

109TH CONGRESS
1ST SESSION

S. _____

To prevent and mitigate identity theft; to ensure privacy; 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

Mr. SPECTER (for himself and Mr. LEAHY) introduced the following bill; which was read twice and referred to the Committee on

A BILL

To prevent and mitigate identity theft; to ensure privacy; 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 2005”.

6 (b) TABLE OF CONTENTS.—The table of contents for
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. Fraud and related criminal activity in connection with unauthorized access to personally identifiable information.
- Sec. 102. Organized criminal activity in connection with unauthorized access to personally identifiable information.
- Sec. 103. Concealment of security breaches involving personally identifiable information.
- Sec. 104. Aggravated fraud in connection with computers.
- Sec. 105. Review and amendment of Federal sentencing guidelines related to fraudulent access to or misuse of digitized or electronic personally identifiable information.

TITLE II—ASSISTANCE FOR STATE AND LOCAL LAW ENFORCEMENT COMBATING CRIMES RELATED TO FRAUDULENT, UNAUTHORIZED, OR OTHER CRIMINAL USE OF PERSONALLY IDENTIFIABLE INFORMATION

- Sec. 201. Grants for State and local enforcement.
- Sec. 202. Authorization of appropriations.

TITLE III—DATA BROKERS

- Sec. 301. Transparency and accuracy of data collection.
- Sec. 302. Enforcement.
- Sec. 303. Relation to State laws.
- Sec. 304. Effective date.

TITLE IV—PRIVACY AND SECURITY OF PERSONALLY IDENTIFIABLE INFORMATION

Subtitle A—Data Privacy and Security Program

- Sec. 401. Purpose and applicability of data privacy and security program.
- Sec. 402. Requirements for a personal data privacy and security program.
- Sec. 403. Enforcement.
- Sec. 404. Relation to State laws.

Subtitle B—Security Breach Notification

- Sec. 421. Right to notice of security breach.
- Sec. 422. Notice procedures.
- Sec. 423. Content of notice.
- Sec. 424. Risk assessment and fraud prevention notice exemptions.
- Sec. 425. Victim protection assistance.
- Sec. 426. Enforcement.
- Sec. 427. Relation to State laws.
- Sec. 428. Study on securing personally identifiable information in the digital era.
- Sec. 429. Authorization of appropriations.
- Sec. 430. Effective date.

TITLE V—PROTECTION OF SOCIAL SECURITY NUMBERS

- Sec. 501. Social Security number protection.
Sec. 502. Limits on personal disclosure of social security numbers for commercial transactions and accounts.
Sec. 503. Public records.
Sec. 504. Treatment of social security numbers on government checks and prohibition of inmate access.
Sec. 505. Study and report.
Sec. 506. Enforcement.
Sec. 507. Relation to State laws.

TITLE VI—GOVERNMENT ACCESS TO AND USE OF COMMERCIAL
DATA

- Sec. 601. General Services Administration review of contracts.
Sec. 602. Requirement to audit information security practices of contractors and third party business entities.
Sec. 603. Privacy impact assessment of government use of commercial information services containing personally identifiable information.
Sec. 604. Implementation of Chief Privacy Officer requirements.

1 **SEC. 2. FINDINGS.**

2 Congress finds that—

3 (1) databases of personal 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;

1 (5) it is important for business entities that
2 own, use, or license personally identifiable informa-
3 tion to adopt reasonable procedures to ensure the se-
4 curity, privacy, and confidentiality of that personally
5 identifiable information;

6 (6) individuals whose personal information has
7 been compromised or who have been victims of iden-
8 tity theft should receive the necessary information
9 and assistance to mitigate their damages and to re-
10 store the integrity of their personal information and
11 identities;

12 (7) data brokers have assumed a significant
13 role in providing identification, authentication, and
14 screening services, and related data collection and
15 analyses for commercial, nonprofit, and government
16 operations;

17 (8) data misuse and use of inaccurate data have
18 the potential to cause serious or irreparable harm to
19 an individual's livelihood, privacy, and liberty and
20 undermine efficient and effective business and gov-
21 ernment operations;

22 (9) there is a need to insure that data brokers
23 conduct their operations in a manner that prioritizes
24 fairness, transparency, accuracy, and respect for the
25 privacy of consumers;

1 (10) government access to commercial data can
2 potentially improve safety, law enforcement, and na-
3 tional security; and

4 (11) because government misuse of commercial
5 data endangers privacy, security, and liberty, there
6 is a need for Congress to exercise oversight over gov-
7 ernment use of commercial data.

8 **SEC. 3. DEFINITIONS.**

9 In this Act:

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

13 (2) AFFILIATE.—The term “affiliate” means
14 persons related by common ownership or affiliated
15 by corporate control.

16 (3) BUSINESS ENTITY.—The term “business
17 entity” means any organization, corporation, trust,
18 partnership, sole proprietorship, unincorporated as-
19 sociation, venture established to make a profit, or
20 nonprofit, and any contractor, subcontractor, affil-
21 iate, or licensee thereof engaged in interstate com-
22 merce.

23 (4) IDENTITY THEFT.—The term “identity
24 theft” means a violation of section 1028 of title 18,

1 United States Code, or any other similar provision
2 of applicable State law.

3 (5) DATA BROKER.—The term “data broker”
4 means a business entity which for monetary fees,
5 dues, or on a cooperative nonprofit basis, regularly
6 engages, in whole or in part, in the practice of col-
7 lecting, transmitting, or otherwise providing person-
8 ally identifiable information on a nationwide basis on
9 more than 5,000 individuals who are not the cus-
10 tomers or employees of the business entity or affil-
11 iate.

12 (6) DATA FURNISHER.—The term “data fur-
13 nisher” means any agency, governmental entity, or-
14 ganization, corporation, trust, partnership, sole pro-
15 prietorship, unincorporated association, venture es-
16 tablished to make a profit, or nonprofit, and any
17 contractor, subcontractor, affiliate, or licensee there-
18 of, that serves as a source of information for a data
19 broker.

20 (7) PERSONAL ELECTRONIC RECORD.—The
21 term “personal electronic record” means the com-
22 pilation of personally identifiable information of an
23 individual (including information associated with
24 that personally identifiable information) in a data-

1 base, networked or integrated databases, or other
2 data system.

3 (8) PERSONALLY IDENTIFIABLE INFORMA-
4 TION.—The term “personally identifiable informa-
5 tion” means any information, or compilation of in-
6 formation, in electronic or digital form serving as a
7 means of identification, as defined by section
8 1028(d)(7) of title 18, United State Code.

9 (9) PUBLIC RECORD.—The term “public
10 record” means any item, collection, or grouping of
11 information about an individual that is maintained
12 by an agency, including—

13 (A) education, financial transactions, med-
14 ical history, and criminal or employment history
15 containing the name of an individual; and

16 (B) the identifying number, symbol, or
17 other identifying particular assigned to an indi-
18 vidual, such as—

19 (i) a fingerprint;

20 (ii) a voice print; or

21 (iii) a photograph.

22 (10) SECURITY BREACH.—

23 (A) IN GENERAL.—The term “security
24 breach” means compromise of the security, con-
25 fidentiality, or integrity of computerized data

1 through misrepresentation or actions that result
2 in, or there is a reasonable basis to conclude
3 has resulted in, the unauthorized acquisition of
4 and access to sensitive personally identifiable
5 information.

6 (B) EXCLUSION.—The term “security
7 breach” does not include a good faith acquisi-
8 tion of sensitive personally identifiable informa-
9 tion if the sensitive personally identifiable infor-
10 mation is not subject to further unauthorized
11 disclosure.

12 (11) SENSITIVE PERSONALLY IDENTIFIABLE IN-
13 FORMATION.—The term “sensitive personally identi-
14 fiable information” means any name or number used
15 in conjunction with any other information to identify
16 a specific individual, including any—

17 (A) name, social security number, date of
18 birth, official State or government issued driv-
19 er’s license or identification number, alien reg-
20 istration number, government passport number,
21 employer or taxpayer identification number;

22 (B) unique biometric data, such as—

23 (i) a fingerprint;

24 (ii) a voice print;

25 (iii) a retina or iris image; or

1 (iv) any other unique physical rep-
2 resentation;

3 (C) unique electronic identification num-
4 ber, address, or routing code; or

5 (D) telecommunication identifying informa-
6 tion or access device (as defined in section
7 1029(e) of title 18, United States Code).

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

13 **SEC. 101. FRAUD AND RELATED CRIMINAL ACTIVITY IN**
14 **CONNECTION WITH UNAUTHORIZED ACCESS**
15 **TO PERSONALLY IDENTIFIABLE INFORMA-**
16 **TION.**

17 Section 1030(a)(2) of title 18, United States Code,
18 is amended—

19 (1) in subparagraph (B), by striking “or” after
20 the semicolon;

21 (2) in subparagraph (C), by inserting “or” after
22 the semicolon; and

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

24 “(D) information contained in the data-
25 bases or systems of a data broker, or in other

1 personal electronic records, as such terms are
2 defined in section 3 of the Personal Data Pri-
3 vacy and Security Act of 2005;”.

4 **SEC. 102. ORGANIZED CRIMINAL ACTIVITY IN CONNECTION**
5 **WITH UNAUTHORIZED ACCESS TO PERSON-**
6 **ALLY IDENTIFIABLE INFORMATION.**

7 Section 1961(1) of title 18, United States Code, is
8 amended by inserting “section 1030(a)(2)(D)(relating to
9 fraud and related activity in connection with unauthorized
10 access to personally identifiable information,” before “sec-
11 tion 1084”.

12 **SEC. 103. CONCEALMENT OF SECURITY BREACHES INVOLV-**
13 **ING PERSONALLY IDENTIFIABLE INFORMA-**
14 **TION.**

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

18 **“§ 1039. Concealment of security breaches involving**
19 **personally identifiable information**

20 “Whoever, having knowledge of a security breach re-
21 quiring notice to individuals under title IV of the Personal
22 Data Privacy and Security Act of 2005, intentionally and
23 willfully conceals the fact of, or information related to,
24 such security breach, shall be fined under this title or im-
25 prisoned not more than 5 years, or both.”.

1 (b) CONFORMING AND TECHNICAL AMENDMENTS.—
2 The table of sections for chapter 47 of title 18, United
3 States Code, is amended by adding at the end the fol-
4 lowing:

5

“1039. Concealment of security breaches involving personally identifiable infor-
mation.”.

6 **SEC. 104. AGGRAVATED FRAUD IN CONNECTION WITH COM-**
7 **PUTERS.**

8 (a) IN GENERAL.—Chapter 47 of title 18, United
9 States Code, is amended by adding after section 1030 the
10 following:

11 **“§ 1030A. Aggravated fraud in connection with com-**
12 **puters**

13 “(a) IN GENERAL.—Whoever, during and in relation
14 to any felony violation enumerated in subsection (c),
15 knowingly obtains, accesses, or transmits, without lawful
16 authority, a means of identification of another person
17 may, in addition to the punishment provided for such fel-
18 ony, be sentenced to a term of imprisonment of up to 2
19 years.

20 “(b) CONSECUTIVE SENTENCES.—Notwithstanding
21 any other provision of law, should a court in its discretion
22 impose an additional sentence under subsection (a)—

23 “(1) no term of imprisonment imposed on a
24 person under this section shall run concurrently, ex-

1 cept as provided in paragraph (3), with any other
2 term of imprisonment imposed on such person under
3 any other provision of law, including any term of im-
4 prisonment imposed for the felony during which the
5 means of identifications was obtained, accessed, or
6 transmitted;

7 “(2) in determining any term of imprisonment
8 to be imposed for the felony during which the means
9 of identification was obtained, accessed, or trans-
10 mitted, a court shall not in any way reduce the term
11 to be imposed for such crime so as to compensate
12 for, or otherwise take into account, any separate
13 term of imprisonment imposed or to be imposed for
14 a violation of this section; and

15 “(3) a term of imprisonment imposed on a per-
16 son for a violation of this section may, in the discre-
17 tion of the court, run concurrently, in whole or in
18 part, only with another term of imprisonment that
19 is imposed by the court at the same time on that
20 person for an additional violation of this section.

21 “(c) DEFINITION.—For purposes of this section, the
22 term ‘felony violation enumerated in subsection (c)’ means
23 any offense that is a felony violation of paragraphs (2)
24 through (7) of section 1030(a).”.

1 (b) CONFORMING AND TECHNICAL AMENDMENTS.—
2 The table of sections for chapter 47 of title 18, United
3 States Code, is amended by inserting after the item relat-
4 ing to section 1030 the following new item:

5

“1030A. Aggravated fraud in connection with computers.”.

6 **SEC. 105. REVIEW AND AMENDMENT OF FEDERAL SEN-**
7 **TENCING GUIDELINES RELATED TO FRAUDU-**
8 **LENT ACCESS TO OR MISUSE OF DIGITIZED**
9 **OR ELECTRONIC PERSONALLY IDENTIFIABLE**
10 **INFORMATION.**

11 (a) REVIEW AND AMENDMENT.—Not later than 180
12 days after the date of enactment of this Act, the United
13 States Sentencing Commission, pursuant to its authority
14 under section 994 of title 28, United States Code, and
15 in accordance with this section, shall review and, if appro-
16 priate, amend the Federal sentencing guidelines (including
17 its policy statements) applicable to persons convicted of
18 using fraud to access, or misuse of, digitized or electronic
19 personally identifiable information, including identity theft
20 or any offense under—

21 (1) sections 1028, 1028A, 1030, 1030A, 2511,
22 and 2701 of title 18, United States Code; or

23 (2) any other relevant provision.

1 (b) REQUIREMENTS.—In carrying out the require-
2 ments of this section, the United States Sentencing Com-
3 mission shall—

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

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

8 (B) the growing incidences of theft and
9 misuse of digitized or electronic personally iden-
10 tifiable information, including identity theft;
11 and

12 (C) the need to deter, prevent, and punish
13 such offenses;

14 (2) consider the extent to which the Federal
15 sentencing guidelines (including its policy state-
16 ments) adequately address violations of the sections
17 amended by this Act to—

18 (A) sufficiently deter and punish such of-
19 fenses; and

20 (B) adequately reflect the enhanced pen-
21 alties established under this Act;

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

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

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

7 (A) the online sale of fraudulently obtained
8 or stolen personally identifiable information;

9 (B) the sale of fraudulently obtained or
10 stolen personally identifiable information to an
11 individual who is engaged in terrorist activity or
12 aiding other individuals engaged in terrorist ac-
13 tivity; or

14 (C) the sale of fraudulently obtained or
15 stolen personally identifiable information to fi-
16 nance terrorist activity or other criminal activi-
17 ties;

18 (6) make any necessary conforming changes to
19 the Federal sentencing guidelines to ensure that
20 such guidelines (including its policy statements) as
21 described in subsection (a) are sufficiently stringent
22 to deter, and adequately reflect crimes related to
23 fraudulent access to, or misuse of, personally identi-
24 fiable information; and

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

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

12 **TITLE II—ASSISTANCE FOR**
13 **STATE AND LOCAL LAW EN-**
14 **FORCEMENT COMBATING**
15 **CRIMES RELATED TO FRAUD-**
16 **ULENT, UNAUTHORIZED, OR**
17 **OTHER CRIMINAL USE OF**
18 **PERSONALLY IDENTIFIABLE**
19 **INFORMATION**

20 **SEC. 201. GRANTS FOR STATE AND LOCAL ENFORCEMENT.**

21 (a) IN GENERAL.—Subject to the availability of
22 amounts provided in advance in appropriations Acts, the
23 Assistant Attorney General for the Office of Justice Pro-
24 grams of the Department of Justice may award a grant
25 to a State to establish and develop programs to increase

1 and enhance enforcement against crimes related to fraud-
2 ulent, unauthorized, or other criminal use of personally
3 identifiable information.

4 (b) APPLICATION.—A State seeking a grant under
5 subsection (a) shall submit an application to the Assistant
6 Attorney General for the Office of Justice Programs of
7 the Department of Justice at such time, in such manner,
8 and containing such information as the Assistant Attorney
9 General may require.

10 (c) USE OF GRANT AMOUNTS.—A grant awarded to
11 a State under subsection (a) shall be used by a State, in
12 conjunction with units of local government within that
13 State, State and local courts, other States, or combina-
14 tions thereof, to establish and develop programs to—

15 (1) assist State and local law enforcement agen-
16 cies in enforcing State and local criminal laws relat-
17 ing to crimes involving the fraudulent, unauthorized,
18 or other criminal use of personally identifiable infor-
19 mation;

20 (2) assist State and local law enforcement agen-
21 cies in educating the public to prevent and identify
22 crimes involving the fraudulent, unauthorized, or
23 other criminal use of personally identifiable informa-
24 tion;

1 (3) educate and train State and local law en-
2 forcement officers and prosecutors to conduct inves-
3 tigations and forensic analyses of evidence and pros-
4 ecutions of crimes involving the fraudulent, unau-
5 thorized, or other criminal use of personally identifi-
6 able information;

7 (4) assist State and local law enforcement offi-
8 cers and prosecutors in acquiring computer and
9 other equipment to conduct investigations and foren-
10 sic analysis of evidence of crimes involving the
11 fraudulent, unauthorized, or other criminal use of
12 personally identifiable information; and

13 (5) facilitate and promote the sharing of Fed-
14 eral law enforcement expertise and information
15 about the investigation, analysis, and prosecution of
16 crimes involving the fraudulent, unauthorized, or
17 other criminal use of personally identifiable informa-
18 tion with State and local law enforcement officers
19 and prosecutors, including the use of multi-jurisdic-
20 tional task forces.

21 (d) ASSURANCES AND ELIGIBILITY.—To be eligible
22 to receive a grant under subsection (a), a State shall pro-
23 vide assurances to the Attorney General that the State—

24 (1) has in effect laws that penalize crimes in-
25 volving the fraudulent, unauthorized, or other crimi-

1 nal use of personally identifiable information, such
2 as penal laws prohibiting—

3 (A) fraudulent schemes executed to obtain
4 personally identifiable information;

5 (B) schemes executed to sell or use fraudu-
6 lently obtained personally identifiable informa-
7 tion; and

8 (C) online sales of personally identifiable
9 information obtained fraudulently or by other
10 illegal means;

11 (2) will provide an assessment of the resource
12 needs of the State and units of local government
13 within that State, including criminal justice re-
14 sources being devoted to the investigation and en-
15 forcement of laws related to crimes involving the
16 fraudulent, unauthorized, or other criminal use of
17 personally identifiable information; and

18 (3) will develop a plan for coordinating the pro-
19 grams funded under this section with other federally
20 funded technical assistant and training programs,
21 including directly funded local programs such as the
22 Local Law Enforcement Block Grant program (de-
23 scribed under the heading “Violent Crime Reduction
24 Programs, State and Local Law Enforcement As-
25 sistance” of the Departments of Commerce, Justice,

1 and State, the Judiciary, and Related Agencies Ap-
2 propriations Act, 1998 (Public Law 105–119)).

3 (e) MATCHING FUNDS.—The Federal share of a
4 grant received under this section may not exceed 90 per-
5 cent of the total cost of a program or proposal funded
6 under this section unless the Attorney General waives,
7 wholly or in part, the requirements of this subsection.

8 **SEC. 202. AUTHORIZATION OF APPROPRIATIONS.**

9 (a) IN GENERAL.—There is authorized to be appro-
10 priated to carry out this title \$25,000,000 for each of fis-
11 cal years 2006 through 2009.

12 (b) LIMITATIONS.—Of the amount made available to
13 carry out this title in any fiscal year not more than 3 per-
14 cent may be used by the Attorney General for salaries and
15 administrative expenses.

16 (c) MINIMUM AMOUNT.—Unless all eligible applica-
17 tions submitted by a State or units of local government
18 within a State for a grant under this title have been fund-
19 ed, the State, together with grantees within the State
20 (other than Indian tribes), shall be allocated in each fiscal
21 year under this title not less than 0.75 percent of the total
22 amount appropriated in the fiscal year for grants pursuant
23 to this title, except that the United States Virgin Islands,
24 American Samoa, Guam, and the Northern Mariana Is-
25 lands each shall be allocated 0.25 percent.

1 (d) GRANTS TO INDIAN TRIBES.—Notwithstanding
2 any other provision of this title, the Attorney General may
3 use amounts made available under this title to make
4 grants to Indian tribes for use in accordance with this
5 title.

6 **TITLE III—DATA BROKERS**

7 **SEC. 301. TRANSPARENCY AND ACCURACY OF DATA COL-** 8 **LECTION.**

9 (a) IN GENERAL.—Data brokers engaging in inter-
10 state commerce are subject to the requirements of this
11 title for any offered product or service offered to third par-
12 ties that allows access, use, compilation, distribution, proc-
13 essing, analyzing, or evaluating personally identifiable in-
14 formation, unless that product or service is currently sub-
15 ject to similar protections under subsections (b) and (g)
16 of this section, the Fair Credit Reporting Act (Public Law
17 91–508), or the Gramm-Leach Bliley Act (Public Law
18 106–102), and implementing regulations.

19 (b) DISCLOSURES TO INDIVIDUALS.—

20 (1) IN GENERAL.—A data broker shall, upon
21 the request of an individual, clearly and accurately
22 disclose to such individual for a reasonable fee all
23 personal electronic records pertaining to that indi-
24 vidual maintained for disclosure to third parties in

1 the databases or systems of the data broker at the
2 time of the request.

3 (2) INFORMATION ON HOW TO CORRECT INAC-
4 CURACIES.—The disclosures required under para-
5 graph (1) shall also include guidance to individuals
6 on the processes and procedures for demonstrating
7 and correcting any inaccuracies.

8 (c) CREATION OF AN ACCURACY RESOLUTION PROC-
9 ESS.—A data broker shall develop and publish on its
10 website timely and fair processes and procedures for re-
11 sponding to claims of inaccuracies, including procedures
12 for correcting inaccurate information in the personal elec-
13 tronic records it maintains on individuals.

14 (d) ACCURACY RESOLUTION PROCESS.—

15 (1) PUBLIC RECORD INFORMATION.—

16 (A) IN GENERAL.—If an individual notifies
17 a data broker of a dispute as to the complete-
18 ness or accuracy of information, and the data
19 broker determines that such information is de-
20 rived from a public record source, the data
21 broker shall determine within 30 days whether
22 the information in its system accurately and
23 completely records the information offered by
24 the public record source.

1 (B) DATA BROKER ACTIONS.—If a data
2 broker determines under subparagraph (A) that
3 the information in its systems—

4 (i) does not accurately and completely
5 record the information offered by a public
6 record source, the data broker shall correct
7 any inaccuracies or incompleteness, and
8 provide to such individual written notice of
9 such changes; and

10 (ii) does accurately and completely
11 record the information offered by a public
12 record source, the data broker shall—

13 (I) provide such individual with
14 the name, address, and telephone con-
15 tact information of the public record
16 source; and

17 (II) notify such individual of the
18 right to add to the personal electronic
19 record of the individual maintained by
20 the data broker a statement disputing
21 the accuracy or completeness of the
22 information for a period of 90 days
23 under subsection (e).

24 (2) INVESTIGATION OF DISPUTED NON-PUBLIC
25 RECORD INFORMATION.—If the completeness or ac-

1 accuracy of any non-public record information dis-
2 closed to an individual under subsection (b) is dis-
3 puted by the individual and such individual notifies
4 the data broker directly of such dispute, the data
5 broker shall, before the end of the 30-day period be-
6 ginning on the date on which the data broker re-
7 ceives the notice of the dispute—

8 (A) investigate free of charge and record
9 the current status of the disputed information;
10 or

11 (B) delete the item from the individuals
12 data file in accordance with paragraph (8).

13 (3) EXTENSION OF PERIOD TO INVESTIGATE.—
14 Except as provided in paragraph (4), the 30-day pe-
15 riod described in paragraph (1) may be extended for
16 not more than 15 additional days if a data broker
17 receives information from the individual during that
18 30-day period that is relevant to the investigation.

19 (4) LIMITATIONS ON EXTENSION OF PERIOD TO
20 INVESTIGATE.—Paragraph (3) shall not apply to any
21 investigation in which, during the 30-day period de-
22 scribed in paragraph (1), the information that is the
23 subject of the investigation is found to be inaccurate
24 or incomplete or a data broker determines that the
25 information cannot be verified.

1 (5) NOTICE IDENTIFYING THE DATA FUR-
2 NISHER.—If the completeness or accuracy of any in-
3 formation disclosed to an individual under sub-
4 section (b) is disputed by the individual, a data
5 broker shall provide upon the request of the indi-
6 vidual, the name, business address, and telephone
7 contact information of any data furnisher who pro-
8 vided an item of information in dispute.

9 (6) DETERMINATION THAT DISPUTE IS FRIVO-
10 LOUS OR IRRELEVANT.—

11 (A) IN GENERAL.—Notwithstanding para-
12 graphs (1) through (4), a data broker may de-
13 cline to investigate or terminate an investiga-
14 tion of information disputed by an individual
15 under those paragraphs if the data broker rea-
16 sonably determines that the dispute by the indi-
17 vidual is frivolous or irrelevant, including by
18 reason of a failure by the individual to provide
19 sufficient information to investigate the dis-
20 puted information.

21 (B) NOTICE.—Not later than 5 business
22 days after making any determination in accord-
23 ance with subparagraph (A) that a dispute is
24 frivolous or irrelevant, a data broker shall no-
25 tify the individual of such determination by

1 mail, or if authorized by the individual, by any
2 other means available to the data broker.

3 (C) CONTENTS OF NOTICE.—A notice
4 under subparagraph (B) shall include—

5 (i) the reasons for the determination
6 under subparagraph (A); and

7 (ii) identification of any information
8 required to investigate the disputed infor-
9 mation, which may consist of a standard-
10 ized form describing the general nature of
11 such information.

12 (7) CONSIDERATION OF INDIVIDUAL INFORMA-
13 TION.—In conducting any investigation with respect
14 to disputed information in the personal electronic
15 record of any individual, a data broker shall review
16 and consider all relevant information submitted by
17 the individual in the period described in paragraph
18 (2) with respect to such disputed information.

19 (8) TREATMENT OF INACCURATE OR UNVERIFI-
20 ABLE INFORMATION.—

21 (A) IN GENERAL.—If, after any review of
22 public record information under paragraph (1)
23 or any investigation of any information disputed
24 by an individual under paragraphs (2) through
25 (4), an item of information is found to be inac-

1 curate or incomplete or cannot be verified, a
2 data broker shall promptly delete that item of
3 information from the individual's personal elec-
4 tronic record or modify that item of informa-
5 tion, as appropriate, based on the results of the
6 investigation.

7 (B) NOTICE TO INDIVIDUALS OF REINSER-
8 TION OF PREVIOUSLY DELETED INFORMA-
9 TION.—If any information that has been de-
10 leted from an individual's personal electronic
11 record pursuant to subparagraph (A) is re-
12 inserted in the personal electronic record of the
13 individual, a data broker shall, not later than 5
14 days after reinsertion, notify the individual of
15 the reinsertion and identify any data furnisher
16 not previously disclosed in writing, or if author-
17 ized by the individual for that purpose, by any
18 other means available to the data broker, unless
19 such notification has been previously given
20 under this subsection.

21 (C) NOTICE OF RESULTS OF INVESTIGA-
22 TION OF DISPUTED NON-PUBLIC RECORD.—

23 (i) IN GENERAL.—Not later than 5
24 business days after the completion of an
25 investigation under paragraph (2), a data

1 broker shall provide written notice to an
2 individual of the results of the investiga-
3 tion, by mail or, if authorized by the indi-
4 vidual for that purpose, by other means
5 available to the data broker.

6 (ii) ADDITIONAL REQUIREMENT.—Be-
7 fore the expiration of the 5-day period, as
8 part of, or in addition to such notice, a
9 data broker shall, in writing, provide to an
10 individual—

11 (I) a statement that the inves-
12 tigation is completed;

13 (II) a report that is based upon
14 the personal electronic record of such
15 individual as that personal electronic
16 record is revised as a result of the in-
17 vestigation;

18 (III) a notice that, if requested
19 by the individual, a description of the
20 procedures used to determine the ac-
21 curacy and completeness of the infor-
22 mation shall be provided to the indi-
23 vidual by the data broker, including
24 the business name, address, and tele-
25 phone number of any data furnisher

1 of information contacted in connection
2 with such information; and

3 (IV) a notice that the individual
4 has the right to request notifications
5 under subsection (g).

6 (D) DESCRIPTION OF INVESTIGATION PRO-
7 CEDURES.—Not later than 15 days after receiv-
8 ing a request from an individual for a descrip-
9 tion referred to in subparagraph (C)(ii)(III), a
10 data broker shall provide to the individual such
11 a description.

12 (E) EXPEDITED DISPUTE RESOLUTION.—
13 If by no later than 3 business days after the
14 date on which a data broker receives notice of
15 a dispute from an individual of information in
16 the personal electronic record of such individual
17 in accordance with paragraph (2), a data
18 broker resolves such dispute in accordance with
19 subparagraph (A) by the deletion of the dis-
20 puted information, then the data broker shall
21 not be required to comply with subsections (e)
22 and (f) with respect to that dispute if the data
23 broker provides—

24 (i) to the individual, by telephone,
25 prompt notice of the deletion; and

1 (ii) to the individual a right to request
2 that the data broker furnish notifications
3 under subsection (g).

4 (e) STATEMENT OF DISPUTE.—

5 (1) IN GENERAL.—If the completeness or accu-
6 racy of any information disclosed to an individual
7 under subsection (b) is disputed, an individual may
8 file a brief statement setting forth the nature of the
9 dispute.

10 (2) CONTENTS OF STATEMENT.—A data broker
11 may limit the statements made pursuant to para-
12 graph (1) to not more than 100 words if it provides
13 an individual with assistance in writing a clear sum-
14 mary of the dispute or until the dispute is resolved,
15 whichever is earlier.

16 (f) NOTIFICATION OF DISPUTE IN SUBSEQUENT RE-
17 PORTS.—Whenever a statement of a dispute is filed under
18 subsection (e), unless there is a reasonable grounds to be-
19 lieve that it is frivolous or irrelevant, a data broker shall,
20 in any subsequent report, product, or service containing
21 the information in question, clearly note that it is disputed
22 by an individual and provide either the statement of such
23 individual or a clear and accurate codification or summary
24 thereof for a period of 90 days after the data broker first
25 posts the statement of dispute.

1 (g) NOTIFICATION OF DELETION OF DISPUTED IN-
2 FORMATION.—Following any deletion of information
3 which is found to be inaccurate or whose accuracy can no
4 longer be verified, a data broker shall, at the request of
5 an individual, furnish notification that the item has been
6 deleted or the statement, codification, or summary pursu-
7 ant to subsection (e) or (f) to any user or customer of
8 the products or services of the data broker who has within
9 90 days received a report with the deleted or disputed in-
10 formation or has electronically accessed the deleted or dis-
11 puted information.

12 **SEC. 302. ENFORCEMENT.**

13 (a) CIVIL PENALTIES.—

14 (1) PENALTIES.—Any data broker that violates
15 the provisions of section 301 shall be subject to civil
16 penalties of not more than \$1,000 per violation per
17 day, with a maximum of \$15,000 per day, while
18 such violations persist.

19 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
20 data broker that intentionally or willfully violates the
21 provisions of section 301 shall be subject to addi-
22 tional penalties in the amount of \$1,000 per viola-
23 tion per day, with a maximum of an additional
24 \$15,000 per day, while such violations persist.

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

5 (4) **OTHER RIGHTS AND REMEDIES.**—The
6 rights and remedies available under this subsection
7 are cumulative and shall not affect any other rights
8 and remedies available under law.

9 (b) **INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-**
10 **ERAL.**—

11 (1) **IN GENERAL.**—Whenever it appears that a
12 data broker to which this title applies has engaged,
13 is engaged, or is about to engage, in any act or prac-
14 tice constituting a violation of this title, the Attorney
15 General may bring a civil action in an appropriate
16 district court of the United States to—

17 (A) enjoin such act or practice;

18 (B) enforce compliance with this title;

19 (C) obtain damages—

20 (i) in the sum of actual damages, res-
21 titution, and other compensation on behalf
22 of the affected residents of a State; and

23 (ii) punitive damages, if the violation
24 is willful or intentional; and

1 (D) obtain such other legal and equitable
2 relief as the court may consider to be appro-
3 priate.

4 (2) NOTICE.—

5 (A) IN GENERAL.—Before filing an action
6 under this subsection, the attorney general of
7 the State involved shall provide to the Attorney
8 General—

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

10 (ii) a copy of the complaint for that
11 action.

12 (B) EXCEPTION.—Subparagraph (A) shall
13 not apply with respect to the filing of an action
14 by an attorney general of a State under this
15 subsection, if the attorney general of a State
16 determines that it is not feasible to provide the
17 notice described in this subparagraph before the
18 filing of the action.

19 (C) NOTIFICATION WHEN PRACTICABLE.—

20 In an action described under subparagraph (B),
21 the attorney general of a State shall provide the
22 written notice and the copy of the complaint to
23 the Attorney General as soon after the filing of
24 the complaint as practicable.

1 (3) ATTORNEY GENERAL AUTHORITY.—Upon
2 receiving notice under paragraph (2), the Attorney
3 General shall have the right to—

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

7 (B) intervene in an action brought under
8 paragraph (1); and

9 (C) file petitions for appeal.

10 (4) PENDING PROCEEDINGS.—If the Attorney
11 General has instituted a proceeding or action for a
12 violation of this Act or any regulations thereunder,
13 no attorney general of a State may, during the pend-
14 ency of such proceeding or action, bring an action
15 under this subsection against any defendant named
16 in such criminal proceeding or civil action for any
17 violation that is alleged in that proceeding or action.

18 (5) RULE OF CONSTRUCTION.—For purposes of
19 bringing any civil action under paragraph (1), noth-
20 ing in this Act shall be construed to prevent an at-
21 torney general of a State from exercising the powers
22 conferred on the attorney general by the laws of that
23 State to—

24 (A) conduct investigations;

25 (B) administer oaths and affirmations; or

1 (C) compel the attendance of witnesses or
2 the production of documentary and other evi-
3 dence.

4 (6) VENUE; SERVICE OF PROCESS.—

5 (A) VENUE.—Any action brought under
6 this subsection may be brought in the district
7 court of the United States that meets applicable
8 requirements relating to venue under section
9 1931 of title 28, United States Code.

10 (B) SERVICE OF PROCESS.—In an action
11 brought under this subsection process may be
12 served in any district in which the defendant—

13 (i) is an inhabitant; or

14 (ii) may be found.

15 **SEC. 303. RELATION TO STATE LAWS.**

16 (a) IN GENERAL.—Except as provided in subsection
17 (b), this title does not annul, alter, affect, or exempt any
18 person subject to the provisions of this title from com-
19 plying with the laws of any State with respect to the ac-
20 cess, use, compilation, distribution, processing, analysis,
21 and evaluation of any personally identifiable information
22 by data brokers, except to the extent that those laws are
23 inconsistent with any provisions of this title, and then only
24 to the extent of such inconsistency.

1 (b) EXCEPTIONS.—No requirement or prohibition
2 may be imposed under the laws of any State with respect
3 to any subject matter regulated under section 301, relat-
4 ing to individual access to, and correction of, personal elec-
5 tronic records.

6 **SEC. 304. EFFECTIVE DATE.**

7 This title shall take effect 180 days after the date
8 of enactment of this Act.

9 **TITLE IV—PRIVACY AND SECU-**
10 **RITY OF PERSONALLY IDEN-**
11 **TIFIABLE INFORMATION**

12 **Subtitle A—Data Privacy and**
13 **Security Program**

14 **SEC. 401. PURPOSE AND APPLICABILITY OF DATA PRIVACY**
15 **AND SECURITY PROGRAM.**

16 (a) PURPOSE.—The purpose of this subtitle is to en-
17 sure standards for developing and implementing adminis-
18 trative, technical, and physical safeguards to protect the
19 privacy, security, confidentiality, integrity, storage, and
20 disposal of personally identifiable information.

21 (b) IN GENERAL.—A business entity engaging in
22 interstate commerce that involves collecting, accessing,
23 transmitting, using, storing, or disposing of personally
24 identifiable information in electronic or digital form on
25 10,000 or more United States persons is subject to the

1 requirements for a data privacy and security program
2 under section 402 for protecting personally identifiable in-
3 formation.

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

6 (1) financial institutions subject to—

7 (A) the data security requirements and im-
8 plementing regulations under the Gramm-
9 Leach-Bliley Act (15 U.S.C. 6801 et seq.); and

10 (B) examinations for compliance with the
11 requirements of this Act by 1 or more Federal
12 functional regulators (as defined in section 509
13 of the Gramm-Leach-Bliley Act (15 U.S.C.
14 6809)); or

15 (2) “covered entities” subject to the Health In-
16 surance Portability and Accountability Act of 1996
17 (42 U.S.C. 1301 et seq.), including the data security
18 requirements and implementing regulations of that
19 Act.

20 **SEC. 402. REQUIREMENTS FOR A PERSONAL DATA PRIVACY**
21 **AND SECURITY PROGRAM.**

22 (a) PERSONAL DATA PRIVACY AND SECURITY PRO-
23 GRAM.—Unless otherwise limited under section 401(c), a
24 business entity subject to this subtitle shall comply with

1 the following safeguards to protect the privacy and secu-
2 rity of personally identifiable information:

3 (1) SCOPE.—A business entity shall implement
4 a comprehensive personal data privacy and security
5 program, written in 1 or more readily accessible
6 parts, that includes administrative, technical, and
7 physical safeguards appropriate to the size and com-
8 plexity of the business entity and the nature and
9 scope of its activities.

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

12 (A) ensure the privacy, security, and con-
13 fidentiality of personal electronic records;

14 (B) protect against any anticipated
15 vulnerabilities to the privacy, security, or integ-
16 rity of personal electronic records; and

17 (C) protect against unauthorized access to
18 use of personal electronic records that could re-
19 sult in substantial harm or inconvenience to any
20 individual.

21 (3) RISK ASSESSMENT.—A business entity
22 shall—

23 (A) identify reasonably foreseeable internal
24 and external vulnerabilities that could result in
25 unauthorized access, disclosure, use, or alter-

1 ation of personally identifiable information or
2 systems containing personally identifiable infor-
3 mation;

4 (B) assess the likelihood of and potential
5 damage from unauthorized access, disclosure,
6 use, or alteration of personally identifiable in-
7 formation; and

8 (C) assess the sufficiency of its policies,
9 technologies, and safeguards in place to control
10 and minimize risks from unauthorized access,
11 disclosure, use, or alteration of personally iden-
12 tifiable information.

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 personally identifiable in-
24 formation, including controls to authen-

1 ticate and permit access only to authorized
2 individuals;

3 (ii) detect actual and attempted
4 fraudulent, unlawful, or unauthorized ac-
5 cess, disclosure, use, or alteration of per-
6 sonally identifiable information, including
7 by employees and other individuals other-
8 wise authorized to have access; and

9 (iii) protect personally identifiable in-
10 formation during use, transmission, stor-
11 age, and disposal by encryption or other
12 reasonable means (including as directed for
13 disposal of records under section 628 of
14 the Fair Credit Reporting Act (15 U.S.C.
15 1681w) and the implementing regulations
16 of such Act as set forth in section 682 of
17 title 16, Code of Federal Regulations).

18 (5) ACCOUNTABILITY.—Each business entity
19 required to establish a data security program under
20 section 401 shall publish on its website or make oth-
21 erwise available the terms of such program to the
22 extent that such terms do not reveal information
23 that compromise data security or privacy.

24 (b) TRAINING.—Each business entity subject to this
25 subtitle shall take steps to ensure employee training and

1 supervision for implementation of the data security pro-
2 gram of the business entity.

3 (c) VULNERABILITY TESTING.—

4 (1) IN GENERAL.—Each business entity subject
5 to this subtitle shall take steps to ensure regular
6 testing of key controls, systems, and procedures of
7 the personal data privacy and security program to
8 detect, prevent, and respond to attacks or intrusions,
9 or other system failures.

10 (2) FREQUENCY.—The frequency and nature of
11 the tests required under paragraph (1) shall be de-
12 termined by the risk assessment of the business enti-
13 ty under subsection (a)(3).

14 (d) RELATIONSHIP TO SERVICE PROVIDERS.—In the
15 event a business entity subject to this subtitle engages
16 service providers not subject to this subtitle, such business
17 entity shall—

18 (1) exercise appropriate due diligence in select-
19 ing those service providers for responsibilities related
20 to personally identifiable information, and take rea-
21 sonable steps to select and retain service providers
22 that are capable of maintaining appropriate safe-
23 guards for the security, privacy, and integrity of the
24 personally identifiable information at issue; and

1 (2) require those service providers by contract
2 to implement and maintain appropriate measures de-
3 signed to meet the objectives and requirements gov-
4 erning entities subject to this section, section 401,
5 and subtitle B.

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

12 (1) technology;

13 (2) the sensitivity of personally identifiable in-
14 formation;

15 (3) internal or external threats to personally
16 identifiable information; and

17 (4) the changing business arrangements of the
18 business entity, such as—

19 (A) mergers and acquisitions;

20 (B) alliances and joint ventures;

21 (C) outsourcing arrangements;

22 (D) bankruptcy; and

23 (E) changes to personally identifiable in-
24 formation systems.

1 (f) IMPLEMENTATION TIME LINE.—Not later than 1
2 year after the date of enactment of this Act, a business
3 entity subject to the provisions of this subtitle shall imple-
4 ment a data privacy and security program pursuant to this
5 subtitle.

6 **SEC. 403. ENFORCEMENT.**

7 (a) CIVIL PENALTIES.—

8 (1) IN GENERAL.—Any business entity that vio-
9 lates the provisions of sections 401 or 402 shall be
10 subject to civil penalties of not more than \$5,000
11 per violation per day, with a maximum of \$35,000
12 per day, while such violations persist.

13 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
14 business entity that intentionally or willfully violates
15 the provisions of sections 401 or 402 shall be subject
16 to additional penalties in the amount of \$5,000 per
17 violation per day, with a maximum of an additional
18 \$35,000 per day, while such violations persist.

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

23 (4) OTHER RIGHTS AND REMEDIES.—The
24 rights and remedies available under this section are

1 cumulative and shall not affect any other rights and
2 remedies available under law

3 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
4 ERAL.—

5 (1) IN GENERAL.—Whenever it appears that a
6 business entity or agency to which this subtitle ap-
7 plies has engaged, is engaged, or is about to engage,
8 in any act or practice constituting a violation of this
9 subtitle, the Attorney General may bring a civil ac-
10 tion in an appropriate district court of the United
11 States to—

12 (A) enjoin such act or practice;

13 (B) enforce compliance with this subtitle;

14 and

15 (C) obtain damages—

16 (i) in the sum of actual damages, res-
17 titution, and other compensation on behalf
18 of the affected residents of a State; and

19 (ii) punitive damages, if the violation
20 is willful or intentional; and

21 (D) obtain such other relief as the court
22 determines to be appropriate.

23 (2) OTHER INJUNCTIVE RELIEF.—Upon a
24 proper showing in the action under paragraph (1),

1 the court shall grant a permanent injunction or a
2 temporary restraining order without bond.

3 (c) STATE ENFORCEMENT.—

4 (1) CIVIL ACTIONS.—In any case in which the
5 attorney general of a State has reason to believe
6 that an interest of the residents of that State has
7 been or is threatened or adversely affected by an act
8 or practice that violates this subtitle, the State may
9 bring a civil action on behalf of the residents of that
10 State in a district court of the United States of ap-
11 propriate jurisdiction, or any other court of com-
12 petent jurisdiction, to—

13 (A) enjoin that act or practice;

14 (B) enforce compliance with this subtitle;

15 (C) obtain—

16 (i) damages in the sum of actual dam-
17 ages, restitution, or other compensation on
18 behalf of affected residents of the State;

19 and

20 (ii) punitive damages, if the violation
21 is willful or intentional; or

22 (D) obtain such other legal and equitable
23 relief as the court may consider to be appro-
24 priate.

25 (2) NOTICE.—

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

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

6 (ii) a copy of the complaint for that
7 action.

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

15 (C) NOTIFICATION WHEN PRACTICABLE.—
16 In an action described under subparagraph (B),
17 the attorney general of a State shall provide the
18 written notice and the copy of the complaint to
19 the Attorney General as soon after the filing of
20 the complaint as practicable.

21 (3) ATTORNEY GENERAL AUTHORITY.—Upon
22 receiving notice under paragraph (2), the Attorney
23 General shall have the right to—

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

4 (B) intervene in an action brought under
5 paragraph (1); and

6 (C) file petitions for appeal.

7 (4) PENDING PROCEEDINGS.—If the Attorney
8 General has instituted a proceeding or action for a
9 violation of this Act or any regulations thereunder,
10 no attorney general of a State may, during the pend-
11 ency of such proceeding or action, bring an action
12 under this subsection against any defendant named
13 in such criminal proceeding or civil action for any
14 violation that is alleged in that proceeding or action.

15 (5) RULE OF CONSTRUCTION.—For purposes of
16 bringing any civil action under paragraph (1) noth-
17 ing in this Act shall be construed to prevent an at-
18 torney general of a State from exercising the powers
19 conferred on the attorney general by the laws of that
20 State to—

21 (A) conduct investigations;

22 (B) administer oaths and affirmations; or

23 (C) compel the attendance of witnesses or
24 the production of documentary and other evi-
25 dence.

1 (6) VENUE; SERVICE OF PROCESS.—

2 (A) VENUE.—Any action brought under
3 this subsection may be brought in the district
4 court of the United States that meets applicable
5 requirements relating to venue under section
6 1931 of title 28, United States Code.

7 (B) SERVICE OF PROCESS.—In an action
8 brought under this subsection process may be
9 served in any district in which the defendant—

10 (i) is an inhabitant; or

11 (ii) may be found.

12 **SEC. 404. RELATION TO STATE LAWS.**

13 (a) IN GENERAL.—Except as provided in subsection
14 (b), this title does not annul, alter, affect, or exempt any
15 person subject to the provisions of this title from com-
16 plying with the laws of any State with respect to security
17 programs for personally identifiable information, except to
18 the extent that those laws are inconsistent with any provi-
19 sions of this title, and then only to the extent of such in-
20 consistency.

21 (b) EXCEPTIONS.—No requirement or prohibition
22 may be imposed under the laws of any State with respect
23 to any subject matter regulated under section 401(c), re-
24 lating to entities exempted from compliance with subtitle
25 A.

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

3 **SEC. 421. RIGHT TO NOTICE OF SECURITY BREACH.**

4 (a) IN GENERAL.—Unless delayed under section
5 422(d) or exempted under section 424, any business entity
6 or agency engaged in interstate commerce that involves
7 collecting, accessing, using, transmitting, storing, or dis-
8 posing of personally identifiable information shall notify,
9 following the discovery of a security breach of its systems
10 or databases in its possession or direct control when such
11 security breach impacts sensitive personally identifiable in-
12 formation—

13 (1) if the security breach impacts more than
14 10,000 individuals nationwide, impacts a database,
15 networked or integrated databases, or other data
16 system associated with more than 1,000,000 individ-
17 uals nationwide, impacts databases owned or used by
18 the Federal Government, or involves sensitive per-
19 sonally identifiable information of employees and
20 contractors of the Federal Government—

21 (A) the United States Secret Service,
22 which shall be responsible for notifying—

23 (i) the Federal Bureau of Investiga-
24 tion, if the security breach involves espio-
25 nage, foreign counterintelligence, informa-

1 tion protected against unauthorized disclo-
2 sure for reasons of national defense or for-
3 foreign relations, or Restricted Data (as that
4 term is defined in section 11y of the Atom-
5 ic Energy Act of 1954 (42 U.S.C.
6 2014(y)), except for offenses affecting the
7 duties of the United States Secret Service
8 under section 3056(a) of title 18, United
9 States Code; and

10 (ii) the United States Postal Inspec-
11 tion Service, if the security breach involves
12 mail fraud; and

13 (B) the attorney general of each State af-
14 fected by the security breach;

15 (2) each consumer reporting agency described
16 in section 603(p) of the Fair Credit Reporting Act
17 (15 U.S.C. 1681a), pursuant to subsection (b); and

18 (3) any resident of the United States whose
19 sensitive personally identifiable information was sub-
20 ject to the security breach, pursuant to sections 422
21 and 423, but in the event a business entity or agen-
22 cy is unable to identify the specific residents of the
23 United States whose sensitive personally identifiable
24 information was impacted by a security breach, the
25 business entity or agency shall consult with the

1 United States Secret Service to determine the scope
2 of individuals who there is a reasonable basis to con-
3 clude have been impacted by such breach and should
4 receive notice.

5 (b) CONSUMER REPORTING AGENCIES.—Any busi-
6 ness entity or agency obligated to provide notice of a secu-
7 rity breach to more than 1,000 residents of the United
8 States under subsection (a)(3) shall inform consumer re-
9 porting agencies of the fact and scope of such notices for
10 the purpose of facilitating and managing potential in-
11 creases in consumer inquiries and mitigating identity theft
12 or other negative consequences of the breach.

13 **SEC. 422. NOTICE PROCEDURES.**

14 (a) TIMELINESS OF NOTICE.—

15 (1) IN GENERAL.—Except as provided in sub-
16 section (c), all notices required under section 421
17 shall be issued expeditiously and without unreason-
18 able delay after discovery of the events requiring no-
19 tice.

20 (2) 14-DAY RULE.—The notices to Federal law
21 enforcement and the attorney general of each State
22 affected by a security breach required under section
23 421(a) shall be delivered not later than 14 days
24 after discovery of the events requiring notice.

1 (3) REQUIRED DISCLOSURE.—In complying
2 with the notices required under section 421, a busi-
3 ness entity or agency shall expeditiously and without
4 unreasonable delay take reasonable measures which
5 are necessary to—

6 (A) determine the scope and assess the im-
7 pact of a breach under section 421; and

8 (B) restore the reasonable integrity of the
9 data system.

10 (b) METHOD.—Any business entity or agency obli-
11 gated to provide notice under section 421 shall be in com-
12 pliance with that section if they provide notice as follows:

13 (1) WRITTEN NOTIFICATION.—By written noti-
14 fication to the last known home address of the indi-
15 vidual whose sensitive personally identifiable infor-
16 mation was breached, or if unknown, notification via
17 telephone call to the last known home telephone
18 number.

19 (2) INTERNET POSTING.—If more than 1,000
20 residents of the United States require notice under
21 section 421 and if the business entity or agency
22 maintains an Internet site, conspicuous posting of
23 the notice on the Internet site of the business entity
24 or agency.

1 (3) MEDIA NOTICE.—If more than 5,000 resi-
2 dents of a State or jurisdiction are impacted, notice
3 to major media outlets serving that State or jurisdic-
4 tion.

5 (c) DELAY OF NOTIFICATION FOR LAW ENFORCE-
6 MENT PURPOSES.—

7 (1) IN GENERAL.—If Federal law enforcement
8 or the attorney general of a State determines that
9 the notices required under section 421(a) would im-
10 pede a criminal investigation, such notices may be
11 delayed until such law enforcement agency deter-
12 mines that the notices will no longer compromise
13 such investigation.

14 (2) EXTENDED DELAY OF NOTIFICATION FOR
15 LAW ENFORCEMENT PURPOSES.—If a business enti-
16 ty or agency has delayed the notices required under
17 paragraphs (2) and (3) of section 421(a) as de-
18 scribed in paragraph (1), the business entity or
19 agency shall give notice 30 days after the day such
20 law enforcement delay was invoked unless Federal
21 law enforcement provides written notification that
22 further delay is necessary.

23 **SEC. 423. CONTENT OF NOTICE.**

24 (a) IN GENERAL.—A business entity or agency obli-
25 gated to provide notice to residents of the United States

1 under section 421(a)(3) shall clearly and concisely detail
2 the nature of the sensitive personally identifiable informa-
3 tion impacted by the security breach.

4 (b) CONTENT OF NOTICE.—A notice under sub-
5 section (a) shall include—

6 (1) the availability of victim protection assist-
7 ance pursuant to section 425;

8 (2) guidance on how to request that a fraud
9 alert be placed in the file of the individual main-
10 tained by consumer reporting agencies, pursuant to
11 section 605A of the Fair Credit Reporting Act (15
12 U.S.C. 1681c–1) and the implications of such ac-
13 tions;

14 (3) the availability of a summary of rights for
15 identity theft victims from consumer reporting agen-
16 cies, pursuant to section 609 of the Fair Credit Re-
17 porting Act (15 U.S.C. 1681g);

18 (4) if applicable, notice that the State where an
19 individual resides has a statute that provides the in-
20 dividual the right to place a security freeze on their
21 credit report; and

22 (5) if applicable, notice that consumer reporting
23 agencies have been notified of the security breach.

24 (c) MARKETING NOT ALLOWED IN NOTICE.—A no-
25 tice under subsection (a) may not include—

- 1 (1) marketing information;
- 2 (2) sales offers; or
- 3 (3) any solicitation regarding the collection of
- 4 additional personally identifiable information from
- 5 an individual.

6 **SEC. 424. RISK ASSESSMENT AND FRAUD PREVENTION NO-**
7 **TICE EXEMPTIONS.**

8 (a) RISK ASSESSMENT EXEMPTION.—A business en-
9 tity will be exempt from the notice requirements under
10 paragraphs (2) and (3) of section 421(a), if a risk assess-
11 ment conducted in consultation with Federal law enforce-
12 ment and the attorney general of each State affected by
13 a security breach concludes that there is a de minimis risk
14 of harm to the individuals whose sensitive personally iden-
15 tifiable information was at issue in the security breach.

16 (b) FRAUD PREVENTION EXEMPTION.—A business
17 entity will be exempt from the notice requirement under
18 section 421(a) if—

- 19 (1) the nature of the sensitive personally identi-
20 fiable information subject to the security breach can-
21 not be used to facilitate transactions or facilitate
22 identity theft to further transactions with another
23 business entity that is not the business entity sub-
24 ject to the security breach notification requirements
25 of section 421;

1 (2) the business entity utilizes a security pro-
2 gram reasonably designed to block the use of the
3 sensitive personally identifiable information to ini-
4 tiate unauthorized transactions before they are
5 charged to the account of the individual; and

6 (3) the business entity has a policy in place to
7 provide notice and provides such notice after a
8 breach of the security of the system has resulted in
9 fraud or unauthorized transactions, but does not
10 necessarily require notice in other circumstances.

11 **SEC. 425. VICTIM PROTECTION ASSISTANCE.**

12 Any business entity or agency obligated to provide no-
13 tice to residents of the United States under section
14 421(a)(3) shall offer to those same residents to cover the
15 cost of—

16 (1) monthly access to a credit report for a pe-
17 riod of 1 year from the date of notice provided under
18 section 421(a)(3); and

19 (2) credit-monitoring services for up to 1 year
20 from the date of notice provided under section
21 421(a)(3).

22 **SEC. 426. ENFORCEMENT.**

23 (a) CIVIL PENALTIES.—

24 (1) IN GENERAL.—Any business entity that vio-
25 lates the provisions of sections 421 through 425

1 shall be subject to civil penalties of not more than
2 \$5,000 per violation per day, with a maximum of
3 \$55,000 per day, while such violations persist.

4 (2) INTENTIONAL OR WILLFUL VIOLATION.—A
5 business entity that intentionally or willfully violates
6 the provisions of sections 421 through 425 shall be
7 subject to additional penalties in the amount of
8 \$5,000 per violation per day, with a maximum of an
9 additional \$55,000 per day, while such violations
10 persist.

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

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

19 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
20 ERAL.—

21 (1) IN GENERAL.—Whenever it appears that a
22 business entity or agency to which this subtitle ap-
23 plies has engaged, is engaged, or is about to engage,
24 in any act or practice constituting a violation of this
25 subtitle, the Attorney General may bring a civil ac-

1 tion in an appropriate district court of the United
2 States to—

3 (A) enjoin such act or practice;

4 (B) enforce compliance with this subtitle;

5 and

6 (C) obtain damages—

7 (i) in the sum of actual damages, res-
8 titution, and other compensation on behalf
9 of the affected residents of a State; and

10 (ii) punitive damages, if the violation
11 is willful or intentional; and

12 (D) obtain such other relief as the court
13 determines to be appropriate.

14 (2) OTHER INJUNCTIVE RELIEF.—Upon a
15 proper showing in the action under paragraph (1),
16 the court shall grant a permanent injunction or a
17 temporary restraining order without bond.

18 (c) STATE ENFORCEMENT.—

19 (1) CIVIL ACTIONS.—In any case in which the
20 attorney general of a State has reason to believe
21 that an interest of the residents of that State has
22 been, or is threatened to be, adversely affected by a
23 violation of this subtitle, the State, as *parens*
24 *patriae*, may bring a civil action on behalf of the
25 residents of that State in a district court of the

1 United States of appropriate jurisdiction, or any
2 other court of competent jurisdiction, to—

3 (A) enjoin that practice;

4 (B) enforce compliance with this subtitle;

5 (C) obtain damages—

6 (i) in the sum of actual damages, res-
7 titution, and other compensation on behalf
8 of the affected residents of that State; and

9 (ii) punitive damages, if the violation
10 is willful or intentional; and

11 (D) obtain such other equitable relief as
12 the court may consider to be appropriate.

13 (2) NOTICE.—

14 (A) IN GENERAL.—Before filing an action
15 under paragraph (1), the attorney general of
16 the State involved shall provide to the Attorney
17 General—

18 (i) written notice of the action; and

19 (ii) a copy of the complaint for the ac-
20 tion.

21 (B) EXCEPTION.—

22 (i) IN GENERAL.—Subparagraph (A)
23 shall not apply with respect to the filing of
24 an action by an attorney general of a State
25 under this subsection, if the attorney gen-

1 eral of a State determines that it is not
2 feasible to provide the notice described in
3 such subparagraph before the filing of the
4 action.

5 (ii) NOTIFICATION WHEN PRAC-
6 TICABLE.—In an action described in clause
7 (i), the attorney general of a State shall
8 provide notice and a copy of the complaint
9 to the Attorney General at the time the at-
10 torney general of a State files the action.

11 (3) ATTORNEY GENERAL AUTHORITY.—Upon
12 receiving notice under paragraph (2), the Attorney
13 General shall have the right to—

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

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

19 (C) file petitions for appeal.

20 (4) PENDING PROCEEDINGS.—If the Attorney
21 General has instituted a proceeding or action for a
22 violation of this Act or any regulations thereunder,
23 no attorney general of a State may, during the pend-
24 ency of such proceeding or action, bring an action
25 under this subsection against any defendant named

1 in such criminal proceeding or civil action for any
2 violation that is alleged in that proceeding or action.

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

9 (A) conduct investigations;

10 (B) administer oaths or 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 **SEC. 427. RELATION TO STATE LAWS.**

2 (a) IN GENERAL.—Except as provided in subsection
3 (b), this title does not annul, alter, affect, or exempt any
4 person subject to the provisions of this title from com-
5 plying with the laws of any State with respect to pro-
6 tecting consumers from the risk of theft or misuse of per-
7 sonally identifiable information, except to the extent that
8 those laws are inconsistent with any provisions of this
9 title, and then only to the extent of such inconsistency.

10 (b) EXCEPTIONS.—No requirement or prohibition
11 may be imposed under the laws of any State with respect
12 to any subject matter regulated under—

13 (1) section 3(9), relating to the definition of
14 “security breach”;

15 (2) paragraphs (1)(A), (2), and (3) of sub-
16 section (a), and subsection (b) of section 421, relat-
17 ing to the right to notice of security breach;

18 (3) section 422, relating to notice procedures;

19 (4) section 423, relating to notice content, ex-
20 cept that nothing in this section shall prevent a
21 State from requiring notice of additional victim pro-
22 tection assistance by that State; and

23 (5) section 424, relating to risk assessment and
24 fraud prevention notice exemptions.

1 **SEC. 428. STUDY ON SECURING PERSONALLY IDENTIFI-**
2 **ABLE INFORMATION IN THE DIGITAL ERA.**

3 (a) REQUIREMENT FOR STUDY.—Not later than 120
4 days after the date of enactment of this Act, the Depart-
5 ment of Justice shall enter into a contract with the Na-
6 tional Research Council of the National Academies to con-
7 duct a study on securing personally identifiable informa-
8 tion in the digital era.

9 (b) MATTERS TO BE ASSESSED IN REVIEW.—The
10 study required under subsection (a) shall include—

11 (1) threats to the public posed by the unauthor-
12 ized or improper disclosure of personally identifiable
13 information, including threats to—

- 14 (A) law enforcement;
15 (B) homeland security;
16 (C) individual citizens; and
17 (D) commerce;

18 (2) an assessment of the benefits and costs of
19 currently available strategies for securing personally
20 identifiable information based on—

- 21 (A) technology;
22 (B) legislation;
23 (C) regulation; or
24 (D) public education;

25 (3) research needed to develop additional strate-
26 gies;

1 (4) recommendations for congressional or other
2 policy actions to further minimize vulnerabilities to
3 the threats described in paragraph (1); and

4 (5) other relevant issues that in the discretion
5 of the National Research Council warrant examina-
6 tion.

7 (c) TIME LINE FOR STUDY AND REQUIREMENT FOR
8 REPORT.—Not later than 18-month period beginning
9 upon completion of the performance of the contract de-
10 scribed in subsection (a), the National Research Council
11 shall conduct the study and report its findings, conclu-
12 sions, and recommendations to Congress.

13 (d) FEDERAL DEPARTMENT AND AGENCY COMPLI-
14 ANCE.—Federal departments and agencies shall comply
15 with requests made by the National Science Foundation,
16 National Research Council, and National Academies for
17 information that is necessary to assist in preparing the
18 report required by subsection (c).

19 (e) AUTHORIZATION OF APPROPRIATIONS.—Of the
20 amounts authorized to be appropriated to the Department
21 of Justice for Department-wide activities, \$850,000 shall
22 be made available to carry out the provisions of this sec-
23 tion for fiscal year 2006.

1 **SEC. 429. AUTHORIZATION OF APPROPRIATIONS.**

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

7 **SEC. 430. EFFECTIVE DATE.**

8 This subtitle shall take effect 90 days after the date
9 of enactment of this Act.

10 **TITLE V—PROTECTION OF**
11 **SOCIAL SECURITY NUMBERS**

12 **SEC. 501. SOCIAL SECURITY NUMBER PROTECTION.**

13 (a) IN GENERAL.—No person may—

14 (1) display any individual's social security num-
15 ber to a third party without the voluntary and af-
16 firmatively expressed consent of such individual; or

17 (2) sell or purchase any social security number
18 of an individual without the voluntary and affirma-
19 tively expressed consent of such individual.

20 (b) PREREQUISITES FOR CONSENT.—To obtain the
21 consent of an individual under paragraphs (1) or (2) of
22 subsection (a), the person displaying, selling, or attempt-
23 ing to sell, purchasing, or attempting to purchase the so-
24 cial security number of such individual shall—

25 (1) inform such individual of the general pur-
26 pose for which the social security number will be

1 used, the types of persons to whom the social secu-
2 rity number may be available, and the scope of
3 transactions permitted by the consent; and

4 (2) obtain the affirmatively expressed consent
5 (electronically or in writing) of such individual.

6 (c) HARVESTED SOCIAL SECURITY NUMBERS.—Sub-
7 section (a) shall apply to any public record of a Federal
8 agency that contains social security numbers extracted
9 from other public records for the purpose of displaying
10 or selling such numbers to the general public.

11 (d) EXCEPTIONS.—Nothing in this section shall be
12 construed to prohibit or limit the display, sale, or purchase
13 of a social security number—

14 (1) as required, authorized, or excepted under
15 Federal law;

16 (2) to the extent necessary for a public health
17 purpose, including the protection of the health or
18 safety of an individual in an emergency situation;

19 (3) to the extent necessary for a national secu-
20 rity purpose;

21 (4) to the extent necessary for a law enforce-
22 ment purpose, including the investigation of fraud
23 and the enforcement of a child support obligation;

24 (5) to the extent necessary for research con-
25 ducted for the purpose of advancing public knowl-

1 edge, on the condition that the researcher provides
2 adequate assurances that—

3 (A) the social security numbers will not be
4 used to harass, target, or publicly reveal infor-
5 mation concerning any individual;

6 (B) information about individuals obtained
7 from the research will not be used to make deci-
8 sions that directly affect the rights, benefits, or
9 privileges of specific individuals; and

10 (C) the researcher has in place appropriate
11 safeguards to protect the privacy and confiden-
12 tiality of any information about individuals;

13 (6) if such a number is required to be sub-
14 mitted as part of the process for applying for any
15 type of Federal, State, or local government benefit
16 or program;

17 (7) when the transmission of the number is in-
18 cidental to, and in the course of, the sale, lease,
19 franchising, or merger of all or a portion of a busi-
20 ness; or

21 (8) to the extent only the last 4 digits of a so-
22 cial security number are displayed.

1 **SEC. 502. LIMITS ON PERSONAL DISCLOSURE OF SOCIAL**
2 **SECURITY NUMBERS FOR COMMERCIAL**
3 **TRANSACTIONS AND ACCOUNTS.**

4 (a) IN GENERAL.—Part A of title XI of the Social
5 Security Act (42 U.S.C. 1301 et seq.) is amended by add-
6 ing the following:

7 **“SEC. 1150A. LIMITS ON PERSONAL DISCLOSURE OF SOCIAL**
8 **SECURITY NUMBERS FOR COMMERCIAL**
9 **TRANSACTIONS AND ACCOUNTS.**

10 “(a) ACCOUNT NUMBERS.—

11 “(1) IN GENERAL.—A business entity may
12 not—

13 “(A) require an individual to use the social
14 security number of such individual as an ac-
15 count number or account identifier when pur-
16 chasing a commercial good or service; or

17 “(B) deny an individual goods or services
18 for refusing to accept the use of the social secu-
19 rity number of such individual as an account
20 number or account identifier.

21 “(2) EXISTING ACCOUNT EXCEPTION.—Para-
22 graph (1) shall not apply to any account number or
23 account identifier established prior to the date of en-
24 actment of this Act.

25 “(b) SOCIAL SECURITY NUMBER PREREQUISITES
26 FOR GOODS AND SERVICES.—A business entity may not

1 require an individual to provide the social security number
2 of such individual when purchasing a commercial good or
3 service or deny an individual goods or services for refusing
4 to provide that number except for any purpose relating
5 to—

6 “(1) obtaining a consumer report for any pur-
7 pose permitted under the Fair Credit Reporting Act
8 (15 U.S.C. 1681 et seq.);

9 “(2) a background check of the individual con-
10 ducted by a landlord, lessor, employer, or voluntary
11 service agency;

12 “(3) law enforcement; or

13 “(4) a Federal, State, or local law requirement.

14 “(c) APPLICATION OF CIVIL MONEY PENALTIES.—
15 A violation of this section shall be deemed to be a violation
16 of section 1129(a).

17 “(d) APPLICATION OF CRIMINAL PENALTIES.—A vio-
18 lation of this section shall be deemed to be a violation of
19 section 208(a)(8).”.

20 **SEC. 503. PUBLIC RECORDS.**

21 (a) IN GENERAL.—Except as provided in paragraph
22 (2), paragraphs (a) and (b) of section 501 shall apply to
23 all public records posted on the Internet or provided in
24 an electronic medium by, or on behalf of, a Federal agen-
25 cy.

1 (b) EXCEPTIONS.—

2 (1) TRUNCATION AND PRIOR DISPLAYS.—Sec-
3 tion 501(a) shall not apply to—

4 (A) a public record which displays only the
5 last 4 digits of the social security number of an
6 individual; and

7 (B) any record or a category of public
8 records first posted on the Internet or provided
9 in an electronic medium by, or on behalf of, a
10 Federal agency prior to the date of enactment
11 of this Act.

12 (2) LAW ENFORCEMENT.—Nothing in this sub-
13 section shall be construed to prevent an entity acting
14 pursuant to a police investigation or regulatory
15 power of a domestic governmental unit from access-
16 ing the full social security number of an individual.

17 **SEC. 504. TREATMENT OF SOCIAL SECURITY NUMBERS ON**
18 **GOVERNMENT CHECKS AND PROHIBITION OF**
19 **INMATE ACCESS.**

20 (a) PROHIBITION OF USE OF SOCIAL SECURITY
21 NUMBERS ON CHECKS ISSUED FOR PAYMENT BY GOV-
22 ERNMENTAL ENTITIES.—

23 (1) IN GENERAL.—Section 205(c)(2)(C) of the
24 Social Security Act (42 U.S.C. 405(c)(2)(C)) is
25 amended by adding at the end the following:

1 “(x) No Federal, State, or local agency may
2 display the social security account number of any in-
3 dividual, or any derivative of such number, on any
4 check issued for any payment by the Federal, State,
5 or local agency.”.

6 (2) EFFECTIVE DATE.—The amendment made
7 under paragraph (1) shall apply with respect to
8 checks issued after the date that is 3 years after the
9 date of enactment of this Act.

10 (b) PROHIBITION ON INMATE ACCESS TO SOCIAL SE-
11 CURITY NUMBERS.—

12 (1) IN GENERAL.—Section 205(c)(2)(C) of the
13 Social Security Act (42 U.S.C. 405(c)(2)(C)), as
14 amended by subsection (b), is further amended by
15 adding at the end the following:

16 “(xi)(I) No Federal, State, or local agency may
17 employ, or enter into a contract for the use or em-
18 ployment of, prisoners in any capacity that would
19 allow such prisoners access to the social security ac-
20 count numbers of other individuals.

21 “(II) For purposes of this clause, the term
22 ‘prisoner’ means an individual confined in a jail,
23 prison, or other penal institution or correctional fa-
24 cility pursuant to conviction of such individual of a
25 criminal offense.”.

1 (2) **EFFECTIVE DATE.**—The amendment made
2 under paragraph (1) shall apply with respect to em-
3 ployment of prisoners, or entry into contract with
4 prisoners, after the date that is 1 year after the date
5 of enactment of this Act.

6 **SEC. 505. STUDY AND REPORT.**

7 (a) **BY THE COMPTROLLER GENERAL.**—The Comp-
8 troller General of the United States (in this section re-
9 ferred to as the “Comptroller General”) shall conduct a
10 study and prepare a report on—

11 (1) all of the uses of social security numbers
12 permitted, required, authorized, or excepted under
13 any Federal law; and

14 (2) the uses of social security numbers in Fed-
15 eral, State, and local public records.

16 (b) **CONTENT OF REPORT.**—The report required
17 under subsection (a) shall—

18 (1) identify users of social security numbers
19 under Federal law;

20 (2) include a detailed description of the uses al-
21 lowed as of the date of enactment of this Act;

22 (3) describe the impact of such uses on privacy
23 and data security;

1 (4) evaluate whether such uses should be con-
2 tinued or discontinued by appropriate legislative ac-
3 tion;

4 (5) examine whether States are complying with
5 prohibitions on the display and use of social security
6 numbers—

7 (A) under the Privacy Act of 1974 (5
8 U.S.C. 552a et seq.); and

9 (B) the Driver's Privacy Protection Act of
10 1994 (18 U.S.C. 2721 et seq.);

11 (6) include a review of the uses of social secu-
12 rity numbers in Federal, State, or local public
13 records;

14 (7) include a review of the manner in which
15 public records are stored (with separate reviews for
16 both paper records and electronic records);

17 (8) include a review of the advantages, utility,
18 and disadvantages of public records that contain so-
19 cial security numbers, including—

20 (A) impact on law enforcement;

21 (B) threats to homeland security; and

22 (C) impact on personal privacy and secu-
23 rity;

24 (9) include an assessment of the costs and ben-
25 efits to State and local governments of truncating,

1 redacting, or removing social security numbers from
2 public records, including a review of current tech-
3 nologies and procedures for truncating, redacting, or
4 removing social security numbers from public
5 records (with separate assessments for both paper
6 and electronic records);

7 (10) include an assessment of the benefits and
8 costs to businesses, non-profit organizations, and the
9 general public of requiring truncation, redaction, or
10 removal of social security numbers on public records
11 (with separate assessments for both paper and elec-
12 tronic records);

13 (11) include an assessment of Federal and
14 State requirements to truncate social security num-
15 bers, and issue recommendations on—

16 (A) how to harmonize those requirements;

17 and

18 (B) whether to further extend truncation
19 requirements, taking into consideration the im-
20 pact on accuracy and use;

21 (12) include recommendations regarding wheth-
22 er subsection (a) should apply to any record or cat-
23 egory of public records first posted on the Internet
24 or provided in an electronic medium by, or on behalf

1 of, a Federal agency prior to the date of enactment
2 of this Act; and

3 (13) include such recommendations for legisla-
4 tion based on criteria the Comptroller General deter-
5 mines to be appropriate.

6 (c) **REQUIRED CONSULTATION.**—In developing the
7 report required under this subsection, the Comptroller
8 General shall consult with—

9 (1) the Administrative Office of the United
10 States Courts;

11 (2) the Conference of State Court Administra-
12 tors;

13 (3) the Department of Justice;

14 (4) the Department of Homeland Security;

15 (5) the Social Security Administration;

16 (6) State and local governments that store,
17 maintain, or disseminate public records; and

18 (7) other stakeholders, including members of
19 the private sector who routinely use public records
20 that contain social security numbers.

21 (d) **TIMING OF REPORT.**—Not later than 1 year after
22 the date of enactment of this Act, the Comptroller General
23 shall report to Congress its findings under this section.

24 **SEC. 506. ENFORCEMENT.**

25 (a) **CIVIL PENALTIES.**—

1 (1) IN GENERAL.—Any person that violates the
2 provisions of sections 501 or 502 shall be subject to
3 civil penalties of not more than \$5,000 per violation
4 per day, with a maximum of \$35,000 per day, while
5 such violations persist.

6 (2) INTENTIONAL OR WILLFUL VIOLATION.—
7 Any person who intentionally or willfully violates the
8 provisions of sections 501 or 502 shall be subject to
9 additional penalties in the amount of \$5,000 per vio-
10 lation per day, with a maximum of an additional
11 \$35,000 per day, while such violations persist.

12 (3) EQUITABLE RELIEF.—Any person who en-
13 engages in interstate commerce that violates this sec-
14 tion may be enjoined from further violations by a
15 court of competent jurisdiction.

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

20 (b) INJUNCTIVE ACTIONS BY THE ATTORNEY GEN-
21 ERAL.—

22 (1) IN GENERAL.—Whenever it appears that a
23 person to which this title applies has engaged, is en-
24 gaged, or is about to engage, in any act or practice
25 constituting a violation of this title, the Attorney

1 General may bring a civil action in an appropriate
2 district court of the United States to—

3 (A) enjoin such act or practice;

4 (B) enforce compliance with this title; and

5 (C) obtain damages—

6 (i) in the sum of actual damages, res-
7 titution, and other compensation on behalf
8 of the affected residents of a State; and

9 (ii) punitive damages, if the violation
10 is willful or intentional; and

11 (D) obtain such other relief as the court
12 determines to be appropriate.

13 (2) OTHER INJUNCTIVE RELIEF.—Upon a
14 proper showing in the action under paragraph (1),
15 the court shall grant a permanent injunction or a
16 temporary restraining order without bond.

17 (c) STATE ENFORCEMENT.—

18 (1) CIVIL ACTIONS.—In any case in which the
19 attorney general of a State has reason to believe
20 that an interest of the residents of that State has
21 been or is threatened or adversely affected by an act
22 or practice that violates this section, the State may
23 bring a civil action on behalf of the residents of that
24 State in a district court of the United States of ap-

1 appropriate jurisdiction, or any other court of com-
2 petent jurisdiction, to—

3 (A) enjoin that act or practice;

4 (B) enforce compliance with this Act;

5 (C) obtain damages, restitution, or other
6 compensation on behalf of residents of that
7 State; or

8 (D) obtain such other legal and equitable
9 relief as the court may consider to be appro-
10 priate.

11 (2) NOTICE.—

12 (A) IN GENERAL.—Before filing an action
13 under this subsection, the attorney general of
14 the State involved shall provide to the Attorney
15 General—

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

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

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

1 (C) NOTIFICATION WHEN PRACTICABLE.—

2 In an action described under subparagraph (B),
3 the attorney general of a State shall provide the
4 written notice and the copy of the complaint to
5 the Attorney General as soon after the filing of
6 the complaint as practicable.

7 (3) ATTORNEY GENERAL AUTHORITY.—Upon
8 receiving notice under paragraph (2), the Attorney
9 General shall have the right to—

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

13 (B) intervene in an action brought under
14 paragraph (1); and

15 (C) file petitions for appeal.

16 (4) PENDING PROCEEDINGS.—If the Attorney
17 General has instituted a proceeding or action for a
18 violation of this Act or any regulations thereunder,
19 no attorney general of a State may, during the pend-
20 ency of such proceeding or action, bring an action
21 under this subsection against any defendant named
22 in such criminal proceeding or civil action for any
23 violation that is alleged in that proceeding or action.

24 (5) RULE OF CONSTRUCTION.—For purposes of
25 bringing any civil action under paragraph (1), noth-

1 ing in this Act shall be construed to prevent an at-
2 torney general of a State from exercising the powers
3 conferred on the attorney general by the laws of that
4 State to—

5 (A) conduct investigations;

6 (B) administer oaths and affirmations;

7 (C) or compel the attendance of witnesses
8 or the production of documentary and other evi-
9 dence.

10 (6) VENUE; SERVICE OF PROCESS.—

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

16 (B) SERVICE OF PROCESS.—In an action
17 brought under this subsection process may be
18 served in any district in which the defendant—

19 (i) is an inhabitant; or

20 (ii) may be found.

21 **SEC. 507. RELATION TO STATE LAWS.**

22 (a) IN GENERAL.—Except as provided in subsection
23 (b), this title does not annul, alter, affect, or exempt any
24 person subject to the provisions of this title from com-
25 plying with the laws of any State with respect to pro-

1 tecting and securing social security numbers, except to the
2 extent that those laws are inconsistent with any provisions
3 of this title, and then only to the extent of such inconsis-
4 tency.

5 (b) EXCEPTIONS.—No requirement or prohibition
6 may be imposed under the laws of any State with respect
7 to any subject matter regulated under—

8 (1) section 501(b), relating to prerequisites for
9 consent for the display, sale, or purchase of social
10 security numbers;

11 (2) section 501(c), relating to harvesting of so-
12 cial security numbers; and

13 (3) section 504, relating to treatment of social
14 security numbers on government checks and prohibi-
15 tion of inmate access.

16 **TITLE VI—GOVERNMENT AC-**
17 **CESS TO AND USE OF COM-**
18 **MERCIAL DATA**

19 **SEC. 601. GENERAL SERVICES ADMINISTRATION REVIEW**
20 **OF CONTRACTS.**

21 (a) IN GENERAL.—In considering contract awards
22 entered into after the date of enactment of this Act, the
23 Administrator of the General Services Administration
24 shall evaluate—

1 (1) the program of a contractor to ensure the
2 privacy and security of data containing personally
3 identifiable information;

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

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

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

13 (b) PENALTIES.—In awarding contracts for products
14 or services related to access, use, compilation, distribution,
15 processing, analyzing, or evaluating personally identifiable
16 information, the Administrator of the General Services
17 Administration shall include the following:

18 (1) Monetary or other penalties—

19 (A) for failure to comply with subtitles A
20 and B of title IV of this Act;

21 (B) if a contractor knows or has reason to
22 know that the personally identifiable informa-
23 tion being provided is inaccurate, and provides
24 such inaccurate information; or

1 (C) if a contractor is notified by an indi-
2 vidual that the personally identifiable informa-
3 tion being provided is inaccurate and it is in
4 fact inaccurate.

5 (2) Accuracy update requirements that obligate
6 a contractor to provide notice to the Federal depart-
7 ment or agency of any changes or corrections to the
8 personally identifiable information provided under
9 the contract.

10 **SEC. 602. REQUIREMENT TO AUDIT INFORMATION SECU-**
11 **RITY PRACTICES OF CONTRACTORS AND**
12 **THIRD PARTY BUSINESS ENTITIES.**

13 Section 3544(b) of title 44, United States Code, is
14 amended—

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

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

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

20 “(9) procedures for evaluating and auditing the
21 information security practices of contractors or third
22 party business entities supporting the information
23 systems or operations of the agency involving per-
24 sonally identifiable information, and ensuring reme-
25 dial action to address any significant deficiencies.”.

1 **SEC. 603. 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 commercial entity (other than news
15 reporting or telephone directories).”.

16 (b) LIMITATION.—Notwithstanding any other provi-
17 sion of law, commencing 60 days after the date of enact-
18 ment of this Act, no Federal department or agency may
19 procure or access any commercially available database
20 consisting primarily of personally identifiable information
21 concerning United States persons (other than news report-
22 ing or telephone directories) unless the head of such de-
23 partment or agency—

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

1 (44 U.S.C. 3501 note), which shall include a de-
2 scription of—

3 (A) such database;

4 (B) the name of the commercial entity
5 from whom it is obtained; and

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

7 (2) adopts regulations that specify—

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

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

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

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

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

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

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

5 (H) mechanisms, if any, for the enforce-
6 ment and independent oversight of existing or
7 planned procedures, policies, or guidelines; and

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

12 (3) incorporates into the contract or other
13 agreement with the commercial entity, provisions—

14 (A) providing for penalties—

15 (i) if the entity knows or has reason
16 to know that the personally identifiable in-
17 formation being provided to the Federal
18 department or agency is inaccurate, and
19 provides such inaccurate information; or

20 (ii) if the entity is notified by an indi-
21 vidual that the personally identifiable in-
22 formation being provided to the Federal
23 department or agency is inaccurate and it
24 is in fact inaccurate; and

1 (B) requiring commercial entities to inform
2 Federal departments or agencies to which they
3 sell, disclose, or provide access to personally
4 identifiable information of any changes or cor-
5 rections to the personally identifiable informa-
6 tion.

7 (c) INDIVIDUAL SCREENING PROGRAMS.—Notwith-
8 standing any other provision of law, commencing 60 days
9 after the date of enactment of this Act, no Federal depart-
10 ment or agency may use commercial databases to imple-
11 ment an individual screening program unless such pro-
12 gram is—

13 (1) congressionally authorized; and

14 (2) subject to regulations developed by notice
15 and comment that—

16 (A) establish a procedure to enable individ-
17 uals, who suffer an adverse consequence be-
18 cause the screening system determined that
19 they might pose a security threat, to appeal
20 such determination and correct information
21 contained in the system;

22 (B) ensure that Federal and commercial
23 databases that will be used to establish the
24 identity of individuals or otherwise make assess-
25 ments of individuals under the system will not

1 produce a large number of false positives or un-
2 justified adverse consequences;

3 (C) ensure the efficacy and accuracy of all
4 of the search tools that will be used and ensure
5 that the department or agency can make an ac-
6 curate predictive assessment of those who may
7 constitute a threat;

8 (D) establish an internal oversight board
9 to oversee and monitor the manner in which the
10 system is being implemented;

11 (E) establish sufficient operational safe-
12 guards to reduce the opportunities for abuse;

13 (F) implement substantial security meas-
14 ures to protect the system from unauthorized
15 access;

16 (G) adopt policies establishing the effective
17 oversight of the use and operation of the sys-
18 tem; and

19 (H) ensure that there are no specific pri-
20 vacy concerns with the technological architec-
21 ture of the system.

22 (d) STUDY OF GOVERNMENT USE.—

23 (1) SCOPE OF STUDY.—Not later than 180
24 days after the date of enactment of this Act, the
25 Comptroller General of the United States shall con-

1 duct a study and audit and prepare a report on Fed-
2 eral agency use of commercial databases, including
3 the impact on privacy and security, and the extent
4 to which Federal contracts include sufficient provi-
5 sions to ensure privacy and security protections, and
6 penalties for failures in privacy and security prac-
7 tices.

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

10 **SEC. 604. 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
16 H of Public Law 108–447; 118 Stat. 3199) that each
17 agency designate a Chief Privacy Officer, the Department
18 of Justice shall implement such requirements by desig-
19 nating a department-wide Chief Privacy Officer, whose
20 primary role shall be to fulfill the duties and responsibil-
21 ities of Chief Privacy Officer and who shall report directly
22 to the 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 603 to
7 conduct privacy impact assessments of the use of
8 commercial data containing personally identifiable
9 information by the Department;

10 (2) promote the use of law enforcement tech-
11 nologies that sustain, rather than erode, privacy pro-
12 tections, and assure that the implementation of such
13 technologies relating to the use, collection, and dis-
14 closure of personally identifiable information pre-
15 serve the privacy and security of such information;
16 and

17 (3) coordinate with the Privacy and Civil Lib-
18 erties Oversight Board, established in the Intel-
19 ligence Reform and Terrorism Prevention Act of
20 2004 (Public Law 108–458), in implementing para-
21 graphs (1) and (2) of this subsection.