to imply by this difference that general knowledge can or should be the subject of a prosecution under section 572. Of course, someone can use their general experience and skills and work for a foreign government. They cannot, however, steal a piece of proprietary economic information for an owner and thereby violate section 572 of this provision. Our point is simply that when a person is working on behalf of a foreign government, instrumentality or agency, that person has to be particularly careful to ensure that the information being used is not proprietary economic information.

Some people have asked whether a piece of proprietary economic information has to be novel or inventive. Unlike patented material, something does not have to be novel, in the patent law sense, in order to be a piece of proprietary economic information. Of course, often it will be because an owner will have a patented invention that he or she has chosen to maintain the material as a piece of proprietary economic information rather than reveal it through the patent process. Even if the material is not novel in the patent law sense, some form of novelty is probably inevitable since ''that which does not possess novelty is usually known; secrecy, in the context of trade secrets implies at least minimal novelty.'' *Kewanee Oil Co.* v. *Bicron Corp.*, 416 U.S. 470, 476 (1974). While we do not strictly impose a novelty or inventiveness requirement in order for material to be considered proprietary economic information, looking at the novelty or uniqueness of a piece of information or knowledge should inform courts in determining whether something is a matter of general knowledge, skill or experience.

Although we do not require novelty or inventiveness, the definition of proprietary economic information includes the provision that an owner have taken reasonable measures under the circumstances to keep the information confidential. We do not with this definition impose any requirements on companies or owners. Each owner must assess the value of the material it seeks to protect, the extent of a threat of theft, and the ease of theft in determining how extensive their protective measures should be. We anticipate that what constitutes reasonable measures in one particular field of knowledge or industry may vary significantly from what is reasonable in another field or industry. However, some common sense measures are likely to be common across the board. For example, it is only natural that an owner would restrict access to proprietary economic information to the people who actually need to use the information. It is only natural also that an owner clearly indicate in some form or another that the information is proprietary. However, owners need not take heroic or extreme protective measures in order for their efforts to be reasonable.

Some people have asked how this legislation might affect reverse engineering. Reverse engineering is a broad term that encompasses a variety of actions. The important thing is to focus on whether the accused has committed one of the prohibited acts of this statute rather than whether he or she has ''reverse engineered.'' If someone has lawfully gained access to a trade secret or a piece or proprietary economic information, and can replicate it without violating copyright, patent or this law, then that form of ''reverse engineering'' should be fine. For example, if a person can drink Coca-Cola and, because he happens to have highly refined taste buds, can figure out what the formula is, then this legislation cannot be used against him. Likewise, if a person can look at a product and, by using their own general skills and expertise, dissect the necessary attributes of the product, then that person should be free from any threat of prosecution.

We have been deeply concerned about the efforts taken by courts to protect the confidentiality of proprietary economic information. It is important that in the early stages of a prosecution the issue whether material is proprietary economic information not be litigated. Rather, courts should, when entering these orders, always assume that the material at issue is in fact proprietary economic information.

We are also concerned that victims of economic espionage receive compensation for their losses. This legislation incorporates through reference existing law to provide procedures to be used in the detention, seizure, forfeiture, and ultimate disposition of property forfeited under the section. Under these procedures, the Attorney General is authorized to grant petitions for mitigation or remission of forfeiture and for the restoration of forfeited property to the victims of an offense. The Attorney General may also take any other necessary or proper action to protect the rights of innocent people in the interest of justice. In practice, under the forfeiture laws, victims are afforded priority in the disposition of forfeited property since it is the policy of the Department of Justice to provide restitution to the victims of criminal acts whenever permitted to do so by the law. Procedures for victims to obtain restitution may be found at Section 9 of Title 28, Code of Federal Regulations.

In addition to requesting redress from the Attorney General, any person—including a victim—asserting an interest in property ordered forfeited may petition for a judicial hearings to adjudicate the validity of the alleged interest and to revise the order of forfeiture. Additionally, forfeitures are subject to a requirement of proportionality under the Eight Amendment; that is, the value of the property forfeited must not be excessively disproportionate to the crimes in question.

Finally, we have required that the Attorney General report back to us on victim restitution two and four years after the enactment of this legislation. We have heard from some companies that they only rarely obtain restitution awards despite their eligibility. We wish to carefully monitor restitution to ensure that the current system is working well and make any changes that may be necessary.

Mr. President, we have worked closely in cooperation with the Administration in drafting this legislation. It is a bipartisan measure, broadly supported, and necessary for our country's future industrial vitality.

NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1996

Mr. STEVENS. Mr. President, I ask unanimous consent the Senate now proceed to the consideration of Calendar No. 563, S. 982.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

A bill (S. 982) to protect the national information infrastructure, and for other purposes.

The PRESIDING OFFICER. Is there objection to the immediate consideration of the bill?

There being no objection, the Senate proceeded to consider the bill which had been reported from the Committee on the Judiciary, with an amendment to strike all after the enacting clause and inserting in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the ''National Information Infrastructure Protection Act of 1996''.

SEC. 2. COMPUTER CRIME.

Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking ''knowingly accesses'' and inserting ''having knowingly accessed'';

(ii) by striking ''exceeds'' and inserting ''exceeding'';

(iii) by striking ''obtains information'' and inserting ''having obtained information'';

(iv) by striking ''the intent or'';

(v) by striking ''is to be used'' and inserting ''could be used''; and

(vi) in inserting before the semicolon at the end the following: ''willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it'';

(B) in paragraph (2)—

(i) by striking ''obtains information'' and inserting ''obtains—

''(A) information''; and

(ii) by adding at the end the following new subparagraphs:

''(B) information from any department or agency of the United States; or

''(C) information from any protected computer if the conduct involved an interstate or foreign communication;'';

(C) in paragraph (3)—

(i) by inserting ''nonpublic'' before ''computer of a department or agency'';

(ii) by striking ''adversely''; and

(iii) by striking ''the use of the Government's operation of such computer'' and inserting

''that use by or for the Government of the United States'';

(D) in paragraph (4)—

(i) by striking ''Federal interest'' and inserting ''protected''; and

(ii) by inserting before the semicolon the following: ''and the value of such use is not more than $5,000 in any 1-year period'';

(E) by striking paragraph (5) and inserting the following:

''(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

''(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

''(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;''; and

(F) by inserting after paragraph (6) the following new paragraph:

''(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;'';

(2) in subsection (c)—

(A) in paragraph (1), by striking ''such subsection'' each place that term appears and inserting ''this section'';

(B) in paragraph (2)—

(i) in subparagraph (A)—

(I) by inserting '', (a)(5)(C),'' after ''(a)(3)''; and

(II) by striking ''such subsection'' and inserting ''this section'';

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting immediately after subparagraph (A) the following:

''(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

''(iii) the value of the information obtained exceeds $5,000;''; and

(iv) in subparagraph (C) (as redesignated)—

(I) by striking ''such subsection'' and inserting ''this section''; and

(II) by adding ''and'' at the end;

(C) in paragraph (3)—

(i) in subparagraph (A)—

(I) by striking ''(a)(4) or (a)(5)(A)'' and inserting ''(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)''; and

(II) by striking ''such subsection'' and inserting ''this section''; and

(ii) in subparagraph (B)—

(I) by striking ''(a)(4) or (a)(5)'' and inserting ''(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)''; and

(II) by striking ''such subsection'' and inserting ''this section''; and

(D) by striking paragraph (4);

(3) in subsection (d), by inserting ''subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of'' before ''this section.'';

(4) in subsection (e)—

(A) in paragraph (2)—

(i) by striking ''Federal interest'' and inserting ''protected'';

(ii) in subparagraph (A), by striking ''the use of the financial institution's operation or the Government's operation of such computer'' and inserting ''that use by or for the financial institution or the Government''; and

(iii) by striking subparagraph (B) and inserting the following:

''(B) which is used in interstate or foreign commerce or communication;'';

(B) in paragraph (6), by striking ''and'' at the end;

(C) in paragraph (7), by striking the period at the end and inserting ''; and''; and

(D) by adding at the end the following new paragraphs:

''(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information, that—

''(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

''(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

''(C) causes physical injury to any person; or

''(D) threatens public health or safety; and

''(9) the term 'government entity' includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country.''; and

(5) in subsection (g)—

(A) by striking '', other than a violation of subsection (a)(5)(B),''; and

(B) by striking ''of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)'' and inserting ''involving damage as defined in subsection (e)(8)(A)''.

AMENDMENTS NOS. 5388 AND 5389 EN BLOC

Mr. STEVENS. Mr. President, I send two amendments to the desk, en bloc, on behalf of Senator HATCH, and I ask for their consideration.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

The Senator from Alaska [Mr. STEVENS], for Mr. HATCH, proposes amendments numbered 5388 and 5389, en bloc.

Mr. STEVENS. Mr. President, I ask unanimous consent that reading of the amendments be dispensed with.

The PRESIDING OFFICER. Without objection, it is so ordered.

The amendments are as follows:

AMENDMENT NO. 5388

(Purpose: To improve the treatment and security of certain persons found not guilty by reason of insanity in the District of Columbia)

At the appropriate place in the bill, add the following:

SEC. ___. TRANSFER OF PERSONS FOUND NOT GUILTY BY REASON OF INSANITY.

(a) AMENDMENT OF SECTION 4243 OF TITLE 18.—Section 4243 of title 18, United States Code, is amended by adding at the end the following new subsection:

''(i) CERTAIN PERSONS FOUND NOT GUILTY BY REASON OF INSANITY IN THE DISTRICT OF COLUMBIA.—

''(1) TRANSFER TO CUSTODY OF THE ATTORNEY GENERAL.—Notwithstanding section 301(h) of title 24 of the District of Columbia Code, and notwithstanding subsection 4247(j) of this title, all persons who have been committed to a hospital for the mentally ill pursuant to section 301(d)(1) of title 24 of the District of Columbia Code, and for whom the United States has continuing financial responsibility, may be transferred to the custody of the Attorney General, who shall hospitalize the person for treatment in a suitable facility.

''(2) APPLICATION.—

''(A) IN GENERAL.—The Attorney General may establish custody over such persons by filing an application in the United States District Court for the District of Columbia, demonstrating that the person to be transferred is a person described in this subsection.

''(B) NOTICE.—The Attorney General shall, by any means reasonably designed to do so, provide written notice of the proposed transfer of custody to such person or such person's guardian, legal representative, or other lawful agent. The person to be transferred shall be afforded an opportunity, not to exceed 15 days, to respond to the proposed transfer of custody, and may, at the court's discretion, be afforded a hearing on the proposed transfer of custody. Such hearing, if granted, shall be limited to a determination of whether the constitutional rights of such person would be violated by the proposed transfer of custody.

''(C) ORDER.—Upon application of the Attorney General, the court shall order the person transferred to the custody of the Attorney General, unless, pursuant to a hearing under this paragraph, the court finds that the proposed transfer would violate a right of such person under the United States Constitution.

''(D) EFFECT.—Nothing in this paragraph shall be construed to—

''(i) create in any person a liberty interest in being granted a hearing or notice on any matter;

''(ii) create in favor of any person a cause of action against the United States or any officer or employee of the United States; or

''(iii) limit in any manner or degree the ability of the Attorney General to move, transfer, or otherwise manage any person committed to the custody of the Attorney General.

''(3) CONSTRUCTION WITH OTHER SECTIONS.—Subsections (f) and (g) and section 4247 shall apply to any person transferred to the custody of the Attorney General pursuant to this subsection.''.

(b) TRANSFER OF RECORDS.—Notwithstanding any provision of the District of Columbia Code or any other provision of law, the District of Columbia and St. Elizabeth's Hospital—

(1) not later than 30 days after the date of enactment of this Act, shall provide to the Attorney General copies of all records in the custody or control of the District or the Hospital on such date of enactment pertaining to persons described in section 4243(i) of title 18, United States Code (as added by subsection (a));

(2) not later than 30 days after the creation of any records by employees, agents, or contractors of the District of Columbia or of St. Elizabeth's Hospital pertaining to persons described in section 4243(i) of title 18, United States Code, provide to the Attorney General copies of all such records created after the date of enactment of this Act;

(3) shall not prevent or impede any employee, agent, or contractor of the District of Columbia or of St. Elizabeth's Hospital who has obtained knowledge of the persons described in section 4243(i) of title 18, United States Code, in the employee's professional capacity from providing that knowledge to the Attorney General, nor shall civil or criminal liability attach to such employees, agents, or contractors who provide such knowledge; and

(4) shall not prevent or impede interviews of persons described in section 4243(i) of title 18, United States Code, by representatives of the Attorney General, if such persons voluntarily consent to such interviews.

(c) CLARIFICATION OF EFFECT ON CERTAIN TESTIMONIAL PRIVILEGES.—The amendments made by this section shall not be construed to affect in any manner any doctor-patient or psychotherapist-patient testimonial privilege that may be otherwise applicable to persons found not guilty by reason of insanity and affected by this section.

(d) SEVERABILITY.—If any provision of this section, an amendment made by this section, or the application of such provision or

amendment to any person or circumstance is held to be unconstitutional, the remainder of this section and the amendments made by this section shall not be affected thereby.

AMENDMENT NO. 5389

(Purpose: To provide funding for the establishment of Boys and Girls Clubs in public housing projects and other distressed areas, and for other purposes)

At the appropriate place in the bill, add the following:

SEC. . ESTABLISHING BOYS AND GIRLS CLUBS.

(a) FINDINGS AND PURPOSE.—

(1) FINDINGS.—The Congress finds that—

(A) the Boys and Girls Clubs of America, chartered by an Act of Congress on December 10, 1991, during its 90-year history as a national organization, has proven itself as a positive force in the communities it serves;

(B) there are 1,810 Boys and Girls Clubs facilities throughout the United States, Puerto Rico, and the United States Virgin Islands, serving 2,420,000 youths nationwide;

(C) 71 percent of the young people who benefit from Boys and Girls Clubs programs live in our inner cities and urban areas;

(D) Boys and Girls Clubs are locally run and have been exceptionally successful in balancing public funds with private sector donations and maximizing community involvement;

(E) Boys and Girls Clubs are located in 289 public housing sites across the Nation;

(F) public housing projects in which there is an active Boys and Girls Club have experienced a 25 percent reduction in the presence of crack cocaine, a 22 percent reduction in overall drug activity, and a 13 percent reduction in juvenile crime;

(G) these results have been achieved in the face of national trends in which overall drug use by youth has increased 105 percent since 1992 and 10.9 percent of the Nation's young people use drugs on a monthly basis; and

(H) many public housing projects and other distressed areas are still underserved by Boys and Girls Clubs.

(2) PURPOSE.—It is the purpose of this section to provide adequate resources in the form of seed money for the Boys and Girls Clubs of America to establish 1,000 additional local Boys and Girls Clubs in public housing projects and other distressed areas by 2001.

(b) DEFINITIONS.—For purposes of this section—

(1) the terms ''public housing'' and ''project'' have the same meanings as in section 3(b) of the United States Housing Act of 1937; and

(2) the term ''distressed area'' means an urban, suburban, or rural area with a high percentage of high risk youth as defined in section 509A of the Public Health Service Act (42 U.S.C. 290aa–8(f)).

(c) ESTABLISHMENT.—

(1) IN GENERAL.—For each of the fiscal years 1997, 1998, 1999, 2000, and 2001, the Director of the Bureau of Justice Assistance of the Department of Justice shall provide a grant to the Boys and Girls Clubs of America for the purpose of establishing Boys and Girls Clubs in public housing projects and other distressed areas.

(2) CONTRACTING AUTHORITY.—Where appropriate, the Secretary of Housing and Urban Development, in consultation with the Attorney General, shall enter into contracts with the Boys and Girls Clubs of America to establish clubs pursuant to the grants under paragraph (1).

(d) REPORT.—Not later than May 1 of each fiscal year for which amounts are made available to carry out this Act, the Attorney General shall submit to the Committees on the Judiciary of the Senate and the House of Representatives a report that details the progress made under this Act in establishing Boys and Girls Clubs in public housing projects and other distressed areas, and the effectiveness of the programs in reducing drug abuse and juvenile crime.

(e) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There are authorized to be appropriated to carry out this section—

(A) $20,000,000 for fiscal year 1997;

(B) $20,000,000 for fiscal year 1998;

(C) $20,000,000 for fiscal year 1999;

(D) $20,000,000 for fiscal year 2000; and

(E) $20,000,000 for fiscal year 2001.

(2) VIOLENT CRIME REDUCTION TRUST FUND.—The sums authorized to be appropriated by this subsection may be made from the Violent Crime Reduction Trust Fund.

Mr. KYL. Mr. President. I rise to comment on S. 982, the National Information Infrastructure Protection Act. I was pleased that the Senate Judiciary Committee unanimously passed the bill that Senator LEAHY and I introduced, which will strengthen current public law on computer crime and protect the national information infrastructure. It will protect banks, hospitals, and other information-intensive businesses which maintain sensitive computer files from those who improperly enter into computer systems.

Although there has never been an accurate nationwide reporting system for computer crime, it is clear that computer crime is rising. For example, the Computer Emergency and Response Team [CERT] at Carnegie-Mellon University reports that computer intrusions have increased from 132 in 1989 to 2,341 last year. A recent Rand Corporation study reported 1,172 hacking incidents during the first 6 months of 1994. Clearly there is a need to reform the current criminal statutes covering computer abuse.

The law needs to keep pace with technology. Crime is increasingly being perpetrated electronically, and we need to amend our laws to stop it. We, therefore, introduced the National Information Infrastructure Protection Act last year. Why is this bill important? First, it will protect against the interstate or foreign theft of information by computer. The provision is necessary because the court held, in the case of United States v. Brown, 925 F.2d 1301, 1308 (10th Cir. 1991), that purely intangible intellectual property, such as computer programs, do not count as goods, wares, merchandise, securities, or moneys which have been stolen, converted, or taken within the meaning of 18 U.S.C. §2314, the Interstate Transportation of Stolen Property. There are no Federal penalties for theft of computer information across state lines or internationally. In most cases, the Department of Justice attempts to use other statutes to prosecute these criminals.

Second, the provision adds a new section to the Computer Fraud and Abuse Act to provide penalties for the interstate or international transmission of threats against computers, computer networks, and their data and programs. Unlawful threats would include interference in any way with the normal operation of the computer or system in question, such as denying access to authorized users, erasing or corrupting data or programs, slowing down the operation of the computer or system, or encrypting data and then demanding money for the key. The provision is important because there have been cases where hackers have threatened to demolish a computer information system unless they were granted free access to accounts. It is sophisticated extortion.

Finally, S. 982 amends 18 U.S.C. §1030(a)(4) to ensure that felony-level sanctions apply when unauthorized use, or use in excess of authorization, is significant. Hackers, for example, have broken into computers only for the purpose of using their processing programs, sometimes amassing computer time worth far more than $5,000. The bill would penalize those whose trespassing, in which only computer use is obtained, amounts to greater than $5,000 during any 1-year period. Companies should not be stuck with the bill for electronic joyriders. Although they may not damage or steal information, hackers who browse through computer systems are a significant liability to businesses who must pay for a new security system, and the expensive time the hacker used.

There is widespread support for changes to the statute. For example, Attorney General Reno, in connection with the June 27, 1995 oversight hearing of the Department of Justice, said that S. 982 would ''address many of the concerns that have been identified by computer security experts with respect to the need for greater protection of networks.''

As FBI Director Louis Freeh responded, when asked during the February 28, 1996 joint hearing with the Select Committee on Intelligence on Economic Espionage, if he would appreciate the Senate acting on S. 982, ''[S. 982] does fill a gap. It's very important.''

On October 11, 1995 the Deputy Assistant Director of Investigations of the United States Secret Service, speaking before the House Committee on Banking and Financial Services Subcommittee on Domestic and International Monetary Policy, listed S. 982 as one of the bills that ''enhance our ability to investigate and prosecute violations domestically, while offering guidelines for foreign government authorities.''

This bill is timely because of the recent incident concerning the Department of Justice's homepage. Hackers penetrated the DOJ's computers, leaving pictures of swastikas and Adolph Hitler for the world to view. The damage caused by these criminals should not be prosecuted by relying on common law criminal mischief statutes. If our bill had been law, Federal prosecutors could have charged the hackers with violating more than trespassing statutes.

Mr. President, the Kyl-Leahy National Information Infrastructure Protection Act of 1995 will deter criminal

activity and protect our Nation's infrastructure. I urge my colleagues to pass the bill.

Mr. LEAHY. Mr. President, I am pleased that the Senate has today taken the important step of passing the National Information Infrastructure Protection Act of 1996, NII Protection Act, which I have sponsored with Senators KYL and GRASSLEY.

This legislation will help safeguard the privacy, security, and reliability of our national computer systems and networks and the information stored in, and carried on, those networks. Those systems and networks are vulnerable to the threat of attack by hackers, high-technology criminals and spies. The NII Protection Act will increase protection for both government and private computers, and the information on those computers, from the growing threat of computer crime.

Our dependency on computers and the growth of the Internet are both integrally linked to people's confidence in the privacy, security, and reliability of computer networks. That is why I have worked over the past decade to make sure the laws we have in place foster both privacy and security, and provide a sound foundation for new communications technologies to flourish.

Every technological advance provides new opportunities for legitimate uses and the potential for criminal exploitation. Existing criminal statutes provide a good framework for prosecuting most types of computer-related criminal conduct. But as technology changes and high-technology criminals devise new ways to use technology to commit offenses we have yet to anticipate, we must be ready to readjust and update our criminal code.

The NII Protection Act closes a number of gaps in the Computer Fraud and Abuse statute, which was originally enacted in 1984. This legislation would strengthen law enforcement's hands in fighting crimes targeted at computers, networks, and computerized information by, among other things, designating new computer crimes, and by extending protection to computer systems used in foreign or interstate commerce or communications.

We need to protect both government and private computers, and the information on those computers, from the very real and growing threat of computer crime. The facts speak for themselves—computer crime is on the rise. On September 12, a computer hacker attack, which shut down an New York Internet access provider with thousands of business and individual customers, made front page news, and revealed the vulnerability of every network service provider to such an attack. The Computer Emergency and Response Team [CERT] at Carnegie-Mellon University reports that over 12,000 Internet computers were attacked in 2,412 incidents in 1995 alone. A 1996 survey conducted jointly by the Computer Security Institute and the FBI showed that 42 percent of the respondents sustained an unauthorized use or intrusion into their computer systems in the past 12 months.

Nevertheless, while our current statute, in section 1030(a)(2), prohibits misuse of a computer to obtain information from a financial institution, it falls short of protecting the privacy and confidentiality of information on computers used in interstate or foreign commerce and communications. This gap in the law has become only more glaring as more Americans have connected their home and business computers to the global Internet.

This is not just a law enforcement issue, but an economic one. Breaches of computer security result in direct financial losses to American companies from the theft of trade secrets and proprietary information. A December 1995 report by the Computer Systems Policy Project, comprised of the CEO's from 13 major computer companies, estimates that financial losses in 1995 from breaches of computer security systems ranged from $2 to $4 billion. The report predicts that these numbers could rise in the year 2000 to $40 to $80 billion worldwide. The estimated amount of these losses is staggering.

The NII Protection Act would extend the protection already given to the computerized information of financial institutions and consumer reporting agencies, to computerized information held on computers used in interstate or foreign commerce on communications, if the conduct involved interstate or foreign communications. The provision is designed to protect against the interstate or foreign theft of information by computer.

Computer hackers have accessed sensitive government data regarding Operation Desert Storm, penetrated NASA computers, and broken into Federal courthouse computer systems containing confidential records. These outside hackers are subject to criminal prosecution under section 1030(a)(3) of the computer fraud and abuse statute. Yet, this statute contains no prohibition against malicious insiders: Those Government employees who abuse their computer access privileges by snooping through confidential tax returns, or selling confidential criminal history information from the National Crime Information Center [NCIC]. The NCIC is currently the Nation's most extensive computerized criminal justice information system, containing criminal history information, files on wanted persons, and information on stolen vehicles and missing persons.

I am very concerned about continuing reports of unauthorized access to highly personal and sensitive government information about individual Americans, such as NCIC data. For example, a ''Dear Abby'' column that appeared on June 20, 1996 in newspapers across the country carried a letter by a woman who claimed her in-laws ''ran her name through the FBI computer'' and, apparently, used access to the NCIC for personal purposes.

This published complaint comes on the heels of a General Accounting Office [GAO] report presented on July 28, 1993, before the House Government Operations Committee, Subcommittee on Information, Justice, Agriculture, and Transportation, on the abuse of NCIC information. Following an investigation, GAO determined that NCIC information had been misused by insiders—individuals with authorized access—some of whom had sold NCIC information to outsiders and determined whether friends and relatives had criminal records. The GAO found that some of the misuse jeopardized the safety of citizens and potentially jeopardized law enforcement personnel. Yet, no Federal or State laws are specifically directed at NCIC misuse and most abusers of NCIC were not criminally prosecuted. GAO concluded that Congress should enact legislation with strong criminal sanctions for the misuse of NCIC data.

This bill would criminalize these activities by amending the privacy protection provision in section 1030(a)(2) and extending its coverage to Federal Government computers. If the information obtained is of minimal value, the penalty is only a misdemeanor. If, on the other hand, the offense is committed for purposes of commercial advantage or private financial gain, for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State, or if the value of the information obtained exceeds $5,000, the penalty is a felony.

The current statute, in section 1030(a)(5), protects computers and computer systems from damage caused by either outside hackers or malicious insiders ''through means of a computer used in interstate commerce or communications.'' It does not, however, expressly prohibit the transmission of harmful computer viruses or programs from abroad, even though, a criminal armed with a modem and a computer can wreak havoc on computers located in the United States from virtually anywhere in the world. This is a significant challenge in fighting cybercrime: There are no borders or passport checkpoints in cyberspace. Communications flow seamlessly through cyberspace across datelines and the reach of local law enforcement.

Indeed, we have seen a number of examples of computer crimes directed from abroad, including the 1994 intrusion into the Rome Laboratory at Grifess Air Force Base in New York from the United Kingdom and the 1996 intrusion into Harvard University's computers from Buenos Aires, Argentina.

Additionally, the statute falls short of protecting our Government and financial institution computers from intrusive codes, such as computer viruses or worms. Generally, hacker intrusions that inject worms or viruses into a government or financial institution computer system, which is not used in -

interstate communications, are not federal offenses. The legislation would change that limitation and extend federal protection from intentionally damaging viruses to government and financial institution computers, even if they are not used in interstate communications.

The NII Protection Act would close these loopholes. Under the legislation, outside hackers—including those using foreign communications—and malicious insiders face criminal liability for intentionally damaging a computer. Outside hackers who break into a computer could also be punished for any reckless or other damage they cause by their trespass.

The current statute protects against computer abuses that cause computer ''damage'', a term that is defined to require either significant financial losses or potential impact on medical treatment. Yet, the NII and other computer systems are used for access to critical services such as emergency response systems, air traffic control, and the electrical power systems. These infrastructures are heavily dependent on computers. A computer attack that damages those computers could have significant repercussions for our public safety and our national security. The definition of ''damage'' in the Computer Fraud and Abuse statute should be sufficiently broad to encompass these types of harm against which people should be protected. The NII Protection Act addresses this concern and broadens the definition of ''damage'' to include causing physical injury to any person and threatening the public health or safety.

Finally, this legislation address a new and emerging problem of computer-age blackmail. This is a high-technology variation on old fashioned extortion. One case has been brought to my attention in which a person threatened to crash a computer system unless he was given free access to the system and an account. One can imagine situations in which hackers penetrate a system, encrypt a database and then demand money for the decoding key. This new provision would ensure law enforcement's ability to prosecute modern-day blackmailers, who threaten to harm or shut down computer networks unless their extortion demands are met.

Confronting cybercrime with up-to-date criminal laws, coupled with tough law enforcement, are critical for safeguarding the privacy, confidentiality and reliability of our critical computer systems and networks. I commend the Attorney General and the prosecutors within the Department of Justice who have worked diligently on this legislation and for their continuing efforts to address this critical area of our criminal law.

In sum, the NII Protection Act will provide much needed protection for our Nation's critical information infrastructure by penalizing those who abuse computers to damage computer networks, steal classified and valuable computer information, and commit other crimes on-line.

Mr. STEVENS. Mr. President, I ask unanimous consent that the amendments be agreed to, the motions to reconsider be laid on the table, en bloc, the committee amendment be agreed to, the bill be deemed read for the third time, passed, as amended, the motion to reconsider be laid upon the table, and that any statements relating to the bill appear at this point in the RECORD.

The PRESIDING OFFICER. Without objection, it is so ordered.

The amendments (Nos. 5388 and 5389), en bloc, were agreed to.

The committee amendment in the nature of a substitute, as amended, was agreed to.

The bill (S. 982), as amended, was deemed read the third time, and passed, as follows:

S. 982

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 ''National Information Infrastructure Protection Act of 1996''.

SEC. 2. COMPUTER CRIME.

Section 1030 of title 18, United States Code, is amended—

(1) in subsection (a)—

(A) in paragraph (1)—

(i) by striking ''knowingly accesses'' and inserting ''having knowingly accessed'';

(ii) by striking ''exceeds'' and inserting ''exceeding'';

(iii) by striking ''obtains information'' and inserting ''having obtained information'';

(iv) by striking ''the intent or'';

(v) by striking ''is to be used'' and inserting ''could be used''; and

(vi) by inserting before the semicolon at the end the following: ''willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it'';

(B) in paragraph (2)—

(i) by striking ''obtains information'' and inserting ''obtains—

''(A) information''; and

(ii) by adding at the end the following new subparagraphs:

''(B) information from any department or agency of the United States; or

''(C) information from any protected computer if the conduct involved an interstate or foreign communication;'';

(C) in paragraph (3)—

(i) by inserting ''nonpublic'' before ''computer of a department or agency'';

(ii) by striking ''adversely''; and

(iii) by striking ''the use of the Government's operation of such computer'' and inserting ''that use by or for the Government of the United States'';

(D) in paragraph (4)—

(i) by striking ''Federal interest'' and inserting ''protected''; and

(ii) by inserting before the semicolon the following: ''and the value of such use is not more than $5,000 in any 1-year period'';

(E) by striking paragraph (5) and inserting the following:

''(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

''(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

''(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage;''; and

(F) by inserting after paragraph (6) the following new paragraph:

''(7) with intent to extort from any person, firm, association, educational institution, financial institution, government entity, or other legal entity, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;'';

(2) in subsection (c)—

(A) in paragraph (1), by striking ''such subsection'' each place that term appears and inserting ''this section'';

(B) in paragraph (2)—

(i) in subparagraph (A)—

(I) by inserting '', (a)(5)(C),'' after ''(a)(3)''; and

(II) by striking ''such subsection'' and inserting ''this section'';

(ii) by redesignating subparagraph (B) as subparagraph (C);

(iii) by inserting immediately after subparagraph (A) the following:

''(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), if—

''(i) the offense was committed for purposes of commercial advantage or private financial gain;

''(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

''(iii) the value of the information obtained exceeds $5,000;''; and

(iv) in subparagraph (C) (as redesignated)—

(I) by striking ''such subsection'' and inserting ''this section''; and

(II) by adding ''and'' at the end;

(C) in paragraph (3)—

(i) in subparagraph (A)—

(I) by striking ''(a)(4) or (a)(5)(A)'' and inserting ''(a)(4), (a)(5)(A), (a)(5)(B), or (a)(7)''; and

(II) by striking ''such subsection'' and inserting ''this section''; and

(ii) in subparagraph (B)—

(I) by striking ''(a)(4) or (a)(5)'' and inserting ''(a)(4), (a)(5)(A), (a)(5)(B), (a)(5)(C), or (a)(7)''; and

(II) by striking ''such subsection'' and inserting ''this section''; and

(D) by striking paragraph (4);

(3) in subsection (d), by inserting ''subsections (a)(2)(A), (a)(2)(B), (a)(3), (a)(4), (a)(5), and (a)(6) of'' before ''this section.'';

(4) in subsection (e)—

(A) in paragraph (2)—

(i) by striking ''Federal interest'' and inserting ''protected'';

(ii) in subparagraph (A), by striking ''the use of the financial institution's operation or the Government's operation of such computer'' and inserting ''that use by or for the financial institution or the Government''; and

(iii) by striking subparagraph (B) and inserting the following:

''(B) which is used in interstate or foreign commerce or communication;'';

(B) in paragraph (6), by striking ''and'' at the end;

(C) in paragraph (7), by striking the period at the end and inserting ''; and''; and

(D) by adding at the end the following new paragraphs:

''(8) the term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information, that—

''(A) causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals;

''(B) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment, or care of one or more individuals;

''(C) causes physical injury to any person; or

''(D) threatens public health or safety; and

''(9) the term 'government entity' includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country.''; and

(5) in subsection (g)—

(A) by striking '', other than a violation of subsection (a)(5)(B),''; and

(B) by striking ''of any subsection other than subsection (a)(5)(A)(ii)(II)(bb) or (a)(5)(B)(ii)(II)(bb)'' and inserting ''involving damage as defined in subsection (e)(8)(A)''.

SEC. 3. TRANSFER OF PERSONS FOUND NOT GUILTY BY REASON OF INSANITY.

(a) AMENDMENT OF SECTION 4243 OF TITLE 18.—Section 4243 of title 18, United States Code, is amended by adding at the end the following new subsection:

''(i) CERTAIN PERSONS FOUND NOT GUILTY BY REASON OF INSANITY IN THE DISTRICT OF COLUMBIA.—

''(1) TRANSFER TO CUSTODY OF THE ATTORNEY GENERAL.—Notwithstanding section 301(h) of title 24 of the District of Columbia Code, and notwithstanding subsection 4247(j) of this title, all persons who have been committed to a hospital for the mentally ill pursuant to section 301(d)(1) of title 24 of the District of Columbia Code, and for whom the United States has continuing financial responsibility, may be transferred to the custody of the Attorney General, who shall hospitalize the person for treatment in a suitable facility.

''(2) APPLICATION.—

''(A) IN GENERAL.—The Attorney General may establish custody over such persons by filing an application in the United States District Court for the District of Columbia, demonstrating that the person to be transferred is a person described in this subsection.

''(B) NOTICE.—The Attorney General shall, by any means reasonably designed to do so, provide written notice of the proposed transfer of custody to such person or such person's guardian, legal representative, or other lawful agent. The person to be transferred shall be afforded an opportunity, not to exceed 15 days, to respond to the proposed transfer of custody, and may, at the court's discretion, be afforded a hearing on the proposed transfer of custody. Such hearing, if granted, shall be limited to a determination of whether the constitutional rights of such person would be violated by the proposed transfer of custody.

''(C) ORDER.—Upon application of the Attorney General, the court shall order the person transferred to the custody of the Attorney General, unless, pursuant to a hearing under this paragraph, the court finds that the proposed transfer would violate a right of such person under the United States Constitution.

''(D) EFFECT.—Nothing in this paragraph shall be construed to—

''(i) create in any person a liberty interest in being granted a hearing or notice on any matter;

''(ii) create in favor of any person a cause of action against the United States or any officer or employee of the United States; or

''(iii) limit in any manner or degree the ability of the Attorney General to move, transfer, or otherwise manage any person committed to the custody of the Attorney General.

''(3) CONSTRUCTION WITH OTHER SECTIONS.—Subsections (f) and (g) and section 4247 shall apply to any person transferred to the custody of the Attorney General pursuant to this subsection.''.

(b) TRANSFER OF RECORDS.—Notwithstanding any provision of the District of Columbia Code or any other provision of law, the District of Columbia and St. Elizabeth's Hospital—

(1) not later than 30 days after the date of enactment of this Act, shall provide to the Attorney General copies of all records in the custody or control of the District or the Hospital on such date of enactment pertaining to persons described in section 4243(i) of title 18, United States Code (as added by subsection (a));

(2) not later than 30 days after the creation of any records by employees, agents, or contractors of the District of Columbia or of St. Elizabeth's Hospital pertaining to persons described in section 4243(i) of title 18, United States Code, provide to the Attorney General copies of all such records created after the date of enactment of this Act;

(3) shall not prevent or impede any employee, agent, or contractor of the District of Columbia or of St. Elizabeth's Hospital who has obtained knowledge of the persons described in section 4243(i) of title 18, United States Code, in the employee's professional capacity from providing that knowledge to the Attorney General, nor shall civil or criminal liability attach to such employees, agents, or contractors who provide such knowledge; and

(4) shall not prevent or impede interviews of persons described in section 4243(i) of title 18, United States Code, by representatives of the Attorney General, if such persons voluntarily consent to such interviews.

(c) CLARIFICATION OF EFFECT ON CERTAIN TESTIMONIAL PRIVILEGES.—The amendments made by this section shall not be construed to affect in any manner any doctor-patient or psychotherapist-patient testimonial privilege that may be otherwise applicable to persons found not guilty by reason of insanity and affected by this section.

(d) SEVERABILITY.—If any provision of this section, an amendment made by this section, or the application of such provision or amendment to any person or circumstance is held to be unconstitutional, the remainder of this section and the amendments made by this section shall not be affected thereby.

SEC. 4. ESTABLISHING BOYS AND GIRLS CLUBS.

(a) FINDINGS AND PURPOSE.—

(1) FINDINGS.—The Congress finds that—

(A) the Boys and Girls Clubs of America, chartered by an Act of Congress on December 10, 1991, during its 90-year history as a national organization, has proven itself as a positive force in the communities it serves;

(B) there are 1,810 Boys and Girls Clubs facilities throughout the United States, Puerto Rico, and the United States Virgin Islands, serving 2,420,000 youths nationwide;

(C) 71 percent of the young people who benefit from Boys and Girls Clubs programs live in our inner cities and urban areas;

(D) Boys and Girls Clubs are locally run and have been exceptionally successful in balancing public funds with private sector donations and maximizing community involvement;

(E) Boys and Girls Clubs are located in 289 public housing sites across the Nation;

(F) public housing projects in which there is an active Boys and Girls Club have experienced a 25 percent reduction in the presence of crack cocaine, a 22 percent reduction in overall drug activity, and a 13 percent reduction in juvenile crime;

(G) these results have been achieved in the face of national trends in which overall drug use by youth has increased 105 percent since 1992 and 10.9 percent of the Nation's young people use drugs on a monthly basis; and

(H) many public housing projects and other distressed areas are still underserved by Boys and Girls Clubs.

(2) PURPOSE.—It is the purpose of this section to provide adequate resources in the form of seed money for the Boys and Girls Clubs of America to establish 1,000 additional local Boys and Girls Clubs in public housing projects and other distressed areas by 2001.

(b) DEFINITIONS.—For purposes of this section—

(1) the terms ''public housing'' and ''project'' have the same meanings as in section 3(b) of the United States Housing Act of 1937; and

(2) the term ''distressed area'' means an urban, suburban, or rural area with a high percentage of high risk youth as defined in section 509A of the Public Health Service Act (42 U.S.C. 290aa–8(f)).

(c) ESTABLISHMENT.—

(1) IN GENERAL.—For each of the fiscal years 1997, 1998, 1999, 2000, and 2001, the Director of the Bureau of Justice Assistance of the Department of Justice shall provide a grant to the Boys and Girls Clubs of America for the purpose of establishing Boys and Girls Clubs in public housing projects and other distressed areas.

(2) CONTRACTING AUTHORITY.—Where appropriate, the Secretary of Housing and Urban Development, in consultation with the Attorney General, shall enter into contracts with the Boys and Girls Clubs of America to establish clubs pursuant to the grants under paragraph (1).

(d) REPORT.—Not later than May 1 of each fiscal year for which amounts are made available to carry out this Act, the Attorney General shall submit to the Committees on the Judiciary of the Senate and the House of Representatives a report that details the progress made under this Act in establishing Boys and Girls Clubs in public housing projects and other distressed areas, and the effectiveness of the programs in reducing drug abuse and juvenile crime.

(e) AUTHORIZATION OF APPROPRIATIONS.—

(1) IN GENERAL.—There are authorized to be appropriated to carry out this section—

(A) $20,000,000 for fiscal year 1997;

(B) $20,000,000 for fiscal year 1998;

(C) $20,000,000 for fiscal year 1999;

(D) $20,000,000 for fiscal year 2000; and

(E) $20,000,000 for fiscal year 2001.

(2) VIOLENT CRIME REDUCTION TRUST FUND.—The sums authorized to be appropriated by this subsection may be made from the Violent Crime Reduction Trust Fund.

HONORARY CITIZENSHIP OF THE UNITED STATES ON MOTHER TERESA

Mr. STEVENS. Mr. President, I now ask unanimous consent that the Senate proceed to the consideration of House Joint Resolution 191, which was received from the House.

The PRESIDING OFFICER. The clerk will report.

The legislative clerk read as follows:

A joint resolution (H.J. Res. 191) to confer honorary citizenship of the United States on Agnes Gonxha Bojaxhiu also known as Mother Teresa.