30,000 of these sex offenders in the State of Florida. In response to the recent tragedies in Florida, Idaho, and North Dakota, several States have enacted stronger laws to protect our children from sex predators. In Florida, for example, the legislature passed a law that will provide tougher sentences for child sex offenders, and aid law enforcement in effectively monitoring those sex offenders. This law will require sex offenders, released back into our communities, to wear a bracelet that will have a global positioning system track them.

I applaud the initiative by Florida, and other States seeking to pass similar laws, and I believe that it is important that there is an appropriate Federal response that will be supportive of the States and local governments that are addressing this problem. To be effective, tough laws on these sexual predators of children must be properly funded, and I believe these tough laws being passed by state legislatures are worth properly funding when they will protect our children.

The Jessica Lunsford and Sarah Lunde Act will support State and local governments that, like Florida, are attempting to protect their children by providing greater monitoring tools for law enforcement. This bill will provide a total of $30 million in grants to States to help implement State laws to get tougher on sex offenders released back into their communities with electronic monitoring technology. The bill will provide for $10 million in grants for fiscal years 2006 through 2008. The bill then directs the Attorney General to provide a report to Congress assessing the effectiveness of the program and making recommendations as to future funding levels.

There are no silver bullets to stop sexual predators from preying on our children, but I believe that tough laws, such as the new Florida statute, are going to go a long way in preventing sex offenders from re-offending.

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. 1407

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 ''Jessica Lunsford and Sarah Lunde Act''.

SEC. 2. SEXUAL PREDATOR MONITORING PROGRAM.

(a) GRANTS AUTHORIZED.—

(1) IN GENERAL.—The Attorney General is authorized to award grants (referred to as ''Jessica Lunsford and Sarah Lunde Grants'') to State and local governments to assist such States and local governments in—

(A) carrying out programs to outfit sexual offenders with electronic monitoring units; and

(B) the employment of law enforcement officials necessary to carry out such programs.

(2) DURATION.—The Secretary shall award grants under this Act for a period not to exceed 3 years.

(b) APPLICATION.—

(1) IN GENERAL.—Each State or local government desiring a grant under this Act shall submit an application to the Attorney General at such time, in such manner, and accompanied by such information as the Attorney General may reasonably require.

(2) CONTENTS.—Each application submitted pursuant to paragraph (1) shall—

(A) describe the activities for which assistance under this Act is sought; and

(B) provide such additional assurances as the Attorney General determines to be essential to ensure compliance with the requirements of this Act.

SEC. 3. INNOVATION.

In making grants under this Act, the Attorney General shall ensure that different approaches to monitoring are funded to allow an assessment of effectiveness.

SEC. 4. DEFINITION.

In this Act, the term ''sexual offender'' means an offender 18 years of age or older who commits a sexual offense against a minor.

SEC. 5. AUTHORIZATION OF APPROPRIATIONS.

(a) IN GENERAL.—There are authorized to be appropriated $10,000,000 for each of the fiscal years 2006 through 2008 to carry out this Act.

(b) REPORT.—Not later than April 1, 2008, the Attorney General shall report to Congress—

(1) assessing the effectiveness and value of programs funded by this Act;

(2) comparing the cost-effectiveness of the electronic monitoring to reduce sex offenses compared to other alternatives; and

(3) making recommendations for continuing funding and the appropriate levels for such funding.

By Mr. SMITH (for himself, Mr. NELSON of Florida, Mr. STEVENS, Mr. INOUYE, Mr. MCCAIN, and Mr. PRYOR):

S. 1408. A bill to strengthen data protection and safeguards, require data breach notification, and further prevent identity theft; to the Committee on Commerce, Science, and Transportation.

Mr. SMITH. Mr. President, I rise today with Senators BILL NELSON, STEVENS, INOUYE, MCCAIN, and PRYOR to introduce the Identity Theft Protection Act of 2005. The introduction of this bill has been a bipartisan effort and I thank my colleagues on the Senate Commerce Committee for helping to negotiate a fair and balanced bill.

Identity theft is one of the fastest growing crimes in America. It is estimated that over 10 million Americans are victims of some form of identity theft each year. The total cost of this crime approaches $50 billion per year, with the average loss from the misuse of a victim's personal information being almost $5,000. In 2004 alone, consumers who were victims of ID theft spent a total of 297 million hours resolving problems that arose from the crime.

Every year, the FTC compiles a list of the top 10 categories of fraud-related complaints. Identity theft has topped that list of complaints each of the past 5 years. My own State of Oregon ranks ninth in the Nation for fraud complaints and identity theft.

Data breaches are becoming an increasingly common type of identity theft that affects millions of consumers nationwide. Last year, there were at least 43 known incidents of security breaches, potentially affecting over 9 million individuals. These breaches range from sloppy record keeping and security procedures by companies to extremely sophisticated online thefts by computer hackers.

Our bipartisan bill ensures that businesses and organizations have the proper security procedures in place to safeguard consumers' sensitive and personal information. This legislation requires any entity that acquires, maintains or utilizes sensitive personal information to have a security program to safeguard such data. Furthermore, we require these entities to verify the credentials of third parties seeking personal and sensitive information and require strict disposal and transfer procedures for such information.

It is imperative that consumers be notified of any potential breach in the security of their personal information. The cost of an incident of identity theft, both in terms of out-of-pocket expense and time spent resolving problems, is significantly smaller if the misuse of the victim's personal information is discovered quickly.

Our bill requires consumer notification if a data breach results in a significant risk of identity theft. Individuals will be notified immediately when any significant breach has occurred. Any breach affecting a minimum of 1,000 individuals also requires the entity to report the breach to the FTC and all the consumer reporting agencies.

We realize that an individual's Social Security Number deserves the utmost security and protection against fraud, manipulation, and theft. To that end, this bill restricts the collection of and access to Social Security Numbers by limiting the solicitation of Social Security Numbers and prohibiting their display on employee and student identification cards.

In addition, our bill will allow consumers to place, lift, and temporarily remove a security freeze on their credit, which would prevent credit from being extended to third parties without authorization from the consumer. We would also pre-empt state law to create uniformity and compliance by businesses and organizations.

Protecting sensitive information is an issue of great importance for all Americans so we are requiring the FTC to establish an Information Working Group comprised of industry participants, consumer groups, and other interested parties to develop best practices to protect sensitive personal information.

Consumers should have confidence when they share their information with others that their information will be protected. At the same time, the ability of legitimate companies to access personal information facilitates commerce and continues to have important benefits to consumers.

We believe our legislation strikes the appropriate balance between ensuring

the continued existence of these critical services and guaranteeing the security of consumer's personal information. I urge my colleagues to co-sponsor this important legislation to protect consumers from future breaches of identity theft.

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

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

S. 1408

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 ''Identity Theft Protection Act''.

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

Sec. 1. Short title; table of contents.
Sec. 2. Protection of sensitive personal information.
Sec. 3. Notification of security breach risk.
Sec. 4. Security freeze.
Sec. 5. Enforcement.
Sec. 6. Enforcement by State attorneys general.
Sec. 7. Preemption of State law.
Sec. 8. Social security and driver's license number protection.
Sec. 9. Information security working group.
Sec. 10. Definitions.
Sec. 11. Authorization of appropriations.
Sec. 12. Effective dates.

SEC. 2. PROTECTION OF SENSITIVE PERSONAL INFORMATION.

(a) IN GENERAL.—In accordance with regulations prescribed by the Federal Trade Commission under subsection (b), a covered entity shall take reasonable steps to protect against security breaches and to prevent unauthorized access to sensitive personal information the covered entity sells, maintains, collects, or transfers.

(b) REGULATIONS.—Not later than 1 year after the date of enactment of this Act, the Commission shall promulgate regulations to implement subsection (a), including regulations that—

(1) require covered entities to develop, implement, and maintain an effective information security program that contains administrative, technical, and physical safeguards for sensitive personal information, taking into account the use of technological safeguards, including encryption, truncation, and other safeguards available or being developed for such purposes;

(2) require procedures for verifying the credentials of any third party seeking to obtain the sensitive personal information of another person; and

(3) require disposal procedures to be followed by covered entities that—

(A) dispose of sensitive personal information; or

(B) transfer sensitive personal information to third parties for disposal.

SEC. 3. NOTIFICATION OF SECURITY BREACH RISK.

(a) SECURITY BREACHES AFFECTING 1,000 OR MORE INDIVIDUALS.—

(1) IN GENERAL.—If a covered entity discovers a breach of security and determines that the breach of security affects the sensitive personal information of 1,000 or more individuals, then, before conducting the notification required by subsection (b), it shall—

(A) report the breach to the Commission (or other appropriate Federal regulator under section 5); and

(B) notify all consumer reporting agencies described in section 603(p)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)(1)) of the breach.

(2) FTC WEBSITE PUBLICATIONS.—Whenever the Commission receives a report under paragraph (1)(A), it shall post a report of the breach of security on its website without disclosing any sensitive personal information or the names of the individuals affected.

(b) NOTIFICATION OF CONSUMERS.—Whenever a covered entity discovers a breach of security and determines that the breach of security has resulted in, or that there is a basis for concluding that a reasonable risk of identity theft to 1 or more individuals, the covered entity shall notify each such individual.

(c) METHODS OF NOTIFICATION; NOTICE CONTENT.—Within 1 year after the date of enactment of this Act, the Commission shall promulgate regulations that establish methods of notification to be followed by covered entities in complying with the requirements of this section and the content of the notices required. In promulgating those regulations, the Commission shall take into consideration the types of sensitive personal information involved, the nature and scope of the security breach, other appropriate factors, and the most effective means of notifying affected individuals.

(d) TIMING OF NOTIFICATION.—

(1) IN GENERAL.—Except as provided in paragraph (2), notice required by subsection (a) shall be given—

(A) in the most expedient manner practicable;

(B) without unreasonable delay, but not later than 90 days after the date on which the breach of security was discovered by the covered entity; and

(C) in a manner that is consistent with any measures necessary to determine the scope of the breach and restore the security and integrity of the data system.

(2) LAW ENFORCEMENT AND HOMELAND SECURITY RELATED DELAYS.—Notwithstanding paragraph (1), the giving of notice as required by that paragraph may be delayed for a reasonable period of time if—

(A) a Federal law enforcement agency determines that the timely giving of notice under subsections (a) and (b), as required by paragraph (1), would materially impede a civil or criminal investigation; or

(B) a Federal national security or homeland security agency determines that such timely giving of notice would threaten national or homeland security.

SEC. 4. SECURITY FREEZE.

(a) In General.—

(1) EMPLACEMENT.—A consumer may place a security freeze on his or her credit report by making a request to a consumer credit reporting agency in writing or by telephone.

(2) CONSUMER DISCLOSURE.—If a consumer requests a security freeze, the consumer credit reporting agency shall disclose to the consumer the process of placing and removing the security freeze and explain to the consumer the potential consequences of the security freeze.

(b) EFFECT OF SECURITY FREEZE.—

(1) RELEASE OF INFORMATION BLOCKED.—If a security freeze is in place on a consumer's credit report, a consumer reporting agency may not release information from the credit report to a third party without prior express authorization from the consumer.

(2) INFORMATION PROVIDED TO THIRD PARTIES.—Paragraph (2) does not prevent a consumer credit reporting agency from advising a third party that a security freeze is in effect with respect to the consumer's credit report. If a third party, in connection with an application for credit, requests access to a consumer credit report on which a security freeze is in place, the third party may treat the application as incomplete.

(c) REMOVAL; TEMPORARY SUSPENSION.—

(1) IN GENERAL.—Except as provided in paragraph (4), a security freeze shall remain in place until the consumer requests that the security freeze be removed. A consumer may remove a security freeze on his or her credit report by making a request to a consumer credit reporting agency in writing or by telephone.

(2) CONDITIONS.—A consumer credit reporting agency may remove a security freeze placed on a consumer's credit report only—

(A) upon the consumer's request, pursuant to paragraph (1); or

(B) if the agency determines that the consumer's credit report was frozen due to a material misrepresentation of fact by the consumer.

(3) NOTIFICATION TO CONSUMER.—If a consumer credit reporting agency intends to remove a freeze upon a consumer's credit report pursuant to paragraph (2)(B), the consumer credit reporting agency shall notify the consumer in writing prior to removing the freeze on the consumer's credit report.

(4) TEMPORARY SUSPENSION.—A consumer may have a security freeze on his or her credit report temporarily suspended by making a request to a consumer credit reporting agency in writing or by telephone and specifying beginning and ending dates for the period during which the security freeze is not to apply to that consumer's credit report.

(d) RESPONSE TIMES; NOTIFICATION OF OTHER ENTITIES.—

(1) IN GENERAL.—A consumer credit reporting agency shall—

(A) place a security freeze on a consumer's credit report under subsection (a) no later than 5 business days after receiving a request from the consumer under subsection (a)(1); and

(B) remove, or temporarily suspend, a security freeze within 3 business days after receiving a request for removal or temporary suspension from the consumer under subsection (c).

(2) NOTIFICATION OF OTHER COVERED ENTITIES.—If the consumer requests in writing or by telephone that other covered entities be notified of the request, the consumer reporting agency shall notify all other consumer reporting agencies described in section 603(p)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)(1)) of the request within 3 days after placing, removing, or temporarily suspending a security freeze on the consumer's credit report under subsection (a), (c)(2)(A), or subsection (c)(4), respectively.

(3) IMPLEMENTATION BY OTHER COVERED ENTITIES.—A consumer reporting agency that is notified of a request under paragraph (2) to place, remove, or temporarily suspend a security freeze on a consumer's credit report shall place, remove, or temporarily suspend the security freeze on that credit report within 3 business days after receiving the notification.

(e) CONFIRMATION.—Whenever a consumer credit reporting agency places, removes, or temporarily suspends a security freeze on a consumer's credit report at the request of that consumer under subsection (a) or (c), respectively, it shall send a written confirmation thereof to the consumer within 10 business days after placing, removing, or temporarily suspending the security freeze on the credit report. This subsection does not apply to the placement, removal, or temporary suspension of a security freeze by a consumer reporting agency because of a notification received under subsection (d)(2).

(f) ID REQUIRED.—A consumer credit reporting agency may not place, remove, or temporarily suspend a security freeze on a consumer's credit report at the consumer's request unless the consumer provides proper identification (within the meaning of section

610(a)(1) of the Fair Credit Reporting Act (15 U.S.C. 1681h) and the regulations thereunder.

(g) EXCEPTIONS.—This section does not apply to the use of a consumer credit report by any of the following:

(1) A person or entity, or a subsidiary, affiliate, or agent of that person or entity, or an assignee of a financial obligation owing by the consumer to that person or entity, or a prospective assignee of a financial obligation owing by the consumer to that person or entity in conjunction with the proposed purchase of the financial obligation, with which the consumer has or had prior to assignment an account or contract, including a demand deposit account, or to whom the consumer issued a negotiable instrument, for the purposes of reviewing the account or collecting the financial obligation owing for the account, contract, or negotiable instrument.

(2) Any Federal, State or local agency, law enforcement agency, trial court, or private collection agency acting pursuant to a court order, warrant, or subpoena.

(3) A child support agency or its agents or assigns acting pursuant to subtitle D of title IV of the Social Security Act (42 U.S.C. et seq.) or similar State law.

(4) The Department of Health and Human Services, a similar State agency, or the agents or assigns of the Federal or State agency acting to investigate medicare or medicaid fraud.

(5) The Internal Revenue Service or a State or municipal taxing authority, or a State department of motor vehicles, or any of the agents or assigns of these Federal, State, or municipal agencies acting to investigate or collect delinquent taxes or unpaid court orders or to fulfill any of their other statutory responsibilities.

(6) The use of consumer credit information for the purposes of prescreening as provided for by the Federal Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

(7) Any person or entity administering a credit file monitoring subscription to which the consumer has subscribed.

(8) Any person or entity for the purpose of providing a consumer with a copy of his or her credit report or credit score upon the consumer's request.

(h) FEES.—

(1) IN GENERAL.—Except as provided in paragraph (2), a consumer credit reporting agency may charge a reasonable fee, as determined by the Commission, for placing, removing, or temporarily suspending a security freeze on a consumer's credit report.

(2) ID THEFT VICTIMS.—A consumer credit reporting agency may not charge a fee for placing, removing, or temporarily suspending a security freeze on a consumer's credit report if—

(A) the consumer is a victim of identity theft; and

(B) the consumer has filed a police report with respect to the theft.

(i) LIMITATION ON INFORMATION CHANGES IN FROZEN REPORTS.—

(1) IN GENERAL.—If a security freeze is in place on a consumer's credit report, a consumer credit reporting agency may not change any of the following official information in that credit report without sending a written confirmation of the change to the consumer within 30 days after the change is made:

(A) Name.

(B) Date of birth.

(C) Social Security number.

(D) Address.

(2) CONFIRMATION.—Paragraph (1) does not require written confirmation for technical modifications of a consumer's official information, including name and street abbreviations, complete spellings, or transposition of numbers or letters. In the case of an address change, the written confirmation shall be sent to both the new address and to the former address.

(j) CERTAIN ENTITY EXEMPTIONS.—

(1) AGREGATORS AND OTHER AGENCIES.—The provisions of subsections (a) through (h) do not apply to a consumer credit reporting agency that acts only as a reseller of credit information by assembling and merging information contained in the data base of another consumer credit reporting agency or multiple consumer credit reporting agencies, and does not maintain a permanent data base of credit information from which new consumer credit reports are produced.

(2) OTHER EXEMPTED ENTITIES.—The following entities are not required to place a security freeze in a credit report:

(A) A check services or fraud prevention services company, which issues reports on incidents of fraud or authorizations for the purpose of approving or processing negotiable instruments, electronic funds transfers, or similar methods of payments.

(B) A deposit account information service company, which issues reports regarding account closures due to fraud, substantial overdrafts, ATM abuse, or similar negative information regarding a consumer, to inquiring banks or other financial institutions for use only in reviewing a consumer request for a deposit account at the inquiring bank or financial institution.

SEC. 5. ENFORCEMENT.

(a) ENFORCEMENT BY COMMISSION.—Except as provided in subsection (c), this Act shall be enforced by the Commission.

(b) VIOLATION IS UNFAIR OR DECEPTIVE ACT OR PRACTICE.—The violation of any provision of this Act shall be treated as an unfair or deceptive act or practice proscribed under a rule issued under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(c) 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; and

(4) the Securities and Exchange Act of 1934 (15 U.S.C. 78a et seq.) by the Securities and Exchange Commission with respect to—

(A) a broker or dealer subject to that Act;

(B) an investment company subject to the Investment Company Act of 1940 (15 U.S.C. 80a-1 et seq.); and

(C) an investment advisor subject to the Investment Advisers Act of 1940 (15 U.S.C. 80b-1 et seq.).

(d) EXERCISE OF CERTAIN POWERS.—For the purpose of the exercise by any agency referred to in subsection (c) 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 (c), 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.

(e) PENALTIES.—

(1) IN GENERAL.—Notwithstanding section 5(m) of the Federal Trade Commission Act (15 U.S.C. 45(m)), the Commission may not obtain a civil penalty under that section for a violation of this Act in excess of—

(A) $11,000 for each such individual; and

(B) $11,000,000 in the aggregate for all such individuals with respect to the same violation.

(2) OTHER AUTHORITY NOT AFFECTED.—Nothing in this Act shall be construed to limit or affect in any way the Commission's authority to bring enforcement actions or take any other measure under the Federal Trade Commission Act (15 U.S.C. 41 et seq.) or any other provision of law.

(f) NO PRIVATE CAUSE OF ACTION.—Nothing in this Act establishes a private cause of action against a covered entity for the violation of any provision of this Act.

(g) COMPLIANCE WITH GRAMM-LEACH-BLILEY ACT.—Any person to which title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.) applies shall be deemed to be in compliance with the notification requirements of this Act with respect to a breach of security if that person is in compliance with the notification requirements of that title with respect to that breach of security.

SEC. 6. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) IN GENERAL.—A State, as parens patriae, may bring a civil action on behalf of its residents in an appropriate district court of the United States to enforce the provisions of this Act, or to impose the civil penalties authorized by section 5, whenever the attorney general of the State has reason to believe that the interests of the residents of the State have been or are being threatened or adversely affected by a covered entity that violates this Act or a regulation under this Act.

(b) NOTICE.—The State shall serve written notice to the Commission (or other appropriate Federal regulator under section 5) of any civil action under subsection (a) prior to initiating such civil action. The notice shall include a copy of the complaint to be filed to initiate such civil action, except that if it is not feasible for the State to provide such prior notice, the State shall provide such notice immediately upon instituting such civil action.

(c) AUTHORITY TO INTERVENE.—Upon receiving the notice required by subsection (b), the Commission (or other appropriate Federal regulator under section 5) may intervene in such civil action and upon intervening—

(1) be heard on all matters arising in such civil action; and

(2) file petitions for appeal of a decision in such civil action.

(d) CONSTRUCTION.—For purposes of bringing any civil action under subsection (a), nothing in this section shall prevent the attorney general of a State from exercising the powers conferred on the attorney general by the laws of such State to conduct investigations or to administer oaths or affirmations or to compel the attendance of witnesses or the production of documentary and other evidence.

(e) VENUE; SERVICE OF PROCESS.—In a civil action brought under subsection (a)—

(1) the venue shall be a judicial district in which—

(A) the covered entity operates;

(B) the covered entity was authorized to do business; or

(C) where the defendant in the civil action is found;

(2) process may be served without regard to the territorial limits of the district or of the State in which the civil action is instituted; and

(3) a person who participated with a covered entity in an alleged violation that is being litigated in the civil action may be joined in the civil action without regard to the residence of the person.

(f) LIMITATION ON STATE ACTION WHILE FEDERAL ACTION IS PENDING.—If the Commission (or other appropriate Federal agency under section 5) has instituted a civil action or an administrative action for violation of this Act, no State attorney general, or official or agency of a State, may bring an action under this subsection during the pendency of that action against any defendant named in the complaint of the Commission or the other agency for any violation of this Act alleged in the complaint.

(g) ENFORCEMENT OF STATE LAW.—Nothing contained in this section shall prohibit an authorized State official from proceeding in State court to enforce a civil or criminal statute of such State.

SEC. 7. PREEMPTION OF STATE LAW.

(a) IN GENERAL.—This Act preempts any State or local law, regulation, or rule that requires a covered entity—

(1) to develop, implement, or maintain information security programs to which this Act applies; or

(2) to notify individuals of breaches of security regarding their sensitive personal information.

(b) LIABILITY.—This Act preempts any State or local law, regulation, rule, administrative procedure, or judicial precedent under which liability is imposed on a covered entity for failure—

(1) to implement and maintain an adequate information security program; or

(2) to notify an individual of any breach of security pertaining to any sensitive personal information about that individual.

(c) SECURITY FREEZE.—This Act preempts any State or local law, regulation, or rule that requires consumer reporting agencies to impose a security freeze on consumer credit reports at the request of a consumer.

SEC. 8. SOCIAL SECURITY NUMBER PROTECTION.

(a) PROHIBITION OF UNNECESSARY SOLICITATION OF SOCIAL SECURITY NUMBERS.—No covered entity may solicit any social security number from an individual unless there is a specific use of the social security number for which no other identifier reasonably can be used.

(b) PROHIBITION OF THE DISPLAY OF SOCIAL SECURITY NUMBERS ON EMPLOYEE IDENTIFICATION CARDS, ETC..—

(1) IN GENERAL.—No covered entity may display the social security number (or any derivative of such number) of an individual on any card or tag that is commonly provided to employees (or to their family members), faculty, staff, or students for purposes of identification.

(2) DRIVER'S LICENSES.—A State may not display the social security number of an individual on driver's licenses issued by that State.

(c) PROHIBITION OF INMATE ACCESS TO SOCIAL SECURITY ACCOUNT NUMBERS.—

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

''(xi) No executive, legislative, or judicial agency or instrumentality of the Federal Government or of a State or political subdivision thereof (or person acting as an agent of such an agency or instrumentality) may employ, or enter into a contract for the use or employment of, prisoners in any capacity that would allow such prisoners access to the social security account numbers of other individuals. For purposes of this clause, the term 'prisoner' means an individual confined in a jail, prison, or other penal institution or correctional facility.''.

(2) TREATMENT OF CURRENT ARRANGEMENTS.—In the case of—

(i) prisoners employed as described in clause (xi) of section 205(c)(2)(C) of the Social Security Act (42 U.S.C. 405(c)(2)(C)), as added by paragraph (1), on the date of enactment of this Act, and

(ii) contracts described in such clause in effect on such date,

the amendment made by this section shall take effect 90 days after the date of enactment of this Act.

SEC. 9. INFORMATION SECURITY WORKING GROUP.

(a) INFORMATION SECURITY WORKING GROUP.—The Chairman of the Commission shall establish an Information Security Working Group to develop best practices to protect sensitive personal information stored and transferred. The Working Group shall be composed of industry participants, consumer groups, and other interested parties.

(b) REPORT.—Not later than 12 months after the date on which the Working Group is established under subsection (a), the Working Group shall submit to Congress a report on their findings.

SEC. 10. DEFINITIONS.

In this Act:

(1) BREACH OF SECURITY.—The term ''breach of security'' means unauthorized access to and acquisition of data in any form or format containing sensitive personal information that compromises the security or confidentiality of such information and establishes a basis to conclude that a reasonable risk of identity theft to an individual exists.

(2) COMMISSION.—The term ''Commission'' means the Federal Trade Commission.

(3) CONSUMER CREDIT REPORTING AGENCY.—The term ''consumer credit reporting agency'' means any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing credit reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing credit reports.

(4) COVERED ENTITY.—The term ''covered entity'' means a sole proprietorship, partnership, corporation, trust, estate, cooperative, association, or other commercial entity, and any charitable, educational, or nonprofit organization, that acquires, maintains, or utilizes sensitive personal information.

(5) CREDIT REPORT.—The term ''credit report'' means a consumer report, as defined in section 603(d) of the Federal Fair Credit Reporting Act (15 U.S.C. 1681a(p)), that is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility for credit for personal, family or household purposes.

(6) IDENTITY THEFT.—The term ''identity theft'' means the unauthorized acquisition, purchase, sale, or use by any person of an individual's sensitive personal information that—

(A) violates section 1028 of title 18, United States Code, or any provision of State law in *pari materia*; or

(B) results in economic loss to the individual whose sensitive personal information was used.

(7) REVIEWING THE ACCOUNT.—The term ''reviewing the account'' includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements.

(8) SENSITIVE PERSONAL INFORMATION.—

(A) IN GENERAL.—Except as provided in subparagraphs (B) and (C), the term ''sensitive personal information'' means an individual's name, address, or telephone number combined with 1 or more of the following data elements related to that individual:

(i) Social security number, taxpayer identification number, or employer identification number.

(ii) Financial account number, or credit card or debit card number of such individual, combined with any required security code, access code, or password that would permit access to such individual's account.

(iii) State driver's license identification number or State resident identification number.

(iv) Consumer credit report.

(v) Employee, faculty, student, or United States armed forces serial number.

(vi) Genetic or biometric information.

(vii) Mother's maiden name.

(B) FTC MODIFICATIONS.—The Commission may, through a rulemaking proceeding, designate other identifying information that may be used to effectuate identity theft as sensitive personal information for purposes of this Act and limit or exclude any information described in subparagraph (A) from the definition of sensitive personal information for purposes of this Act.

(C) PUBLIC RECORDS.—Nothing in this Act prohibits a covered entity from obtaining, aggregating, or using sensitive personal information it lawfully obtains from public records in a manner that does not violate this Act.

SEC. 11. AUTHORIZATION OF APPROPRIATIONS.

There are authorized to be appropriated to the Commission $1,000,000 for each of fiscal years 2006 through 2010 to carry out this Act.

SEC. 12. EFFECTIVE DATES.

(a) IN GENERAL.—Except as provided in subsection (b), the provisions of this Act take effect upon its enactment.

(b) PROVISIONS REQUIRING RULEMAKING.—The Commission shall initiate 1 or more rulemaking proceedings under sections 2, 3, and 4 within 45 days after the date of enactment of this Act. The Commission shall promulgate all final rules pursuant to those rulemaking proceedings within 1 year after the date of enactment of this Act. The provisions of sections 2, 3, and 4 shall take effect on the same date 6 months after the date on which the Commission promulgates the last final rule under the proceeding or proceedings commenced under the preceding sentence.

(c) PREEMPTION.—Section 7 shall take effect at the same time as sections 2, 3, and 4 take effect.

Mr. STEVENS. Mr. President, I am pleased to join Senators INOUYE, SMITH, MCCAIN, NELSON, and PRYOR in introducing a bipartisan bill to address the growing perpetration of identity theft against American consumers. The bipartisan bill, the ''Identity Theft Protection Act,'' is the product of two Commerce Committee hearings that featured testimony from businesses that aggregate and sell consumer information as a commodity, and the full

Federal Trade Commission, FTC, which recommended much of what is contained in this legislation.

The occurrence of identity theft in the United States has reached epidemic proportions. The incidence of this crime rose 15 percent in 2002, and 80 percent in 2003. The FTC stated in February 2005 that each year nearly 10 million Americans—or roughly 4.6 percent of the domestic adult population—are victimized by identity thieves. The FTC indicates that physical and online identity theft accounted for 39 percent of the more than 635,000 consumer fraud complaints filed last year with the agency. The costs associated with identity theft are enormous. In 2003, the FTC estimated that the losses to businesses and financial institutions due to identity theft totaled $48 billion, and the out-of-pocket losses to consumers totaled $5 billion, which does not take into account the average 300 hours spent by victims restoring their good names.

This year alone, there have been at least 43 reported information breaches affecting potentially more than 9 million Americans. This string of data theft has focused the attention of Congress, consumers, and privacy proponents. It has raised questions concerning the business practices of data brokers and whether consumers' personal information is adequately protected from identity thieves. The difficulty of finding solutions to this and other types of identity theft is striking a balance between ensuring adequate security of sensitive personal information while not inhibiting the legitimate free flow of information that is vital to the domestic economy and law enforcement.

The bill that we introduce today will not end all identity theft. No legislation can accomplish that objective. But this bill would require bolstered information safeguards and ensure notification of consumers whose sensitive personal information has been acquired without authorization. More specifically, the bill, among other things, would direct the FTC to develop rules that would require all covered entities that handle sensitive personal information to develop, implement, and maintain appropriate safeguards to protect such information, and provide effective notice to consumers in the event of a breach. The bill would limit the solicitation of Social Security numbers by covered entities, and restrict employers, State agencies, or educational institutions from displaying social security numbers on identification tags for employees and students, and for drivers licenses. The bill also would allow consumers to freeze their credit for a reasonable fee to protect themselves from identity theft, and preempt similar State or local law in an effort to provide a uniform Federal standard rather than a patchwork of widely varying State or local laws.

I look forward to working with my colleagues on legislation that will mitigate to the greatest extent possible the occurrence of identity theft in this country, but without inhibiting an information sharing system that yields extraordinary benefits to every American.

By Ms. MURKOWSKI:

S. 1409. A bill to amend the Safe Drinking Water Act Amendments of 1996 to modify the grant program to improve sanitation in rural and Native villages in the State of Alaska; to the Committee on Environment and Public Works.

Ms. MURKOWSKI. Mr. President, I rise to introduce a bill that will allow the Environmental Protection Agency to continue to provide grant funding and technical assistance to small, rural communities in Alaska for critical water and sewer projects. These rural communities are only accessible by either aircraft or boat.

This important funding was originally authorized as part of the Safe Drinking Water Act Amendments of 1996 and was reauthorized in 2000. The authorization for this program expires at the end of fiscal year 2005. Every fiscal year, the EPA transfers funding authorized by this program to the State of Alaska's Village Safe Water Program, which is managed by the Alaska Department of Environmental Conservation.

The water and sewer conditions in the villages in Alaska that still need this critical funding rival the conditions in rural communities in third world countries. For example, residents in some villages in Alaska have to go to a central source in the community to get fresh water. This source is usually a well. Instead of flushing toilets, residents have to use a device called a ''honeybucket.'' This device is a large bucket with a toilet seat on top. When the honeybucket is full, it is usually dumped in a lagoon or on land. Sometimes, these dump locations are near sources of drinking water.

The Village Safe Water program has been a success over the years. Many homes in Alaska's rural communities now have plumbing due to funds authorized by this program. However, thirty-three percent of homes in these communities still do not have in-house plumbing. It is unacceptable that the residents of these communities still do not have access to conventional plumbing in their homes in 2005.

Earlier this year, the Office of Management and Budget published a Program Assessment Rating Tool report concerning this program. This report found several deficiencies concerning the administration of this program. However, I have been assured that the EPA and the Alaska Department of Environmental Conservation are working closely together to correct these deficiencies.

It is imperative that we reauthorize this critically important program before the end of this fiscal year. The health and well-being of rural Alaskans is at stake.

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

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

S. 1409

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

SECTION 1. GRANTS TO ALASKA TO IMPROVE SANITATION IN RURAL AND NATIVE VILLAGES.

Section 303 of the Safe Drinking Water Act Amendments of 1996 (33 U.S.C. 1263a) is amended—

(1) in subsection (b), by striking ''50 percent'' and inserting ''75 percent''; and

(2) in subsection (e)—

(A) by striking ''$40,000,000'' and inserting ''$45,000,000''; and

(B) by striking ''2005'' and inserting ''2010''.

AMENDMENTS SUBMITTED AND PROPOSED

SA 1222. Mr. REID (for himself, Mr. LEVIN, Mr. ROCKEFELLER, Mr. BIDEN, and Mr. SCHUMER) proposed an amendment to the bill H.R. 2360, making appropriations for the Department of Homeland Security for the fiscal year ending September 30, 2006, and for other purposes.

SA 1223. Mr. FRIST proposed an amendment to the bill H.R. 2360, supra.

SA 1224. Mr. REID (for Mr. BYRD (for himself and Ms. STABENOW)) proposed an amendment to the bill H.R. 2360, supra.

SA 1225. Mr. GREGG (for Mr. KENNEDY) proposed an amendment to amendment SA 1139 proposed by Mr. SESSIONS (for himself and Mr. HATCH) to the bill H.R. 2360, supra.

TEXT OF AMENDMENTS

SA 1222. Mr. REID (for himself, Mr. LEVIN, Mr. ROCKEFELLER, Mr. BIDEN, and Mr. SCHUMER) proposed an amendment to the bill H.R. 2360, making appropriations for the Department of Homeland Security for the fiscal year ending September 30, 2006, and for other purposes; as follows:

At the appropriate place, insert the following:

SEC. ___. No Federal employee who discloses, or has disclosed, classified information, including the identity of a covert agent of the Central Intelligence Agency, to a person not authorized to receive such information shall be permitted to hold a security clearance for access to such information.

SA 1223. Mr. FRIST proposed an amendment to the bill H.R. 2360, making appropriations for the Department of Homeland Security for the fiscal year ending September 30, 2006, and for other purposes; as follows:

At the appropriate place, insert the following:

SEC. Any federal officeholder who makes reference to a classified Federal Bureau of Investigation report on the floor of the United States Senate, or any federal officeholder that makes a statement based on an FBI agent's comments which is used as propaganda by terrorist organizations thereby putting our servicemen and women at risk, shall not be permitted access to such information or to hold a security clearance for access to such information.

SA 1224. Mr. REID (for Mr. BYRD (for himself and Ms. STABENOW)) proposed