

110TH CONGRESS
2D SESSION

H. R. 7118

To protect citizens and legal residents of the United States from unreasonable searches and seizures of electronic equipment at the border, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

SEPTEMBER 26, 2008

Mr. SMITH of Washington introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on the Judiciary, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To protect citizens and legal residents of the United States from unreasonable searches and seizures of electronic equipment at the border, and for other purposes.

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

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Travelers’ Privacy Pro-
5 tection Act of 2008”.

6 **SEC. 2. FINDINGS.**

7 Congress finds the following:

1 (1) Law-abiding citizens and legal residents of
2 the United States, regardless of their race, ethnicity,
3 religion, or national origin, have a reasonable expect-
4 ation of privacy in the contents of their laptops, cell
5 phones, personal handheld devices, and other elec-
6 tronic equipment.

7 (2) The Department of Homeland Security has
8 taken the position that laptops and other electronic
9 devices should not be treated any differently from
10 suitcases or other “closed containers” and may be
11 inspected by customs or immigration agents at the
12 border or in international airports without suspicion
13 of wrongdoing.

14 (3) The Department of Homeland Security pub-
15 lished a policy on July 16, 2008, allowing customs
16 and immigration agents at the border and in inter-
17 national airports to “detain” electronic equipment
18 and “review and analyze” the contents of electronic
19 equipment “absent individualized suspicion”. The
20 policy applies to any person entering the United
21 States, including citizens and other legal residents of
22 the United States returning from overseas travel.

23 (4) The privacy interest in the contents of a
24 laptop computer differs in kind and in amount from

1 the privacy interest in other “closed containers” for
2 many reasons, including the following:

3 (A) Unlike any other “closed container”
4 that can be transported across the border,
5 laptops and similar electronic devices can con-
6 tain the equivalent of a full library of informa-
7 tion about a person, including medical records,
8 financial records, e-mails and other personal
9 and business correspondence, journals, and
10 privileged work product.

11 (B) Most people do not know, and cannot
12 control, all of the information contained on
13 their laptops, such as records of websites pre-
14 viously visited and deleted files.

15 (C) Electronic search tools render searches
16 of electronic equipment more invasive than
17 searches of physical locations or objects.

18 (5) Requiring citizens and other legal residents
19 of the United States to submit to a government re-
20 view and analysis of thousands of pages of their
21 most personal information without any suspicion of
22 wrongdoing is incompatible with the values of liberty
23 and personal freedom on which the United States
24 was founded.

1 (6) Searching the electronic equipment of per-
2 sons for whom no individualized suspicion exists is
3 an inefficient and ineffective use of limited law en-
4 forcement resources.

5 (7) Some citizens and legal residents of the
6 United States who have been subjected to electronic
7 border searches have reported being asked inappro-
8 priate questions about their religious practices, polit-
9 ical beliefs, or national allegiance, indicating that the
10 search may have been premised in part on percep-
11 tions about their race, ethnicity, religion, or national
12 origin.

13 (8) Targeting citizens and legal residents of the
14 United States for electronic border searches based
15 on race, ethnicity, religion, or national origin is
16 wholly ineffective as a matter of law enforcement
17 and repugnant to the values and constitutional prin-
18 ciples of the United States.

19 **SEC. 3. DEFINITIONS.**

20 In this Act:

21 (1) **BORDER.**—The term “border” includes the
22 border and the functional equivalent of the border.

23 (2) **COPIES.**—The term “copies”, as applied to
24 the contents of electronic equipment, includes print-
25 outs, electronic copies or images, or photographs of,

1 or notes reproducing or describing, any contents of
2 the electronic equipment.

3 (3) CONTRABAND.—The term “contraband”
4 means any item the importation of which is prohib-
5 ited by the laws enforced by officials of the Depart-
6 ment of Homeland Security.

7 (4) ELECTRONIC EQUIPMENT.—The term “elec-
8 tronic equipment” has the meaning given the term
9 “computer” in section 1030(e)(1) of title 18, United
10 States Code.

11 (5) FOREIGN INTELLIGENCE INFORMATION.—
12 The term “foreign intelligence information” means
13 information described in section 101(e)(1) of the
14 Foreign Intelligence Surveillance Act of 1978 (50
15 U.S.C. 1801(e)(1)).

16 (6) FOREIGN INTELLIGENCE SURVEILLANCE
17 COURT.—The term “Foreign Intelligence Surveil-
18 lance Court” means the court established under sec-
19 tion 103(a) of the Foreign Intelligence Surveillance
20 Act of 1978 (50 U.S.C. 1803(a)).

21 (7) OFFICIALS OF THE DEPARTMENT OF HOME-
22 LAND SECURITY.—The term “officials of the Depart-
23 ment of Homeland Security” means officials and
24 employees of the Department of Homeland Security,
25 including officials and employees of U.S. Customs

1 and Border Protection and U.S. Immigration and
2 Customs Enforcement, who are authorized to con-
3 duct searches at the border.

4 (8) PERMANENTLY DESTROYED.—The term
5 “permanently destroyed”, with respect to informa-
6 tion stored electronically, means the information has
7 been deleted and cannot be reconstructed or re-
8 trieved through any means.

9 (9) REASONABLE SUSPICION.—The term “rea-
10 sonable suspicion” means a suspicion that has a par-
11 ticularized and objective basis.

12 (10) SEARCH.—

13 (A) IN GENERAL.—The term “search”
14 means any inspection of any of the contents of
15 any electronic equipment, including a visual
16 scan of icons or file names.

17 (B) EXCEPTION.—The term “search” does
18 not include asking a person to turn electronic
19 equipment on or off or to engage in similar ac-
20 tions to ensure that the electronic equipment is
21 not itself dangerous.

22 (11) SEIZURE.—

23 (A) IN GENERAL.—The term “seizure”
24 means the retention of electronic equipment or

1 copies of any contents of electronic equipment
2 for a period longer than 24 hours.

3 (B) EXCEPTIONS.—The term “seizure”
4 does not include the retention of electronic
5 equipment or copies of any contents of elec-
6 tronic equipment—

7 (i) for a period of not more than 3
8 days after the expiration of the 24-hour
9 period specified in section 5(e) if an appli-
10 cation for a warrant is being prepared or
11 pending in a district court of the United
12 States;

13 (ii) for a period of not more than 21
14 days after the expiration of the 24-hour
15 period specified in section 5(e) if an appli-
16 cation for an order from the Foreign Intel-
17 ligence Surveillance Court with respect to
18 such equipment or copies is being pre-
19 pared; or

20 (iii) if an application for an order
21 from the Foreign Intelligence Surveillance
22 Court with respect to such equipment or
23 copies is pending before that Court.

24 (12) UNITED STATES RESIDENT.—The term
25 “United States resident” means a United States cit-

1 izen, an alien lawfully admitted for permanent resi-
2 dence under section 245 of the Immigration and Na-
3 tionality Act (8 U.S.C. 1255), or a nonimmigrant
4 alien described in section 101(a)(15) of such Act (8
5 U.S.C. 1101(a)(15)) who is lawfully residing in the
6 United States.

7 **SEC. 4. STANDARDS FOR SEARCHES AND SEIZURES.**

8 (a) SEARCHES.—Except as provided in subsection
9 (c), electronic equipment transported by a United States
10 resident may be searched at the border only if an official
11 of the Department of Homeland Security has a reasonable
12 suspicion that the resident—

13 (1) is carrying contraband or is otherwise
14 transporting goods or persons in violation of the
15 laws enforced by officials of the Department of
16 Homeland Security; or

17 (2) is inadmissible or otherwise not entitled to
18 enter the United States under the laws enforced by
19 officials of the Department of Homeland Security.

20 (b) SEIZURES.—Except as provided in subsection (c),
21 electronic equipment transported by a United States resi-
22 dent may be seized at the border only if—

23 (1) the Secretary of Homeland Security obtains
24 a warrant based on probable cause to believe that
25 the equipment contains information or evidence rel-

1 evant to a violation of any law enforced by the De-
2 partment of Homeland Security;

3 (2) another Federal, State, or local law enforce-
4 ment agency obtains a warrant based on probable
5 cause to believe that the equipment contains infor-
6 mation or evidence relevant to a violation of any law
7 enforced by that agency; or

8 (3) an agency or department of the United
9 States obtains an order from the Foreign Intel-
10 ligence Surveillance Court authorizing the seizure of
11 foreign intelligence information.

12 (c) EXCEPTIONS.—Nothing in this Act shall be con-
13 strued to affect the authority of any law enforcement offi-
14 cial to conduct a search incident to arrest, a search based
15 upon voluntary consent, or any other search predicated on
16 an established exception, other than the exception for bor-
17 der searches, to the warrant requirement of the fourth
18 amendment to the Constitution of the United States.

19 **SEC. 5. PROCEDURES FOR SEARCHES.**

20 (a) INITIATING SEARCH.—Before beginning a search
21 of electronic equipment transported by a United States
22 resident at the border, the official of the Department of
23 Homeland Security initiating the search shall—

24 (1) obtain supervisory approval to engage in the
25 search;

1 (2) record—

2 (A) the nature of the reasonable suspicion
3 and the specific basis or bases for that sus-
4 picion;

5 (B) if travel patterns are cited as a basis
6 for suspicion, the specific geographic area or
7 areas of concern to which the resident traveled;

8 (C) the age of the resident;

9 (D) the sex of the resident;

10 (E) the country of origin of the resident;

11 (F) the citizenship or immigration status
12 of the resident; and

13 (G) the race or ethnicity of the resident, as
14 perceived by the official of the Department of
15 Homeland Security initiating the search.

16 (b) CONDITIONS OF SEARCH.—

17 (1) PRESENCE OF UNITED STATES RESI-
18 DENT.—The United States resident transporting the
19 electronic equipment to be searched shall be per-
20 mitted to remain present during the search, whether
21 the search occurs on- or off-site.

22 (2) PRESENCE OF OFFICIALS OF THE DEPART-
23 MENT OF HOMELAND SECURITY.—Not fewer than 2
24 officials of the Department of Homeland Security,

1 including 1 supervisor, shall be present during the
2 search.

3 (3) ENVIRONMENT.—The search shall take
4 place in a secure environment where only the United
5 States resident transporting the electronic equip-
6 ment and officials of the Department of Homeland
7 Security are able to view the contents of the elec-
8 tronic equipment.

9 (c) SCOPE OF SEARCH.—The search shall—

10 (1) be tailored to the reasonable suspicion re-
11 corded by the official of the Department of Home-
12 land Security before the search began; and

13 (2) be confined to documents, files, or other
14 stored electronic information that could reasonably
15 contain—

16 (A) contraband;

17 (B) evidence that the United States resi-
18 dent is transporting goods or persons in viola-
19 tion of the laws enforced by the Department of
20 Homeland Security; or

21 (C) evidence that the person is inadmis-
22 sible or otherwise not entitled to enter the
23 United States under the laws enforced by offi-
24 cials of the Department of Homeland Security.

1 (d) RECORD OF SEARCH.—At the time of the search,
2 the official or agent of the Department of Homeland Secu-
3 rity conducting the search shall record a detailed descrip-
4 tion of the search conducted, including the documents,
5 files, or other stored electronic information searched.

6 (e) CONCLUSION OF WARRANTLESS SEARCH.—At
7 the conclusion of the 24-hour period following commence-
8 ment of a search of electronic equipment or the contents
9 of electronic equipment at the border—

10 (1) no further search of the electronic equip-
11 ment or any contents of the electronic equipment is
12 permitted without a warrant or an order from the
13 Foreign Intelligence Surveillance Court authorizing
14 the seizure of the electronic equipment or the con-
15 tents of the electronic equipment; and

16 (2) except as specified in section 6, the elec-
17 tronic equipment shall immediately be returned to
18 the United States resident and any copies of the
19 contents of the electronic equipment shall be perma-
20 nently destroyed not later than 3 days after the con-
21 clusion of the search.

22 **SEC. 6. PROCEDURES FOR SEIZURES.**

23 (a) APPLICATION FOR WARRANT BY THE DEPART-
24 MENT OF HOMELAND SECURITY.—If, after completing a
25 search under section 5, an official of the Department of

1 Homeland Security has probable cause to believe that the
2 electronic equipment of a United States resident contains
3 information or evidence relevant to a violation of any law
4 enforced by the Department, the Secretary of Homeland
5 Security shall immediately apply for a warrant describing
6 with particularity the electronic equipment or contents of
7 the electronic equipment to be searched (if further search
8 is required) and the contents to be seized.

9 (b) DISCLOSURE OF INFORMATION AND APPLICA-
10 TION BY OTHER FEDERAL, STATE, OR LOCAL GOVERN-
11 MENT DEPARTMENTS OR AGENCIES.—

12 (1) DISCLOSURE TO OTHER AGENCIES OR DE-
13 PARTMENTS.—

14 (A) IN GENERAL.—If an official of the De-
15 partment of Homeland Security discovers, dur-
16 ing a search that complies with the require-
17 ments of section 5, information or evidence rel-
18 evant to a potential violation of a law with re-
19 spect to which another Federal, State, or local
20 law enforcement agency has jurisdiction, the
21 Secretary of Homeland Security may transmit a
22 copy of that information or evidence to that law
23 enforcement agency.

24 (B) FOREIGN INTELLIGENCE INFORMA-
25 TION.—If an official the Department of Home-

1 land Security discovers, during a search that
2 complies with the requirements of section 5, in-
3 formation that the Secretary of Homeland Se-
4 curity believes to be foreign intelligence infor-
5 mation, the Secretary may transmit a copy of
6 that information to the appropriate agency or
7 department of the United States.

8 (2) PROHIBITION ON TRANSMISSION OF OTHER
9 INFORMATION.—The Secretary may not transmit
10 any information or evidence with respect to the con-
11 tents of the electronic equipment other than the in-
12 formation or evidence described in paragraph (1).

13 (3) APPLICATION FOR WARRANT OR COURT
14 ORDER.—

15 (A) IN GENERAL.—A Federal, State, or
16 local law enforcement agency to which the Sec-
17 retary of Homeland Security transmits a copy
18 of information or evidence pursuant to para-
19 graph (1)(A) may use the information or evi-
20 dence as the basis for an application for a war-
21 rant authorizing the seizure of the electronic
22 equipment or any other contents of the elec-
23 tronic equipment.

24 (B) FOREIGN INTELLIGENCE INFORMA-
25 TION.—An agency or department of the United

1 States to which the Secretary transmits a copy
2 of information pursuant to paragraph (1)(B)
3 may use the information as the basis for an ap-
4 plication for an order from the Foreign Intel-
5 ligence Surveillance Court authorizing the sei-
6 zure of the electronic equipment or any con-
7 tents of the electronic equipment.

8 (c) RETENTION WHILE AN APPLICATION FOR A WAR-
9 RANT OR A COURT ORDER IS PENDING.—

10 (1) ELECTRONIC EQUIPMENT.—The Secretary
11 of Homeland Security—

12 (A) may retain possession of the electronic
13 equipment or copies of any contents of the elec-
14 tronic equipment—

15 (i) for a period not to exceed 3 days
16 after the expiration of the 24-hour period
17 specified in section 5(e) if an application
18 for a warrant described in subsection (a)
19 or subsection (b)(3)(A) is being prepared
20 or pending;

21 (ii) for a period not to exceed 21 days
22 after the expiration of the 24-hour period
23 specified in section 5(e) while an applica-
24 tion for an order from the Foreign Intel-

1 intelligence Surveillance Court described in
2 subsection (b)(3)(B) is being prepared; or
3 (iii) while an application for an order
4 from the Foreign Intelligence Surveillance
5 Court described in subsection (b)(3)(B) is
6 pending before that Court; and

7 (B) may not further search the electronic
8 equipment or the contents of the electronic
9 equipment during a period described in sub-
10 paragraph (A).

11 (2) INFORMATION TRANSMITTED TO OTHER
12 AGENCIES.—

13 (A) IN GENERAL.—Any Federal, State, or
14 local law enforcement agency that receives a
15 copy of information or evidence pursuant to
16 subsection (b)(1)(A) shall permanently destroy
17 the copy not later than 3 days after receiving
18 the copy unless the agency has obtained a war-
19 rant authorizing the seizure of the electronic
20 equipment or copies of any contents of the elec-
21 tronic equipment.

22 (B) FOREIGN INTELLIGENCE INFORMA-
23 TION.—Any agency or department of the
24 United States that receives a copy of informa-

1 tion pursuant to subsection (b)(1)(B) shall per-
2 manently destroy the copy—

3 (i) not later than 21 days after receiv-
4 ing the copy if a court order authorizing
5 the seizure of the electronic equipment or
6 copies of any contents of the electronic
7 equipment has not been obtained or denied
8 and an application for such an order is not
9 pending before the Foreign Intelligence
10 Surveillance Court; or

11 (ii) not later than 3 days after a de-
12 nial by the Foreign Intelligence Surveil-
13 lance Court of an application for a court
14 order.

15 (d) RETENTION UPON EXECUTION OF A WARRANT
16 OR COURT ORDER.—

17 (1) IN GENERAL.—Upon execution of a warrant
18 or an order of the Foreign Intelligence Surveillance
19 Court, officials of the Department of Homeland Se-
20 curity, the Federal, State, or local law enforcement
21 agency obtaining the warrant pursuant to subsection
22 (b)(3)(A), or the agency or department of the
23 United States obtaining the court order pursuant to
24 subsection (b)(3)(B), as the case may be, may retain
25 copies of the contents of the electronic equipment

1 that the warrant or court order authorizes to be
2 seized.

3 (2) DESTRUCTION OF CONTENTS NOT AUTHOR-
4 IZED TO BE SEIZED.—Copies of any contents of the
5 electronic equipment that are not authorized to be
6 seized pursuant to the warrant or court order de-
7 scribed in paragraph (1) shall be permanently de-
8 stroyed and the electronic equipment shall be re-
9 turned to the United States resident unless the war-
10 rant or court order authorizes seizure of the elec-
11 tronic equipment.

12 (e) NONRETENTION UPON DENIAL OF WARRANT OR
13 COURT ORDER.—If the application for a warrant de-
14 scribed in subsection (a) or subsection (b)(3)(A) or for a
15 court order described in subsection (b)(3)(B) is denied,
16 the electronic equipment shall be returned to the United
17 States resident and any copies of the contents of the elec-
18 tronic equipment shall be permanently destroyed not later
19 than 3 days after the denial of the warrant or court order.

20 (f) RECEIPT AND DISCLOSURE.—Any United States
21 resident whose electronic equipment is removed from the
22 resident's possession for longer than a 24-hour period
23 shall be provided with—

24 (1) a receipt;

1 (2) a statement of the rights of the resident
2 and the remedies available to the resident under this
3 Act; and

4 (3) the name and telephone number of an offi-
5 cial of the Department of Homeland Security who
6 can provide the resident with information about the
7 status of the electronic equipment.

8 **SEC. 7. PROHIBITION ON PROFILING.**

9 (a) IN GENERAL.—An official of the Department of
10 Homeland Security may not consider race, ethnicity, na-
11 tional origin, or religion in selecting United States resi-
12 dents for searches of electronic equipment or in deter-
13 mining the scope or substance of such a search except as
14 provided in subsection (b).

15 (b) EXCEPTION WITH RESPECT TO DESCRIPTIONS
16 OF PARTICULAR PERSONS.—An official of the Depart-
17 ment of Homeland Security may consider race, ethnicity,
18 national origin, or religion in selecting United States resi-
19 dent for searches of electronic equipment only to the ex-
20 tent that race, ethnicity, national origin, or religion, as
21 the case may be, is included among other factors in a de-
22 scription of a particular person for whom reasonable sus-
23 picion is present, based on factors unrelated to race, eth-
24 nicity, national origin, or religion.

25 (c) REPORTS.—

1 (1) IN GENERAL.—Not later than 1 year after
2 the date of the enactment of this Act, and annually
3 thereafter, the Inspector General and the Officer for
4 Civil Rights and Civil Liberties of the Department
5 of Homeland Security shall jointly issue a public re-
6 port that—

7 (A) assesses the compliance of the Depart-
8 ment of Homeland Security with the prohibition
9 under subsection (a);

10 (B) assesses the impact of searches of elec-
11 tronic equipment by the Department of Home-
12 land Security on racial, ethnic, national, and re-
13 ligious minorities, including whether such
14 searches have a disparate impact; and

15 (C) includes any recommendations for
16 changes to the policies and procedures of the
17 Department of Homeland Security with respect
18 to searches of electronic equipment to improve
19 the compliance of the Department with the pro-
20 hibition under subsection (a).

21 (2) RESOURCES.—The Secretary of Homeland
22 Security shall ensure that the Inspector General and
23 the Officer for Civil Rights and Civil Liberties are
24 provided the necessary staff, resources, data, and
25 documentation to issue the reports required under

1 paragraph (1), including the information described
2 in sections 5(a)(2) and 5(d) if requested by the In-
3 spector General or the Officer for Civil Rights and
4 Civil Liberties.

5 (d) SURVEY.—To facilitate an understanding of the
6 impact on racial, ethnic, national, and religious minorities
7 of searches of electronic equipment at the border, the Sec-
8 retary of Homeland Security shall conduct a random sam-
9 pling of a statistically significant number of travelers and
10 record for such travelers the demographic information de-
11 scribed in subparagraphs (C) through (G) of section
12 5(a)(2). That information shall be maintained by the De-
13 partment of Homeland Security in aggregate form only.

14 **SEC. 8. LIMITS ON ACCESS AND DISCLOSURE.**

15 (a) SCOPE.—The limitations on access and disclosure
16 set forth in this section apply to any electronic equipment,
17 copies of contents of electronic equipment, or information
18 acquired pursuant to a search of electronic equipment at
19 the border, other than such equipment, copies, or informa-
20 tion seized pursuant to a warrant or court order.

21 (b) ACCESS.—No official, employee, or agent of the
22 Department of Homeland Security or any Federal, State,
23 or local government agency or department may have ac-
24 cess to electronic equipment or copies of the contents of
25 the electronic equipment acquired pursuant to a search of

1 electronic equipment at the border other than such an offi-
2 cial, employee, or agent who requires such access in order
3 to perform a function specifically provided for under this
4 Act.

5 (c) SECURITY.—The Secretary of Homeland Security
6 and the head of any Federal, State, or local government
7 agency or departments that comes into possession of elec-
8 tronic equipment or any copies of the contents of elec-
9 tronic equipment pursuant to a search of electronic equip-
10 ment at the border shall ensure that—

11 (1) the electronic equipment is secured against
12 theft or unauthorized access; and

13 (2) any electronic copies of the contents of elec-
14 tronic equipment are encrypted or otherwise secured
15 against theft or unauthorized access.

16 (d) GENERAL PROHIBITION ON DISCLOSURE.—No
17 information acquired by officials, employees, or agents of
18 the Department of Homeland Security or any Federal,
19 State, or local government agency or department pursuant
20 to a search of electronic equipment at the border shall be
21 shared with or disclosed to any other Federal, State, or
22 local government agency or official or any private person
23 except as specifically provided in this Act.

24 (e) COURT ORDER EXCEPTION.—If the Secretary of
25 Homeland Security or any other Federal, State, or local

1 government agency or department determines that a dis-
2 closure of information that is not authorized by this Act
3 is necessary to prevent grave harm to persons or property,
4 the Secretary or agency or department, as the case may
5 be, may apply ex parte to a district court of the United
6 States for an order permitting such disclosure.

7 (f) PRIVILEGES.—Any disclosure of privileged infor-
8 mation that results directly from a search of electronic
9 equipment at the border shall not operate as a waiver of
10 the privilege.

11 (g) APPLICABILITY OF PRIVACY ACT.—The limita-
12 tions on access and disclosure under this Act supplement
13 rather than supplant any applicable limitations set forth
14 in section 552a of title 5, United States Code.

15 **SEC. 9. IMPLEMENTATION.**

16 (a) REGULATIONS.—The Secretary of Homeland Se-
17 curity shall issue regulations to carry out this Act.

18 (b) TRAINING.—The Secretary of Homeland Security
19 shall ensure that all officials and agents of the Depart-
20 ment of Homeland Security engaged in searches of elec-
21 tronic equipment at the border are thoroughly and ade-
22 quately trained in the laws and procedures related to such
23 searches.

24 (c) ACCOUNTABILITY.—The Secretary of Homeland
25 Security shall implement procedures to detect and dis-

1 cipline violations of this Act by officials, employees, and
2 agents of the Department of Homeland Security.

3 **SEC. 10. RECORDKEEPING AND REPORTING.**

4 (a) REPORTS TO CONGRESS.—

5 (1) EXISTING POLICIES AND GUIDELINES.—Not
6 later than 30 days after the date of the enactment
7 of this Act, the Secretary of Homeland Security
8 shall submit to Congress a report that includes—

9 (A) the policies and guidelines of the De-
10 partment of Homeland Security, including field
11 supervision and intelligence directives, relating
12 to searches of electronic equipment at the bor-
13 der in effect on the date of the enactment of
14 this Act;

15 (B) any training programs or materials re-
16 lating to such searches being utilized on such
17 date of enactment; and

18 (C) any personnel review and account-
19 ability procedures, or memoranda of under-
20 standing with other government agencies, relat-
21 ing to such searches in effect on such date of
22 enactment.

23 (2) UPDATED POLICIES AND GUIDELINES.—Not
24 later than 30 days after revising any of the policies,
25 guidelines, programs, materials, procedures, or

1 memoranda described in paragraph (1) or developing
2 new such policies, guidelines, programs, materials,
3 procedures, or memoranda, the Secretary of Home-
4 land Security shall submit to Congress a report con-
5 taining the revised or new policies, guidelines, pro-
6 grams, materials, procedures, or memoranda.

7 (3) INFORMATION ABOUT IMPLEMENTATION.—

8 (A) REQUESTS.—The information de-
9 scribed in subsection (b)(1)(B) and sections
10 5(a)(2) and 5(d) shall be made available to
11 Congress promptly upon the request of any
12 Member of Congress.

13 (B) REPORTS.—The information described
14 in section 5(a)(2) shall be provided to Congress
15 in aggregate form every 6 months.

16 (4) PUBLIC AVAILABILITY.—The Secretary of
17 Homeland Security shall make the information in
18 the reports required under paragraphs (1), (2), and
19 (3)(B) available to the public, but may redact any
20 information in those reports if the Secretary deter-
21 mines that public disclosure of the information
22 would cause harm to national security.

23 (b) MAINTENANCE OF RECORDS.—

24 (1) IN GENERAL.—The Secretary of Homeland
25 Security shall maintain records with respect to—

1 (A) the information described in sections
2 5(a)(2) and 5(d); and

3 (B) any disclosures of information ac-
4 quired through searches of electronic equipment
5 at the border to other agencies, officials, or pri-
6 vate persons, and the reasons for such disclo-
7 sures.

8 (2) LIMITATIONS ON ACCESS AND DISCLO-
9 SURE.—The information described in paragraph
10 (1)—

11 (A) may be used or disclosed only as spe-
12 cifically provided in this Act or another Federal
13 law and access to that information shall be lim-
14 ited to officials or agents of the Department of
15 Homeland Security who require access in order
16 to effectuate an authorized use or disclosure;
17 and

18 (B) shall be encrypted or otherwise pro-
19 tected against theft or authorized access.

20 (3) USE IN LITIGATION.—If otherwise discover-
21 able, the information in subsection (b)(1)(B) and
22 sections 5(a)(2) and 5(d) may be provided to a per-
23 son who files a civil action under section 12(a) or a
24 criminal defendant seeking to suppress evidence ob-

1 tained through a search of electronic equipment at
2 the border pursuant to section 12(d).

3 **SEC. 11. COMPENSATION FOR DAMAGE OR LOSS OF ELEC-**
4 **TRONIC EQUIPMENT.**

5 (a) IN GENERAL.—A United States resident who be-
6 lieves that the electronic equipment of the resident, or con-
7 tents of the electronic equipment, were damaged as a re-
8 sult of a search or seizure under this Act may file a claim
9 with the Secretary of Homeland Security for compensa-
10 tion. If the resident demonstrates that the search or sei-
11 zure resulted in damage to the electronic equipment or the
12 contents of the electronic equipment, the Secretary shall
13 compensate the resident for any resulting economic loss
14 using existing appropriations available for the Department
15 of Homeland Security.

16 (b) CLAIMS PROCESS.—The Secretary of Homeland
17 Security shall establish an administrative claims process
18 to handle the claims described in subsection (a). The com-
19 pensation decisions of the Secretary shall constitute final
20 agency actions for purposes of judicial review under chap-
21 ter 5 of title 5, United States Code.

22 **SEC. 12. ENFORCEMENT AND REMEDIES.**

23 (a) CIVIL ACTIONS.—

24 (1) IN GENERAL.—Any person injured by a vio-
25 lation of this Act may file a civil action in a district

1 court of the United States against the United States
2 or an individual officer or agent of the United States
3 for declaratory or injunctive relief or damages.

4 (2) STATUTE OF LIMITATIONS.—A civil action
5 under paragraph (1) shall be filed not later than 2
6 years after the later of—

7 (A) the date of the alleged violation of this

8 Act; or

9 (B) the date on which the person who files
10 the civil action reasonably should have known of
11 the alleged violation.

12 (3) DAMAGES.—A person who demonstrates
13 that the person has been injured by a violation of
14 this Act may receive liquidated damages of \$1,000
15 or actual economic damages, whichever is higher.

16 (4) SPECIAL RULE WITH RESPECT TO CIVIL AC-
17 TIONS FOR PROFILING.—In the case of a civil action
18 filed under paragraph (1) that alleges a violation of
19 section 7, proof that searches of the electronic equip-
20 ment of United States residents at the border have
21 a disparate impact on racial, ethnic, religious, or na-
22 tional minorities shall constitute prima facie evi-
23 dence of the violation.

24 (5) ATTORNEY'S FEES.—In any civil action
25 filed under paragraph (1), the district court may

1 allow a prevailing plaintiff reasonable attorney's fees
2 and costs, including expert fees.

3 (b) ADMISSIBILITY OF INFORMATION IN CRIMINAL
4 ACTIONS.—In any criminal prosecution brought in a dis-
5 trict court of the United States, the court may exclude
6 evidence obtained as a direct or indirect result of a viola-
7 tion of this Act if the exclusion would serve the interests
8 of justice.

○