18 (C) file petitions for appeal.

19 (4) PENDING PROCEEDINGS.—If the Federal
20 Trade Commission has instituted a proceeding or
21 civil action for a violation of this title, no attorney
22 general of a State may, during the pendency of such
23 proceeding or civil action, bring an action under this
24 subsection against any defendant named in such civil

1 action for any violation that is alleged in that civil
2 action.

3 (5) RULE OF CONSTRUCTION.—For purposes of
4 bringing any civil action under paragraph (1), noth-
5 ing in this title shall be construed to prevent an at-
6 torney general of a State from exercising the powers
7 conferred on the attorney general by the laws of that
8 State to—

9 (A) conduct investigations;

10 (B) administer oaths and affirmations; or

11 (C) compel the attendance of witnesses or
12 the production of documentary and other evi-
13 dence.

14 (6) VENUE; SERVICE OF PROCESS.—

15 (A) VENUE.—Any action brought under
16 this subsection may be brought in the district
17 court of the United States that meets applicable
18 requirements relating to venue under section
19 1391 of title 28, United States Code.

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

23 (i) is an inhabitant; or

24 (ii) may be found.

1 (d) NO PRIVATE CAUSE OF ACTION.—Nothing in
 2 this title establishes a private cause of action against a
 3 data broker for violation of any provision of this title.

4 **SEC. 203. RELATION TO STATE LAWS.**

5 No requirement or prohibition may be imposed under
 6 the laws of any State with respect to any subject matter
 7 regulated under section 201, relating to individual access
 8 to, and correction of, personal electronic records held by
 9 data brokers.

10 **SEC. 204. EFFECTIVE DATE.**

11 This title shall take effect 180 days after the date
 12 of enactment of this Act.

13 **TITLE III—PRIVACY AND SECU-**
 14 **RITY OF PERSONALLY IDEN-**
 15 **TIFIABLE INFORMATION**

16 **Subtitle A—A Data Privacy and**
 17 **Security Program**

18 **SEC. 301. PURPOSE AND APPLICABILITY OF DATA PRIVACY**
 19 **AND SECURITY PROGRAM.**

20 (a) PURPOSE.—The purpose of this subtitle is to en-
 21 sure standards for developing and implementing adminis-
 22 trative, technical, and physical safeguards to protect the
 23 security of sensitive personally identifiable information.

24 (b) IN GENERAL.—A business entity engaging in
 25 interstate commerce that involves collecting, accessing,

1 transmitting, using, storing, or disposing of sensitive per-
2 sonally identifiable information in electronic or digital
3 form on 10,000 or more United States persons is subject
4 to the requirements for a data privacy and security pro-
5 gram under section 302 for protecting sensitive personally
6 identifiable information.

7 (c) LIMITATIONS.—Notwithstanding any other obli-
8 gation under this subtitle, this subtitle does not apply to:

9 (1) FINANCIAL INSTITUTIONS.—Financial insti-
10 tutions—

11 (A) subject to the data security require-
12 ments and implementing regulations under the
13 Gramm-Leach-Bliley Act (15 U.S.C. 6801 et
14 seq.); and

15 (B) subject to—

16 (i) examinations for compliance with
17 the requirements of this Act by a Federal
18 Functional Regulator or State Insurance
19 Authority (as those terms are defined in
20 section 509 of the Gramm-Leach-Bliley
21 Act (15 U.S.C. 6809)); or

22 (ii) compliance with part 314 of title
23 16, Code of Federal Regulations.

24 (2) HIPPA REGULATED ENTITIES.—

1 (A) COVERED ENTITIES.—Covered entities
2 subject to the Health Insurance Portability and
3 Accountability Act of 1996 (42 U.S.C. 1301 et
4 seq.), including the data security requirements
5 and implementing regulations of that Act.

6 (B) BUSINESS ENTITIES.—A business enti-
7 ty shall be deemed in compliance with the pri-
8 vacy and security program requirements under
9 section 302 if the business entity is acting as
10 a “business associate” as that term is defined
11 in the Health Insurance Portability and Ac-
12 countability Act of 1996 (42 U.S.C. 1301 et
13 seq.) and is in compliance with requirements
14 imposed under that Act and its implementing
15 regulations.

16 (3) PUBLIC RECORDS.—Public records not oth-
17 erwise subject to a confidentiality or nondisclosure
18 requirement, or information obtained from a news
19 report or periodical.

20 (d) SAFE HARBORS.—

21 (1) IN GENERAL.—A business entity shall be
22 deemed in compliance with the privacy and security
23 program requirements under section 302 if the busi-
24 ness entity complies with or provides protection
25 equal to industry standards, as identified by the

1 Federal Trade Commission, that are applicable to
2 the type of sensitive personally identifiable informa-
3 tion involved in the ordinary course of business of
4 such business entity.

5 (2) LIMITATION.—Nothing in this subsection
6 shall be construed to permit, and nothing does per-
7 mit, the Federal Trade Commission to issue regula-
8 tions requiring, or according greater legal status to,
9 the implementation of or application of a specific
10 technology or technological specifications for meeting
11 the requirements of this title.

12 **SEC. 302. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**
13 **AND SECURITY PROGRAM.**

14 (a) PERSONAL DATA PRIVACY AND SECURITY PRO-
15 GRAM.—A business entity subject to this subtitle shall
16 comply with the following safeguards and any other ad-
17 ministrative, technical, or physical safeguards identified by
18 the Federal Trade Commission in a rulemaking process
19 pursuant to section 553 of title 5, United States Code,
20 for the protection of sensitive personally identifiable infor-
21 mation:

22 (1) SCOPE.—A business entity shall implement
23 a comprehensive personal data privacy and security
24 program that includes administrative, technical, and
25 physical safeguards appropriate to the size and com-

1 plexity of the business entity and the nature and
2 scope of its activities.

3 (2) DESIGN.—The personal data privacy and
4 security program shall be designed to—

5 (A) ensure the privacy, security, and con-
6 fidentiality of sensitive personally identifying in-
7 formation;

8 (B) protect against any anticipated
9 vulnerabilities to the privacy, security, or integ-
10 rity of sensitive personally identifying informa-
11 tion; and

12 (C) protect against unauthorized access to
13 use of sensitive personally identifying informa-
14 tion that could result in substantial harm or in-
15 convenience to any individual.

16 (3) RISK ASSESSMENT.—A business entity
17 shall—

18 (A) identify reasonably foreseeable internal
19 and external vulnerabilities that could result in
20 unauthorized access, disclosure, use, or alter-
21 ation of sensitive personally identifiable infor-
22 mation or systems containing sensitive person-
23 ally identifiable information;

24 (B) assess the likelihood of and potential
25 damage from unauthorized access, disclosure,

1 use, or alteration of sensitive personally identifi-
2 able information;

3 (C) assess the sufficiency of its policies,
4 technologies, and safeguards in place to control
5 and minimize risks from unauthorized access,
6 disclosure, use, or alteration of sensitive person-
7 ally identifiable information; and

8 (D) assess the vulnerability of sensitive
9 personally identifiable information during de-
10 struction and disposal of such information, in-
11 cluding through the disposal or retirement of
12 hardware.

13 (4) RISK MANAGEMENT AND CONTROL.—Each
14 business entity shall—

15 (A) design its personal data privacy and
16 security program to control the risks identified
17 under paragraph (3); and

18 (B) adopt measures commensurate with
19 the sensitivity of the data as well as the size,
20 complexity, and scope of the activities of the
21 business entity that—

22 (i) control access to systems and fa-
23 cilities containing sensitive personally iden-
24 tifiable information, including controls to

1 authenticate and permit access only to au-
2 thorized individuals;

3 (ii) detect actual and attempted
4 fraudulent, unlawful, or unauthorized ac-
5 cess, disclosure, use, or alteration of sen-
6 sitive personally identifiable information,
7 including by employees and other individ-
8 uals otherwise authorized to have access;

9 (iii) protect sensitive personally identi-
10 fiable information during use, trans-
11 mission, storage, and disposal by
12 encryption, redaction, or access controls
13 that are widely accepted as an effective in-
14 dustry practice or industry standard, or
15 other reasonable means (including as di-
16 rected for disposal of records under section
17 628 of the Fair Credit Reporting Act (15
18 U.S.C. 1681w) and the implementing regu-
19 lations of such Act as set forth in section
20 682 of title 16, Code of Federal Regula-
21 tions);

22 (iv) ensure that sensitive personally
23 identifiable information is properly de-
24 stroyed and disposed of, including during
25 the destruction of computers, diskettes,

1 and other electronic media that contain
2 sensitive personally identifiable informa-
3 tion;

4 (v) trace access to records containing
5 sensitive personally identifiable information
6 so that the business entity can determine
7 who accessed or acquired such sensitive
8 personally identifiable information per-
9 taining to specific individuals; and

10 (vi) ensure that no third party or cus-
11 tomer of the business entity is authorized
12 to access or acquire sensitive personally
13 identifiable information without the busi-
14 ness entity first performing sufficient due
15 diligence to ascertain, with reasonable cer-
16 tainty, that such information is being
17 sought for a valid legal purpose.

18 (b) TRAINING.—Each business entity subject to this
19 subtitle shall take steps to ensure employee training and
20 supervision for implementation of the data security pro-
21 gram of the business entity.

22 (c) VULNERABILITY TESTING.—

23 (1) IN GENERAL.—Each business entity subject
24 to this subtitle shall take steps to ensure regular
25 testing of key controls, systems, and procedures of

1 the personal data privacy and security program to
2 detect, prevent, and respond to attacks or intrusions,
3 or other system failures.

4 (2) FREQUENCY.—The frequency and nature of
5 the tests required under paragraph (1) shall be de-
6 termined by the risk assessment of the business enti-
7 ty under subsection (a)(3).

8 (d) RELATIONSHIP TO SERVICE PROVIDERS.—In the
9 event a business entity subject to this subtitle engages
10 service providers not subject to this subtitle, such business
11 entity shall—

12 (1) exercise appropriate due diligence in select-
13 ing those service providers for responsibilities related
14 to sensitive personally identifiable information, and
15 take reasonable steps to select and retain service
16 providers that are capable of maintaining appro-
17 priate safeguards for the security, privacy, and in-
18 tegrity of the sensitive personally identifiable infor-
19 mation at issue; and

20 (2) require those service providers by contract
21 to implement and maintain appropriate measures de-
22 signed to meet the objectives and requirements gov-
23 erning entities subject to section 301, this section,
24 and subtitle B.

1 (e) PERIODIC ASSESSMENT AND PERSONAL DATA
2 PRIVACY AND SECURITY MODERNIZATION.—Each busi-
3 ness entity subject to this subtitle shall on a regular basis
4 monitor, evaluate, and adjust, as appropriate its data pri-
5 vacy and security program in light of any relevant changes
6 in—

7 (1) technology;

8 (2) the sensitivity of personally identifiable in-
9 formation;

10 (3) internal or external threats to personally
11 identifiable information; and

12 (4) the changing business arrangements of the
13 business entity, such as—

14 (A) mergers and acquisitions;

15 (B) alliances and joint ventures;

16 (C) outsourcing arrangements;

17 (D) bankruptcy; and

18 (E) changes to sensitive personally identifi-
19 able information systems.

20 (f) IMPLEMENTATION TIMELINE.—Not later than 1
21 year after the date of enactment of this Act, a business
22 entity subject to the provisions of this subtitle shall imple-
23 ment a data privacy and security program pursuant to this
24 subtitle.

1 **SEC. 303. ENFORCEMENT.**

2 (a) CIVIL PENALTIES.—

3 (1) IN GENERAL.—Any business entity that vio-
4 lates the provisions of sections 301 or 302 shall be
5 subject to civil penalties of not more than \$5,000
6 per violation per day while such a violation exists,
7 with a maximum of \$500,000 per violation.

8 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
9 business entity that intentionally or willfully violates
10 the provisions of sections 301 or 302 shall be subject
11 to additional penalties in the amount of \$5,000 per
12 violation per day while such a violation exists, with
13 a maximum of an additional \$500,000 per violation.

14 (3) EQUITABLE RELIEF.—A business entity en-
15 gaged in interstate commerce that violates this sec-
16 tion may be enjoined from further violations by a
17 court of competent jurisdiction.

18 (4) OTHER RIGHTS AND REMEDIES.—The
19 rights and remedies available under this section are
20 cumulative and shall not affect any other rights and
21 remedies available under law.

22 (b) FEDERAL TRADE COMMISSION AUTHORITY.—
23 Any data broker shall have the provisions of this subtitle
24 enforced against it by the Federal Trade Commission.

25 (c) STATE ENFORCEMENT.—

1 (1) CIVIL ACTIONS.—In any case in which the
2 attorney general of a State or any State or local law
3 enforcement agency authorized by the State attorney
4 general or by State statute to prosecute violations of
5 consumer protection law, has reason to believe that
6 an interest of the residents of that State has been
7 or is threatened or adversely affected by the acts or
8 practices of a data broker that violate this subtitle,
9 the State may bring a civil action on behalf of the
10 residents of that State in a district court of the
11 United States of appropriate jurisdiction, or any
12 other court of competent jurisdiction, to—

13 (A) enjoin that act or practice;

14 (B) enforce compliance with this subtitle;

15 or

16 (C) obtain civil penalties of not more than
17 \$5,000 per violation per day while such viola-
18 tions persist, up to a maximum of \$500,000 per
19 violation.

20 (2) NOTICE.—

21 (A) IN GENERAL.—Before filing an action
22 under this subsection, the attorney general of
23 the State involved shall provide to the Federal
24 Trade Commission—

25 (i) a written notice of that action; and

1 (ii) a copy of the complaint for that
2 action.

3 (B) EXCEPTION.—Subparagraph (A) shall
4 not apply with respect to the filing of an action
5 by an attorney general of a State under this
6 subsection, if the attorney general of a State
7 determines that it is not feasible to provide the
8 notice described in this subparagraph before the
9 filing of the action.

10 (C) NOTIFICATION WHEN PRACTICABLE.—
11 In an action described under subparagraph (B),
12 the attorney general of a State shall provide the
13 written notice and the copy of the complaint to
14 the Federal Trade Commission as soon after
15 the filing of the complaint as practicable.

16 (3) FEDERAL TRADE COMMISSION AUTHOR-
17 ITY.—Upon receiving notice under paragraph (2),
18 the Federal Trade Commission shall have the right
19 to—

20 (A) move to stay the action, pending the
21 final disposition of a pending Federal pro-
22 ceeding or action as described in paragraph (4);

23 (B) intervene in an action brought under
24 paragraph (1); and

25 (C) file petitions for appeal.

1 (4) PENDING PROCEEDINGS.—If the Federal
2 Trade Commission has instituted a proceeding or ac-
3 tion for a violation of this subtitle or any regulations
4 thereunder, no attorney general of a State may, dur-
5 ing the pendency of such proceeding or action, bring
6 an action under this subsection against any defend-
7 ant named in such criminal proceeding or civil ac-
8 tion for any violation that is alleged in that pro-
9 ceeding or action.

10 (5) RULE OF CONSTRUCTION.—For purposes of
11 bringing any civil action under paragraph (1) noth-
12 ing in this subtitle shall be construed to prevent an
13 attorney general of a State from exercising the pow-
14 ers conferred on the attorney general by the laws of
15 that State to—

16 (A) conduct investigations;

17 (B) administer oaths and affirmations; or

18 (C) compel the attendance of witnesses or
19 the production of documentary and other evi-
20 dence.

21 (6) VENUE; SERVICE OF PROCESS.—

22 (A) VENUE.—Any action brought under
23 this subsection may be brought in the district
24 court of the United States that meets applicable

1 requirements relating to venue under section
2 1391 of title 28, United States Code.

3 (B) SERVICE OF PROCESS.—In an action
4 brought under this subsection, process may be
5 served in any district in which the defendant—

6 (i) is an inhabitant; or

7 (ii) may be found.

8 (d) NO PRIVATE CAUSE OF ACTION.—Nothing in
9 this subtitle establishes a private cause of action against
10 a business entity for violation of any provision of this sub-
11 title.

12 **SEC. 304. RELATION TO OTHER LAWS.**

13 (a) IN GENERAL.—No State may require any busi-
14 ness entity subject to this subtitle to comply with any re-
15 quirements with respect to administrative, technical, and
16 physical safeguards for the protection of sensitive person-
17 ally identifying information.

18 (b) LIMITATIONS.—Nothing in this subtitle shall be
19 construed to modify, limit, or supersede the operation of
20 the Gramm-Leach-Bliley Act or its implementing regula-
21 tions, including those adopted or enforced by States.

1 **Subtitle B—Security Breach** 2 **Notification**

3 **SEC. 311. NOTICE TO INDIVIDUALS.**

4 (a) IN GENERAL.—Any agency, or business entity en-
5 gaged in interstate commerce, that uses, accesses, trans-
6 mits, stores, disposes of or collects sensitive personally
7 identifiable information shall, following the discovery of a
8 security breach of such information, notify any resident
9 of the United States whose sensitive personally identifiable
10 information has been, or is reasonably believed to have
11 been, accessed, or acquired.

12 (b) OBLIGATION OF OWNER OR LICENSEE.—

13 (1) NOTICE TO OWNER OR LICENSEE.—Any
14 agency, or business entity engaged in interstate com-
15 merce, that uses, accesses, transmits, stores, dis-
16 poses of, or collects sensitive personally identifiable
17 information that the agency or business entity does
18 not own or license shall notify the owner or licensee
19 of the information following the discovery of a secu-
20 rity breach involving such information.

21 (2) NOTICE BY OWNER, LICENSEE OR OTHER
22 DESIGNATED THIRD PARTY.—Nothing in this sub-
23 title shall prevent or abrogate an agreement between
24 an agency or business entity required to give notice
25 under this section and a designated third party, in-

1 including an owner or licensee of the sensitive person-
2 ally identifiable information subject to the security
3 breach, to provide the notifications required under
4 subsection (a).

5 (3) BUSINESS ENTITY RELIEVED FROM GIVING
6 NOTICE.—A business entity obligated to give notice
7 under subsection (a) shall be relieved of such obliga-
8 tion if an owner or licensee of the sensitive person-
9 ally identifiable information subject to the security
10 breach, or other designated third party, provides
11 such notification.

12 (c) TIMELINESS OF NOTIFICATION.—

13 (1) IN GENERAL.—All notifications required
14 under this section shall be made without unreason-
15 able delay following the discovery by the agency or
16 business entity of a security breach.

17 (2) REASONABLE DELAY.—Reasonable delay
18 under this subsection may include any time nec-
19 essary to determine the scope of the security breach,
20 prevent further disclosures, and restore the reason-
21 able integrity of the data system and provide notice
22 to law enforcement when required.

23 (3) BURDEN OF PROOF.—The agency, business
24 entity, owner, or licensee required to provide notifi-
25 cation under this section shall have the burden of

1 demonstrating that all notifications were made as re-
2 quired under this subtitle, including evidence dem-
3 onstrating the reasons for any delay.

4 (d) DELAY OF NOTIFICATION AUTHORIZED FOR LAW
5 ENFORCEMENT PURPOSES.—

6 (1) IN GENERAL.—If a Federal law enforce-
7 ment agency determines that the notification re-
8 quired under this section would impede a criminal
9 investigation, such notification shall be delayed upon
10 written notice from such Federal law enforcement
11 agency to the agency or business entity that experi-
12 enced the breach.

13 (2) EXTENDED DELAY OF NOTIFICATION.—If
14 the notification required under subsection (a) is de-
15 layed pursuant to paragraph (1), an agency or busi-
16 ness entity shall give notice 30 days after the day
17 such law enforcement delay was invoked unless a
18 Federal law enforcement agency provides written no-
19 tification that further delay is necessary.

20 (3) LAW ENFORCEMENT IMMUNITY.—No cause
21 of action shall lie in any court against any law en-
22 forcement agency for acts relating to the delay of
23 notification for law enforcement purposes under this
24 subtitle.

1 **SEC. 312. EXEMPTIONS.**

2 (a) EXEMPTION FOR NATIONAL SECURITY AND LAW
3 ENFORCEMENT.—

4 (1) IN GENERAL.—Section 311 shall not apply
5 to an agency or business entity if the agency or busi-
6 ness entity certifies, in writing, that notification of
7 the security breach as required by section 311 rea-
8 sonably could be expected to—

9 (A) cause damage to the national security;

10 or

11 (B) hinder a law enforcement investigation
12 or the ability of the agency to conduct law en-
13 forcement investigations.

14 (2) LIMITS ON CERTIFICATIONS.—An agency or
15 business entity may not execute a certification under
16 paragraph (1) to—

17 (A) conceal violations of law, inefficiency,
18 or administrative error;

19 (B) prevent embarrassment to a business
20 entity, organization, or agency; or

21 (C) restrain competition.

22 (3) NOTICE.—In every case in which an agency
23 or business agency issues a certification under para-
24 graph (1), the certification, accompanied by a de-
25 scription of the factual basis for the certification,

1 shall be immediately provided to the United States
2 Secret Service.

3 (4) SECRET SERVICE REVIEW OF CERTIFI-
4 CATIONS.—

5 (A) IN GENERAL.—The United States Se-
6 cret Service may review a certification provided
7 by an agency under paragraph (3), and shall re-
8 view a certification provided by a business enti-
9 ty under paragraph (3), to determine whether
10 an exemption under paragraph (1) is merited.
11 Such review shall be completed not later than
12 10 business days after the date of receipt of the
13 certification, except as provided in paragraph
14 (5)(C).

15 (B) NOTICE.—Upon completing a review
16 under subparagraph (A) the United States Se-
17 cret Service shall immediately notify the agency
18 or business entity, in writing, of its determina-
19 tion of whether an exemption under paragraph
20 (1) is merited.

21 (C) EXEMPTION.—The exemption under
22 paragraph (1) shall not apply if the United
23 States Secret Service determines under this
24 paragraph that the exemption is not merited.

1 (5) ADDITIONAL AUTHORITY OF THE SECRET
2 SERVICE.—

3 (A) IN GENERAL.—In determining under
4 paragraph (4) whether an exemption under
5 paragraph (1) is merited, the United States Se-
6 cret Service may request additional information
7 from the agency or business entity regarding
8 the basis for the claimed exemption, if such ad-
9 ditional information is necessary to determine
10 whether the exemption is merited.

11 (B) REQUIRED COMPLIANCE.—Any agency
12 or business entity that receives a request for
13 additional information under subparagraph (A)
14 shall cooperate with any such request.

15 (C) TIMING.—If the United States Secret
16 Service requests additional information under
17 subparagraph (A), the United States Secret
18 Service shall notify the agency or business enti-
19 ty not later than 10 business days after the
20 date of receipt of the additional information
21 whether an exemption under paragraph (1) is
22 merited.

23 (b) SAFE HARBOR.—An agency or business entity
24 will be exempt from the notice requirements under section
25 311, if—

1 (1) a risk assessment concludes that—

2 (A) there is no significant risk that a secu-
3 rity breach has resulted in, or will result in,
4 harm to the individuals whose sensitive person-
5 ally identifiable information was subject to the
6 security breach, with the encryption of such in-
7 formation establishing a presumption that no
8 significant risk exists; or

9 (B) there is no significant risk that a secu-
10 rity breach has resulted in, or will result in,
11 harm to the individuals whose sensitive person-
12 ally identifiable information was subject to the
13 security breach, with the rendering of such sen-
14 sitive personally identifiable information indeci-
15 pherable through the use of best practices or
16 methods, such as redaction, access controls, or
17 other such mechanisms, which are widely ac-
18 cepted as an effective industry practice, or an
19 effective industry standard, establishing a pre-
20 sumption that no significant risk exists;

21 (2) without unreasonable delay, but not later
22 than 45 days after the discovery of a security
23 breach, unless extended by the United States Secret
24 Service, the agency or business entity notifies the
25 United States Secret Service, in writing, of—

1 (A) the results of the risk assessment; and

2 (B) its decision to invoke the risk assess-
3 ment exemption; and

4 (3) the United States Secret Service does not
5 indicate, in writing, within 10 business days from re-
6 ceipt of the decision, that notice should be given.

7 (c) FINANCIAL FRAUD PREVENTION EXEMPTION.—

8 (1) IN GENERAL.—A business entity will be ex-
9 empt from the notice requirement under section 311
10 if the business entity utilizes or participates in a se-
11 curity program that—

12 (A) is designed to block the use of the sen-
13 sitive personally identifiable information to ini-
14 tiate unauthorized financial transactions before
15 they are charged to the account of the indi-
16 vidual; and

17 (B) provides for notice to affected individ-
18 uals after a security breach that has resulted in
19 fraud or unauthorized transactions.

20 (2) LIMITATION.—The exemption by this sub-
21 section does not apply if—

22 (A) the information subject to the security
23 breach includes sensitive personally identifiable
24 information, other than a credit card or credit
25 card security code, of any type of the sensitive

1 personally identifiable information identified in
2 section 3; or

3 (B) the security breach includes both the
4 individual's credit card number and the individ-
5 ual's first and last name.

6 **SEC. 313. METHODS OF NOTICE.**

7 An agency or business entity shall be in compliance
8 with section 311 if it provides both:

9 (1) **INDIVIDUAL NOTICE.**—Notice to individuals
10 by 1 of the following means:

11 (A) Written notification to the last known
12 home mailing address of the individual in the
13 records of the agency or business entity.

14 (B) Telephone notice to the individual per-
15 sonally.

16 (C) E-mail notice, if the individual has
17 consented to receive such notice and the notice
18 is consistent with the provisions permitting elec-
19 tronic transmission of notices under section 101
20 of the Electronic Signatures in Global and Na-
21 tional Commerce Act (15 U.S.C. 7001).

22 (2) **MEDIA NOTICE.**—Notice to major media
23 outlets serving a State or jurisdiction, if the number
24 of residents of such State whose sensitive personally
25 identifiable information was, or is reasonably be-

1 lieved to have been, acquired by an unauthorized
2 person exceeds 5,000.

3 **SEC. 314. CONTENT OF NOTIFICATION.**

4 (a) IN GENERAL.—Regardless of the method by
5 which notice is provided to individuals under section 313,
6 such notice shall include, to the extent possible—

7 (1) a description of the categories of sensitive
8 personally identifiable information that was, or is
9 reasonably believed to have been, acquired by an un-
10 authorized person;

11 (2) a toll-free number—

12 (A) that the individual may use to contact
13 the agency or business entity, or the agent of
14 the agency or business entity; and

15 (B) from which the individual may learn
16 what types of sensitive personally identifiable
17 information the agency or business entity main-
18 tained about that individual; and

19 (3) the toll-free contact telephone numbers and
20 addresses for the major credit reporting agencies.

21 (b) ADDITIONAL CONTENT.—Notwithstanding sec-
22 tion 319, a State may require that a notice under sub-
23 section (a) shall also include information regarding victim
24 protection assistance provided for by that State.

1 **SEC. 315. COORDINATION OF NOTIFICATION WITH CREDIT**
2 **REPORTING AGENCIES.**

3 If an agency or business entity is required to provide
4 notification to more than 5,000 individuals under section
5 311(a), the agency or business entity shall also notify all
6 consumer reporting agencies that compile and maintain
7 files on consumers on a nationwide basis (as defined in
8 section 603(p) of the Fair Credit Reporting Act (15
9 U.S.C. 1681a(p)) of the timing and distribution of the no-
10 tices. Such notice shall be given to the consumer credit
11 reporting agencies without unreasonable delay and, if it
12 will not delay notice to the affected individuals, prior to
13 the distribution of notices to the affected individuals.

14 **SEC. 316. NOTICE TO LAW ENFORCEMENT.**

15 (a) SECRET SERVICE.—Any business entity or agen-
16 cy shall notify the United States Secret Service of the fact
17 that a security breach has occurred if—

18 (1) the number of individuals whose sensitive
19 personally identifying information was, or is reason-
20 ably believed to have been acquired by an unauthor-
21 ized person exceeds 10,000;

22 (2) the security breach involves a database,
23 networked or integrated databases, or other data
24 system containing the sensitive personally identifi-
25 able information of more than 1,000,000 individuals
26 nationwide;

1 (3) the security breach involves databases
2 owned by the Federal Government; or

3 (4) the security breach involves primarily sen-
4 sitive personally identifiable information of individ-
5 uals known to the agency or business entity to be
6 employees and contractors of the Federal Govern-
7 ment involved in national security or law enforce-
8 ment.

9 (b) NOTICE TO OTHER LAW ENFORCEMENT AGEN-
10 CIES.—The United States Secret Service shall be respon-
11 sible for notifying—

12 (1) the Federal Bureau of Investigation, if the
13 security breach involves espionage, foreign counter-
14 intelligence, information protected against unauthor-
15 ized disclosure for reasons of national defense or for-
16 eign relations, or Restricted Data (as that term is
17 defined in section 11y of the Atomic Energy Act of
18 1954 (42 U.S.C. 2014(y)), except for offenses af-
19 fecting the duties of the United States Secret Serv-
20 ice under section 3056(a) of title 18, United States
21 Code;

22 (2) the United States Postal Inspection Service,
23 if the security breach involves mail fraud; and

24 (3) the attorney general of each State affected
25 by the security breach.

1 (c) TIMING OF NOTICES.—The notices required
2 under this section shall be delivered as follows:

3 (1) Notice under subsection (a) shall be deliv-
4 ered as promptly as possible, but not later than 14
5 days after discovery of the events requiring notice.

6 (2) Notice under subsection (b) shall be deliv-
7 ered not later than 14 days after the Service receives
8 notice of a security breach from an agency or busi-
9 ness entity.

10 **SEC. 317. ENFORCEMENT.**

11 (a) CIVIL ACTIONS BY THE ATTORNEY GENERAL.—
12 The Attorney General may bring a civil action in the ap-
13 propriate United States district court against any business
14 entity that engages in conduct constituting a violation of
15 this subtitle and, upon proof of such conduct by a prepon-
16 derance of the evidence, such business entity shall be sub-
17 ject to a civil penalty of not more than \$1,000 per day
18 per individual whose sensitive personally identifiable infor-
19 mation was, or is reasonably believed to have been,
20 accessed or acquired by an unauthorized person, up to a
21 maximum of \$1,000,000 per violation, unless such conduct
22 is found to be willful or intentional.

23 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
24 ERAL.—

1 (1) IN GENERAL.—If it appears that a business
2 entity has engaged, or is engaged, in any act or
3 practice constituting a violation of this subtitle, the
4 Attorney General may petition an appropriate dis-
5 trict court of the United States for an order—

6 (A) enjoining such act or practice; or

7 (B) enforcing compliance with this subtitle.

8 (2) ISSUANCE OF ORDER.—A court may issue
9 an order under paragraph (1), if the court finds that
10 the conduct in question constitutes a violation of this
11 subtitle.

12 (c) OTHER RIGHTS AND REMEDIES.—The rights and
13 remedies available under this subtitle are cumulative and
14 shall not affect any other rights and remedies available
15 under law.

16 (d) FRAUD ALERT.—Section 605A(b)(1) of the Fair
17 Credit Reporting Act (15 U.S.C. 1681e–1(b)(1)) is
18 amended by inserting “, or evidence that the consumer
19 has received notice that the consumer’s financial informa-
20 tion has or may have been compromised,” after “identity
21 theft report”.

22 **SEC. 318. ENFORCEMENT BY STATE ATTORNEYS GENERAL.**

23 (a) IN GENERAL.—

24 (1) CIVIL ACTIONS.—In any case in which the
25 attorney general of a State or any State or local law

1 enforcement agency authorized by the State attorney
2 general or by State statute to prosecute violations of
3 consumer protection law, has reason to believe that
4 an interest of the residents of that State has been
5 or is threatened or adversely affected by the engage-
6 ment of a business entity in a practice that is pro-
7 hibited under this subtitle, the State or the State or
8 local law enforcement agency on behalf of the resi-
9 dents of the agency's jurisdiction, may bring a civil
10 action on behalf of the residents of the State or ju-
11 risdiction in a district court of the United States of
12 appropriate jurisdiction or any other court of com-
13 petent jurisdiction, including a State court, to—

14 (A) enjoin that practice;

15 (B) enforce compliance with this subtitle;

16 or

17 (C) civil penalties of not more than \$1,000
18 per day per individual whose sensitive person-
19 ally identifiable information was, or is reason-
20 ably believed to have been, accessed or acquired
21 by an unauthorized person, up to a maximum
22 of \$1,000,000 per violation, unless such con-
23 duct is found to be willful or intentional.

24 (2) NOTICE.—

1 (A) IN GENERAL.—Before filing an action
2 under paragraph (1), the attorney general of
3 the State involved shall provide to the Attorney
4 General of the United States—

5 (i) written notice of the action; and

6 (ii) a copy of the complaint for the ac-
7 tion.

8 (B) EXEMPTION.—

9 (i) IN GENERAL.—Subparagraph (A)
10 shall not apply with respect to the filing of
11 an action by an attorney general of a State
12 under this subtitle, if the State attorney
13 general determines that it is not feasible to
14 provide the notice described in such sub-
15 paragraph before the filing of the action.

16 (ii) NOTIFICATION.—In an action de-
17 scribed in clause (i), the attorney general
18 of a State shall provide notice and a copy
19 of the complaint to the Attorney General
20 at the time the State attorney general files
21 the action.

22 (b) FEDERAL PROCEEDINGS.—Upon receiving notice
23 under subsection (a)(2), the Attorney General shall have
24 the right to—

1 (1) move to stay the action, pending the final
2 disposition of a pending Federal proceeding or ac-
3 tion;

4 (2) initiate an action in the appropriate United
5 States district court under section 317 and move to
6 consolidate all pending actions, including State ac-
7 tions, in such court;

8 (3) intervene in an action brought under sub-
9 section (a)(2); and

10 (4) file petitions for appeal.

11 (c) PENDING PROCEEDINGS.—If the Attorney Gen-
12 eral has instituted a proceeding or action for a violation
13 of this subtitle or any regulations thereunder, no attorney
14 general of a State may, during the pendency of such pro-
15 ceeding or action, bring an action under this subtitle
16 against any defendant named in such criminal proceeding
17 or civil action for any violation that is alleged in that pro-
18 ceeding or action.

19 (d) CONSTRUCTION.—For purposes of bringing any
20 civil action under subsection (a), nothing in this subtitle
21 regarding notification shall be construed to prevent an at-
22 torney general of a State from exercising the powers con-
23 ferred on such attorney general by the laws of that State
24 to—

25 (1) conduct investigations;

1 (2) administer oaths or affirmations; or

2 (3) compel the attendance of witnesses or the
3 production of documentary and other evidence.

4 (e) VENUE; SERVICE OF PROCESS.—

5 (1) VENUE.—Any action brought under sub-
6 section (a) may be brought in—

7 (A) the district court of the United States
8 that meets applicable requirements relating to
9 venue under section 1391 of title 28, United
10 States Code; or

11 (B) another court of competent jurisdic-
12 tion.

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

16 (A) is an inhabitant; or

17 (B) may be found.

18 (f) NO PRIVATE CAUSE OF ACTION.—Nothing in this
19 subtitle establishes a private cause of action against a
20 business entity for violation of any provision of this sub-
21 title.

22 **SEC. 319. EFFECT ON FEDERAL AND STATE LAW.**

23 The provisions of this subtitle shall supersede any
24 other provision of Federal law or any provision of law of
25 any State relating to notification by a business entity en-

1 gaged in interstate commerce or an agency of a security
2 breach, except as provided in section 314(b).

3 **SEC. 320. AUTHORIZATION OF APPROPRIATIONS.**

4 There are authorized to be appropriated such sums
5 as may be necessary to cover the costs incurred by the
6 United States Secret Service to carry out investigations
7 and risk assessments of security breaches as required
8 under this subtitle.

9 **SEC. 321. REPORTING ON RISK ASSESSMENT EXEMPTIONS.**

10 The United States Secret Service shall report to Con-
11 gress not later than 18 months after the date of enactment
12 of this Act, and upon the request by Congress thereafter,
13 on—

14 (1) the number and nature of the security
15 breaches described in the notices filed by those busi-
16 ness entities invoking the risk assessment exemption
17 under section 312(b) and the response of the United
18 States Secret Service to such notices; and

19 (2) the number and nature of security breaches
20 subject to the national security and law enforcement
21 exemptions under section 312(a), provided that such
22 report may not disclose the contents of any risk as-
23 sessment provided to the United States Secret Serv-
24 ice pursuant to this subtitle.

1 **SEC. 322. EFFECTIVE DATE.**

2 This subtitle shall take effect on the expiration of the
3 date which is 90 days after the date of enactment of this
4 Act.

5 **Subtitle C—Office of Federal**
6 **Identity Protection**

7 **SEC. 331. OFFICE OF FEDERAL IDENTITY PROTECTION.**

8 (a) ESTABLISHMENT.—There is established in the
9 Federal Trade Commission an Office of Federal Identity
10 Protection.

11 (b) DUTIES.—The Office of Federal Identity Protec-
12 tion shall be responsible for assisting each consumer
13 with—

14 (1) addressing the consequences of the theft or
15 compromise of the personally identifiable informa-
16 tion of that consumer;

17 (2) accessing remedies provided under Federal
18 law and providing information about remedies avail-
19 able under State law;

20 (3) restoring the accuracy of—

21 (A) the personally identifiable information
22 of that consumer; and

23 (B) records containing the personally iden-
24 tifiable information of that consumer that were
25 stolen or compromised; and

1 (4) retrieving any stolen or compromised per-
2 sonally identifiable information of that consumer.

3 (c) ACTIVITIES.—In order to perform the duties re-
4 quired under subsection (b), the Office of Federal Identity
5 Protection shall carry out the following activities:

6 (1) Establish a website, easily and conspicu-
7 ously accessible from ftc.gov, dedicated to assisting
8 consumers with the retrieval of the stolen or com-
9 promised personally identifiable information of the
10 consumer.

11 (2) Maintain a toll-free phone number to help
12 answer questions concerning identity theft from con-
13 sumers.

14 (3) Establish online and offline consumer-serv-
15 ice teams to assist consumers seeking the retrieval
16 of the personally identifiable information of the con-
17 sumer.

18 (4) Provide guidance and information to service
19 organizations or pro bono legal services programs
20 that offer individualized assistance or counseling to
21 victims of identity theft.

22 (5) Establish a reasonable standard for deter-
23 mining when an individual becomes a victim of iden-
24 tity theft.

1 (6) Issue certifications to individuals who,
2 under the standard described in paragraph (5), are
3 identity theft victims.

4 (7) Permit an individual to use the Office of
5 Federal Identity Protection certification—

6 (A) in all Federal, State, and local juris-
7 dictions, in lieu of a police report or any other
8 document required by State or local law, as a
9 prerequisite to accessing business records of
10 transactions done by someone claiming to be
11 the individual; and

12 (B) to establish the eligibility of that indi-
13 vidual for—

14 (i) the fraud alert protections under
15 section 605A of the Fair Credit Reporting
16 Act (15 U.S.C. 1681c-1); and

17 (ii) the reporting protections under
18 section 605B(a) of the Fair Credit Report-
19 ing Act (15 U.S.C. 1681c-2(a)).

20 (8) Coordinate, as the Office determines nec-
21 essary, with the designated Chief Privacy Officer of
22 each Federal agency, or any other designated senior
23 official in such agency in charge of privacy, in order
24 to meet the duties of assisting consumers as re-
25 quired under subsection (b).

1 (9) In addition to the requirements in para-
2 graphs (1) through (7), the Federal Trade Commis-
3 sion shall promulgate regulations that enable the Of-
4 fice of Federal Identity Protection to help consumers
5 restore their stolen or otherwise compromised per-
6 sonally identifiable information quickly and inexpen-
7 sively.

8 (d) AUTHORIZATION OF APPROPRIATIONS.—There
9 are authorized to be appropriated for the Office of Federal
10 Identity Protection such sums as are necessary for fiscal
11 year 2010 and each of the 4 succeeding fiscal years.

12 **TITLE IV—GOVERNMENT AC-**
13 **CESS TO AND USE OF COM-**
14 **MERCIAL DATA**

15 **SEC. 401. GENERAL SERVICES ADMINISTRATION REVIEW**
16 **OF CONTRACTS.**

17 (a) IN GENERAL.—In considering contract awards
18 totaling more than \$500,000 and entered into after the
19 date of enactment of this Act with data brokers, the Ad-
20 ministrator of the General Services Administration shall
21 evaluate—

22 (1) the data privacy and security program of a
23 data broker to ensure the privacy and security of
24 data containing personally identifiable information,
25 including whether such program adequately address-

1 es privacy and security threats created by malicious
2 software or code, or the use of peer-to-peer file shar-
3 ing software;

4 (2) the compliance of a data broker with such
5 program;

6 (3) the extent to which the databases and sys-
7 tems containing personally identifiable information
8 of a data broker have been compromised by security
9 breaches; and

10 (4) the response by a data broker to such
11 breaches, including the efforts by such data broker
12 to mitigate the impact of such security breaches.

13 (b) COMPLIANCE SAFE HARBOR.—The data privacy
14 and security program of a data broker shall be deemed
15 sufficient for the purposes of subsection (a), if the data
16 broker complies with or provides protection equal to indus-
17 try standards, as identified by the Federal Trade Commis-
18 sion, that are applicable to the type of personally identifi-
19 able information involved in the ordinary course of busi-
20 ness of such data broker.

21 (c) PENALTIES.—In awarding contracts with data
22 brokers for products or services related to access, use,
23 compilation, distribution, processing, analyzing, or evalu-
24 ating personally identifiable information, the Adminis-
25 trator of the General Services Administration shall—

1 (1) include monetary or other penalties—

2 (A) for failure to comply with subtitles A
3 and B of title III; or

4 (B) if a contractor knows or has reason to
5 know that the personally identifiable informa-
6 tion being provided is inaccurate, and provides
7 such inaccurate information; and

8 (2) require a data broker that engages service
9 providers not subject to subtitle A of title III for re-
10 sponsibilities related to sensitive personally identifi-
11 able information to—

12 (A) exercise appropriate due diligence in
13 selecting those service providers for responsibil-
14 ities related to personally identifiable informa-
15 tion;

16 (B) take reasonable steps to select and re-
17 tain service providers that are capable of main-
18 taining appropriate safeguards for the security,
19 privacy, and integrity of the personally identifi-
20 able information at issue; and

21 (C) require such service providers, by con-
22 tract, to implement and maintain appropriate
23 measures designed to meet the objectives and
24 requirements in title III.

1 (d) LIMITATION.—The penalties under subsection (c)
2 shall not apply to a data broker providing information that
3 is accurately and completely recorded from a public record
4 source or licensor.

5 **SEC. 402. REQUIREMENT TO AUDIT INFORMATION SECUR-**
6 **RITY PRACTICES OF CONTRACTORS AND**
7 **THIRD PARTY BUSINESS ENTITIES.**

8 Section 3544(b) of title 44, United States Code, is
9 amended—

10 (1) in paragraph (7)(C)(iii), by striking “and”
11 after the semicolon;

12 (2) in paragraph (8), by striking the period and
13 inserting “; and”; and

14 (3) by adding at the end the following:

15 “(9) procedures for evaluating and auditing the
16 information security practices of contractors or third
17 party business entities supporting the information
18 systems or operations of the agency involving per-
19 sonally identifiable information (as that term is de-
20 fined in section 3 of the Personal Data Privacy and
21 Security Act of 2009) and ensuring remedial action
22 to address any significant deficiencies.”.

1 **SEC. 403. PRIVACY IMPACT ASSESSMENT OF GOVERNMENT**
2 **USE OF COMMERCIAL INFORMATION SERV-**
3 **ICES CONTAINING PERSONALLY IDENTIFI-**
4 **ABLE INFORMATION.**

5 (a) **IN GENERAL.**—Section 208(b)(1) of the E-Gov-
6 ernment Act of 2002 (44 U.S.C. 3501 note) is amended—

7 (1) in subparagraph (A)(i), by striking “or”;

8 and

9 (2) in subparagraph (A)(ii), by striking the pe-
10 riod and inserting “; or”; and

11 (3) by inserting after clause (ii) the following:

12 “(iii) purchasing or subscribing for a
13 fee to personally identifiable information
14 from a data broker (as such terms are de-
15 fined in section 3 of the Personal Data
16 Privacy and Security Act of 2009).”.

17 (b) **LIMITATION.**—Notwithstanding any other provi-
18 sion of law, commencing 1 year after the date of enact-
19 ment of this Act, no Federal agency may enter into a con-
20 tract with a data broker to access for a fee any database
21 consisting primarily of personally identifiable information
22 concerning United States persons (other than news report-
23 ing or telephone directories) unless the head of such de-
24 partment or agency—

25 (1) completes a privacy impact assessment
26 under section 208 of the E-Government Act of 2002

1 (44 U.S.C. 3501 note), which shall subject to the
2 provision in that Act pertaining to sensitive informa-
3 tion, include a description of—

4 (A) such database;

5 (B) the name of the data broker from
6 whom it is obtained; and

7 (C) the amount of the contract for use;

8 (2) adopts regulations that specify—

9 (A) the personnel permitted to access, ana-
10 lyze, or otherwise use such databases;

11 (B) standards governing the access, anal-
12 ysis, or use of such databases;

13 (C) any standards used to ensure that the
14 personally identifiable information accessed,
15 analyzed, or used is the minimum necessary to
16 accomplish the intended legitimate purpose of
17 the Federal agency;

18 (D) standards limiting the retention and
19 redisclosure of personally identifiable informa-
20 tion obtained from such databases;

21 (E) procedures ensuring that such data
22 meet standards of accuracy, relevance, com-
23 pleteness, and timeliness;

1 (F) the auditing and security measures to
2 protect against unauthorized access, analysis,
3 use, or modification of data in such databases;

4 (G) applicable mechanisms by which indi-
5 viduals may secure timely redress for any ad-
6 verse consequences wrongly incurred due to the
7 access, analysis, or use of such databases;

8 (H) mechanisms, if any, for the enforce-
9 ment and independent oversight of existing or
10 planned procedures, policies, or guidelines; and

11 (I) an outline of enforcement mechanisms
12 for accountability to protect individuals and the
13 public against unlawful or illegitimate access or
14 use of databases; and

15 (3) incorporates into the contract or other
16 agreement totaling more than \$500,000, provi-
17 sions—

18 (A) providing for penalties—

19 (i) for failure to comply with title III
20 of this Act; or

21 (ii) if the entity knows or has reason
22 to know that the personally identifiable in-
23 formation being provided to the Federal
24 department or agency is inaccurate, and
25 provides such inaccurate information; and

1 (B) requiring a data broker that engages
2 service providers not subject to subtitle A of
3 title III for responsibilities related to sensitive
4 personally identifiable information to—

5 (i) exercise appropriate due diligence
6 in selecting those service providers for re-
7 sponsibilities related to personally identifi-
8 able information;

9 (ii) take reasonable steps to select and
10 retain service providers that are capable of
11 maintaining appropriate safeguards for the
12 security, privacy, and integrity of the per-
13 sonally identifiable information at issue;
14 and

15 (iii) require such service providers, by
16 contract, to implement and maintain ap-
17 propriate measures designed to meet the
18 objectives and requirements in title III.

19 (c) LIMITATION ON PENALTIES.—The penalties
20 under subsection (b)(3)(A) shall not apply to a data
21 broker providing information that is accurately and com-
22 pletely recorded from a public record source.

23 (d) STUDY OF GOVERNMENT USE.—

24 (1) SCOPE OF STUDY.—Not later than 180
25 days after the date of enactment of this Act, the

1 Comptroller General of the United States shall con-
2 duct a study and audit and prepare a report on Fed-
3 eral agency actions to address the recommendations
4 in the Government Accountability Office's April
5 2006 report on agency adherence to key privacy
6 principles in using data brokers or commercial data-
7 bases containing personally identifiable information.

8 (2) REPORT.—A copy of the report required
9 under paragraph (1) shall be submitted to Congress.

10 **SEC. 404. IMPLEMENTATION OF CHIEF PRIVACY OFFICER**
11 **REQUIREMENTS.**

12 (a) DESIGNATION OF THE CHIEF PRIVACY OFFI-
13 CER.—Pursuant to the requirements under section 522 of
14 the Transportation, Treasury, Independent Agencies, and
15 General Government Appropriations Act, 2005 (division H
16 of Public Law 108–447; 118 Stat. 3199) that each agency
17 designate a Chief Privacy Officer, the Department of Jus-
18 tice shall implement such requirements by designating a
19 department-wide Chief Privacy Officer, whose primary
20 role shall be to fulfill the duties and responsibilities of
21 Chief Privacy Officer and who shall report directly to the
22 Deputy Attorney General.

23 (b) DUTIES AND RESPONSIBILITIES OF CHIEF PRI-
24 VACY OFFICER.—In addition to the duties and responsibil-
25 ities outlined under section 522 of the Transportation,

1 Treasury, Independent Agencies, and General Government
2 Appropriations Act, 2005 (division H of Public Law 108–
3 447; 118 Stat. 3199), the Department of Justice Chief
4 Privacy Officer shall—

5 (1) oversee the Department of Justice’s imple-
6 mentation of the requirements under section 403 to
7 conduct privacy impact assessments of the use of
8 commercial data containing personally identifiable
9 information by the Department; and

10 (2) coordinate with the Privacy and Civil Lib-
11 erties Oversight Board, established in the Intel-
12 ligence Reform and Terrorism Prevention Act of
13 2004 (Public Law 108–458), in implementing this
14 section.

○