on the Recreation Lakes Study, the Chairman and I spent some time discussing how children today do not take full advantage of the outdoor opportunities that are available to them. It is so important that we encourage our children to enjoy the great outdoors that often times is less than an hour's drive away.

As the mother of twin 4-year-old boys, I feel we need to encourage our children to be children, not to become adults too quickly, to learn how to enjoy the outdoors. The only way we can do that is by exposing them to it early and often.

In this nation we have nearly 1,800 federally-managed lakes and reservoirs. There are 38 in my home state of Arkansas. With so many federal lakes spread throughout the country, there's no reason why we shouldn't do all we can to promote recreation on our federal lakes. I know that in Arkansas, we don't think twice about getting away to the lake for the weekend to go boating or fishing, or to just get away from the day-to-day grind. And that doesn't even begin to get into the tremendous economic impact from recreation on our federal lakes.

Mr. President, this bill is not an attempt to completely rewrite how federal lakes in this country are managed or to put recreation in front of all other authorized purposes at federal lakes.

The Recreation Lakes Act of 2000 will work with all current laws and regulations to ensure that recreation is merely given a seat at the table when the management decisions are made for our federal lakes.

Mr. President, this is a good bill. In everything from the creation of jobs to the money that tourists like myself spend at the marinas and local stores surrounding the lake—our Federal lakes and reservoirs have an immense recreational value that can and does bring revenues into our local economies. The best way to encourage and expand this aspect is to ensure that recreation is given a higher priority in the management of our federal lakes.

I encourage my colleagues to support this legislation and look forward to the debate on how we can promote recreation on our federal lakes.

By Mr. EDWARDS:

S. 3180. A bill to provide for the disclosure of the collection of information through computer software, and for other purposes; to the Committee on Commerce, Science, and Transportation.

THE SPYWARE CONTROL AND PRIVACY PROTECTION ACT

Mr. EDWARDS. Mr. President, how would you feel if someone was eavesdropping on your private phone conversations without your knowledge? Well, if it happened to me, I would be very disturbed. And I think that most Americans would be very disturbed to know that something similar may be happening every time they use their computers.

The shocking fact is that many software programs contain something called spyware. Spyware is computer code that surreptitiously uses our Internet connection to transmit information about things like our purchasing patterns and our health and financial status. This information is collected without our knowledge or explicit permission and the spyware programs run undetected while you surf the Internet.

Spyware has been found in Quicken software, which is manufactured by Intuit, Inc. So let me use this as an example. Imagine you purchase Quicken software or download it from the Internet. You install it on your computer to help you with your finances. However, unbeknownst to you, Quicken does more than install financial planning tools on your computer. It also installs a little piece of spyware. The spyware lies dormant until one day when you get on the Internet.

As you start surfing the Internet, the spyware sends back information to Intuit about what you buy and what you are interested in. And all of this happens without your knowledge. You could be on Amazon.com or researching health issues and at the very same time Intuit spyware is using your Internet connection, transmitting some of your most private data to someone you never heard of.

In the months since it was reported that Quicken contained spyware, the folks at Intuit may have decided to remove the spyware from Quicken. However, Quicken is not the only software program that may contain spyware. One computer expert recently found spyware programs in popular children's software that is designed to help them learn, such as Mattel Interactive's Reader Rabbit and Arthur's Thinking Games. And, according to another expert's assessment, spyware is present in four hundred software programs, including commonly used software such as RealNetworks RealDownload, Netscape/AOL Smart Download, and NetZip Download Demon. Spyware in these software programs can transmit information about every file you download from the Internet.

I rise today to introduce the Spyware Control and Privacy Protection Act of 2000. I believe that this legislation will help Americans regain some control over their personal information and will help stop the loss of their privacy and the privacy of their families.

My proposal is common-sense and simple. It incorporates all four fair information practices of notice, choice, access and security—practices that I believe are essential to effective computer privacy legislation.

First, the Act requires that any software that contains spyware must provide consumers with clear and conspicuous notice—at the time the software is installed—that the software contains spyware. The notice must also describe the information that the spyware will collect and indicate to whom it will be transmitted.

Another critical provision of my bill requires that software users must first give their affirmative consent before the spyware is enabled and allowed to start obtaining and sharing users' personal information with third parties. In other words, software users must ''opt-in'' to the collection and transmission of their information. My bill gives software users a choice whether they will allow the spyware to collect and share their information.

The Spyware Control and Privacy Protection Act allows for some common-sense exceptions to the notice and opt-in requirements. Under my proposal, software users would not have to receive notice and give their permission to enable the spyware if the software user's information is gathered in order to provide technical support for use of the software. In addition, users' information may be collected if it is necessary to determine if they are licensed users of the software. And finally, the legislation would not apply to situations where employers are using spyware to monitor Internet usage by their employees. I believe that this last issue is a serious one and deserves to be addressed in separate legislation.

Another important aspect of the Spyware Control and Privacy Protection Act is that it would incorporate the fair information practice known as ''access.'' What this means is that an individual software user would have the ability to find out what information has been collected about them, and would be given a reasonable chance to correct any errors.

And finally, the fourth fair information practice guaranteed by my bill is ''security.'' Anyone that uses spyware to collect information about software users must establish procedures to keep that information confidential and safe from hackers.

Spyware is a modern day Trojan horse. You install software on your computer thinking it's designed to help you, and it turns out that something else is hidden inside that may be quite harmful.

I have been closely following the privacy debate for some time now. And I am struck by how often I discover new ways in which our privacy is being eroded. Spyware is among the more startling examples of how this erosion is occurring.

Most people would agree that modern technology has been extraordinarily beneficial. It has enabled us to obtain information more quickly and easily than ever before. And companies have streamlined their processes for providing goods and services.

But these remarkable developments can have a startling downside. They have made it easier to track personal information such as medical and financial records, and buying habits. In

turn, our ability to keep our personal information private is being eroded.

Even sophisticated computer software users are unlikely to be aware that information is being collected about their Internet surfing habits and is likely being fed into a growing personal profile maintained at a data warehouse. They don't know that companies can and do extract the information from the warehouse to create a so-called cyber-profile of what they are likely to buy, what the status of their health may be, what their family is like, and what their financial situation may be.

I believe that in the absence of government regulation, it is difficult, if not impossible for people to control the use of their own personal information. Consumers are not properly informed, and businesses are under no legal obligation to protect consumers' privacy.

I believe that the Spyware Control and Privacy Protection Act is a reasonable way to help Americans regain some of their privacy. My legislation does not prevent software manufacturers from using their software to collect a consumer's online information. However, it gives back some control to the consumer by allowing him or her to decide whether their information may be gathered.

My bill protects consumer privacy, while enabling software companies and marketing firms to continue obtaining consumers' information if the consumer so chooses. Confidence in these companies will be enhanced if they are able to assure their customers that they will not collect their personal information without their permission.

Privacy protections should not stop with computer software. I am also proud to be a cosponsor of the Consumer Privacy Protection Act, a much-needed measure that would prevent Internet service providers, individual web sites, network advertisers, and other third parties from gathering information about our online surfing habits without our permission.

And last fall, I introduced the Telephone Call Privacy Act in order to prevent phone companies from disclosing consumers' private phone records without their permission. Although there are only a few weeks left in this congressional session, it is my hope that Congress will pass meaningful privacy legislation soon.

Increasingly, technology is impacting our lives and the lives of our families. I believe that while it is important to encourage technological growth, we must also balance new developments with our fundamental right to privacy. Otherwise, we may wake up one day and realize that our privacy has been so thoroughly eroded that it is impossible to recover.

I urge my colleagues to support the Spyware Control and Privacy Protection Act.

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. 3180

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 ''Spyware Control and Privacy Protection Act of 2000''.

SEC. 2. COLLECTION OF INFORMATION BY COMPUTER SOFTWARE.

(a) NOTICE AND CHOICE REQUIRED.—

(1) IN GENERAL.—Any computer software made available to the public, whether by sale or without charge, that includes a capability to collect information about the user of such computer software, the hardware on which such computer software is used, or the manner in which such computer software is used, and to disclose to such information to any person other than the user of such computer software, shall include—

(A) a clear and conspicuous written notice, on the first electronic page of the instructions for the installation of such computer software, that such computer software includes such capability;

(B) a description of the information subject to collection and the name and address of each person to whom such computer software will transmit or otherwise communicate such information; and

(C) a clear and conspicuous written electronic notice, in a manner reasonably calculated to provide the user of such computer software with easily understood instructions on how to disable such capability without affecting the performance or operation of such computer software for the purposes for which such computer software was intended.

(2) ENABLEMENT OF CAPABILITY.—A capability of computer software described in paragraph (1) may not be enabled unless the user of such computer software provides affirmative consent, in advance, to the enablement of the capability.

(3) EXCEPTION.—The requirements in paragraphs (1) and (2) shall not apply to any capability of computer software that is reasonably needed to—

(A) determine whether or not the user is a licensed or authorized user of such computer software;

(B) provide, upon request of the user, technical support of the use of such computer software by the user; or

(C) enable an employer to monitor computer usage by its employees while such employees are within the scope of employment as authorized by applicable Federal, State, or local law.

(4) USE OF INFORMATION COLLECTED THROUGH EXCEPTED CAPABILITY.—Any information collected through a capability described in paragraph (1) for a purpose referred to in paragraph (3) may be utilized only for the purpose for which such information is collected under paragraph (3).

(5) ACCESS TO INFORMATION COLLECTED THROUGH EXCEPTED CAPABILITY.—Any person collecting information about a user of computer software through a capability described in paragraph (1) shall—

(A) upon request of the user, provide reasonable access by user to information so collected;

(B) provide a reasonable opportunity for the user to correct, delete, or supplement such information; and

(C) make the correction or supplementary information a part of the information about the user for purposes of any future use of such information under this subsection.

(6) SECURITY OF INFORMATION COLLECTED THROUGH EXCEPTED CAPABILITY.—Any person collecting information through a capability described in paragraph (1) shall establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of such information.

(b) PREINSTALLATION.—In the case of computer software described in subsection (a)(1) that is installed on a computer by someone other than the user of such computer software, whether through preinstallation by the provider of such computer or computer software, by installation by someone before delivery of such computer to the user, or otherwise, the notice and instructions under that subsection shall be provided in electronic form to the user before the first use of such computer software by the user.

(c) VIOLATIONS.—A violation of subsection (a) or (b) shall be treated as an unfair or deceptive act or practice proscribed by section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)).

(d) DISCLOSURE TO LAW ENFORCEMENT OR UNDER COURT ORDER.—

(1) IN GENERAL.—Notwithstanding any other provision of this section, a computer software provider that collects information about users of the computer software may disclose information about a user of the computer software—

(A) to a law enforcement agency in response to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent State warrant, or a court order issued in accordance with paragraph (3); or

(B) in response to a court order in a civil proceeding granted upon a showing of compelling need for the information that cannot be accommodated by any other means if—

(i) the user to whom the information relates is given reasonable notice by the person seeking the information of the court proceeding at which the order is requested; and

(ii) the user is afforded a reasonable opportunity to appear and contest the issuance of the requested order or to narrow its scope.

(2) SAFEGUARDS AGAINST FURTHER DISCLOSURE.—A court that issues an order described in paragraph (1) shall impose appropriate safeguards on the use of the information to protect against its unauthorized disclosure.

(3) COURT ORDERS.—A court order authorizing disclosure under paragraph (1)(A) may issue only with prior notice to the user and only if the law enforcement agency shows that there is probable cause to believe that the user has engaged, is engaging, or is about to engage in criminal activity and that the records or other information sought are material to the investigation of such activity. In the case of a State government authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this paragraph, on a motion made promptly by the computer software provider may quash or modify such order if the information or records requested are unreasonably voluminous in nature or if compliance with such order otherwise would cause an unreasonable burden on the provider.

(e) PRIVATE RIGHT OF ACTION.—

(1) ACTIONS AUTHORIZED.—A person may, if otherwise permitted by the laws or rules of court of a State, bring in an appropriate Federal court, if such laws or rules prohibit such actions, either or both of the actions as follows:

(A) An action based on a violation of subsection (a) or (b) to enjoin such violation.

(B) An action to recover actual monetary loss for a violation of subsection (a) or (b) in an amount equal to the greater of—

(i) the amount of such actual monetary loss; or

(ii) $2,500 for such violation, not to exceed a total amount of $500,000.

(2) ADDITIONAL REMEDY.—If the court in an action under paragraph (1) finds that the defendant willfully, knowingly, or repeatedly violated subsection (a) or (b), the court may, in its discretion, increase the amount of the award under paragraph (1)(B) to an amount not greater than three times the amount available under paragraph (1)(B)(ii).

(3) LITIGATION COSTS AND ATTORNEY FEES.—In any action under paragraph (1), the court may, in its discretion, require an undertaking for the payment of the costs of such action and assess reasonable costs, including reasonable attorney fees, against the defendant.

(4) VENUE.—In addition to any contractual provision otherwise, venue for an action under paragraph (1) shall lie where the computer software concerned was installed or used or where the person alleged to have committed the violation concerned is found.

(5) PROTECTION OF TRADE SECRETS.—At the request of any party to an action under paragraph (1), or any other participant in such action, the court may, in its discretion, issue a protective order and conduct proceedings in such action so as to protect the secrecy and security of the computer, computer network, computer data, computer program, and computer software involved in order to—

(A) prevent possible recurrence of the same or a similar act by another person; or

(B) protect any trade secrets of such party or participant.

(f) DEFINITIONS.—In this section:

(1) COLLECT.—The term ''collect'' means the gathering of information about a computer or a user of computer software by any means, whether direct or indirect and whether active or passive.

(2) COMPUTER.—The term ''computer'' means a programmable electronic device that can store, retrieve, and process data.

(3) COMPUTER SOFTWARE.—(A) Except as provided in subparagraph (B), the term ''computer software'' means any program designed to cause a computer to perform a desired function or functions.

(B) The term does not include a text file, or cookie, placed on a person's computer system by an Internet service provider, interactive computer service, or commercial Internet website to return information to the Internet service provider, interactive computer service, commercial Internet website, or third party if the person subsequently uses the Internet service provider or interactive computer service, or accesses the commercial Internet website.

(4) INFORMATION.—The term ''information'' means information that personally identifies a user of computer software, including the following:

(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 and name of a city or town.

(C) An electronic mail address.

(D) A telephone number.

(E) A social security number.

(F) A credit card number, any access code associated with the credit card, or both.

(G) A birth date, birth certificate number, or place of birth.

(H) Any other unique information identifying an individual that a computer software provider, Internet service provider, interactive computer service, or operator of a commercial Internet website collects and combines with information described in subparagraphs (A) through (G) of this paragraph.

(5) 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)).

(6) USER.—The term ''user'' means an individual who acquires, through purchase or otherwise, computer software for purposes other than resale.

(g) EFFECTIVE DATE.—This section shall take effect 180 days after the date of the enactment of this Act.

ADDITIONAL COSPONSORS

S. 61

At the request of Mr. DEWINE, the name of the Senator from Utah (Mr. HATCH) was added as a cosponsor of S. 61, a bill to amend the Tariff Act of 1930 to eliminate disincentives to fair trade conditions.

S. 821

At the request of Mr. LAUTENBERG, the name of the Senator from California (Mrs. FEINSTEIN) was added as a cosponsor of S. 821, a bill to provide for the collection of data on traffic stops.

S. 1020

At the request of Mr. GRASSLEY, the name of the Senator from Hawaii (Mr. AKAKA) was added as a cosponsor of S. 1020, a bill to amend chapter 1 of title 9, United States Code, to provide for greater fairness in the arbitration process relating to motor vehicle franchise contracts.

S. 1110

At the request of Mr. EDWARDS, his name was added as a cosponsor of S. 1110, a bill to amend the Public Health Service Act to establish the National Institute of Biomedical Imaging and Engineering.

S. 1197

At the request of Mr. ROTH, the name of the Senator from Vermont (Mr. LEAHY) was added as a cosponsor of S. 1197, a bill to prohibit the importation of products made with dog or cat fur, to prohibit the sale, manufacture, offer for sale, transportation, and distribution of products made with dog or cat fur in the United States, and for other purposes.

S. 1536

At the request of Mr. DEWINE, the names of the Senator from South Dakota (Mr. JOHNSON), the Senator from California (Mrs. BOXER), the Senator from New Mexico (Mr. BINGAMAN), the Senator from Michigan (Mr. ABRAHAM), the Senator from New Jersey (Mr. LAUTENBERG), the Senator from Ohio (Mr. VOINOVICH), the Senator from Alabama (Mr. SESSIONS), the Senator from Tennessee (Mr. THOMPSON), the Senator from Nebraska (Mr. KERREY), and the Senator from Pennsylvania (Mr. SPECTER) were added as cosponsors of S. 1536, a bill to amend the Older Americans Act of 1965 to extend authorizations of appropriations for programs under the Act, to modernize programs and services for older individuals, and for other purposes.

S. 2242

At the request of Mr. THOMAS, the name of the Senator from Michigan (Mr. ABRAHAM) was added as a cosponsor of S. 2242, a bill to amend the Federal Activities Inventory Reform Act of 1998 to improve the process for identifying the functions of the Federal Government that are not inherently governmental functions, for determining the appropriate organizations for the performance of such functions on the basis of competition, and for other purposes.

S. 2358

At the request of Mr. INHOFE, the name of the Senator from Maine (Ms. SNOWE) was added as a cosponsor of S. 2358, a bill to amend the Public Health Service Act with respect to the operation by the National Institutes of Health of an experimental program to stimulate competitive research.

S. 2609

At the request of Mr. CRAIG, the name of the Senator from New Hampshire (Mr. SMITH) was added as a cosponsor of S. 2609, a bill to amend the Pittman-Robertson Wildlife Restoration Act and the Dingell-Johnson Sport Fish Restoration Act to enhance the funds available for grants to States for fish and wildlife conservation projects, and to increase opportunities for recreational hunting, bow hunting, trapping, archery, and fishing, by eliminating chances for waste, fraud, abuse, maladministration, and unauthorized expenditures for administration and implementation of those Acts, and for other purposes.

S. 2725

At the request of Mr. SMITH of New Hampshire, the names of the Senator from New York (Mr. MOYNIHAN), the Senator from Delaware (Mr. ROTH), and the Senator from Nevada (Mr. REID) were added as cosponsors of S. 2725, a bill to provide for a system of sanctuaries for chimpanzees that have been designated as being no longer needed in research conducted or supported by the Public Health Service, and for other purposes.

S. 2967

At the request of Mr. ROBB, his name was added as a cosponsor of S. 2967, a bill to amend the Internal Revenue Code of 1986 to facilitate competition in the electric power industry.

S. 3045

At the request of Mr. SESSIONS, the name of the Senator from Texas (Mr. GRAMM) was added as a cosponsor of S. 3045, a bill to improve the quality, timeliness, and credibility of forensic science services for criminal justice purposes.

S. 3089

At the request of Mr. HAGEL, the names of the Senator from Rhode Island (Mr. REED) and the Senator from Texas (Mrs. HUTCHISON) were added as cosponsors of S. 3089, a bill to authorize the design and construction of a temporary education center at the Vietnam Veterans Memorial.

S. 3091

At the request of Mr. GRASSLEY, the names of the Senator from Indiana (Mr. LUGAR) and the Senator from Kansas (Mr. ROBERTS) were added as cosponsors of S. 3091, a bill to implement