

110TH CONGRESS  
2D SESSION

# S. 3612

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 SENATE OF THE UNITED STATES

SEPTEMBER 26 (legislative day, SEPTEMBER 17), 2008

Mr. FEINGOLD (for himself, Ms. CANTWELL, Mr. AKAKA, and Mr. WYDEN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

---

## 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:

8 (1) Law-abiding citizens and legal residents of  
9 the United States, regardless of their race, ethnicity,

1 religion, or national origin, have a reasonable expect-  
2 tation of privacy in the contents of their laptops, cell  
3 phones, personal handheld devices, and other elec-  
4 tronic equipment.

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

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

21 (4) The privacy interest in the contents of a  
22 laptop computer differs in kind and in amount from  
23 the privacy interest in other “closed containers” for  
24 many reasons, including the following:

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

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

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

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

23 (6) Searching the electronic equipment of per-  
24 sons for whom no individualized suspicion exists is

1 an inefficient and ineffective use of limited law en-  
2 forcement resources.

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

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

17 **SEC. 3. DEFINITIONS.**

18 In this Act:

19 (1) BORDER.—The term “border” includes the  
20 border and the functional equivalent of the border.

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

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

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

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

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

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

1 Customs Enforcement, who are authorized to con-  
2 duct searches at the border.

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

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

11 (10) SEARCH.—

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

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

21 (11) SEIZURE.—

22 (A) IN GENERAL.—The term “seizure”  
23 means the retention of electronic equipment or  
24 copies of any contents of electronic equipment  
25 for a period longer than 24 hours.

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

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

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

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

22 (12) UNITED STATES RESIDENT.—The term  
23 “United States resident” means a United States citi-  
24 zen, an alien lawfully admitted for permanent resi-  
25 dence under section 245 of the Immigration and Na-

1 tionality Act (8 U.S.C. 1255), or a nonimmigrant  
2 alien described in section 101(a)(15) of such Act (8  
3 U.S.C. 1101(a)(15)) who is lawfully residing in the  
4 United States.

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

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

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

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

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

21 (1) the Secretary of Homeland Security obtains  
22 a warrant based on probable cause to believe that  
23 the equipment contains information or evidence rel-  
24 evant to a violation of any law enforced by the De-  
25 partment of Homeland Security;

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

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

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

17          **SEC. 5. PROCEDURES FOR SEARCHES.**

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

22                  (1) obtain supervisory approval to engage in the  
23                  search;

24                  (2) record—

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

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

7 (C) the age of the resident;

8 (D) the sex of the resident;

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

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

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

15 (b) CONDITIONS OF SEARCH.—

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

21 (2) PRESENCE OF OFFICIALS OF THE DEPART-  
22 MENT OF HOMELAND SECURITY.—Not fewer than 2  
23 officials of the Department of Homeland Security,  
24 including 1 supervisor, shall be present during the  
25 search.

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

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

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

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

14                   (A) contraband;

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

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

23           (d) RECORD OF SEARCH.—At the time of the search,  
24 the official or agent of the Department of Homeland Secu-  
25 rity conducting the search shall record a detailed descrip-

1 tion of the search conducted, including the documents,  
2 files, or other stored electronic information searched.

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

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

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

19 **SEC. 6. PROCEDURES FOR SEIZURES.**

20 (a) APPLICATION FOR WARRANT BY THE DEPART-  
21 MENT OF HOMELAND SECURITY.—If, after completing a  
22 search under section 5, an official of the Department of  
23 Homeland Security has probable cause to believe that the  
24 electronic equipment of a United States resident contains  
25 information or evidence relevant to a violation of any law

1 enforced by the Department, the Secretary of Homeland  
2 Security shall immediately apply for a warrant describing  
3 with particularity the electronic equipment or contents of  
4 the electronic equipment to be searched (if further search  
5 is required) and the contents to be seized.

6 (b) DISCLOSURE OF INFORMATION AND APPLICA-  
7 TION BY OTHER FEDERAL, STATE, OR LOCAL GOVERN-  
8 MENT DEPARTMENTS OR AGENCIES.—

9 (1) DISCLOSURE TO OTHER AGENCIES OR DE-  
10 PARTMENTS.—

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

21 (B) FOREIGN INTELLIGENCE INFORMA-  
22 TION.—If an official the Department of Home-  
23 land Security discovers, during a search that  
24 complies with the requirements of section 5, in-  
25 formation that the Secretary of Homeland Se-

1           curity believes to be foreign intelligence infor-  
2           mation, the Secretary may transmit a copy of  
3           that information to the appropriate agency or  
4           department of the United States.

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

10          (3) APPLICATION FOR WARRANT OR COURT  
11          ORDER.—

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

21                 (B) FOREIGN INTELLIGENCE INFORMA-  
22                 TION.—An agency or department of the United  
23                 States to which the Secretary transmits a copy  
24                 of information pursuant to paragraph (1)(B)  
25                 may use the information as the basis for an ap-

1           plication for an order from the Foreign Intel-  
2           ligence Surveillance Court authorizing the sei-  
3           zure of the electronic equipment or any con-  
4           tents of the electronic equipment.

5           (c) RETENTION WHILE AN APPLICATION FOR A WAR-  
6 WARRANT OR A COURT ORDER IS PENDING.—

7           (1) ELECTRONIC EQUIPMENT.—The Secretary  
8 of Homeland Security—

9           (A) may retain possession of the electronic  
10 equipment or copies of any contents of the elec-  
11 tronic equipment—

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

18           (ii) for a period not to exceed 21 days  
19 after the expiration of the 24-hour period  
20 specified in section 5(e) while an applica-  
21 tion for an order from the Foreign Intel-  
22 ligence Surveillance Court described in  
23 subsection (b)(3)(B) is being prepared; or

24           (iii) while an application for an order  
25 from the Foreign Intelligence Surveillance

1 Court described in subsection (b)(3)(B) is  
2 pending before that Court; and

3 (B) may not further search the electronic  
4 equipment or the contents of the electronic  
5 equipment during a period described in sub-  
6 paragraph (A).

7 (2) INFORMATION TRANSMITTED TO OTHER  
8 AGENCIES.—

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

18 (B) FOREIGN INTELLIGENCE INFORMA-  
19 TION.—Any agency or department of the  
20 United States that receives a copy of informa-  
21 tion pursuant to subsection (b)(1)(B) shall per-  
22 manently destroy the copy—

23 (i) not later than 21 days after receiv-  
24 ing the copy if a court order authorizing  
25 the seizure of the electronic equipment or

1           copies of any contents of the electronic  
2           equipment has not been obtained or denied  
3           and an application for such an order is not  
4           pending before the Foreign Intelligence  
5           Surveillance Court; or

6                   (ii) not later than 3 days after a de-  
7           nial by the Foreign Intelligence Surveil-  
8           lance Court of an application for a court  
9           order.

10       (d) RETENTION UPON EXECUTION OF A WARRANT  
11 OR COURT ORDER.—

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

23           (2) DESTRUCTION OF CONTENTS NOT AUTHOR-  
24       IZED TO BE SEIZED.—Copies of any contents of the  
25       electronic equipment that are not authorized to be

1 seized pursuant to the warrant or court order de-  
2 scribed in paragraph (1) shall be permanently de-  
3 stroyed and the electronic equipment shall be re-  
4 turned to the United States resident unless the war-  
5 rant or court order authorizes seizure of the elec-  
6 tronic equipment.

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

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

19 (1) a receipt;

20 (2) a statement of the rights of the resident  
21 and the remedies available to the resident under this  
22 Act; and

23 (3) the name and telephone number of an offi-  
24 cial of the Department of Homeland Security who

1 can provide the resident with information about the  
2 status of the electronic equipment.

3 **SEC. 7. PROHIBITION ON PROFILING.**

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

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

20 (c) REPORTS.—

21 (1) IN GENERAL.—Not later than 1 year after  
22 the date of the enactment of this Act, and annually  
23 thereafter, the Inspector General and the Officer for  
24 Civil Rights and Civil Liberties of the Department

1 of Homeland Security shall jointly issue a public re-  
2 port that—

3 (A) assesses the compliance of the Depart-  
4 ment of Homeland Security with the prohibition  
5 under subsection (a);

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

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

17 (2) RESOURCES.—The Secretary of Homeland  
18 Security shall ensure that the Inspector General and  
19 the Officer for Civil Rights and Civil Liberties are  
20 provided the necessary staff, resources, data, and  
21 documentation to issue the reports required under  
22 paragraph (1), including the information described  
23 in sections 5(a)(2) and 5(d) if requested by the In-  
24 spector General or the Officer for Civil Rights and  
25 Civil Liberties.

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

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

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

17 (b) ACCESS.—No official, employee, or agent of the  
18 Department of Homeland Security or any Federal, State,  
19 or local government agency or department may have ac-  
20 cess to electronic equipment or copies of the contents of  
21 the electronic equipment acquired pursuant to a search of  
22 electronic equipment at the border other than such an offi-  
23 cial, employee, or agent who requires such access in order  
24 to perform a function specifically provided for under this  
25 Act.

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

7           (1) the electronic equipment is secured against  
8 theft or unauthorized access; and

9           (2) any electronic copies of the contents of elec-  
10 tronic equipment are encrypted or otherwise secured  
11 against theft or unauthorized access.

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

20          (e) COURT ORDER EXCEPTION.—If the Secretary of  
21 Homeland Security or any other Federal, State, or local  
22 government agency or department determines that a dis-  
23 closure of information that is not authorized by this Act  
24 is necessary to prevent grave harm to persons or property,  
25 the Secretary or agency or department, as the case may

1 be, may apply ex parte to a district court of the United  
2 States for an order permitting such disclosure.

3 (f) PRIVILEGES.—Any disclosure of privileged infor-  
4 mation that results directly from a search of electronic  
5 equipment at the border shall not operate as a waiver of  
6 the privilege.

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

11 **SEC. 9. IMPLEMENTATION.**

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

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

20 (c) ACCOUNTABILITY.—The Secretary of Homeland  
21 Security shall implement procedures to detect and dis-  
22 cipline violations of this Act by officials, employees, and  
23 agents of the Department of Homeland Security.

24 **SEC. 10. RECORDKEEPING AND REPORTING.**

25 (a) REPORTS TO CONGRESS.—

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

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

11           (B) any training programs or materials re-  
12 lating to such searches being utilized on such  
13 date of enactment; and

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

19           (2) UPDATED POLICIES AND GUIDELINES.—Not  
20 later than 30 days after revising any of the policies,  
21 guidelines, programs, materials, procedures, or  
22 memoranda described in paragraph (1) or developing  
23 new such policies, guidelines, programs, materials,  
24 procedures, or memoranda, the Secretary of Home-  
25 land Security shall submit to Congress a report con-

1 taining the revised or new policies, guidelines, pro-  
2 grams, materials, procedures, or memoranda.

3 (3) INFORMATION ABOUT IMPLEMENTATION.—

4 (A) REQUESTS.—The information de-  
5 scribed in subsection (b)(1)(B) and sections  
6 5(a)(2) and 5(d) shall be made available to  
7 Congress promptly upon the request of any  
8 Member of Congress.

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

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

19 (b) MAINTENANCE OF RECORDS.—

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

22 (A) the information described in sections  
23 5(a)(2) and 5(d); and

24 (B) any disclosures of information ac-  
25 quired through searches of electronic equipment

1 at the border to other agencies, officials, or pri-  
2 vate persons, and the reasons for such disclo-  
3 sures.

4 (2) LIMITATIONS ON ACCESS AND DISCLO-  
5 SURE.—The information described in paragraph  
6 (1)—

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

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

16 (3) USE IN LITIGATION.—If otherwise discover-  
17 able, the information in subsection (b)(1)(B) and  
18 sections 5(a)(2) and 5(d) may be provided to a per-  
19 son who files a civil action under section 12(a) or a  
20 criminal defendant seeking to suppress evidence ob-  
21 tained through a search of electronic equipment at  
22 the border pursuant to section 12(d).

1 **SEC. 11. COMPENSATION FOR DAMAGE OR LOSS OF ELEC-**  
2 **TRONIC EQUIPMENT.**

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

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

20 **SEC. 12. ENFORCEMENT AND REMEDIES.**

21 (a) CIVIL ACTIONS.—

22 (1) IN GENERAL.—Any person injured by a vio-  
23 lation of this Act may file a civil action in a district  
24 court of the United States against the United States  
25 or an individual officer or agent of the United States  
26 for declaratory or injunctive relief or damages.

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

4                   (A) the date of the alleged violation of this  
5 Act; or

6                   (B) the date on which the person who files  
7 the civil action reasonably should have known of  
8 the alleged violation.

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

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

21           (5) ATTORNEY'S FEES.—In any civil action  
22 filed under paragraph (1), the district court may  
23 allow a prevailing plaintiff reasonable attorney's fees  
24 and costs, including expert fees.

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

○