110TH CONGRESS
2D SESSION

S. _____

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

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

---

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Travelers' Privacy Protection Act of 2008''.

SEC. 2. FINDINGS.

Congress finds the following:

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

religion, or national origin, have a reasonable expectation of privacy in the contents of their laptops, cell phones, personal handheld devices, and other electronic equipment.

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

(3) The Department of Homeland Security published a policy on July 16, 2008, allowing customs and immigration agents at the border and in international airports to ''detain'' electronic equipment and ''review and analyze'' the contents of electronic equipment ''absent individualized suspicion''. The policy applies to any person entering the United States, including citizens and other legal residents of the United States returning from overseas travel.

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

(A) Unlike any other ''closed container'' that can be transported across the border, laptops and similar electronic devices can contain the equivalent of a full library of information about a person, including medical records, financial records, e-mails and other personal and business correspondence, journals, and privileged work product.

(B) Most people do not know, and cannot control, all of the information contained on their laptops, such as records of websites previously visited and deleted files.

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

(5) Requiring citizens and other legal residents of the United States to submit to a government review and analysis of thousands of pages of their most personal information without any suspicion of wrongdoing is incompatible with the values of liberty and personal freedom on which the United States was founded.

(6) Searching the electronic equipment of persons for whom no individualized suspicion exists is

an inefficient and ineffective use of limited law enforcement resources.

(7) Some citizens and legal residents of the United States who have been subjected to electronic border searches have reported being asked inappropriate questions about their religious practices, political beliefs, or national allegiance, indicating that the search may have been premised in part on perceptions about their race, ethnicity, religion, or national origin.

(8) Targeting citizens and legal residents of the United States for electronic border searches based on race, ethnicity, religion, or national origin is wholly ineffective as a matter of law enforcement and repugnant to the values and constitutional principles of the United States.

SEC. 3. DEFINITIONS.

In this Act:

(1) BORDER.—The term ''border'' includes the border and the functional equivalent of the border.

(2) COPIES.—The term ''copies'', as applied to the contents of electronic equipment, includes printouts, electronic copies or images, or photographs of, or notes reproducing or describing, any contents of the electronic equipment.

(3) CONTRABAND.—The term ''contraband'' means any item the importation of which is prohibited by the laws enforced by officials of the Department of Homeland Security.

(4) ELECTRONIC EQUIPMENT.—The term ''electronic equipment'' has the meaning given the term ''computer'' in section 1030(e)(1) of title 18, United States Code.

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

(6) FOREIGN INTELLIGENCE SURVEILLANCE COURT.—The term ''Foreign Intelligence Surveillance Court'' means the court established under section 103(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1803(a)).

(7) OFFICIALS OF THE DEPARTMENT OF HOMELAND SECURITY.—The term ''officials of the Department of Homeland Security'' means officials and employees of the Department of Homeland Security, including officials and employees of U.S. Customs and Border Protection and U.S. Immigration and

Customs Enforcement, who are authorized to conduct searches at the border.

(8) PERMANENTLY DESTROYED.—The term ''permanently destroyed'', with respect to information stored electronically, means the information has been deleted and cannot be reconstructed or retrieved through any means.

(9) REASONABLE SUSPICION.—The term ''reasonable suspicion'' means a suspicion that has a particularized and objective basis.

(10) SEARCH.—

(A) IN GENERAL.—The term ''search'' means any inspection of any of the contents of any electronic equipment, including a visual scan of icons or file names.

(B) EXCEPTION.—The term ''search'' does not include asking a person to turn electronic equipment on or off or to engage in similar actions to ensure that the electronic equipment is not itself dangerous.

(11) SEIZURE.—

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

(B) EXCEPTIONS.—The term ''seizure'' does not include the retention of electronic equipment or copies of any contents of electronic equipment—

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

(ii) for a period of not more than 30 days after the expiration of the 24-hour period specified in section 5(e) if an application for an order from the Foreign Intelligence Surveillance Court with respect to such equipment or copies is being prepared; or

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

(12) UNITED STATES RESIDENT.—The term ''United States resident'' means a United States citizen, an alien lawfully admitted for permanent residence under section 245 of the Immigration and Na-

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

SEC. 4. STANDARDS FOR SEARCHES AND SEIZURES.

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

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

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

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

(1) the Secretary of Homeland Security obtains a warrant based on probable cause to believe that the equipment contains information or evidence relevant to a violation of any law enforced by the Department of Homeland Security;

(2) another Federal, State, or local law enforcement agency obtains a warrant based on probable cause to believe that the equipment contains information or evidence relevant to a violation of any law enforced by that agency; or

(3) an agency or department of the United States obtains an order from the Foreign Intelligence Surveillance Court authorizing the seizure of foreign intelligence information.

(c) EXCEPTIONS.—Nothing in this Act shall be construed to affect the authority of any law enforcement official to conduct a search incident to arrest, a search based upon voluntary consent, or any other search predicated on an established exception, other than the exception for border searches, to the warrant requirement of the fourth amendment to the Constitution of the United States.

SEC. 5. PROCEDURES FOR SEARCHES.

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

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

(2) record—

(A) the nature of the reasonable suspicion and the specific basis or bases for that suspicion;

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

(C) the age of the resident;

(D) the sex of the resident;

(E) the country of origin of the resident;

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

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

(b) CONDITIONS OF SEARCH.—

(1) PRESENCE OF UNITED STATES RESIDENT.—The United States resident transporting the electronic equipment to be searched shall be permitted to remain present during the search, whether the search occurs on- or off-site.

(2) PRESENCE OF OFFICIALS OF THE DEPARTMENT OF HOMELAND SECURITY.—Not fewer than 2 officials of the Department of Homeland Security, including 1 supervisor, shall be present during the search.

(3) ENVIRONMENT.—The search shall take place in a secure environment where only the United States resident transporting the electronic equipment and officials of the Department of Homeland Security are able to view the contents of the electronic equipment.

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

(1) be tailored to the reasonable suspicion recorded by the official of the Department of Homeland Security before the search began; and

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

(A) contraband;

(B) evidence that the United States resident is transporting goods or persons in violation of the laws enforced by the Department of Homeland Security; or

(C) evidence that the person is inadmissible or otherwise not entitled to enter the United States under the laws enforced by officials of the Department of Homeland Security.

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

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

(e) CONCLUSION OF WARRANTLESS SEARCH.—At the conclusion of the 24-hour period following commencement of a search of electronic equipment or the contents of electronic equipment at the border—

(1) no further search of the electronic equipment or any contents of the electronic equipment is permitted without a warrant or an order from the Foreign Intelligence Surveillance Court authorizing the seizure of the electronic equipment or the contents of the electronic equipment; and

(2) except as specified in section 6, the electronic equipment shall immediately be returned to the United States resident and any copies of the contents of the electronic equipment shall be permanently destroyed not later than 3 days after the conclusion of the search.

SEC. 6. PROCEDURES FOR SEIZURES.

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

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

(b) DISCLOSURE OF INFORMATION AND APPLICATION BY OTHER FEDERAL, STATE, OR LOCAL GOVERNMENT DEPARTMENTS OR AGENCIES.—

(1) DISCLOSURE TO OTHER AGENCIES OR DEPARTMENTS.—

(A) IN GENERAL.—If an official of the Department of Homeland Security discovers, during a search that complies with the requirements of section 5, information or evidence relevant to a potential violation of a law with respect to which another Federal, State, or local law enforcement agency has jurisdiction, the Secretary of Homeland Security may transmit a copy of that information or evidence to that law enforcement agency.

(B) FOREIGN INTELLIGENCE INFORMATION.—If an official the Department of Homeland Security discovers, during a search that complies with the requirements of section 5, information that may be foreign intelligence in-

formation, the Secretary of Homeland Security may transmit a copy of that information to the appropriate agency or department of the United States.

(2) PROHIBITION ON TRANSMISSION OF OTHER INFORMATION.—The Secretary may not transmit any information or evidence with respect to the contents of the electronic equipment other than the information or evidence described in paragraph (1).

(3) APPLICATION FOR WARRANT OR COURT ORDER.—

(A) IN GENERAL.—A Federal, State, or local law enforcement agency to which the Secretary of Homeland Security transmits a copy of information or evidence pursuant to paragraph (1)(A) may use the information or evidence as the basis for an application for a warrant authorizing the seizure of the electronic equipment or any other contents of the electronic equipment.

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

plication for an order from the Foreign Intelligence Surveillance Court authorizing the seizure of the electronic equipment or any contents of the electronic equipment.

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

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

(A) may retain possession of the electronic equipment or copies of any contents of the electronic equipment—

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

(ii) for a period not to exceed 30 days after the expiration of the 24-hour period specified in section 5(e) while an application for an order from the Foreign Intelligence Surveillance Court described in subsection (b)(3)(B) is being prepared; or

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

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

(B) may not further search the electronic equipment or the contents of the electronic equipment during a period described in subparagraph (A).

(2) INFORMATION TRANSMITTED TO OTHER AGENCIES.—

(A) IN GENERAL.—Any Federal, State, or local law enforcement agency that receives a copy of information or evidence pursuant to subsection (b)(1)(A) shall permanently destroy the copy not later than 3 days after receiving the copy unless the agency has obtained a warrant authorizing the seizure of the electronic equipment or copies of any contents of the electronic equipment.

(B) FOREIGN INTELLIGENCE INFORMATION.—Any agency or department of the United States that receives a copy of information pursuant to subsection (b)(1)(B) shall permanently destroy the copy—

(i) not later than 30 days after receiving the copy if a court order authorizing the seizure of the electronic equipment or

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

(ii) not later than 3 days after a denial by the Foreign Intelligence Surveillance Court of an application for a court order.

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

(1) IN GENERAL.—Upon execution of a warrant or an order of the Foreign Intelligence Surveillance Court, officials of the Department of Homeland Security, the Federal, State, or local law enforcement agency obtaining the warrant pursuant to subsection (b)(3)(A), or the agency or department of the United States obtaining the court order pursuant to subsection (b)(3)(B), as the case may be, may retain copies of the contents of the electronic equipment that the warrant or court order authorizes to be seized.

(2) DESTRUCTION OF CONTENTS NOT AUTHORIZED TO BE SEIZED.—Copies of any contents of the electronic equipment that are not authorized to be

seized pursuant to the warrant or court order described in paragraph (1) shall be permanently destroyed and the electronic equipment shall be returned to the United States resident unless the warrant or court order authorizes seizure of the electronic equipment.

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

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

(1) a receipt;

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

(3) the name and telephone number of an official of the Department of Homeland Security who

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

SEC. 7. PROHIBITION ON PROFILING.

(a) IN GENERAL.—An official of the Department of Homeland Security may not consider race, ethnicity, national origin, or religion in selecting United States residents for searches of electronic equipment or in determining the scope or substance of such a search except as provided in subsection (b).

(b) EXCEPTION WITH RESPECT TO DESCRIPTIONS OF PARTICULAR PERSONS.—An official of the Department of Homeland Security may consider race, ethnicity, national origin, or religion in selecting United States resident for searches of electronic equipment only to the extent that race, ethnicity, national origin, or religion, as the case may be, is included among other factors in a description of a particular person for whom reasonable suspicion is present, based on factors unrelated to race, ethnicity, national origin, or religion.

(c) REPORTS.—

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

of Homeland Security shall jointly issue a public report that—

(A) assesses the compliance of the Department of Homeland Security with the prohibition under subsection (a);

(B) assesses the impact of searches of electronic equipment by the Department of Homeland Security on racial, ethnic, national, and religious minorities, including whether such searches have a disparate impact; and

(C) includes any recommendations for changes to the policies and procedures of the Department of Homeland Security with respect to searches of electronic equipment to improve the compliance of the Department with the prohibition under subsection (a).

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

(d) SURVEY.—To facilitate an understanding of the impact on racial, ethnic, national, and religious minorities of searches of electronic equipment at the border, the Secretary of Homeland Security shall conduct a random sampling of a statistically significant number of travelers and record for such travelers the demographic information described in subparagraphs (C) through (G) of section 5(a)(2). That information shall be maintained by the Department of Homeland Security in aggregate form only.

SEC. 8. LIMITS ON ACCESS AND DISCLOSURE.

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

(b) ACCESS.—No official, employee, or agent of the Department of Homeland Security or any Federal, State, or local government agency or department may have access to electronic equipment or copies of the contents of the electronic equipment acquired pursuant to a search of electronic equipment at the border other than such an official, employee, or agent who requires such access in order to perform a function specifically provided for under this Act.

(c) SECURITY.—The Secretary of Homeland Security and the head of any Federal, State, or local government agency or departments that comes into possession of electronic equipment or any copies of the contents of electronic equipment pursuant to a search of electronic equipment at the border shall ensure that—

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

(2) any electronic copies of the contents of electronic equipment are encrypted or otherwise secured against theft or unauthorized access.

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

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

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

(f) PRIVILEGES.—Any disclosure of privileged information that results directly from a search of electronic equipment at the border shall not operate as a waiver of the privilege.

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

SEC. 9. IMPLEMENTATION.

(a) REGULATIONS.—The Secretary of Homeland Security shall issue regulations to carry out this Act.

(b) TRAINING.—The Secretary of Homeland Security shall ensure that all officials and agents of the Department of Homeland Security engaged in searches of electronic equipment at the border are thoroughly and adequately trained in the laws and procedures related to such searches.

(c) ACCOUNTABILITY.—The Secretary of Homeland Security shall implement procedures to detect and discipline violations of this Act by officials, employees, and agents of the Department of Homeland Security.

SEC. 10. RECORDKEEPING AND REPORTING.

(a) REPORTS TO CONGRESS.—

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

(A) the policies and guidelines of the Department of Homeland Security, including field supervision and intelligence directives, relating to searches of electronic equipment at the border in effect on the date of the enactment of this Act;

(B) any training programs or materials relating to such searches being utilized on such date of enactment; and

(C) any personnel review and accountability procedures, or memoranda of understanding with other government agencies, relating to such searches in effect on such date of enactment.

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

taining the revised or new policies, guidelines, programs, materials, procedures, or memoranda.

(3) INFORMATION ABOUT IMPLEMENTATION.—

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

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

(4) PUBLIC AVAILABILITY.—The Secretary of Homeland Security shall make the information in the reports required under paragraphs (1), (2), and (3)(B) available to the public, but may redact any information in those reports if the Secretary determines that public disclosure of the information would cause harm to national security.

(b) MAINTENANCE OF RECORDS.—

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

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

(B) any disclosures of information acquired through searches of electronic equipment

at the border to other agencies, officials, or private persons, and the reasons for such disclosures.

(2) LIMITATIONS ON ACCESS AND DISCLOSURE.—The information described in paragraph (1)—

(A) may be used or disclosed only as specifically provided in this Act or another Federal law and access to that information shall be limited to officials or agents of the Department of Homeland Security who require access in order to effectuate an authorized use or disclosure; and

(B) shall be encrypted or otherwise protected against theft or authorized access.

(3) USE IN LITIGATION.—If otherwise discoverable, the information in subsection (b)(1)(B) and sections 5(a)(2) and 5(d) may be provided to a person who files a civil action under section 12(a) or a criminal defendant seeking to suppress evidence obtained through a search of electronic equipment at the border pursuant to section 12(d).

SEC. 11. COMPENSATION FOR DAMAGE OR LOSS OF ELECTRONIC EQUIPMENT.

(a) IN GENERAL.—A United States resident who believes that the electronic equipment of the resident, or contents of the electronic equipment, were damaged as a result of a search or seizure under this Act may file a claim with the Secretary of Homeland Security for compensation. If the resident demonstrates that the search or seizure resulted in damage to the electronic equipment or the contents of the electronic equipment, the Secretary shall compensate the resident for any resulting economic loss using existing appropriations available for the Department of Homeland Security.

(b) CLAIMS PROCESS.—The Secretary of Homeland Security shall establish an administrative claims process to handle the claims described in subsection (a). The compensation decisions of the Secretary shall constitute final agency actions for purposes of judicial review under chapter 5 of title 5, United States Code.

SEC. 12. ENFORCEMENT AND REMEDIES.

(a) CIVIL ACTIONS.—

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

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

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

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

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

(4) SPECIAL RULE WITH RESPECT TO CIVIL ACTIONS FOR PROFILING.—In the case of a civil action filed under paragraph (1) that alleges a violation of section 7, proof that searches of the electronic equipment of United States residents at the border have a disparate impact on racial, ethnic, religious, or national minorities shall constitute prima facie evidence of the violation.

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

(b) ADMISSIBILITY OF INFORMATION IN CRIMINAL ACTIONS.—In any criminal prosecution brought in a district court of the United States, the court may exclude evidence obtained as a direct or indirect result of a violation of this Act if the exclusion would serve the interests of justice.