Calendar No. 467

109TH CONGRESS *2nd Session*	SENATE	REPORT 109–262

SOFTWARE PRINCIPLES YIELDING BETTER LEVELS OF CONSUMER KNOWLEDGE ACT

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 687

JUNE 12, 2006.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
49–010 WASHINGTON : 2006

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

TED STEVENS, Alaska, *Chairman*
DANIEL K. INOUYE, Hawaii, *Co-Chairman*

JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA SUTHERLAND, *Staff Director*
CHRISTINE DRAGER KURTH, *Deputy Staff Director*
KENNETH NAHIGIAN, *Chief Counsel*
MARGARET CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL WHITEHORN, *Democratic Deputy Staff Director and General Counsel*

Calendar No. 467

109TH CONGRESS *2nd Session* | SENATE | REPORT 109–262

SOFTWARE PRINCIPLES YIELDING BETTER LEVELS OF CONSUMER KNOWLEDGE ACT

JUNE 12, 2006.—Ordered to be printed

Mr. STEVENS, from the Committee on Commerce, Science, and Transportation, submitted the following

R E P O R T

[To accompany S. 687]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 687) to regulate the unauthorized installation of computer software, to require clear disclosure to computer users of certain computer software features that may pose a threat to user privacy, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

The purpose of this legislation is to prohibit a variety of unfair or deceptive software and online practices that may result in spyware, adware or other unwanted software surreptitiously being placed on consumers' computers. The Committee substitute amended S. 687 to focus on unfair and deceptive practices involving software, not on legitimate software applications or legitimate uses of information. The legislation would prohibit the unauthorized installation of software that: (1) takes control of or modifies a user's computer or prevents reasonable efforts by the user to block, disable, or uninstall such software, (2) collects sensitive personal information without the user's prior consent, (3) collects and transmits personally identifiable information without prior disclosure to, or the knowledge of the user, and (4) causes advertising windows to appear on the user's computer, except when certain conditions are met or exceptions apply. The legislation also would clarify that the installation of software on a user's computer shall be consid-

ered an unfair or deceptive practice in violation of section 5 of the Federal Trade Commission Act (15 U.S.C. 41 et seq.), and provide a uniform national standard governing regulation of spyware and adware without overriding State common law or generally applicable consumer protection law. The legislation would not inhibit "anti-spyware" software programs that remove spyware from user computers.

SUMMARY OF PROVISIONS

S. 687, the SPYBLOCK Act of 2005, would provide consumers with protection against the unauthorized installation of software commonly referred to as "spyware" that takes control of a computer, modifies settings on a computer for various improper purposes, and evades user efforts to uninstall the software. The legislation also would provide a disclosure and consent regime for the collection of sensitive personal information by software programs and a disclosure regime for personally identifiable information that is collected. It also would prohibit adware that cannot be uninstalled and that does not identify that it is triggering advertisements. Specific exceptions are included to protect legitimate software functionality.

LEGISLATIVE HISTORY

On March 20, 2005, Senator Burns introduced S. 687, the "SPYBLOCK Act of 2005." Senators Wyden and Boxer were original co-sponsors, and were later joined by Senators Snowe and Bill Nelson. On May 11, 2005, Senator Allen introduced S. 1004, the "Enhanced Consumer Protection Against Spyware Act of 2005", with Senators Ensign and Smith as original co-sponsors. Senators DeMint, Enzi and Sununu also co-sponsored S. 1004. On May 11, 2005, the Full Committee held a hearing on the topic of spyware. Witnesses included industry associations, anti-Spyware companies, consumer groups, and others. On October 5, 2005, the Trade, Tourism and Economic Development Subcommittee held another hearing on Spyware, with Chairwoman Majoras of the Federal Trade Commission (FTC or Commission) as the sole witness.

On November 17, 2005, the Committee met in open Executive Session to consider an amendment in the nature of a substitute to S. 687 offered by Senator Burns. This amendment was adopted 14-8 by a roll call vote. An amendment in the nature of a substitute offered by Senator Allen to substitute the text of S. 1004 was defeated by a 13-9 roll call vote. Senator Sununu offered an amendment, which was accepted on voice vote. Senator Sununu's amendment would double the FTC penalties for an unfair or deceptive act or practice that exploits popular reaction to a national emergency, major disaster, or international disaster. The bill, as amended, was ordered to be reported.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

DECEMBER 12, 2005

Hon. TED STEVENS,
Chairman, Committee on Commerce, Science, and Transportation
U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 687, a bill to regulate the unauthorized installation of computer software, to require clear disclosure to computer users of certain computer software features that may pose a threat to user privacy, and for other purposes.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Melissa Z. Petersen (for federal costs), Sarah Puro (for the impact on state and local governments), and Paige Piper/Bach (for the impact on the private sector.

Sincerely,

DOUGLAS HOLTZ-EAKIN,
Director.

Enclosure

S. 687—A bill to regulate the unauthorized installation of computer software, to require clear disclosure to computer users of certain computer software features that may pose a threat to user privacy, and for other purposes

Summary: S. 687 would prohibit the use of computer software (known as spyware) to collect personal information and to monitor the behavior of computer users without a user's consent. The Federal Trade Commission (FTC) would be directed to enforce this bill's provisions relating to spyware. S. 687 also would direct the FTC to assess and collect civil penalties for violations of laws relating to spyware and for unfair or deceptive business practices committed during designated emergency periods. (Civil penalties are recorded in the federal budget as revenues.) Finally, S. 687 would establish criminal penalties for certain unauthorized uses of a computer. (Collections of criminal fines are recorded in the budget as revenues, deposited in the Crime Victims Fund, and spent in subsequent years.)

Based on information provided by the FTC, CBO estimates that enacting S. 687 would not have a significant effect on revenues or direct spending. Assuming appropriation of the necessary amounts, CBO estimates that implementing the bill would cost about $1 million in 2006 and about $7 million over the 2006–2010 period.

S. 687 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that the resulting costs for state, local, and tribal governments would be minimal and would not exceed the threshold established in UMRA ($62 million in 2005, adjusted annually for inflation).

S. 687 would impose private-sector mandates, as defined in UMRA, on persons who cause the installation of certain software on computers owned by another person. Based on information from the industry and the FTC, CBO expects that the aggregate direct cost to comply with those mandates would be small and fall below the annual threshold established by UMRA for private-sector mandates ($123 million in 2005, adjusted annually for inflation).

Estimated cost to the Federal Government: The estimated budgetary impact of S. 687 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—				
	2006	2007	2008	2009	2010
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Estimated authorization level	1	1	1	2	2
Estimated outlays	1	1	1	2	2

Basis of estimate: For this estimate, CBO assumes that the bill will be enacted in 2006. We also assume that amounts needed to implement S. 687 will be appropriated for each year and that outlays will follow historical trends for similar programs. Implementing the bill would increase spending by the FTC for enforcing the bill's provisions related to spyware, subject to the availability of appropriated funds. Based on information from the agency, CBO estimates that such activities would cost about $1 million 2006 and about $7 million over the 2006–2010 period.

Enacting S. 687 could increase federal revenues from civil penalties assessed for violating laws related to spyware and from increasing penalties assessed for unfair or deceptive business practices committed during designated emergency periods. Collections of civil fines are recorded in the budget as revenues. Based on information provided by the FTC, CBO estimates that any new collections would be less than $500,000 a year.

Enacting S. 687 also could increase federal revenues as a result of increasing the maximum civil penalty assessed for certain unauthorized uses of computers. Collections of criminal fines are recorded in the budget as revenues, deposited in the Crime Victims Fund, and spent in subsequent years. Based on information provided by the FTC, CBO expects that under S. 687 any additional receipts and direct spending would total less than $500,000 each year.

Estimated impact on state, local, and tribal governments: S. 687 contains intergovernmental mandates as defined in UMRA, but CBO estimates that any costs to state, local, or tribal governments would be insignificant and would fall significantly below the threshold established in UMRA ($62 million in 2005, adjusted annually for inflation).

Section 109 would require the Attorney General of a state who files a civil suit to notify the FTC and would grant the FTC the right to intervene in such a suit. This requirement on the officers of a state constitutes a mandate as defined in UMRA.

Section 11 (b) would preempt state laws that prohibit the use of certain types of computer software and would establish penalties for violators. Section 110(b) would prohibit states from creating civil penalties that specifically reference the statute. These preemptions and prohibitions, while mandates as defined in UMRA, are narrow and would specifically preserve state authority to pursue fraud, trespass, contract, and tort cases under state law. They also

would not prohibit states from passing similar criminal and civil statutes.

Estimated impact on the private sector: S. 687 would impose private-sector mandates, as defined in UMRA, on persons who cause the installation of certain software on computers owned by another person. Based on information from the industry and the FTC, CBO expects that the aggregate direct cost to comply with those mandates would be small and fall below the annual threshold established by UMRA for private-sector mandates ($123 million in 2005, adjusted annually for inflation).

The bill would impose mandates on persons who cause the installation of software that can be used to collect information from or take control of a computer without the consent of the authorized user. Currently, the FTC is prosecuting various cases against persons who cause the unauthorized installation of software on another person's computer under the unfair or deceptive practices provisions of the Federal Trade Commission Act. The bill would impose new private-setor mandates on persons to the extent that its provisions would prohibit activities allowed under current law. According to the FTC, the requirements contained in this bill represent only marginal changes to current law, if any. Based on information from the industry and the FTC, CBO expects that the aggregate direct cost to comply with any incremental requirements in the bill would be small and fall below UMRA's annual threshold for private-sector mandates.

Estimate prepared by: Federal costs: Melissa Z. Petersen; impact on state, local, and tribal governments: Sarah Pauro; impact on the private sector: Paige Piper/Bach.

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

S. 687 would establish Federal regulations for certain practices that may result in spyware, adware, or other types of unwanted software being placed or hidden on consumers' computers without their knowledge or consent. The bill would, therefore, cover persons or entities that cause the installation of such software in a proscribed manner on consumers' computers, subject to certain limitations set forth in the legislation.

ECONOMIC IMPACT

S. 687 would require software distributors, websites, and other online entities involved in the distribution, download, installation, operation, or removal of software programs, or in the delivery of advertisements through adware programs, to comply with the consumer safeguards set forth. Many companies already may refrain from the practices prohibited by the legislation or voluntarily provide protections for consumers that would be sufficient to avoid potential liability. Overall, the reduction of spyware should have a

positive impact on consumer confidence and electronic commerce. The legislation could create compliance costs for some companies in the form of software upgrades or personnel additions in order to ensure that their practices satisfy the new Federal requirements. Such expenditures may have an economic impact on such businesses, which could be passed on to consumers.

PRIVACY

S. 687 likely would increase consumer privacy by imposing limitations on the installation of software that may surreptitiously collect and transmit sensitive personal information or personally identifiable information.

PAPERWORK

S. 687 is expected to have minimal or no impact on current paperwork levels.

SECTION-BY-SECTION ANALYSIS

TITLE I—SPYWARE

Section 101. Short title

Section 101 would set forth the short title for the bill as the "Software Principles Yielding Better Levels of Consumer Knowledge Act" or the "SPY BLOCK Act".

Section 102. FTC authority to combat deceptive acts or practices relating to spyware

Section 102 would clarify that the installation of software shall be considered an unfair or deceptive act or practice in violation of section 5 of the FTC Act. It also would make clear that title I does not limit the range of unfair or deceptive acts or practices that violate the FTC Act to those acts or practices that are enumerated in the bill.

Section 103. Prohibited behaviors

Section 103 would prohibit the unauthorized installation of software that: (1) takes control of a computer, (2) modifies settings on a computer for various improper purposes, or (3) evades user efforts to decline installation or disable or uninstall software.

Specifically, paragraph (1) addresses:

(A) "zombies" software that takes control of a computer connected to a network to transmit or relay spam or computer viruses from that computer without the authorization of an authorized user of the computer;

(B) "modem hijacking" software that accesses or uses an authorized user's modem or Internet service for the purpose of causing either damage or fees to be incurred;

(C) "denial of service attacks" software that uses multiple computers for the purpose of causing damage to other computers; and

(D) "endless loop pop-up advertisement" software that opens multiple pop-up advertising windows on a user's computer without the authorization of the user. This prohibition would not cover communications originated by the computer's oper-

ating system, by software the user knowingly chooses to activate, by a service the user chooses to activate, or for any of the purposes addressed in section 106.

Specifically, paragraph (2) addresses:

(A) "enabling identity theft" by modifying the security or other settings related to access or use of the Internet that protect information about the authorized user;

(B) "disabling security" by modifying the security settings of a networked computer for the purpose of causing damage to the computer or another computer; and

(C) "browser settings" by modifying the authorized user's home page, default Internet access or search provider, search bookmarks, or web proxy through which the authorized user's Internet traffic flows.

Specifically, paragraph (3) addresses:

(A) "falsifying option to decline installs" by preventing, without permission of the authorized user, a user's reasonable efforts to prevent installation of, disable, or uninstall software; and

(B) "evading uninstalls by unfair or deceptive means" by misrepresenting that the software has been removed or creating obstacles to the removal of the software.

Section 104. Installing personal information collection features on a user's computer

Subsection (a) would prohibit causing the installation on a user's computer of software that collects sensitive personal information without first providing clear and conspicuous disclosure to the user and obtaining the user's consent. It would require disclosure and consent to extract from the computer an authorized user's social security number, tax identification number, driver's license number, passport number, other government-issued identification number, as well as financial account or credit or debit card number, account balance or overdraft history or other sensitive personal information. It is not the Committee's intent that disclosure and consent be required each time that such a piece of data is collected so long as disclosure and consent to such an ongoing practice is provided and is consistent with such disclosure and the consumer's reasonable expectations.

Subsection (b) would prohibit causing the installation of four types of software that collect personally identifiable information if they are installed without providing clear and conspicuous notice to the user or without the knowledge of the user and for a purpose unrelated to any of the purposes of the software or service described to the user. Subsection (b)(1) addresses keystroke logging functions that record all or substantially all of the keystrokes made on the computer. Subsection (b)(2) addresses surreptitiously installing a software program that collects a history of all or substantially all of the websites the user visits and correlates it with personally identifiable information. Subsection (b)(3) addresses extracting from the computer's storage medium the substantive contents of files, data, software or other information that an authorized user has knowingly saved or installed and extracting from the computer's storage medium the substantive contents of communica-

tions sent from the computer to other computers. This would not include "data that provide a purely technical function".

Subsection (c) would provide an exemption permitting the installation of software that collects information for the provider of an online service or website that the user knowingly has used or subscribed to if the information is used only to affect the user's experience while using the online service or website.

Subsection (d)(1) would prohibit causing the installation of software that performs any of the functions described in subsections (a) or (b) if the software cannot be uninstalled or disabled through a program removal function that is usual and customary with the computer's operating system. Subsection (d)(2) would exempt programs that allow one authorized user of a computer to prevent other authorized users from uninstalling or disabling the program, provided that at least one authorized user (such as a system administrator or parent) retains the ability to uninstall or disable the program. This subsection also would make clear that the uninstall requirement does not require that the user be able separately to uninstall different features or functions, upgrades, or elements of a software or software/hardware bundle.

Section 105. Adware that conceals its operation

Subsection (a) would prohibit causing the installation of software that triggers advertising windows to appear on a user's computer regardless of whether any other functionality of the software is activated by the user or conspicuously active on the computer unless the software complies with subsection (b).

Subsection (b) would provide an exception to the prohibition in subsection (a) if a clear and conspicuous label identifying to the user which software is responsible for the ads' delivery and a clear and conspicuous hypertext link to instructions regarding how to uninstall the adware program are present.

Subsection (c) would clarify that the labeling requirements of this section do not apply to advertising software that displays ads only when the user accesses a particular website or service that either: (1) is owned or operated by the author or publisher of the software or (2) the owner or operator has authorized the display of the ads.

Section 106. Limitations on liability

Subsection (a) would ensure that monitoring or interaction, by means of a software program, with a subscriber's computer or network connection or service by or at the direction of a telecommunications carrier, cable operator, provider of computer hardware or software, financial institution, provider of an information service, or of an interactive computer service would be exempt from the restrictions in sections 103, 104, and 105 of the Act if performed for: (1) network of computer security, (2) diagnostics, (3) technical support, (4) repair, (5) network management, (6) authorized updates, (7) authorized remote system management, (8) authorized protection of users from objectionable content, (9) authorized scanning for software used in violation of sections 103, 104, or 105 for removal by an authorized user, or (10) preventing or detecting unauthorized use of software, fraudulent, or other unlawful activities.

Subsection (b) would exempt manufacturers and retailers of computers from potential liability for causing the installation of pre-in-

stalled, third-party branded software unless the manufacturer or retailer uses the software to collect information about a user or his or her use of the computer, or knows that the software will display advertisements of the manufacturer or retailer, or derives a direct financial benefit from other advertisements displayed on the computer.

Subsection (c) would clarify that nothing in title I prohibits lawful investigative, protective or intelligence activity—for example, placing a keystroke logging program on the computer of a person who is the target of a law enforcement investigation, where permitted by law.

Subsection (d) would clarify that it is not a violation of title I for a multichannel video programming distributor to use a navigation device to provide service, or to collect or disclose subscriber information if such practices are covered by the Communications Act of 1934.

Section 107. FTC Administration and enforcement

Subsection (a) would provide that the Act would be enforced by the FTC as if the violation of this Act were an unfair or deceptive act or practice proscribed by an FTC trade rule or regulation pursuant to the Commission's authority under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B)), except as provided in sections 108, 109, and 110 of the Act.

Subsection (b) would permit the FTC to obtain up to treble the penalties authorized under section 5 of the FTC Act and to seek a civil penalty for a pattern or practice of activity violating this Act of not more than $3 million for each violation.

Subsections (c) and (d) would give the Commission authority to seek seizure and forfeiture of the assets of a violator attributable to a violation of title I, and to require disgorgement of ill-gotten gains procured through unfair or deceptive acts or practices in violation of title I.

Subsection (e) would charge the FTC with enforcing this Act as it would the Federal Trade Commission Act and clarify that this Act does not limit the FTC's existing authority.

Section 108. Enforcement by other agencies

This section would provide for enforcement by other agencies for entities subject to their jurisdiction due to the jurisdictional limitations of the FTC. These agencies would be permitted under the Act to exercise authority provided by their own statutory grants to enforce the substantive provisions of this legislation.

Section 109. State enforcement

Subsection (a) would provide State attorneys general the right to bring a civil action for violations of title I. A State may bring an action in parens patriae for aggrieved residents of the State in a district court of the United States of appropriate jurisdiction to enjoin practices, enforce compliance with a rule that has been violated, obtain damages, restitution or other compensation on behalf of its residents, or obtain such other relief as the court may consider appropriate.

Except where an attorney general determines that it is not feasible prior to the filing of an action, subsection (b) would require

a State to provide the FTC with written notice of the action and a copy of the complaint for that action prior to its filing. In the event such prior notification is not feasible, the State would be required to provide such notification simultaneously with the filing of the action. Upon receipt of the notice, the FTC would have the right to intervene in the action, and if it intervenes, would have the further right to be heard with respect to any matter that arises in that action and to file a petition for appeal.

Section 110. Other enforcement

Subsection (a) would provide a civil right of action for telecommunications carriers who incur costs as a result of modem-hijacking. The carrier could recover the charges it is obligated to pay other carriers or information service providers as a result of the violation, the costs of handling customer inquiries or complaints, costs and reasonable attorney's fees and an order to enjoin the violation.

Subsection (b) would preclude any person from bringing a lawsuit under State or local law—such as a State unfair or deceptive trade practice statute that provides for a private right of action for violations of Federal law—premised in whole or in part upon the defendant's violating this Act.

Section 111. Effect on other laws

Subsection (a) would clarify that nothing in the Act should be construed to limit or affect in any way the FTC's authority to bring enforcement actions or take any other measures under the FTC Act or any other provision of law.

Subsection (b) would provide a general rule preempting any statute, regulation, or rule of a State or political subdivision that relates to or confers a remedy for (1) the installation or use of software to deliver advertisements to a protected computer, (2) the installation or use of software to collect information about a user of a protected computer, or the user's use of that computer, (3) the installation or use of software to allow a person other than an authorized user to direct or control a protected computer, or (4) the method or way of uninstalling or disabling software that performs any of the three functions described above.

Subsection (c) would provide that title I does not preempt actions or remedies based upon a State's generally applicable common law or any provision of generally applicable State consumer protection law.

Section 112. Definitions

Section 112 would define "advertising window", "authorized user", "bundle", "cause the installation", "commission", "cookie", "damage", "install", "loss", "person", "protected computer", "personally identifying information", "sensitive personal information", "software" and "unfair or deceptive act or practice".

Section 113. Criminal penalties for certain unauthorized activities relating to computers

Section 113 would provide criminal liability for certain acts carried out using software without the authorization of the user of the computer. This section would make it a crime to intentionally ac-

cess a computer without authorization, or intentionally exceed authorized access, by causing a computer program or code to be copied onto the computer and using that program or code in furtherance of another Federal criminal offense. Such conduct would be punishable by fine or imprisonment for up to five years or both. Additionally, this section would make it a crime to intentionally access a computer without authorization, or intentionally exceed authorized access, by causing a computer program or code to be copied onto the computer and using that program or code to intentionally impair the security protections of a computer. Such conduct would be punishable by fine or imprisonment for up to two years or both.

Section 113 would provide an exemption from criminal liability for individuals and network providers under certain circumstances.

Section 114. Effective date

Section 114 would provide that the provisions of title I would take effect 180 days after the date of enactment.

TITLE II—INCREASE IN CERTAIN PENALTIES

Section 201. Increase in penalties for unfair or deceptive act or practices exploiting reaction to certain emergencies and major disasters.

Subsection (a) would double the civil penalty for engaging in an unfair or deceptive act or practice in violation of section 5 of the Federal Trade Commission Act committed during national emergency period, international disaster or disaster period.

Subsection (b) would provide for a penalty of up to $22,000 for each violation of section 13 of the Federal Trade Commission Act committed during national emergency, international disaster or disaster period.

"National emergency period" describes the a one year period beginning with the President declaring a national emergency under the National Emergencies Act.

"Disaster period" describes the one year period beginning with the President declaring an emergency or major disaster under the Robert T. Stafford Disaster Relief and Emergency Assistance Act.

"International Disaster" describes any natural or man-made disaster in which the President furnishes assistance to a foreign country, international organization or private voluntary organization pursuant to the Foreign Assistance Act.

ROLLCALL VOTES IN COMMITTEE

In accordance with paragraph 7(c) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following description of the record votes during its consideration of S. 687:

Senator Burns offered an amendment in the nature of a substitute. By rollcall vote of 14 yeas and 8 nays as follows, the amendment was adopted:

YEAS—14	NAYS—8
Mr. Burns	Mr. McCain[1]
Mr. Lott[1]	Mr. Smith
Mrs. Hutchison	Mr. Ensign

Ms. Snowe[1]
Mr. Inouye
Mr. Rockefeller[1]
Mr. Kerry[1]
Mr. Dorgan[1]
Mrs. Boxer[1]
Mr. Nelson of Florida
Ms. Cantwell
Mr. Lautenberg[1]
Mr. Pryor
Mr. Stevens
Mr. Allen
Mr. Sununu
Mr. DeMint
Mr. Vitter[1]
Mr. Nelson of Nebraska

[1]By proxy

Senator Allen offered an amendment in the nature of a substitute to substitute the text of S. 1004. By rollcall vote of 9 yeas and 13 nays as follows, the amendment was defeated:

YEAS—9

Mr. McCain[1]
Mr. Smith
Mr. Ensign
Mr. Allen
Mr. Sununu
Mr. DeMint
Mr. Vitter[1]
Ms. Cantwell
Mr. Nelson of Nebraska

NAYS—13

Mr. Burns
Mr. Lott[1]
Mrs. Hutchison
Ms. Snowe
Mr. Inouye
Mr. Rockefeller[1]
Mr. Kerry[1]
Mr. Dorgan[1]
Mrs. Boxer[1]
Mr. Nelson of Florida
Mr. Lautenberg[1]
Mr. Pryor
Mr. Stevens

[1]By proxy

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman):

FEDERAL TRADE COMMISSION ACT

SEC. 5. UNFAIR METHODS OF COMPETITION UNLAWFUL; PREVENTION BY COMMISSION.

[15 U.S.C. 45]

(a) DECLARATION OF UNLAWFULNESS; POWER TO PROHIBIT UNFAIR PRACTICES; INAPPLICABILITY TO FOREIGN TRADE.—

(1) Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.

(2) The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 18(f)(3), Federal credit unions described in section 18(f)(4), common carriers

subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to the Federal Aviation Act of 1958, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended, except as provided in section 406(b) of said Act, from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.

(3) This subsection shall not apply to unfair methods of competition involving commerce with foreign nations (other than import commerce) unless—

(A) such methods of competition have a direct, substantial, and reasonably foreseeable effect—

(i) on commerce which is not commerce with foreign nations, or on import commerce with foreign nations; or

(ii) on export commerce with foreign nations, of a person engaged in such commerce in the United States; and

(B) such effect gives rise to a claim under the provisions of this subsection, other than this paragraph. If this subsection applies to such methods of competition only because of the operation of subparagraph (A)(ii), this subsection shall apply to such conduct only for injury to export business in the United States.

(b) PROCEEDING BY COMMISSION; MODIFYING AND SETTING ASIDE ORDERS.— Whenever the Commission shall have reason to believe that any such person, partnership, or corporation has been or is using any unfair method of competition or unfair or deceptive act or practice in or affecting commerce, and if it shall appear to the Commission that a proceeding by it in respect thereof would be to the interest of the public, it shall issue and serve upon such person, partnership, or corporation a complaint stating its charges in that respect and containing a notice of a hearing upon a day and at a place therein fixed at least thirty days after the service of said complaint. The person, partnership, or corporation so complained of shall have the right to appear at the place and time so fixed and show cause why an order should not be entered by the Commission requiring such person, partnership, or corporation to cease and desist from the violation of the law so charged in said complaint. Any person, partnership, or corporation may make application, and upon good cause shown may be allowed by the Commission to intervene and appear in said proceeding by counsel or in person. The testimony in any such proceeding shall be reduced to writing and filed in the office of the Commission. If upon such hearing the Commission shall be of the opinion that the method of competition or the act or practice in question is prohibited by this Act, it shall make a report in writing in which it shall state its findings as to the facts and shall issue and cause to be served on such person, partnership, or corporation an order requiring such person, partnership, or corporation to cease and desist from using such method of competition or such act or practice. Until the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, or, if a petition for review has been filed within such time then until the record in the proceeding has been filed in a court of appeals of the United States, as herein-

after provided, the Commission may at any time, upon such notice and in such manner as it shall deem proper, modify or set aside, in whole or in part, any report or any order made or issued by it under this section. After the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time, the Commission may at any time, after notice and opportunity for hearing, reopen and alter, modify, or set aside, in whole or in part, any report or order made or issued by it under this section, whenever in the opinion of the Commission conditions of fact or of law have so changed as to require such action or if the public interest shall so require, except that—

(1) the said person, partnership, or corporation may, within sixty days after the service upon him or it of said report or order entered after such a reopening, obtain a review thereof in the appropriate court of appeals of the United States, in the manner provided in subsection (c) of this section; and

(2) in the case of an order, the Commission shall reopen any such order to consider whether such order (including any affirmative relief provision contained in such order) should be altered, modified, or set aside, in whole or in part, if the person, partnership, or corporation involved files a request with the Commission which makes a satisfactory showing that changed conditions of law or fact require such order to be altered, modified, or set aside, in whole or in part. The Commission shall determine whether to alter, modify, or set aside any order of the Commission in response to a request made by a person, partnership, or corporation under paragraph (2) not later than 120 days after the date of the filing of such request.

(c) REVIEW OF ORDER; REHEARING.—Any person, partnership, or corporation required by an order of the Commission to cease and desist from using any method of competition or act or practice may obtain a review of such order in the court of appeals of the United States, within any circuit where the method of competition or the act or practice in question was used or where such person, partnership, or corporation resides or carries on business, by filing in the court, within sixty days from the date of the service of such order, a written petition praying that the order of the Commission be set aside. A copy of such petition shall be forthwith transmitted by the clerk of the court to the Commission, and thereupon the Commission shall file in the court the record in the proceeding, as provided in section 2112 of title 28, United States Code. Upon such filing of the petition the court shall have jurisdiction of the proceeding and of the question determined therein concurrently with the Commission until the filing of the record and shall have power to make and enter a decree affirming, modifying, or setting aside the order of the Commission, and enforcing the same to the extent that such order is affirmed and to issue such writs as are ancillary to its jurisdiction or are necessary in its judgment to prevent injury to the public or to competitors pendente lite. The findings of the Commission as to the facts, if supported by evidence, shall be conclusive. To the extent that the order of the Commission is affirmed, the court shall thereupon issue its own order commanding obedience to the terms of such order of the Commission. If either party shall apply to the court for leave to adduce additional evidence, and shall show to the satisfaction of the court that such additional evidence

is material and that there were reasonable grounds for the failure to adduce such evidence in the proceeding before the Commission, the court may order such additional evidence to be taken before the Commission and to be adduced upon the hearing in such manner and upon such terms and conditions as to the court may seem proper. The Commission may modify its findings as to the facts, or make new findings, by reason of the additional evidence so taken, and it shall file such modified or new findings, which, if supported by evidence, shall be conclusive, and its recommendation, if any, for the modification or setting aside of its original order, with the return of such additional evidence. The judgment and decree of the court shall be final, except that the same shall be subject to review by the Supreme Court upon certiorari, as provided in section 240 of the Judicial Code (28 U.S.C. 1254).

(d) JURISDICTION OF COURT.—Upon the filing of the record with it the jurisdiction of the court of appeals of the United States to affirm, enforce, modify, or set aside orders of the Commission shall be exclusive.

(e) EXTENSION FROM LIABILITY.—No order of the Commission or judgment of court to enforce the same shall in anywise relieve or absolve any person, partnership, or corporation from any liability under the Antitrust Acts.

(f) SERVICE OF COMPLAINTS, ORDERS AND OTHER PROCESSES; RETURN.—Complaints, orders, and other processes of the Commission under this section may be served by anyone duly authorized by the Commission, either (a) by delivering a copy thereof to the person to be served, or to a member of the partnership to be served, or the president, secretary, or other executive officer or a director of the corporation to be served; or (b) by leaving a copy thereof at the residence or the principal office or place of business of such person, partnership, or corporation; or by mailing a copy thereof by registered mail or by certified mail addressed to such person, partnership, or corporation at his or its residence or principal office or place of business. The verified return by the person so serving said complaint, order, or other process setting forth the manner of said service shall be proof of the same, and the return post office receipt for said complaint, order, or other process mailed by registered mail or by certified mail as aforesaid shall be proof of the service of the same.

(g) FINALITY OF ORDER.—An order of the Commission to cease and desist shall become final—

(1) Upon the expiration of the time allowed for filing a petition for review, if no such petition has been duly filed within such time; but the Commission may thereafter modify or set aside its order to the extent provided in the last sentence of subsection (b).

(2) Except as to any order provision subject to paragraph (4), upon the sixtieth day after such order is served, if a petition for review has been duly filed; except that any such order may be stayed, in whole or in part and subject to such conditions as may be appropriate, by—

(A) the Commission;

(B) an appropriate court of appeals of the United States, if

(i) a petition for review of such order is pending in such court, and

(ii) an application for such a stay was previously submitted to the Commission and the Commission, within the 30-day period beginning on the date the application was received by the Commission, either denied the application or did not grant or deny the application; or

(C) the Supreme Court, if an applicable petition for certiorari is pending.

(3) For purposes of subsection (m)(1)(B) and of section 19(a)(2) (15 U.S.C. 57b(a)(2)), if a petition for review of the order of the Commission has been filed—

(A) upon the expiration of the time allowed for filing a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals and no petition for certiorari has been duly filed;

(B) upon the denial of a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals; or

(C) upon the expiration of 30 days from the date of issuance of a mandate of the Supreme Court directing that the order of the Commission be affirmed or the petition for review be dismissed.

(4) In the case of an order provision requiring a person, partnership, or corporation to divest itself of stock, other share capital, or assets, if a petition for review of such order of the Commission has been filed—

(A) upon the expiration of the time allowed for filing a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals and no petition for certiorari has been duly filed;

(B) upon the denial of a petition for certiorari, if the order of the Commission has been affirmed or the petition for review has been dismissed by the court of appeals; or

(C) upon the expiration of 30 days from the date of issuance of a mandate of the Supreme Court directing that the order of the Commission be affirmed or the petition for review be dismissed.

(h) MODIFICATION OR SETTING ASIDE OF ORDER BY SUPREME COURT.—If the Supreme Court directs that the order of the Commission be modified or set aside, the order of the Commission rendered in accordance with the mandate of the Supreme Court shall become final upon the expiration of thirty days from the time it was rendered, unless within such thirty days either party has instituted proceedings to have such order corrected to accord with the mandate, in which event the order of the Commission shall become final when so corrected.

(i) MODIFICATION OR SETTING ASIDE OF ORDER BY COURT OF APPEALS.—If the order of the Commission is modified or set aside by the court of appeals, and if (1) the time allowed for filing a petition for certiorari has expired and no such petition has been duly filed, or (2) the petition for certiorari has been denied, or (3) the decision

of the court has been affirmed by the Supreme Court, then the order of the Commission rendered in accordance with the mandate of the court of appeals shall become final on the expiration of thirty days from the time such order of the Commission was rendered, unless within such thirty days either party has instituted proceedings to have such order corrected so that it will accord with the mandate, in which event the order of the Commission shall become final when so corrected.

(j) REHEARING UPON ORDER OR REMAND.—If the Supreme Court orders a rehearing; or if the case is remanded by the court of appeals to the Commission for a rehearing, and if (1) the time allowed for filing a petition for certiorari has expired, and no such petition has been duly filed, or (2) the petition for certiorari has been denied, or (3) the decision of the court has been affirmed by the Supreme Court, then the order of the Commission rendered upon such rehearing shall become final in the same manner as though no prior order of the Commission had been rendered.

(k) "MANDATE" DEFINED.—As used in this section the term "mandate," in case a mandate has been recalled prior to the expiration of thirty days from the date of issuance thereof, means the final mandate.

(l) PENALTY FOR VIOLATION OF ORDER; INJUNCTIONS AND OTHER APPROPRIATE EQUITABLE RELIEF.—Any person, partnership, or corporation who violates an order of the Commission after it has become final, and while such order is in effect, shall forfeit and pay to the United States a civil penalty of not more than $10,000 for each violation, which shall accrue to the United States and may be recovered in a civil action brought by the Attorney General of the United States. Each separate violation of such an order shall be a separate offense, except that in the case of a violation through continuing failure to obey or neglect to obey a final order of the Commission, each day of continuance of such failure or neglect shall be deemed a separate offense. In such actions, the United States district courts are empowered to grant mandatory injunctions and such other and further equitable relief as they deem appropriate in the enforcement of such final orders of the Commission.

(m) CIVIL ACTIONS FOR RECOVERY OF PENALTIES FOR KNOWING VIOLATIONS OF RULES AND CEASE AND DESIST ORDERS RESPECTING UNFAIR OR DECEPTIVE ACTS OR PRACTICES; JURISDICTION; MAXIMUM AMOUNT OF PENALTIES; CONTINUING VIOLATIONS; DE NOVO DETERMINATIONS; COMPROMISE OR SETTLEMENT PROCEDURE.—

(1)(A) The Commission may commence a civil action to recover a civil penalty in a district court of the United States against any person, partnership, or corporation which violates any rule under this Act respecting unfair or deceptive acts or practices (other than an interpretive rule or a rule violation of which the Commission has provided is not an unfair or deceptive act or practice in violation of subsection (a)(1)) with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule. In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than $10,000 for each violation.

(B) If the Commission determines in a proceeding under subsection (b) that any act or practice is unfair or deceptive, and

issues a final cease and desist order, other than a consent order, with respect to such act or practice, then the Commission may commence a civil action to obtain a civil penalty in a district court of the United States against any person, partnership, or corporation which engages in such act or practice—

(1) after such cease and desist order becomes final (whether or not such person, partnership, or corporation was subject to such cease and desist order), and

(2) with actual knowledge that such act or practice is unfair or deceptive and is unlawful under subsection (a)(1) of this section.

In such action, such person, partnership, or corporation shall be liable for a civil penalty of not more than $10,000 for each violation.

(C) In the case of a violation through continuing failure to comply with a rule or with section 5(a)(1), each day of continuance of such failure shall be treated as a separate violation, for purposes of subparagraphs (A) and (B). In determining the amount of such a civil penalty, the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.

(D) In the case of a violation involving an unfair or deceptive act or practice in a national emergency period or disaster period, or relating to an international disaster, the amount of the civil penalty under this paragraph shall be double the amount otherwise provided in this paragraph, if the act or practice exploits popular reaction to the national emergency or major disaster that is the basis for such period, or to the international disaster.

(E) In this paragraph:

(i) The term "national emergency period" means the period that—

(I) begins on the date the President declares a national emergency under the National Emergencies Act (50 U.S.C. 1601 et seq.); and

(II) ends on the expiration of the 1-year period beginning on the date of the termination of the national emergency.

(ii) The term "disaster period" means the 1-year period beginning on the date the President declares an emergency or major disaster under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(iii) The term "international disaster" means any natural or man-made disaster in response to which the President furnishes assistance to any foreign country, international organization, or private voluntary organization pursuant to section 491 of the Foreign Assistance Act (22 U.S.C. 2292(b)).

(2) If the cease and desist order establishing that the act or practice is unfair or deceptive was not issued against the defendant in a civil penalty action under paragraph (1)(B) the issues of fact in such action against such defendant shall be tried de novo. Upon request of any party to such an action against such defendant, the court shall also review the determination of law made by the Commission in the proceeding under subsection (b) that the act or practice which was the

subject of such proceeding constituted an unfair or deceptive act or practice in violation of subsection (a).

(3) The Commission may compromise or settle any action for a civil penalty if such compromise or settlement is accompanied by a public statement of its reasons and is approved by the court.

(n) DEFINITION OF UNFAIR ACTS OR PRACTICES.—The Commission shall have no authority under this section or section 18 to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination.

FEDERAL TRADE COMMISSION ACT

SEC. 13. FALSE ADVERTISEMENTS; INJUNCTIONS AND RESTRAINING ORDERS.

[15 U.S.C. 53]

(a) POWER OF COMMISSION; JURISDICTION OF COURTS.—Whenever the Commission has reason to believe—

(1) that any person, partnership, or corporation is engaged in, or is about to engage in, the dissemination or the causing of the dissemination of any advertisement in violation of section 12, and

(2) that the enjoining thereof pending the issuance of a complaint by the Commission under section 5, and until such complaint is dismissed by the Commission or set aside by the court on review, or the order of the Commission to cease and desist made thereon has become final within the meaning of section 5, would be to the interest of the public,

the Commission by any of its attorneys designated by it for such purpose may bring suit in a district court of the United States or in the United States court of any Territory, to enjoin the dissemination or the causing of the dissemination of such advertisement. Upon proper showing a temporary injunction or restraining order shall be granted without bond. Any suit may be brought where such person, partnership, or corporation resides or transacts business, or wherever venue is proper under section 1391 of title 28, United States Code. In addition, the court may, if the court determines that the interests of justice require that any other person, partnership, or corporation should be a party in such suit, cause such other person, partnership, or corporation to be added as a party without regard to whether venue is otherwise proper in the district in which the suit is brought. In any suit under this section, process may be served on any person, partnership, or corporation wherever it may be found.

(b) TEMPORARY RESTRAINING ORDERS; PRELIMINARY INJUNCTIONS.—Whenever the Commission has reason to believe

(1) that any person, partnership, or corporation is violating, or is about to violate, any provision of law enforced by the Federal Trade Commission, and

(2) that the enjoining thereof pending the issuance of a complaint by the Commission and until such complaint is dismissed by the Commission or set aside by the court on review, or until the order of the Commission made thereon has become final, would be in the interest of the public

the Commission by any of its attorneys designated by it for such purpose may bring suit in a district court of the United States to enjoin any such act or practice. Upon a proper showing that, weighing the equities and considering the Commission's likelihood of ultimate success, such action would be in the public interest, and after notice to the defendant, a temporary restraining order or a preliminary injunction may be granted without bond: *Provided, however,* That if a complaint is not filed within such period (not exceeding 20 days) as may be specified by the court after issuance of the temporary restraining order or preliminary injunction, the order or injunction shall be dissolved by the court and be of no further force and effect: *Provided further,* That in proper cases the Commission may seek, and after proper proof, the court may issue, a permanent injunction. Any suit may be brought where such person, partnership, or corporation resides or transacts business, or wherever venue is proper under section 1391 of title 28, United States Code. In addition, the court may, if the court determines that the interests of justice require that any other person, partnership, or corporation should be a party in such suit, cause such other person, partnership, or corporation to be added as a party without regard to whether venue is otherwise proper in the district in which the suit is brought. In any suit under this section, process may be served on any person, partnership, or corporation wherever it may be found.

(c) SERVICE OF PROCESS OF THE COMMISSION; PROOF OF SERVICE.—Any process of the Commission under this section may be served by any person duly authorized by the Commission—

(1) by delivering a copy of such process to the person to be served, to a member of the partnership to be served, or to the president, secretary, or other executive officer or a director of the corporation to be served;

(2) by leaving a copy of such process at the residence or the principal office or place of business of such person, partnership, or corporation; or

(3) by mailing a copy of such process by registered mail or certified mail addressed to such person, partnership, or corporation at his, or her, or its residence, principal office, or principal place or business. The verified return by the person serving such process setting forth the manner of such service shall be proof of the same.

(d) EXCEPTION OF PERIODICAL PUBLICATIONS.—Whenever it appears to the satisfaction of the court in the case of a newspaper, magazine, periodical, or other publication, published at regular intervals—

(1) that restraining the dissemination of a false advertisement in any particular issue of such publication would delay the delivery of such issue after the regular time therefor, and

(2) that such delay would be due to the method by which the manufacture and distribution of such publication is customarily conducted by the publisher in accordance with sound

business practice, and not to any method or device adopted for the evasion of this section or to prevent or delay the issuance of an injunction or restraining order with respect to such false advertisement or any other advertisement,

the court shall exclude such issue from the operation of the restraining order or injunction.

(e) NATIONAL EMERGENCY OR DISASTER PERIOD.—

(1) IN GENERAL.—If a person, partnership, or corporation is found, in an action under subsection (b), to have committed a violation involving an unfair or deceptive act or practice in a national emergency period or a disaster period, or relating to an international disaster, and if the act or practice exploits popular reaction to the national emergency or major disaster that is the basis for such period, or to the international disaster, the court, after awarding equitable relief (if any) under any other authority of the court, shall hold the person, partnership, or corporation liable for a civil penalty of not more than $22,000 for each such violation.

(2) DEFINITIONS.—In this subsection:

(A) NATIONAL EMERGENCY PERIOD.—The term "national emergency period" means the period that—

(i) begins on the date the President declares a national emergency under the National Emergencies Act (50 U.S.C. 1601 et seq.); and

(ii) ends on the expiration of the 1-year period beginning on the date of the termination of the national emergency.

(B) DISASTER PERIOD.—The term "disaster period" means the 1-year period beginning on the date the President declares an emergency or major disaster under the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 et seq.).

(C) INTERNATIONAL DISASTER.—The term "international disaster" means any natural or man-made disaster in response to which the President furnishes assistance to any foreign country, international organization, or private voluntary organization pursuant to section 491 of the Foreign Assistance Act (22 U.S.C. 2292(b)).

TITLE 18, UNITED STATES CODE

CHAPTER 47. FRAUD AND FALSE STATEMENTS

§ 1030A. Illicit indirect use of protected computers

(a) FURTHERANCE OF CRIMINAL OFFENSE.—Whoever intentionally accesses a protected computer without authorization, or exceeds authorized access to a protected computer, by causing a computer program or code to be copied onto the protected computer, and intentionally uses that program or code in furtherance of another Federal criminal offense shall be fined under this title or imprisoned not more than 5 years, or both.

(b) SECURITY PROTECTION.—Whoever intentionally accesses a protected computer without authorization, or exceeds authorized access to a protected computer, by causing a computer program or code to be copied onto the protected computer, and by means of that program or code intentionally impairs the security protection of the pro-

tected computer shall be fined under this title or imprisoned not more than 2 years, or both.

(c) INDIVIDUAL EXEMPTION.—A person shall not violate this section who solely provides—

(1) an Internet connection, telephone connection, or other transmission or routing function through which software is delivered to a protected computer for installation;

(2) the storage or hosting of software, or of an Internet website, through which software is made available for installation to a protected computer; or

(3) an information location tool, such as a directory, index, reference, pointer, or hypertext link, through which a user of a protected computer locates software available for installation.

(d) NETWORK EXEMPTION.—A provider of a network or online service that an authorized user of a protected computer uses or subscribes to shall not violate this section by any monitoring or, interaction with, or installation of software for the purpose of—

(1) protecting the security of the network, service, or computer;

(2) facilitating diagnostics, technical support, maintenance, network management, or repair; or

(3) preventing or detecting unauthorized, fraudulent, or otherwise unlawful uses of the network or service.

(e) DEFINITIONS.—In this section:

(1) COMPUTER; PROTECTED COMPUTER.—The terms "computer" and "protected computer" have the meanings given such terms in section 1030(e) of this title.

(2) STATE.—The term "State" includes each of the several States, the District of Columbia, Puerto Rico, and any other territory or possession of the United States.

○