

(Mr. CORZINE), the Senator from West Virginia (Mr. ROCKEFELLER), the Senator from Massachusetts (Mr. KENNEDY), the Senator from Louisiana (Ms. LANDRIEU), the Senator from Michigan (Mr. LEVIN) and the Senator from South Dakota (Mr. JOHNSON) were added as cosponsors of S. 2057, a bill to require the Secretary of Defense to reimburse members of the United States Armed Forces for certain transportation expenses incurred by the members in connection with leave under the Central Command Rest and Recuperation Leave Program before the program was expanded to include domestic travel.

S. 2076

At the request of Mr. BAUCUS, the name of the Senator from Nebraska (Mr. NELSON) was added as a cosponsor of S. 2076, a bill to amend title XI of the Social Security Act to provide direct congressional access to the office of the Chief Actuary in the Centers for Medicare & Medicaid Services.

S. 2084

At the request of Mr. ALEXANDER, the name of the Senator from Illinois (Mr. DURBIN) was added as a cosponsor of S. 2084, a bill to revive and extend the Internet Tax Freedom Act for 2 years, and for other purposes.

S. 2090

At the request of Mr. DASCHLE, the name of the Senator from Connecticut (Mr. LIEBERMAN) was added as a cosponsor of S. 2090, a bill to amend the Worker Adjustment and Retraining Notification Act to provide protections for employees relating to the offshoring of jobs.

S.J. RES. 26

At the request of Mr. ALLARD, the name of the Senator from Mississippi (Mr. LOTT) was added as a cosponsor of S.J. Res. 26, a joint resolution proposing an amendment to the Constitution of the United States relating to marriage.

S.J. RES. 28

At the request of Mr. CAMPBELL, the name of the Senator from Oklahoma (Mr. INHOFE) was added as a cosponsor of S.J. Res. 28, a joint resolution recognizing the 60th anniversary of the Allied landing at Normandy during World War II.

S. CON. RES. 81

At the request of Mrs. FEINSTEIN, the names of the Senator from Oklahoma (Mr. INHOFE) and the Senator from Oklahoma (Mr. NICKLES) were added as cosponsors of S. Con. Res. 81, a concurrent resolution expressing the deep concern of Congress regarding the failure of the Islamic Republic of Iran to adhere to its obligations under a safeguards agreement with the International Atomic Energy Agency and the engagement by Iran in activities that appear to be designed to develop nuclear weapons.

S. CON. RES. 88

At the request of Mr. SARBANES, the name of the Senator from Connecticut

(Mr. LIEBERMAN) was added as a cosponsor of S. Con. Res. 88, a concurrent resolution expressing the sense of Congress that there should continue to be parity between the adjustments in the pay of members of the uniformed services and the adjustments in the pay of civilian employees of the United States.

S. CON. RES. 90

At the request of Mr. LEVIN, the names of the Senator from Michigan (Ms. STABENOW) and the Senator from Wisconsin (Mr. FEINGOLD) were added as cosponsors of S. Con. Res. 90, a concurrent resolution expressing the sense of the Congress regarding negotiating, in the United States-Thailand Free Trade Agreement, access to the United States automobile industry.

S. RES. 298

At the request of Mr. CAMPBELL, the name of the Senator from Oregon (Mr. WYDEN) was added as a cosponsor of S. Res. 298, a resolution designating May 2004 as "National Cystic Fibrosis Awareness Month".

AMENDMENT NO. 2617

At the request of Ms. CANTWELL, the names of the Senator from Massachusetts (Mr. KENNEDY), the Senator from Michigan (Mr. LEVIN), the Senator from New York (Mr. SCHUMER), the Senator from Washington (Mrs. MURRAY), the Senator from New York (Mrs. CLINTON), the Senator from Rhode Island (Mr. REED), the Senator from Connecticut (Mr. LIEBERMAN), the Senator from Oregon (Mr. SMITH), the Senator from Delaware (Mr. BIDEN), the Senator from Indiana (Mr. BAYH), the Senator from Vermont (Mr. LEAHY) and the Senator from Maryland (Mr. SARBANES) were added as cosponsors of amendment No. 2617 proposed to S. 1805, a bill to prohibit civil liability actions from being brought or continued against manufacturers, distributors, dealers, or importers of firearms or ammunition for damages resulting from the misuse of their products by others.

At the request of Mr. BYRD, his name was added as a cosponsor of amendment No. 2617 proposed to S. 1805, *supra*.

At the request of Mrs. FEINSTEIN, her name was added as a cosponsor of amendment No. 2617 proposed to S. 1805, *supra*.

STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

By Mr. BURNS (for himself, Mr. WYDEN, and Mrs. BOXER):

S. 2131. A bill to regulate the unauthorized installation of computer software, to require clear disclosure to computer users of certain computer software features that may pose a threat to user privacy, and for other purposes; to the Committee on Commerce, Science, and Transportation.

Mr. WYDEN. Mr. President, my good friend Senator BURNS and I have pioneered a number of legislative efforts

aimed at protecting ordinary computer users from the tricks and schemes of those who would abuse the open and interconnected nature of the Internet. From online privacy to spam, we have sought to establish some basic, commonsense rules to address sleazy, intrusive, and anti-consumer practices that have arisen in the new world of the Internet. In each case, our goal has not been to stifle or restrict legitimate and innovative modes of e-commerce, but rather to promote them by reining in unfair and annoying behavior that undermines consumer confidence and use of the Internet.

Today, we continue on that path by introducing the "SPY BLOCK" Act, together with our colleague Senator BOXER.

This legislation will put the brakes on the growing problem of software being installed secretly on people's computers, for purposes they might object to if given the chance. Sometimes, the problem is a "drive-by download," where the consumer's mere visit to a website or decision to click on an advertisement secretly triggers the downloading of software onto the consumer's machine. Or, it can be a "double whammy download," where the consumer's voluntary download of one software program also triggers the inadvertent download of a second software program which, although it may serve a very different purpose, has been bundled together with the first one.

Once installed, the unwanted software operates in the background, performing functions that ordinary computer users cannot detect. As a result, the computer user may never even know the software is there, let alone what it is doing. And to add insult to injury, software that spreads in this fashion often is designed to be nearly impossible to uninstall.

What might such software do, once it is installed? The legislation we are introducing today identifies several possible functions that pose concerns. First, some software, often referred to as "spyware," collects information about the computer user and transmits that information over the Internet to the spyware's author. Second, software sometimes referred to as "adware" causes pop-up ads to appear on the user's computer, perhaps based on the user's apparent interests or on the websites he or she visits. Third, some software essentially hijacks the computer's processing and communications capability to forward spam, viruses, or other messages, all without the user's knowledge. Finally, some software changes user settings—for example, overriding the user's intended choice of homepage.

If a computer user truly understands what the software is going to do and knowingly consents to it, that's fine. The issue really comes down to user knowledge and control. Too often, software like this allows a third party to wrest control of some of the computer's functions and commandeer

them for the third party's own purposes. The software is essentially a parasite—it attaches itself without consent to the host computer and taps into the host's resources, making use of them for its own selfish purposes. Our bill would make such unauthorized practices clearly unlawful.

How common is all this? There is little hard data, but one report last year estimated that 20 million people have downloaded software that serves them targeted advertising. I have to suspect that many of these downloads did not involve informed consent. It has also been widely reported that many of the most popular peer-to-peer file sharing software programs come packaged with other software that is not clearly disclosed to the user. So the number of affected users is likely very high.

The bill we are introducing today would, for the first time, establish a clear legal principle that you cannot cause software to be installed on somebody else's computer without that person's knowledge and consent. This general notice and consent requirement could be satisfied by something as simple as an on-screen dialogue box telling the user that clicking "ok" will trigger the download of, say, a particular game program. In addition, the bill says that software must be capable of being uninstalled without resorting to extraordinary and highly technical procedures.

Beyond these general requirements, the legislation calls for certain types of software features—those performing the four functions I discussed a moment ago—to be specifically and separately brought to the user's attention prior to installation. For example, if a software program has a spyware feature designed to collect and transmit information about the user, the user would need to be provided with sufficient notice based on criteria set forth in the bill. That notice would need to explain the types of information that would be collected and the purposes for which the information would be used. Following this notice, the user would have the option of granting or withholding consent. In the absence of such notice and consent, it would be unlawful to download the software onto the user's computer, or subsequently to use the software to gather information about that user.

The bill contains some exceptions, for example, for pre-installed software and software features that are necessary to make basic features like e-mail or Internet browsing function properly. Enforcement under the bill would be by the Federal Trade Commission and state Attorneys General.

I recognize that the bill we introduce today may benefit from further attention and input on the particular wording of the definitions, on the types of software or software features that should be listed in the exceptions, and so forth. Senator BURNS, Senator BOXER, and I are open to further discussion about fine tuning the scope of

the bill, so that we don't create a regime that ends up being impractical or imposing undue burdens on legitimate and useful software. This is the starting point, not the end point.

It is important, however, to get this process moving. I believe it's time to send a clear message that unauthorized and privacy-compromising spyware, adware, and other software are unlawful and punishable. I urge my colleagues to join Senators BURNS, BOXER, and myself in supporting this bill.

Mr. BURNS. Mr. President, I rise in support of a measure that I introduce today, with the support of my colleague, Senator WYDEN. We worked closely on the CAN SPAM bill together, and after four years of effort finally saw its successful passage last year. I am pleased to work with Senator WYDEN again on another critical issue which is potentially of even greater concern than junk email given its invasive nature—that of spyware. I also appreciate the support of another of my colleagues on the Senate Commerce Committee, Senator BOXER. Together, we have crafted legislation aimed at ending the insidious operation of spyware, the SPYBLOCK Act of 2004. By introducing this legislation today, we take the first step in giving consumers the control to stop this deceitful practice.

Spyware refers to software that is downloaded onto users' computers without their knowledge or consent. This sneaky software is then often used to track the movements of consumers online or even to steal passwords. The porous gaps spyware creates in a computer's security may be difficult to close. For example, one popular peer-to-peer file sharing network routinely installs spyware to track users' information and retrieves targeted banner ads and popups. As noted by a recent article in PC Magazine these file-sharing networks may be free, but at the cost of privacy, not money. Of the 60 million users, few know they are being watched. Of those who do discover spyware, uninstalling it may prove more difficult than other software programs. Some spyware includes tricklers, which reinstall the files as you delete them. Users may think they are getting rid of the problem, but the reality of the situation is far different.

The creators of spyware have engineered the technology so that once it is installed on a computer, it is difficult and sometimes impossible to remove and in some cases requires the entire hard drive to be erased to get rid of this poisonous product. Such drastic measures must be taken, because often spyware tells the installer what websites a user visits, steals passwords or other sensitive documents on a personal computer, and also redirects Internet traffic through certain web sites.

One of the most disturbing aspects about the spyware problem is that so few consumers are even aware of it. Bearing this factor in mind, the

SPYBLOCK bill relies on a common-sense approach which prohibits the installation of software on consumers' computers without notice, consent and reasonable "uninstall" procedures.

The notice and consent approach which SPYBLOCK takes would end the practice of so-called "drive-by downloads" which some bad actors use to secretly download programs onto users' computers without their knowledge. Under SPYBLOCK, software providers must give consumers clear and conspicuous notice that a software program will be downloaded to their computers and requires user consent. This simple provision could be fulfilled by clicking "yes" on a dialog box, for example.

SPYBLOCK also requires notice and consent for other types of software. In the case of "Adware," providers are required to tell consumers what types of ads will pop up on users' screens and with what frequency. Consent is required for software that modifies user settings or uses "distributed computing" methods to utilize the processing power of individual computers to create larger networks. Finally, software providers must allow for their programs to be easily "uninstalled" by users after they are downloaded. As with the CAN-SPAM law, enforcement authority would be given to the Federal Trade Commission. States attorneys general could take action against the purveyors of spyware.

Clearly, it is time to call the bad actors to account. It is impossible to understand how any of the individuals or companies using spyware believe tracking Internet usage, stealing passwords, and hijacking the processors of someone else's computer, all without their knowledge, is justifiable.

Working closely with my colleagues Senator WYDEN and Senator BOXER, I am confident we can make major progress on this critical legislation, before spyware infects a critical mass of computers and renders them useless. Just trying to keep up with the latest anti-spyware software poses a tremendous cost to businesses, let alone individuals who have to spend their time online worried about the next spyware infestation. Again, I would like to thank Senators WYDEN and BOXER for their hard work on this vital issue, and I urge my colleagues to support this measure. I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 2131

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 "Controlling Invasive and Unauthorized Software Act".

SEC. 2. UNAUTHORIZED INSTALLATION OF COMPUTER SOFTWARE.

(a) NOTICE, CHOICE, AND UNINSTALL PROCEDURES.—It is unlawful for any person who is

not the user of a protected computer to install computer software on that computer, or to authorize, permit, or cause the installation of computer software on that computer, unless—

(1) the user of the computer has received notice that satisfies the requirements of section 3;

(2) the user of the computer has granted consent that satisfies the requirements of section 3; and

(3) the computer software's uninstall procedures satisfy the requirements of section 3.

(b) **RED HERRING PROHIBITION.**—It is unlawful for any person who is not the user of a protected computer to install computer software on that computer, or to authorize, permit, or cause the installation of computer software on that computer, if the design or operation of the computer software is intended, or may reasonably be expected, to confuse or mislead the user of the computer concerning the identity of the person or service responsible for the functions performed or content displayed by such computer software.

SEC. 3. NOTICE, CONSENT, AND UNINSTALL REQUIREMENTS.

(a) **NOTICE.**—For purposes of section 2(a)(1), notice to the user of a computer shall—

(1) include a clear notification, displayed on the screen until the user either grants or denies consent to installation, of the name and general nature of the computer software that will be installed if the user grants consent; and

(2) include a separate disclosure, with respect to each information collection, advertising, distributed computing, and settings modification feature contained in the computer software, that—

(A) remains displayed on the screen until the user either grants or denies consent to that feature;

(B) in the case of an information collection feature, provides a clear description of—

(i) the type of personal or network information to be collected and transmitted by the computer software; and

(ii) the purpose for which the personal or network information is to be collected, transmitted, and used;

(C) in the case of an advertising feature, provides—

(i) a representative full-size example of each type of advertisement that may be delivered by the computer software;

(ii) a clear description of the estimated frequency with which each type of advertisement may be delivered; and

(iii) a clear description of how the user can distinguish each type of advertisement that the computer software delivers from advertisements generated by other software, Internet website operators, or services;

(D) in the case of a distributed computing feature, provides a clear description of—

(i) the types of information or messages the computer software will cause the computer to transmit;

(ii) the estimated frequency with which the computer software will cause the computer to transmit such messages or information;

(iii) the estimated volume of such information or messages, and the likely impact, if any, on the processing or communications capacity of the user's computer; and

(iv) the nature, volume, and likely impact on the computer's processing capacity of any computational or processing tasks the computer software will cause the computer to perform in order to generate the information or messages the computer software will cause the computer to transmit;

(E) in the case of a settings modification feature, provides a clear description of the nature of the modification, its function, and

any collateral effects the modification may produce; and

(F) provides a clear description of procedures the user may follow to turn off such feature or uninstall the computer software.

(b) **CONSENT.**—For purposes of section 2(a)(2), consent requires—

(1) consent by the user of the computer to the installation of the computer software; and

(2) separate affirmative consent by the user of the computer to each information collection feature, advertising feature, distributed computing feature, and settings modification feature contained in the computer software.

(c) **UNINSTALL PROCEDURES.**—For purposes of section 2(a)(3), computer software shall—

(1) appear in the "Add/Remove Programs" menu or any similar feature, if any, provided by each operating system with which the computer software functions;

(2) be capable of being removed completely using the normal procedures provided by each operating system with which the computer software functions for removing computer software; and

(3) in the case of computer software with an advertising feature, include an easily identifiable link clearly associated with each advertisement that the software causes to be displayed, such that selection of the link by the user of the computer generates an on-screen window that informs the user about how to turn off the advertising feature or uninstall the computer software.

SEC. 4. UNAUTHORIZED USE OF CERTAIN COMPUTER SOFTWARE.

It is unlawful for any person who is not the user of a protected computer to use an information collection, advertising, distributed computing, or settings modification feature of computer software installed on that computer, if—

(1) the computer software was installed in violation of section 2;

(2) the use in question falls outside the scope of what was described to the user of the computer in the notice provided pursuant to section 3(a); or

(3) in the case of an information collection feature, the person using the feature fails to establish and maintain reasonable procedures to protect the security and integrity of personal information so collected.

SEC. 5. EXCEPTIONS.

(a) **PREINSTALLED SOFTWARE.**—A person who installs, or authorizes, permits, or causes the installation of, computer software on a protected computer before the first retail sale of the computer shall be deemed to be in compliance with this Act if the user of the computer receives notice that would satisfy section 3(a)(2) and grants consent that would satisfy section 3(b)(2) prior to—

(1) the initial collection of personal or network information, in the case of any information collection feature contained in the computer software;

(2) the initial generation of an advertisement on the computer, in the case of any advertising feature contained in the computer software;

(3) the initial transmission of information or messages, in the case of any distributed computing feature contained in the computer software; and

(4) the initial modification of user settings, in the case of any settings modification feature.

(b) **OTHER EXCEPTIONS.**—Sections 3(a)(2), 3(b)(2), and 4 do not apply to any feature of computer software that is reasonably needed to—

(1) provide capability for general purpose online browsing, electronic mail, or instant messaging, or for any optional function that

is directly related to such capability and that the user knowingly chooses to use;

(2) determine whether or not the user of the computer is licensed or authorized to use the computer software; and

(3) provide technical support for the use of the computer software by the user of the computer.

(c) **PASSIVE TRANSMISSION, HOSTING, OR LINK.**—For purposes of this Act, a person shall not be deemed to have installed computer software, or authorized, permitted, or caused the installation of computer software, on a computer solely because that person provided—

(1) the Internet connection or other transmission capability through which the software was delivered to the computer for installation;

(2) the storage or hosting, at the direction of another person and without selecting the content to be stored or hosted, of the software or of an Internet website through which the software was made available for installation; or

(3) a link or reference to an Internet website the content of which was selected and controlled by another person, and through which the computer software was made available for installation.

(d) **SOFTWARE RESIDENT IN TEMPORARY MEMORY.**—In the case of an installation of computer software that falls within the meaning of section 7(10)(B) but not within the meaning of section 7(10)(A), the requirements set forth in subsections (a)(1), (b)(1), and (c) of section 3 shall not apply.

(e) **FEATURES ACTIVATED BY USER OPTIONS.**—In the case of an information collection, advertising, distributed computing, or settings modification feature that remains inactive or turned off unless the user of the computer subsequently selects certain optional settings or functions provided by the computer software, the requirements of subsections (a)(2) and (b)(2) of section 3 may be satisfied by providing the applicable disclosure and obtaining the applicable consent at the time the user selects the option that activates the feature, rather than at the time of initial installation.

SEC. 6. ADMINISTRATION AND ENFORCEMENT.

(a) **IN GENERAL.**—Except as provided in subsection (b), this Act shall be enforced by the Commission as if the violation of this Act were an unfair or deceptive act or practice proscribed under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(b) **ENFORCEMENT BY CERTAIN OTHER AGENCIES.**—Compliance with this Act shall be enforced under—

(1) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), in the case of—

(A) national banks, and Federal branches and Federal agencies of foreign banks, by the Office of the Comptroller of the Currency;

(B) member banks of the Federal Reserve System (other than national banks), branches and agencies of foreign banks (other than Federal branches, Federal agencies, and insured State branches of foreign banks), commercial lending companies owned or controlled by foreign banks, and organizations operating under section 25 or 25A of the Federal Reserve Act (12 U.S.C. 601 and 611), by the Board; and

(C) banks insured by the Federal Deposit Insurance Corporation (other than members of the Federal Reserve System) and insured State branches of foreign banks, by the Board of Directors of the Federal Deposit Insurance Corporation;

(2) section 8 of the Federal Deposit Insurance Act (12 U.S.C. 1818), by the Director of the Office of Thrift Supervision, in the case of a savings association the deposits of which

are insured by the Federal Deposit Insurance Corporation;

(3) the Federal Credit Union Act (12 U.S.C. 1751 et seq.) by the National Credit Union Administration Board with respect to any Federal credit union;

(4) part A of subtitle VII of title 49, United States Code, by the Secretary of Transportation with respect to any air carrier or foreign air carrier subject to that part;

(5) the Packers and Stockyards Act, 1921 (7 U.S.C. 181 et seq.) (except as provided in section 406 of that Act (7 U.S.C. 226, 227)), by the Secretary of Agriculture with respect to any activities subject to that Act; and

(6) the Farm Credit Act of 1971 (12 U.S.C. 2001 et seq.) by the Farm Credit Administration with respect to any Federal land bank, Federal land bank association, Federal intermediate credit bank, or production credit association.

(c) **EXERCISE OF CERTAIN POWERS.**—For the purpose of the exercise by any agency referred to in subsection (b) of its powers under any Act referred to in that subsection, a violation of this Act is deemed to be a violation of a requirement imposed under that Act. In addition to its powers under any provision of law specifically referred to in subsection (b), each of the agencies referred to in that subsection may exercise, for the purpose of enforcing compliance with any requirement imposed under this Act, any other authority conferred on it by law.

(d) **ACTIONS BY THE COMMISSION.**—The Commission shall prevent any person from violating this Act in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the Federal Trade Commission Act (15 U.S.C. 41 et seq.) were incorporated into and made a part of this Act. Any entity that violates any provision of that section is subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act in the same manner, by the same means, and with the same jurisdiction, power, and duties as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of that section.

(e) **PRESERVATION OF COMMISSION AUTHORITY.**—Nothing contained in this section shall be construed to limit the authority of the Commission under any other provision of law.

SEC. 7. ACTIONS BY STATES.

(a) **IN GENERAL.**—

(1) **CIVIL ACTIONS.**—In any case in which the attorney general of a State has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that this Act prohibits, the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction—

(A) to enjoin that practice;

(B) to enforce compliance with the rule;

(C) to obtain damage, restitution, or other compensation on behalf of residents of the State; or

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

(2) **NOTICE.**—

(A) **IN GENERAL.**—Before filing an action under paragraph (1), the attorney general of the State involved shall provide to the Commission—

(i) written notice of that action; and

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

(B) **EXEMPTION.**—

(i) **IN GENERAL.**—Subparagraph (A) shall not apply with respect to the filing of an action by an attorney general of a State under

this subsection, if the attorney general determines that it is not feasible to provide the notice described in that subparagraph before the filing of the action.

(ii) **NOTIFICATION.**—In an action described in clause (i), the attorney general of a State shall provide notice and a copy of the complaint to the Commission at the same time as the attorney general files the action.

(b) **INTERVENTION.**—

(1) **IN GENERAL.**—On receiving notice under subsection (a)(2), the Commission shall have the right to intervene in the action that is the subject of the notice.

(2) **EFFECT OF INTERVENTION.**—If the Commission intervenes in an action under subsection (a), it shall have the right—

(A) to be heard with respect to any matter that arises in that action; and

(B) to file a petition for appeal.

(c) **CONSTRUCTION.**—For purposes of bringing any civil action under subsection (a), nothing in this subtitle shall be construed to prevent an attorney general of a State from exercising the powers conferred on the attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

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

(d) **ACTIONS BY THE COMMISSION.**—In any case in which an action is instituted by or on behalf of the Commission for violation of section 2 of this Act, no State may, during the pendency of that action, institute an action under subsection (a) against any defendant named in the complaint in that action for violation of that section.

(e) **VENUE; SERVICE OF PROCESS.**—

(1) **VENUE.**—Any action brought under subsection (a) may be brought in the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code.

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

(A) is an inhabitant; or

(B) may be found.

SEC. 8. DEFINITIONS.

In this Act:

(1) **ADVERTISEMENT.**—The term “advertisement” means a commercial promotion for a product or service, but does not include promotions for products or services that appear on computer software help or support pages that are displayed in response to a request by the user.

(2) **ADVERTISING FEATURE.**—The term “advertising feature” means a function of computer software that, when installed on a computer, delivers advertisements to the user of that computer.

(3) **AFFIRMATIVE CONSENT.**—The term “affirmative consent” means consent expressed through action by the user of a computer other than default action specified by the installation sequence and independent from any other consent solicited from the user during the installation process.

(4) **CLEAR DESCRIPTION.**—The term “clear description” means a description that is clear, conspicuous, concise, and in a font size that is at least as large as the largest default font displayed to the user by the software.

(5) **COMPUTER SOFTWARE.**—The term “computer software”—

(A) means any program designed to cause a computer to perform a desired function or functions; and

(B) does not include any cookie.

(6) **COOKIE.**—The term “cookie” means a text file—

(A) that is placed on a computer by an Internet service provider, interactive computer service, or Internet website; and

(B) the sole function of which is to record information that can be read or recognized by an Internet service provider, interactive computer service, or Internet website when the user of the computer uses or accesses such provider, service, or website.

(7) **DISTRIBUTED COMPUTING FEATURE.**—The term “distributed computing feature” means a function of computer software that, when installed on a computer, transmits information or messages, other than personal or network information about the user of the computer, to any other computer without the knowledge or direction of the user and for purposes unrelated to the tasks or functions the user intentionally performs using the computer.

(8) **FIRST RETAIL SALE.**—The term “first retail sale” means the first sale of a computer, for a purpose other than resale, after the manufacture, production, or importation of the computer. For purposes of this paragraph, the lease of a computer shall be considered a sale of the computer at retail.

(9) **INFORMATION COLLECTION FEATURE.**—The term “information collection feature” means a function of computer software that, when installed on a computer, collects personal or network information about the user of the computer and transmits such information to any other party on an automatic basis or at the direction of a party other than the user of the computer.

(10) **INSTALL.**—The term “install” means—

(A) to write computer software to a computer's persistent storage medium, such as the computer's hard disk, in such a way that the computer software is retained on the computer after the computer is turned off and subsequently restarted; or

(B) to write computer software to a computer's temporary memory, such as random access memory, in such a way that the software is retained and continues to operate after the user of the computer turns off or exits the Internet service, interactive computer service, or Internet website from which the computer software was obtained.

(11) **NETWORK INFORMATION.**—The term “network information” means—

(A) an Internet protocol address or domain name of a user's computer;

(B) a cookie or other unique identifier of a computer user or a computer user's computer; or

(C) a Uniform Resource Locator or other information that identifies Internet web sites or other online resources accessed by a user of a computer.

(12) **PERSONAL INFORMATION.**—The term “personal information” means—

(A) a first and last name, whether given at birth or adoption, assumed, or legally changed;

(B) a home or other physical address including street name, name of a city or town, and zip code;

(C) an electronic mail address or online username;

(D) a telephone number;

(E) a social security number;

(F) any personal identification number;

(G) a credit card number, any access code associated with the credit card, or both;

(H) a birth date, birth certificate number, or place of birth; or

(I) any password or access code.

(13) **PERSON.**—The term “person” has the meaning given that term in section 3(32) of the Communications Act of 1934 (47 U.S.C. 153(32)).

(14) **PROTECTED COMPUTER.**—The term “protected computer” has the meaning given that term in section 1030(e)(2)(B) of title 18, United States Code.

(15) **SETTINGS MODIFICATION FEATURE.**—The term “settings modification feature” means

a function of computer software that, when installed on a computer—

(A) modifies an existing user setting, without direction from the user of the computer, with respect to another computer software application previously installed on that computer; or

(B) enables a user setting with respect to another computer software application previously installed on that computer to be modified in the future without advance notification to and consent from the user of the computer.

(16) USER OF A COMPUTER.—The term “user of a computer” means an individual who operates a computer with the authorization of the computer’s lawful owner.

SEC. 9. EFFECTIVE DATE.

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

By Mr. FEINGOLD (for himself, Mr. CORZINE, Mrs. CLINTON, Mr. LAUTENBERG, Mr. KENNEDY, Mr. SCHUMER, Mr. DURBIN, Mr. KERRY, Mrs. BOXER, Mr. REID, Mr. DODD, Ms. CANTWELL, Ms. MIKULSKI, and Mr. EDWARDS):

S. 2132. A bill to prohibit racial profiling; to the Committee on the Judiciary.

Mr. FEINGOLD. Mr. President, three years ago tomorrow, in his first address to a joint session of Congress, President Bush declared that racial profiling is wrong and pledged to end it in America. He then directed his Attorney General to implement this policy.

It is now three years later, and the American people are still waiting for the President to follow through on his pledge to end racial profiling.

So, today I join with Representative JOHN CONYERS, the distinguished ranking member of the House Judiciary Committee, in re-introducing the End Racial Profiling Act. We first introduced this bill in 2001, shortly after the President made his pledge and the Attorney General asserted that he would work with us on our legislation.

The End Racial Profiling Act would do exactly what the President promised to do: it would ban racial profiling once and for all and require Federal, State, and local law enforcement to take steps to end and prevent racial profiling.

I am very pleased that several of my distinguished colleagues have joined me on this bill Senators CORZINE, CLINTON, LAUTENBERG, KENNEDY, SCHUMER, DURBIN, KERRY, BOXER, REID, DODD, CANTWELL, MIKULSKI, and EDWARDS.

Racial profiling is the practice by which some law enforcement agents routinely stop African Americans, Latinos, Asian Americans, Arab Americans and others simply because of their race, ethnicity, or national origin. Reports in States from New Jersey to Florida, and Maryland to Texas all show that African Americans, Hispanics, and members of other minority groups are being stopped by some police far in excess of their share of the population and the rate at which they engage in criminal conduct.

I might add that the urgency for legislation banning racial profiling is

compounded by concerns post-September 11 that racial profiling—not good police work and following up on legitimate leads—is being used against Arab and Muslim Americans, or Americans perceived to be Arab or Muslim.

The September 11 attacks were horrific and I share the determination of many Americans that finding those responsible and preventing future attacks should be this Nation’s top priority. This is a challenge that our country can and must meet. But we need improved intelligence and law enforcement, not racial, ethnic or religious stereotypes, to protect our Nation from crime and future terrorist attacks.

In fact, I believe that the End Racial Profiling Act is a pro-law enforcement bill. It will help to restore the trust and confidence of the communities our law enforcement have pledged to serve and protect. That confidence is crucial to our success in stopping crime, and in stopping terrorism. The End Racial Profiling Act is good for law enforcement and good for America.

I’m very pleased that many state and local law enforcement officials stand with the sponsors of this bill in condemning racial profiling. Many law enforcement officials across the country agree that racial profiling is wrong and should not take place in America. In fact, many State and local law enforcement officials have begun to take steps to address the problem, or even the perception of a problem. For example, in my own State of Wisconsin, law enforcement officials have taken steps to train police officers, improve academy training, establish model policies prohibiting racial profiling, and improve relations with our State’s diverse communities. I applaud the efforts of Wisconsin law enforcement.

But the Federal Government has a vital role in protecting civil rights and acting as a model for State and local law enforcement. Last June, the Justice Department issued a policy guidance to Federal law enforcement agencies banning racial profiling. But while this guidance is a useful first step, it does not achieve the President’s stated goal of ending racial profiling in America. It does not carry the force of law and does not apply to State and local law enforcement. Federal legislation is still very much needed.

Our bill, the End Racial Profiling Act, would ban racial profiling and allow the Justice Department or individuals the ability to enforce this prohibition by filing a suit for injunctive relief. The bill would also require Federal, state, and local law enforcement agencies to adopt policies prohibiting racial profiling; to implement effective complaint procedures; to implement disciplinary procedures for officers who engage in the practice; and to collect data on stops. In addition, it requires the Attorney General to report to Congress to allow Congress and the American people to monitor whether the steps outlined in the bill to prevent

and end racial profiling have been effective.

Like the bill we introduced last Congress, the bill also authorizes the Attorney General to provide incentive grants to help law enforcement comply with the ban on racial profiling, including funds to conduct training of police officers or purchase in-car video cameras.

Finally, we have revised the bill to conform with the definition of racial profiling in the Justice Department’s guidance and to reflect concerns about racial profiling based on religion in a post-September 11 America.

Let me emphasize that local, State, and Federal law enforcement agents play a vital role in protecting the public from crime and protecting the Nation from terrorism. The vast majority of law enforcement agents nationwide discharge their duties professionally and without bias and we are all indebted to them for their courage and dedication. This bill should not be misinterpreted as a criticism of those who put their lives on the line for the rest of us every day. Rather, it is a statement that the use of race, ethnicity, religion, or national origin in deciding which persons should be subject to traffic stops, stops and frisks, questioning, searches, and seizures is wrong and ineffective, except where there is specific information linking persons of a particular race, ethnicity, religion, or national origin to a crime.

Now, perhaps more than ever before, our Nation cannot afford to waste precious law enforcement resources or alienate Americans by tolerating discriminatory practices. It is past time for Congress and the President to enact comprehensive federal legislation that will end racial profiling once and for all.

I urge the President to make good on his pledge to end racial profiling, and I urge my colleagues to join me in supporting the End Racial Profiling Act.

I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 2132

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

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the “End Racial Profiling Act of 2004”.

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

Sec. 1. Short title; table of contents.

Sec. 2. Findings and purposes.

TITLE I—PROHIBITION OF RACIAL PROFILING

Sec. 101. Prohibition.

Sec. 102. Enforcement.

TITLE II—PROGRAMS TO ELIMINATE RACIAL PROFILING BY FEDERAL LAW ENFORCEMENT AGENCIES

Sec. 201. Policies to eliminate racial profiling.

TITLE III—PROGRAMS TO ELIMINATE RACIAL PROFILING BY STATE AND LOCAL LAW ENFORCEMENT AGENCIES

Sec. 301. Policies required for grants.
 Sec. 302. Best practices development grants.
TITLE IV—DEPARTMENT OF JUSTICE REPORTS ON RACIAL PROFILING IN THE UNITED STATES

Sec. 401. Attorney General to issue reports on racial profiling in the United States.

Sec. 402. Limitation on use of data.

TITLE V—DEFINITIONS AND MISCELLANEOUS PROVISIONS

Sec. 501. Definitions.
 Sec. 502. Severability.
 Sec. 503. Savings clause.

SEC. 2. FINDINGS AND PURPOSES.

(a) **FINDINGS.**—Congress finds the following:

(1) Federal, State, and local law enforcement agents play a vital role in protecting the public from crime and protecting the Nation from terrorism. The vast majority of law enforcement agents nationwide discharge their duties professionally and without bias.

(2) The use by police officers of race, ethnicity, religion, or national origin in deciding which persons should be subject to traffic stops, stops and frisks, questioning, searches, and seizures is improper.

(3) In his address to a Joint Session of Congress on February 27, 2001, President George W. Bush declared that “racial profiling is wrong and we will end it in America.” He directed the Attorney General to implement this policy.

(4) In June 2003, the Department of Justice issued a Policy Guidance regarding racial profiling by Federal law enforcement agencies which stated: “Racial profiling in law enforcement is not merely wrong, but also ineffective. Race-based assumptions in law enforcement perpetuate negative racial stereotypes that are harmful to our rich and diverse democracy, and materially impair our efforts to maintain a fair and just society.”

(5) The Department of Justice Guidance is a useful first step, but does not achieve the President’s stated goal of ending racial profiling in America: it does not apply to State and local law enforcement agencies, does not contain a meaningful enforcement mechanism, does not require data collection, and contains an overbroad exception for immigration and national security matters.

(6) Current efforts by State and local governments to eradicate racial profiling and redress the harms it causes, while also laudable, have been limited in scope and insufficient to address this national problem. Therefore, Federal legislation is needed.

(7) Statistical evidence from across the country demonstrates that racial profiling is a real and measurable phenomenon.

(8) As of November 15, 2000, the Department of Justice had 14 publicly noticed, ongoing, pattern or practice investigations involving allegations of racial profiling, and had filed 5 pattern and practice lawsuits involving allegations of racial profiling, with 4 of those cases resolved through consent decrees.

(9) A large majority of individuals subjected to stops and other enforcement activities based on race, ethnicity, religion, or national origin are found to be law abiding and therefore racial profiling is not an effective means to uncover criminal activity.

(10) A 2001 Department of Justice report on citizen-police contacts in 1999 found that, although African-Americans and Hispanics were more likely to be stopped and searched, they were less likely to be in possession of contraband. On average, searches and sei-

zures of African-American drivers yielded evidence only 8 percent of the time, searches and seizures of Hispanic drivers yielded evidence only 10 percent of the time, and searches and seizures of white drivers yielded evidence 17 percent of the time.

(11) A 2000 General Accounting Office report on the activities of the United States Customs Service during fiscal year 1998 found that—

(A) black women who were United States citizens were 9 times more likely than white women who were United States citizens to be x-rayed after being frisked or patted down;

(B) black women who were United States citizens were less than half as likely as white women who were United States citizens to be found carrying contraband; and

(C) in general, the patterns used to select passengers for more intrusive searches resulted in women and minorities being selected at rates that were not consistent with the rates of finding contraband.

(12) In some jurisdictions, local law enforcement practices such as ticket and arrest quotas, and similar management practices, may have the unintended effect of encouraging law enforcement agents to engage in racial profiling.

(13) Racial profiling harms individuals subjected to it because they experience fear, anxiety, humiliation, anger, resentment, and cynicism when they are unjustifiably treated as criminal suspects. By discouraging individuals from traveling freely, racial profiling impairs both interstate and intrastate commerce.

(14) Racial profiling damages law enforcement and the criminal justice system as a whole by undermining public confidence and trust in the police, the courts, and the criminal law.

(15) In the wake of the September 11, 2001, terrorist attacks, many Arabs, Muslims, Central and South Asians, and Sikhs, as well as other immigrants and Americans of foreign descent, were treated with generalized suspicion and subjected to searches and seizures based upon religion and national origin, without trustworthy information linking specific individuals to criminal conduct. Such profiling has failed to produce tangible benefits, yet has created a fear and mistrust of law enforcement agencies in these communities.

(16) Racial profiling violates the equal protection clause of the Constitution. Using race, ethnicity, religion, or national origin as a proxy for criminal suspicion violates the constitutional requirement that police and other government officials accord to all citizens the equal protection of the law. *Arlington Heights v. Metropolitan Housing Development Corporation*, 429 U.S. 252 (1977).

(17) Racial profiling is not adequately addressed through suppression motions in criminal cases for two reasons. First, the Supreme Court held, in *Whren v. United States*, 517 U.S. 806 (1996), that the racially discriminatory motive of a police officer in making an otherwise valid traffic stop does not warrant the suppression of evidence. Second, since most stops do not result in the discovery of contraband, there is no criminal prosecution and no evidence to suppress.

(18) A comprehensive national solution is needed to address racial profiling at the Federal, State, and local levels. Federal support is needed to combat racial profiling through specialized training of law enforcement agents, improved management systems, and the acquisition of technology such as in-car video cameras.

(b) **PURPOSES.**—The purposes of this Act are—

(1) to enforce the constitutional right to equal protection of the laws, pursuant to the Fifth Amendment and section 5 of the 14th

Amendment to the Constitution of the United States;

(2) to enforce the constitutional right to protection against unreasonable searches and seizures, pursuant to the Fourth Amendment to the Constitution of the United States;

(3) to enforce the constitutional right to interstate travel, pursuant to section 2 of article IV of the Constitution of the United States; and

(4) to regulate interstate commerce, pursuant to clause 3 of section 8 of article I of the Constitution of the United States.

TITLE I—PROHIBITION OF RACIAL PROFILING

SEC. 101. PROHIBITION.

No law enforcement agent or law enforcement agency shall engage in racial profiling.

SEC. 102. ENFORCEMENT.

(a) **REMEDY.**—The United States, or an individual injured by racial profiling, may enforce this title in a civil action for declaratory or injunctive relief, filed either in a State court of general jurisdiction or in a district court of the United States.

(b) **PARTIES.**—In any action brought pursuant to this title, relief may be obtained against—

(1) any governmental unit that employed any law enforcement agent who engaged in racial profiling;

(2) any agent of such unit who engaged in racial profiling; and

(3) any person with supervisory authority over such agent.

(c) **NATURE OF PROOF.**—Proof that the routine or spontaneous investigatory activities of law enforcement agents in a jurisdiction have had a disparate impact on racial, ethnic, or religious minorities shall constitute prima facie evidence of a violation of this title.

(d) **ATTORNEY’S FEES.**—In any action or proceeding to enforce this title against any governmental unit, the court may allow a prevailing plaintiff, other than the United States, reasonable attorney’s fees as part of the costs, and may include expert fees as part of the attorney’s fee.

TITLE II—PROGRAMS TO ELIMINATE RACIAL PROFILING BY FEDERAL LAW ENFORCEMENT AGENCIES

SEC. 201. POLICIES TO ELIMINATE RACIAL PROFILING.

(a) **IN GENERAL.**—Federal law enforcement agencies shall—

(1) maintain adequate policies and procedures designed to eliminate racial profiling; and

(2) cease existing practices that encourage racial profiling.

(b) **POLICIES.**—The policies and procedures described in subsection (a)(1) shall include—

(1) a prohibition on racial profiling;

(2) the collection of data on routine investigatory activities sufficient to determine if law enforcement agents are engaged in racial profiling and submission of that data to the Attorney General;

(3) independent procedures for receiving, investigating, and responding meaningfully to complaints alleging racial profiling by law enforcement agents of the agency;

(4) procedures to discipline law enforcement agents who engage in racial profiling; and

(5) such other policies or procedures that the Attorney General deems necessary to eliminate racial profiling.

TITLE III—PROGRAMS TO ELIMINATE RACIAL PROFILING BY STATE AND LOCAL LAW ENFORCEMENT AGENCIES

SEC. 301. POLICIES REQUIRED FOR GRANTS.

(a) **IN GENERAL.**—An application by a State or governmental unit for funding under a

covered program shall include a certification that such unit and any agency to which it is redistributing program funds—

(1) maintains adequate policies and procedures designed to eliminate racial profiling; and

(2) has ceased any existing practices that encourage racial profiling.

(b) **POLICIES.**—The policies and procedures described in subsection (a) shall include—

(1) a prohibition on racial profiling;

(2) the collection of data on routine investigatory activities sufficient to determine if law enforcement agents are engaged in racial profiling, and submission of that data to the Attorney General;

(3) independent procedures for receiving, investigating, and responding meaningfully to complaints alleging racial profiling by law enforcement agents;

(4) procedures to discipline law enforcement agents who engage in racial profiling; and

(5) such other policies or procedures that the Attorney General deems necessary to eliminate racial profiling.

(c) **NONCOMPLIANCE.**—If the Attorney General determines that a grantee is not in compliance with conditions established under this title, the Attorney General shall withhold the grant, in whole or in part, until the grantee establishes compliance. The Attorney General shall provide notice regarding State grants and opportunities for private parties to present evidence to the Attorney General that a grantee is not in compliance with conditions established under this title.

SEC. 302. BEST PRACTICES DEVELOPMENT GRANTS.

(a) **GRANT AUTHORIZATION.**—The Attorney General may make grants to States, law enforcement agencies and other governmental units, Indian tribal governments, or other public and private entities, to develop and implement best practice devices and systems to ensure the racially neutral administration of justice.

(b) **USES.**—The funds provided pursuant to subsection (a) may be used to support—

(1) development and implementation of training to prevent racial profiling and to encourage more respectful interaction with the public;

(2) acquisition and use of technology to facilitate the collection of data regarding routine investigatory activities in order to determine if law enforcement agents are engaged in racial profiling;

(3) acquisition and use of technology to verify the accuracy of data collection, including in-car video cameras and portable computer systems;

(4) development and acquisition of early warning systems and other feedback systems that help identify officers or units of officers engaged in or at risk of racial profiling or other misconduct, including the technology to support such systems;

(5) establishment or improvement of systems and procedures for receiving, investigating, and responding meaningfully to complaints alleging racial, ethnic, or religious bias by law enforcement agents; and

(6) establishment or improvement of management systems to ensure that supervisors are held accountable for the conduct of their subordinates.

(c) **EQUITABLE DISTRIBUTION.**—The Attorney General shall ensure that grants under this section are awarded in a manner that reserves an equitable share of funding for small and rural law enforcement agencies.

(d) **AUTHORIZATION OF APPROPRIATIONS.**—The Attorney General shall make available such sums as are necessary to carry out this section from amounts appropriated for programs administered by the Attorney General.

TITLE IV—DEPARTMENT OF JUSTICE REPORTS ON RACIAL PROFILING IN THE UNITED STATES

SEC. 401. ATTORNEY GENERAL TO ISSUE REPORTS ON RACIAL PROFILING IN THE UNITED STATES.

(a) **REPORTS.**—

(1) **IN GENERAL.**—Not later than 2 years after the enactment of this Act, and each year thereafter, the Attorney General shall submit to Congress a report on racial profiling by Federal, State, and local law enforcement agencies in the United States.

(2) **SCOPE.**—The reports issued pursuant to paragraph (1) shall include—

(A) a summary of data collected pursuant to sections 201(b)(2) and 301(b)(2) and any other reliable source of information regarding racial profiling in the United States;

(B) the status of the adoption and implementation of policies and procedures by Federal law enforcement agencies pursuant to section 201;

(C) the status of the adoption and implementation of policies and procedures by State and local law enforcement agencies pursuant to sections 301 and 302; and

(D) a description of any other policies and procedures that the Attorney General believes would facilitate the elimination of racial profiling.

(b) **DATA COLLECTION.**—Not later than 6 months after the enactment of this Act, the Attorney General shall by regulation establish standards for the collection of data under sections 201(b)(2) and 301(b)(2), including standards for setting benchmarks against which collected data shall be measured. Such standards shall result in the collection of data, including data with respect to stops, searches, seizures, and arrests, that is sufficiently detailed to determine whether law enforcement agencies are engaged in racial profiling and to monitor the effectiveness of policies and procedures designed to eliminate racial profiling.

(c) **PUBLIC ACCESS.**—Data collected under sections 201(b)(2) and 301(b)(2) shall be available to the public.

SEC. 402. LIMITATION ON USE OF DATA.

Information released pursuant to section 401 shall not reveal the identity of any individual who is detained or any law enforcement officer involved in a detention.

TITLE V—DEFINITIONS AND MISCELLANEOUS PROVISIONS

SEC. 501. DEFINITIONS.

In this Act:

(1) **COVERED PROGRAM.**—The term “covered program” means any program or activity funded in whole or in part with funds made available under—

(A) the Edward Byrne Memorial State and Local Law Enforcement Assistance Programs (part E of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3750 et seq.));

(B) the “Cops on the Beat” program under part Q of title I of the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3796dd et seq.), but not including any program, project, or other activity specified in section 1701(d)(8) of that Act (42 U.S.C. 3796dd(d)(8)); and

(C) the Local Law Enforcement Block Grant program of the Department of Justice, as described in appropriations Acts.

(2) **GOVERNMENTAL UNIT.**—The term “governmental unit” means any department, agency, special purpose district, or other instrumentality of Federal, State, local, or Indian tribal government.

(3) **LAW ENFORCEMENT AGENCY.**—The term “law enforcement agency” means a Federal, State, local, or Indian tribal public agency engaged in the prevention, detection, or investigation of violations of criminal, immigration, or customs laws.

(4) **LAW ENFORCEMENT AGENT.**—The term “law enforcement agent” means any Federal, State, local, or Indian tribal official responsible for enforcing criminal, immigration, or customs laws, including police officers and other agents of Federal, State, and local law enforcement agencies.

(5) **RACIAL PROFILING.**—The term “racial profiling” means the practice of a law enforcement agent relying, to any degree, on race, ethnicity, religion, or national origin in selecting which individuals to subject to routine or spontaneous investigatory activities, or in deciding upon the scope and substance of law enforcement activity following the initial investigatory procedure, except when there is trustworthy information, relevant to the locality and timeframe, that links persons of a particular race, ethnicity, religion, or national origin to an identified criminal incident or scheme.

(6) **ROUTINE OR SPONTANEOUS INVESTIGATORY ACTIVITIES.**—The term “routine or spontaneous investigatory activities” means the following activities by law enforcement agents: interviews; traffic stops; pedestrian stops; frisks and other types of body searches; consensual or nonconsensual searches of the persons or possessions (including vehicles) of motorists or pedestrians; inspections and interviews of entrants into the United States that are more extensive than those customarily carried out; immigration related workplace investigations; and such other types of law enforcement encounters compiled by the FBI and the Justice Department’s Bureau of Justice Statistics.

SEC. 502. SEVERABILITY.

If any provision of this Act or the application of such provision to any person or circumstance is held to be unconstitutional, the remainder of this Act and the application of the provisions of such to any person or circumstance shall not be affected thereby.

SEC. 503. SAVINGS CLAUSE.

Nothing in this Act shall be construed to limit legal or administrative remedies under section 1979 of the Revised Statutes of the United States (42 U.S.C. 1983), section 210401 of the Violent Crime Control and Law Enforcement Act of 1994 (42 U.S.C. 14141), the Omnibus Crime Control and Safe Streets Act of 1968 (42 U.S.C. 3701 et seq.), and title VI of the Civil Rights Act of 1964 (42 U.S.C. 2000d et seq.).

Mr. CORZINE. Mr. President, I am very pleased to be joining my colleague Senator RUSSELL FEINGOLD and 12 others in reintroducing the End Racial Profiling Act.

I first want to recognize Senator RUSS FEINGOLD who has been a tremendous leader on this issue—during the last two sessions he held the first Senate hearings on racial profiling and he and his staff have worked tirelessly to elevate the importance of this issue as a matter of civil rights. I also want to commend Representative JOHN CONYERS, who is introducing companion legislation in the House of Representatives today. This is just an example of his indefatigable work to address inequities in our society. I also want to thank Reverend Reginald Jackson, Executive Director of the New Jersey Black Ministers’ Council. He and the entire council have worked tirelessly for years to address the issue of racial profiling in New Jersey and have provided immeasurable assistance in crafting this legislation.

The practice of racial profiling is the antithesis of America's belief in fairness and equal protection under the law.

Stopping people on our highways, our streets, and at our borders because of the color of their skin tears at the very fabric of American society.

We are a Nation of laws and everyone should receive equal protection under the law. Our Constitution tolerates nothing less. We should demand nothing less.

There is no equal protection—there is no equal justice—if law enforcement agencies engage in policies and practices that are premised on a theory that the way to stop crime is to go after black and brown people on the hunch that they are more likely to be criminals.

Let me add, that not only is racial profiling wrong, it is simply not an effective law enforcement tool. There is no evidence that stopping people of color adds up to catching bad guys.

In fact, there is statistical evidence which points out that singling out black motorist or Hispanic motorists for stops and searches doesn't lead to a higher percentage of arrests. Minority motorists are simply no more likely to be breaking the law than white motorists.

But unfortunately racial profiling persists.

In 2001, minority motorists accounted for 73 percent of those searched on the New Jersey turnpike. But even the State Attorney General admitted that State troopers were twice—I repeat twice—as likely to find drugs or other illegal items when searching vehicles driven by whites.

Or take the example of the March 2000 Government Accounting Office report on the U.S. Customs Service.

The report found that black, Asian, and Hispanic women were four to nine times more likely than white women to be subjected to X rays after being frisked or patted down.

But on the basis of the X ray results, black women were less than half as likely as white women to be found carrying contraband.

This is law enforcement by hunch. No warrants. No probable cause.

And what is the hunch based on?

Race—plain and simple.

No where was this more evident, than in my own home State six years ago.

Four young men on the New Jersey Turnpike in a minivan—on their way to North Carolina, hoping to go to school on basketball scholarships.

Two State troopers pulled them off the road, the frightened driver lost control of the van, two dozens shots rang out. Three of the four kids were shot.

I spoke to these kids a while ago. One of the them told me he was asleep when the van was pulled over.

He told me, "What woke me up was a bullet."

Stories like this should wake us all up.

The practice of racial profiling broadly undermines the confidence of the American people in the institutions that we depend on to protect and defend us. Different rules for different people do not work.

Now—We know that many law enforcement agencies, including some from my home State, have acknowledged the danger of the practice and have taken steps to combat it. Indeed, I am proud to report that New Jersey has banned racial profiling. I commend them for their efforts.

That said, it is clear that this is a national problem that requires a national response applicable to all.

That is why Senator FEINGOLD and I and many others introduced the End Racial Profiling Act in 2001 to end this practice. The legislation provided a clear, enforceable ban on racial profiling and established a "carrot and stick" approach to encourage law enforcement to take steps to end the practice.

The legislation helped bring much-needed attention to this critical issue and was positively received by the civil rights community and many in law enforcement. Soon after introduction, Senator FEINGOLD held very informative hearings on the bill, at which I testified. We heard from several law enforcement leaders, including Oakland Police Chief Ronald Davis and Raymond Kelly, former Commissioner of the U.S. Customs Service and the New York City Police Department, on the pernicious impact of racial profiling on the trust between law enforcement and communities that is essential for successful police work. They testified that racial profiling is contrary to effective law enforcement and indeed takes energy and focus away from finding real criminals.

Then, in June 2003, the U.S. Department of Justice issued guidelines to prohibit racial profiling by federal law enforcement agencies, following up on President Bush's statement in his February 27, 2001, address to a Joint Session of Congress, that racial profiling is "wrong and we will end it in America."

In this guidance, the Department stated:

Racial profiling in law enforcement is not merely wrong, but also ineffective. Race-based assumptions in law enforcement perpetuate negative racial stereotypes that are harmful to our rich and diverse democracy, and materially impair our efforts to maintain a fair and just society.

These guidelines, as well as current efforts by State and local governments, to eradicate racial profiling and redress the harms it causes, while laudable, have been limited in scope and insufficient to address this national problem. Quite simply, federal legislation is still very much needed.

In most respects the legislation we are now introducing today is very similar to the bill that we introduced in 2001.

It clearly defines racial profiling and bans it.

No routine stops based solely on race, religion, national origin or ethnicity. Religion is a new addition to the category of protected classes, in acknowledgment of some of the new law enforcement tactics developed after the September 11, 2001, terrorist attacks. For example, in the wake of the attacks, Arab-American, Muslim-American, South Asian-American and Sikh-American communities were made the target of generalized suspicion and subjected to searches and seizures based upon their religion and national origin, which has created a fear and mistrust of law enforcement agencies and failed to produce tangible investigative benefit.

We will also require the collection of statistics to accurately measure whether progress is being made. By collecting this data, we will get a fair picture of law enforcement at work. And we will provide law enforcement with the information they need to detect problems early on.

It is not our intention to micro-manage law enforcement. Our bill does not tell law enforcement agencies what data should be collected. Instead, we direct the Attorney General to develop the standards for data collection, and he presumably would work with law enforcement in developing those standards. Our legislation also specifically directs the Attorney General to also establish standards for setting benchmarks against which the collected data should be measured—so that no data is taken out of context, as some in law enforcement rightly fear.

If the numbers reveal a portrait of continued racial profiling, then the Justice Department or independent third parties can seek relief in Federal court ordering that remedies be put into effect to end racial profiling.

Our bill would also put in place procedures to receive and investigate complaints alleging racial profiling.

It will require procedures to discipline law enforcement officers engaging in racial profiling.

Finally, we will encourage a climate of cultural change in law enforcement with a carrot and a stick.

First, the carrot: We recognize that law enforcement shouldn't be expected to do this alone. So we are saying that if you do the job right—fairly and equitably—you can be eligible to receive a best practices development grant—to help pay for programs dealing with advanced training.

To help pay for the computer technology that is necessary to collect the data and statistics we have demanded.

We'll help pay for video cameras and recorders for your patrol cars.

We'll help pay for establishing or improving systems for handling complaints alleging ethnic or racial profiling.

We'll help to establish management systems to ensure that supervisors are held accountable for the conduct of subordinates.

But if you don't do the job right, there is the stick. If State and local

law enforcement agencies refuse to implement procedures to end and prevent profiling, they will be subject to a loss of Federal law enforcement funds.

Let me be clear, this bill is not about blaming law enforcement, and it is not designed to prevent law enforcement from doing its job. In fact, we believe that it will help our officers maintain the public trust they need to do their jobs.

If race is a part of a description of a specific suspect involved in an investigation, this law does not prevent that information from being distributed. But stopping people on a random or race-based hunch will be outlawed. Race has been a never-ending battle in this country. It began with our constitution, when the founding fathers argued over the rights of slaves. And then we fought a war over race. We fought a war that ripped our country apart.

Our country emerged whole, but discrimination continued for decades—discrimination sanctioned in part, unfortunately, by our own Supreme Court.

But our country's history has always been about change, about growth, about recognizing those things that weaken us from within.

A generation ago, we began to fight another war—a war founded in peaceful principles, but a war that killed our heroes, burned our cities, and shook us once again to the very core.

But we advanced, with important civil rights initiatives like the Voting Rights Act. Like the public accommodations law. We demanded and gained laws to fight discrimination in employment, in housing, in education. Today, it is time for us to take another step. Racial profiling has bred humiliation, anger, resentment and cynicism throughout this country. It has weakened respect for the law—by everyone, not just those offended.

Simply put—it is wrong and we must end it. Today we pledge to do just that—to define it, to ban it, and to enforce that ban.

By Mrs. FEINSTEIN (for herself, Mr. CAMPBELL, Mr. DOMENICI, and Mr. SMITH):

S. 2134. A bill to authorize the Secretary of Agriculture and the Secretary of the Interior to enter into an agreement or contract with Indian tribes meeting certain criteria to carry out projects to protect Indian forest land; to the Committee on Indian Affairs.

Mrs. FEINSTEIN. Mr. President, I am pleased to introduce a bipartisan bill today that gives Native American tribes a chance to protect their reservation lands from catastrophic fire. I want to thank my cosponsors, Chairman PETE DOMENICI of the Energy and Natural Resources Committee, and Chairman BEN NIGHTHORSE CAMPBELL of the Committee on Indian Affairs.

Like other Americans, many Native American tribes are concerned about

the risk of catastrophic forest fires spreading from nearby Federal lands onto their own lands. Last summer, at least 18 reservations were invaded by fire from adjacent Federal public forest lands.

This bill attempts to give the tribes a chance to defend themselves and their ancestral lands by involving them in brush-clearing projects on Federal lands near their reservations.

This is not just a theoretical problem, as tribes from my State know all too well.

Last fall's devastating wildfires in southern California caused disproportionate suffering for Native Americans: Over 30,000 acres burned on 11 tribal reservations. Most tragically, 10 lives were lost on or near reservations.

I am determined to give the tribes of my State and from around the country the opportunity to prevent this tragedy from recurring: The bill sets up a process for the Forest Service or the Bureau of Land Management to enter into contracts with the tribes for fuel reduction purposes. If a tribe requests a brush-clearing project on federal lands near its reservation, the agencies are encouraged to respond within specific timeframes and suggest remedies for any agency concerns with the tribe's proposal. There remains free and open competition for timber contracts on Federal land. However, in determining the recipients of the contracts, the agencies are encouraged to consider such factors as tribal treaty rights or cultural and historical affiliation to the land involved.

Nearly 100 Native American tribes support this legislation, including most, if not all, the tribes in the State of California.

So I am pleased to introduce this bill today, and I hope my colleagues will support it.

By Mrs. MURRAY (for herself and Ms. CANTWELL):

S. 2135. A bill to amend title XVIII of the Social Security Act to improve the provision of items and services provided to Medicare beneficiaries residing in rural areas; to the Committee on Finance.

Mrs. MURRAY. Mr. President, I rise today to again join my colleague, Senator CANTWELL, in introducing the MediFair Act of 2004. My bill will restore fairness to the Medicare program and provide equity for health care providers participating in Medicare. Most importantly, it will open doors of care to more seniors and the disabled in my State.

Today, unfair Medicare reimbursement rates are causing doctors to limit their care for Medicare beneficiaries. Throughout my State, seniors and the disabled are having a hard time finding a doctor who will accept new Medicare patients.

Unfortunately, the recently-passed Medicare Prescription Drug, Improvement and Modernization Act of 2003 further compromises health care in

Washington State because it reduces Washington State's per beneficiary payments from 42nd to 45th nationwide. This reduction places health care providers in my State at an economic disadvantage and further limits access to health care in Washington State.

My bill will reduce the regional inequities that have resulted in vastly different levels of care and access to care by ensuring that every State receives at least the national average of per-patient spending. This measure will encourage more doctors to accept Medicare patients and will also guarantee that seniors are not penalized when they choose to retire in the State of Washington.

In addition to ensuring that no State receives less than the national average, my legislation will encourage healthy outcomes and efficient use of Medicare payments. The current Medicare system punishes health care providers who practice efficient healthcare and healthy outcomes. Physicians and hospitals in my State are proud of the pioneering role they have played in providing high quality, cost effective medicine. Unfortunately, they have been rewarded for their exceptional service by being paid a fraction of their actual costs.

On the other hand, States that are inefficient and that over-utilize the system are rewarded with higher states of reimbursement. As we grapple with an ever-increasing budget deficit. We need to make sure that every dollar spent on Medicare is used as effectively as possible. I ask each and every one of my colleagues to join me in restoring fairness to the Medicare program and increasing access to health care for Medicare beneficiaries by supporting the MediFair Act.

I want to acknowledge the lead sponsor of the MediFair bill in the House, Representative ADAM SMITH, as well as the other cosponsors, Representative BAIRD, Representative DICKS, Representative INSLEE, Representative LARSEN, and Representative McDERMOTT.

I have been working on addressing the issue of inequitable Medicare reimbursement policies for a number of years, and I am pleased that we have made inroads in addressing this issue. I especially appreciate the efforts by the Department of Health and Human Services (HHS) to reward healthy outcomes, and I look forward to working with HHS in the future to meet these goals.

Medicare should reward States like Washington that have a proven tradition of efficient and effective health care. Passing the MediFair Act will go a long way to improving health care access for seniors in States like Washington and ensuring that Federal health care dollars produce the best results possible for our patients.

By Mr. ROBERTS:

S. 2136. An original bill to extend the final report date and termination date

of the National Commission on Terrorist Attacks Upon the United States, to provide additional funding for the Commission, and for other purposes; from the Select Committee on Intelligence; placed on the calendar.

Mr. ROBERTS. Mr. President, I ask unanimous consent that the text of the bill be printed in the RECORD.

There being no objection, the bill was ordered to be printed in the RECORD, as follows:

S. 2136

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

SECTION 1. EXTENSION OF NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES.

(a) FINAL REPORT DATE.—Subsection (b) of section 610 of the Intelligence Authorization Act for Fiscal Year 2003 (Public Law 107-306; 6 U.S.C. 101 note; 116 Stat. 2413) is amended by striking “18 months” and inserting “20 months”.

(b) TERMINATION DATE.—Subsection (c) of that section is amended—

(1) in paragraph (1), by striking “60 days” and inserting “30 days”; and

(2) in paragraph (2), by striking “60-day period” and inserting “30-day period”.

(c) ADDITIONAL FUNDING.—Section 611 of that Act (6 U.S.C. 101 note; 116 Stat. 2413) is amended—

(1) by redesignating subsection (b) as subsection (c);

(2) by inserting after subsection (a) the following new subsection (b):

“(b) ADDITIONAL FUNDING.—In addition to the amounts made available to the Commission under subsection (a) and under chapter 2 of title II of the Emergency Wartime Supplemental Appropriations Act, 2003 (Public Law 108-11; 117 Stat. 591), of the amounts appropriated for the programs and activities of the Federal Government for fiscal year 2004 that remain available for obligation, not more than \$1,000,000 shall be available for transfer to the Commission for purposes of the activities of the Commission under this title.”; and

(3) in subsection (c), as so redesignated, by striking “subsection (a)” and inserting “this section”.

By Mrs. CLINTON:

S. 2139. A bill to provide coverage under the Energy Employees Occupational Illness Compensation Program for individuals employed at atomic weapons employer facilities during periods of residual contamination; to the Committee on Health, Education, Labor, and Pensions.

Mrs. CLINTON. Mr. President, I rise to introduce an important piece of legislation to assist our atomic weapons workers. The legislation addresses a major flaw in the Energy Employees Occupational Illness Compensation Program by expanding eligibility for benefits.

Under the Energy Employees Occupational Illness Compensation Program Act (EEOICPA), workers are eligible for a payment of \$150,000 and medical coverage for expenses associated with the treatment of diseases contracted due to exposure to radiation at atomic weapons plants. However, under EEOICPA, workers who became sick from working in contaminated atomic

weapons plants after weapons production ceased are not eligible for benefits.

In 2003, the National Institute of Occupational Safety and Health released a Congressionally-mandated report, entitled “Report on Residual Radioactive and Beryllium Contamination in Atomic Weapons Employer and Beryllium Vendor Facilities.” The report concluded that “significant” residual radioactive contamination existed in many of these plants for years and decades after weapons production ceased, posing a risk of radiation-related cancers or disease to unknowing workers.

In fact, the report found that: 97, 44 percent, of covered facilities have potential for significant residual radioactive contamination outside of the periods in which atomic weapons-related production occurred; 88, 40 percent, of such facilities have little potential for significant residual radioactive contamination outside of the periods in which atomic weapons-related production occurred; and 34, 16 percent, of such facilities have insufficient information to make a determination.

In my State of New York, 16 of 31 covered facilities were found to have the potential for significant contamination, 10 had little potential for significant contamination, and 5 of the 31 had insufficient information.

In other words, more than half of the New York Atomic Weapons Employer Facilities in New York were contaminated after weapons production ceased. As a result, workers were exposed to radiation, and deserve to be eligible for benefits under EEOICPA.

That is why I am introducing the Residual Radioactive Contamination Compensation Act (RRCCA) today. The bill would extend eligibility for benefits under EEOICPA to workers who were employed at facilities where NIOSH has found potential for significant radioactive contamination.

In addition to expanding eligibility to workers employed at facilities where NIOSH has found potential for significant radioactive contamination, the Residual Radioactive Contamination Compensation Act would require NIOSH to update the list of such facilities annually. This addresses the fact that there was insufficient information for NIOSH to characterize a number of sites in its 2003 report.

I would also like to take the opportunity to draw attention to another important issue—the special cohort rule. Under EEOICPA, the Department of Health and Human Services was to establish procedures so that workers can petition the government to be included in a “special cohort”—meaning that they would be eligible for the program—if their radiation doses are difficult to estimate but it is likely that they have radiation-caused illnesses. Despite this important mandate, the letter notes that “. . . nearly 39 months after EEOICPA was signed into law, the promise of “timely, uniform and adequate compensation” has not been met.

As a result, I sent a letter to Secretary Thompson, along with Senator VOINOVICH and 16 of my other Senate colleagues—Senators HARKIN, KENNEDY, SCHUMER, MURRAY, DEWINE, ALEXANDER, CRAIG, BOND, and TALENT, REID, GRASSLEY, HOLLINGS, CANTWELL, DOMENICI, CAMPBELL, and BINGAMAN. The letter requested that the Secretary immediately put out the special cohort rule. I ask unanimous consent that a copy of that letter be printed in the RECORD.

More than two weeks after the letter was sent, I have still not received a response. This is unacceptable. The Administration seems to have no sense of urgency in addressing this issue. But each day that passes only delays long overdue justice for the Cold War heroes who worked in our weapons facilities.

I ask unanimous consent that the text of the Residual Radioactive Contamination Compensation Act be printed in the RECORD.

There being no objection, the material was ordered to be printed in the RECORD, as follows:

FEBRUARY 11, 2004.

Hon. TOMMY G. THOMPSON,
Secretary, U.S. Department of Health and Human Services, 200 Independence Avenue, SW., Washington, DC.

DEAR MR. SECRETARY: On October 30, 2000, the Energy Employees Occupational Illness Compensation Program Act (EEOICPA) was signed into law (PL 106-386) as part of the FY 01 Defense Authorization Act. Enactment of EEOICPA was recognition by Congress and the President that the federal government needed to act quickly to remedy long-standing injustices against atomic weapons program workers. The findings of the Act make the need for the Program abundantly clear, and include the acknowledgment that:

“Since the inspection of the nuclear weapons program and for several decades afterwards, a large number of nuclear weapons workers at sites of the Department of Energy and at sites of vendors who supplied the Cold War effort were put at risk without their knowledge and consent for reasons that, documents reveal, were driven by fears of adverse publicity, liability, and employee demands for hazardous duty pay.”

The Act further states that:

“the purpose of the compensation program is to provide for timely, uniform, and adequate compensation of covered employees and, where applicable, survivors of such employees, suffering from illnesses incurred by such employees in the performance of duty for the Department of Energy and certain of its contractors and subcontractors.”

Yet nearly 39 months after EEOICPA was signed into law, the promise of “timely, uniform and adequate compensation” has not been met. We are very concerned about the delay in finalizing the “special exposure cohort” petition procedures by the Department of Health and Human Services (HHS) pursuant to 42 USC 7384(q).

In this regard, EEOICPA specifically provides:

“. . . members of a class of employees at a Department of Energy facility, or at an atomic weapons employer facility, may be treated as members of the Special Exposure Cohort for purposes of the compensation program if the President, upon recommendation of the Advisory Board on Radiation and Worker Health, determines that—

(1) it is not feasible to estimate with sufficient accuracy the radiation dose that the class received; and

(2) there is reasonable likelihood that such radiation dose may have endangered the health of members of the class."

The law further states that, "the President shall consider such petitions pursuant to procedures established by the President."

Procedures for Designating Classes of Employees as Members of the Special Exposure Cohort were first proposed through a rule-making, and then subsequently withdrawn in 2002 after uniform criticism. Revised rules were proposed in March of 2003, but to date they have not been finalized. Workers have and continue to be blocked from filing petitions to become members of the Special Exposure Cohort because HHS has failed to meet its statutory responsibility to issue these regulations.

Further delay is denying long-overdue justice for those who were intended to be covered by the special exposure cohort provisions of the Act. After over three years, HHS has had ample time to study this matter, and further delay is simply inexcusable.

Therefore, we urge you to finalize the special exposure cohort rules and publish them in the Federal Register immediately. Our atomic weapons program workers, who are true Cold War heroes, helped protect our nation and deserve nothing less. We thank you for your prompt attention to this matter.

Sincerely,

MEMBERS OF CONGRESS.

S. 2139

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 "Residual Radioactive Contamination Compensation Act".

SEC. 2. FINDINGS.

Congress finds the following:

(1) Beginning in the early 1940s, the Department of Energy and its predecessors, the Atomic Energy Commission and the Manhattan Engineering District, relied upon hundreds of private-sector factories and laboratories to develop, test, and produce atomic weapons for use by the military, and these facilities became contaminated with radioactive materials during the process of producing material used for atomic weapons production.

(2) The Energy Employees Occupational Illness Compensation Program Act of 2000 (in this section referred to as EEOICPA) provides health care and lump-sum benefits for radiation-related cancers and other illnesses to certain covered workers made sick while they toiled in the nation's nuclear weapons factories, including vendor facilities. EEOICPA defines these private-sector vendor facilities as atomic weapons employer facilities, and employees working in such facilities while their employers were under contract to process nuclear weapons materials are defined as atomic weapons employees.

(3) Many of the atomic weapons employer facilities were not properly decontaminated after processing radioactive materials such as thorium, uranium, and radium and retained significant levels of contamination. Workers who were hired and employed in such atomic weapons employer facilities after the date that contracts were ended for production were potentially exposed to significant amounts of radiation. Congress was not aware of the presence of residual radioactive contamination in these facilities when it enacted EEOICPA, thus inadvertently denying coverage under the law to those who were unwittingly exposed to radiation left over from nuclear weapons activities.

(4) In December 2001, the National Defense Authorization Act for Fiscal Year 2002 (Pub-

lic Law 107-107) was enacted, which required in section 3151(b) that the National Institute for Occupational Safety and Health study and issue a final report to Congress by December 2002 describing which of the atomic weapons employer facilities had significant residual radioactive contamination remaining in them after processing materials for use in atomic weapons and during what time periods such radioactive contamination remained.

(5) In October 2003, the Institute issued a report, titled Report on Residual Radioactive and Beryllium Contamination in Atomic Weapons Employer and Beryllium Vendor Facilities. The report found that, out of 219 atomic weapons employer facilities—

(A) 97 (44 percent) of such facilities have potential for significant residual radioactive contamination outside of the periods in which atomic weapons-related production occurred;

(B) 88 (40 percent) of such facilities have little potential for significant residual radioactive contamination outside of the periods in which atomic weapons-related production occurred; and

(C) 34 (16 percent) of such facilities have insufficient information to make a determination.

(6) Congress is now aware that workers were employed in a substantial number of atomic weapons employer facilities years after the Manhattan Project ended. These workers were potentially harmed by legacy residual radioactive contamination that permeated the walls, the floors, and the air of their worksites well after the Atomic Energy Commission and the Department of Energy terminated contracts for production activities. This exposure to residual radioactive contamination took place without the knowledge or consent of these workers.

(7) Congress therefore declares that, based on the scientific assessment by the Institute, those workers hired and employed in such facilities during the period after Cold War production stopped but during which the Institute found there was significant residual radioactive contamination should be defined as atomic weapons employees under EEOICPA, should be eligible to apply for compensation under subtitle B of EEOICPA, and should have their claims evaluated on the same basis as those atomic weapons employees who were employed during the period when processing of radioactive materials was underway as part of the atomic weapons program.

SEC. 3. COVERAGE UNDER ENERGY EMPLOYEES OCCUPATIONAL ILLNESS COMPENSATION PROGRAM OF INDIVIDUALS EMPLOYED AT ATOMIC WEAPONS EMPLOYER FACILITIES DURING PERIODS OF RESIDUAL CONTAMINATION

Paragraph (3) of section 3621 of the Energy Employees Occupational Illness Compensation Program Act of 2000 (42 U.S.C. 73841) is amended to read as follows:

(3) The term atomic weapons employee means any of the following:

(A) An individual employed at an atomic weapons employer facility during a period when the employer was processing or producing, for the use by the United States, material that emitted radiation and was used in the production of an atomic weapon, excluding uranium mining and milling.

(B) An individual employed—

(i) at an atomic weapons employer facility with respect to which the National Institute for Occupational Safety and Health, in its report dated October 2003 and titled Report on Residual Radioactive and Beryllium Contamination at Atomic Weapons Employer Facilities and Beryllium Vendor Facilities, or any update to that report, found that

there is a potential (not including a case in which the Institute found that there is little potential) for significant residual contamination outside of the period in which weapons-related production occurred; and

(ii) during a period, as specified in such report or any update to such report, of significant residual contamination at that facility.

SEC. 4. UPDATE TO REPORT

In each of 2005, 2006, and 2007, the Director of the National Institute for Occupational Safety and Health shall submit to Congress, not later than December 31 of that year, an update to the report required by section 3151(b) of the National Defense Authorization Act for Fiscal Year 2002 (Public Law 107-107; 42 U.S.C. 7384 note). Each such update shall—

(1) for each facility for which such report, or any update to such report, found that insufficient information was available to determine whether significant residual contamination was present, determine whether significant residual contamination was present;

(2) for each facility for which such report, or any update to such report, found that significant residual contamination remained present as of the date of the report, determine the date on which such contamination ceased to be present;

(3) for each facility for which such report, or any update to such report, found that significant residual contamination was present but for which the Director has been unable to determine the extent to which such contamination is attributable to beryllium or atomic weapons-related activities, identify the specific dates of coverage attributable to such activities and, in so identifying, presume that such contamination is attributable to such activities until there is evidence of decontamination of residual contamination identified with beryllium or atomic weapons-related activities; and

(4) if new information that pertains to the report has been made available to the Director since that report was submitted, identify and describe such information.

SEC. 5. PUBLICATION IN FEDERAL REGISTER

The Director shall ensure that the report referred to in section 4, and each update required by section 4, are published in the Federal Register not later than 15 days after being released.

By Ms. CANTWELL (for herself and Mrs. MURRAY):

S. 2140. A bill to expand the boundary of the Mount Rainier National Park; to the Committee on Energy and Natural Resources.

Ms. CANTWELL. Mr. President, I rise today to introduce—along with my colleague Senator MURRAY—the Expanding and Making Mount Rainier National Park More Accessible Act.

This bill authorizes a boundary expansion of Mount Rainier National Park to allow the National Park Service to acquire 800 acres of land from private landowners, on a willing seller basis. These lands are located near the Carbon River and, if acquired, they would be included in Mount Rainier National Park, one of America's great national parks.

If enacted, the proposed expansion will improve access for visitors, allow for a new campsite to be built, and save taxpayers money that will no longer be needed to repair a frequently washed out road.

While this legislation will make Mount Rainier National Park safer and

more accessible for families and outdoor enthusiasts, it is important to note that this expansion will also promote the local economy. Outdoor recreation is more than an activity in the Northwest, it is also a key part of our economy. By improving access to the park, my bill will make it easier for visitors to enjoy the park and to purchase goods and services in nearby communities.

This expansion will ensure continued access to the park because the northwest entrance road is continually washed out by seasonal fluctuations of the glacier-fed Carbon River. The river, which now flows at a higher elevation than the roadbed, has blocked visitors from accessing the National Park Service's Ipsut Creek campground and nearby hiking trails inside the park. The repairs to this road have proven both costly and short-lived and have strained the National Park Service's already limited maintenance budget. In the long run, the expansion will save taxpayers money because the road will not have to be maintained to current standards. If this bill is enacted, the National Park Service plans to provide a shuttle service to take visitors to the Carbon Glacier trailhead. That way, visitors will still be able to hike to the Carbon Glacier during day trips.

If this bill is enacted, local conservation groups and the National Park Service will work to reach agreements with landowners in the proposed expansion area. I am pleased that the current landowners actively participated in the process and enthusiastically support this legislation. In fact, they are eager to sell their land to the National Park Service so that these lands will be permanently protected for the enjoyment of future generations.

I look forward to working with my colleagues in the Senate as well as other members of the Washington state congressional delegation to ensure swift passage of this important legislation.

SUBMITTED RESOLUTIONS

SENATE CONCURRENT RESOLUTION 93—AUTHORIZING THE USE OF THE ROTUNDA OF THE CAPITOL BY THE JOINT CONGRESSIONAL COMMITTEE ON INAUGURAL CEREMONIES

Mr. LOTT (for himself and Mr. DODD) submitted the following concurrent resolution; which was considered and agreed to:

S. CON. RES. 93

Resolved by the Senate (the House of Representatives concurring),

SECTION 1. USE OF THE ROTUNDA OF THE CAPITOL BY THE JOINT CONGRESSIONAL COMMITTEE ON INAUGURAL CEREMONIES.

The rotunda of the United States Capitol is authorized to be used on January 20, 2005, by the Joint Congressional Committee on Inaugural Ceremonies in connection with the proceedings and ceremonies conducted for the

inauguration of the President-elect and the Vice President-elect of the United States.

SENATE CONCURRENT RESOLUTION 94—ESTABLISHING THE JOINT CONGRESSIONAL COMMITTEE ON INAUGURAL CEREMONIES

Mr. LOTT (for himself and Mr. DODD) submitted the following concurrent resolution; which was considered and agreed to:

S. CON. RES. 94

Resolved by the Senate (the House of Representatives concurring),

SECTION 1. ESTABLISHMENT OF JOINT COMMITTEE.

There is established a Joint Congressional Committee on Inaugural Ceremonies (in this resolution referred to as the "joint committee"), consisting of 3 Senators and 3 Members of the House of Representatives appointed by the President of the Senate and the Speaker of the House of Representatives, respectively. The joint committee is authorized to make the necessary arrangements for the inauguration of the President-elect and the Vice President-elect of the United States.

SEC. 2. SUPPORT OF THE JOINT COMMITTEE.

The joint committee—

(1) is authorized to utilize appropriate equipment and the services of appropriate personnel of departments and agencies of the Federal Government, under arrangements between the joint committee and the heads of the departments and agencies, in connection with the inaugural proceedings and ceremonies; and

(2) may accept gifts and donations of goods and services to carry out its responsibilities.

AMENDMENTS SUBMITTED & PROPOSED

SA 2619. Mr. KENNEDY submitted an amendment intended to be proposed by him to the bill S. 1805, to prohibit civil liability actions from being brought or continued against manufacturers, distributors, dealers, or importers of firearms or ammunition for damages resulting from the misuse of their products by others.

SA 2620. Mrs. BOXER submitted an amendment intended to be proposed by her to the bill S. 1805, supra.

SA 2621. Mr. DASCHLE (for himself, Mr. CRAIG, and Mr. BAUCUS) proposed an amendment to the bill S. 1805, supra.

SA 2622. Mr. KOHL proposed an amendment to amendment SA 2620 submitted by Mrs. BOXER to the bill S. 1805, supra.

SA 2623. Mr. HATCH (for Mr. CAMPBELL (for himself, Mr. LEAHY, Mr. HATCH, Mr. DEWINE, Mr. SESSIONS, Mr. CRAIG, Mr. REID, and Mrs. BOXER)) proposed an amendment to the bill S. 1805, supra.

SA 2624. Mr. WARNER submitted an amendment intended to be proposed by him to the bill S. 1805, supra; which was ordered to lie on the table.

SA 2625. Mr. CRAIG (for Mr. FRIST (for himself and Mr. CRAIG)) proposed an amendment to the bill S. 1805, supra.

SA 2626. Mr. FRIST (for himself and Mr. MCCONNELL) proposed an amendment to the bill S. 1805, supra.

SA 2627. Ms. MIKULSKI (for herself, Mr. SARBANES, Mr. LAUTENBERG, Mr. CORZINE, and Mrs. CLINTON) proposed an amendment to the bill S. 1805, supra.

SA 2628. Mr. CRAIG (for Mr. FRIST (for himself and Mr. CRAIG)) proposed an amendment to the bill S. 1805, supra.

SA 2629. Mr. CORZINE (for himself, Mr. LAUTENBERG, Ms. MIKULSKI, Mr. KENNEDY, Mrs. CLINTON, and Mrs. BOXER) submitted an amendment intended to be proposed by him to the bill S. 1805, supra.

SA 2630. Mr. CRAIG (for Mr. FRIST (for himself and Mr. CRAIG)) proposed an amendment to the bill S. 1805, supra.

TEXT OF AMENDMENTS

SA 2619. Mr. KENNEDY submitted an amendment intended to be proposed by him to the bill S. 1805, to prohibit civil liability actions from being brought or continued against manufacturers, distributors, dealers, or importers of firearms or ammunition for damages resulting from the misuse of their products by others; as follows:

On page 11, after line 19, add the following:

SEC. 5. ARMOR PIERCING AMMUNITION.

(a) EXPANSION OF DEFINITION OF ARMOR PIERCING AMMUNITION.—Section 921(a)(17)(B) of title 18, United States Code, is amended—

(1) in clause (i), by striking "or" at the end;

(2) in clause (ii), by striking the period at the end and inserting a semicolon; and

(3) by adding at the end the following:

"(iii) a projectile that may be used in a handgun and that the Attorney General determines, pursuant to section 926(d), to be capable of penetrating body armor; or

"(iv) a projectile for a centerfire rifle, designed or marketed as having armor piercing capability, that the Attorney General determines, pursuant to section 926(d), to be more likely to penetrate body armor than standard ammunition of the same caliber."

(b) DETERMINATION OF THE CAPABILITY OF PROJECTILES TO PENETRATE BODY ARMOR.—Section 926 of title 18, United States Code, is amended by adding at the end the following:

"(d)(1) Not later than 1 year after the date of enactment of this subsection, the Attorney General shall promulgate standards for the uniform testing of projectiles against Body Armor Exemplar.

"(2) The standards promulgated pursuant to paragraph (1) shall take into account, among other factors, variations in performance that are related to the length of the barrel of the handgun or centerfire rifle from which the projectile is fired and the amount and kind of powder used to propel the projectile.

"(3) As used in paragraph (1), the term 'Body Armor Exemplar' means body armor that the Attorney General determines meets minimum standards for the protection of law enforcement officers."

SA 2620. Mrs. BOXER submitted an amendment intended to be proposed by her to the bill S. 1805, to prohibit civil liability actions from being brought or continued against manufacturers, distributors, dealers, or importers of firearms or ammunition for damages resulting from the misuse of their products by others; as follows:

On page 11, after line 19, add the following:

SEC. 5. REQUIREMENT OF CHILD HANDGUN SAFETY DEVICES.

(a) SHORT TITLE.—This section may be cited as the "Child Safety Device Act of 2004".

(b) DEFINITIONS.—Section 921(a) of title 18, United States Code, is amended by adding at the end the following:

"(36) The term 'locking device' means a device or locking mechanism that is approved by a licensed firearms manufacturer for use