S 687

SPY BLOCK Act

Congress: 109 (2005–2007, Ended)
Chamber: Senate
Policy Area: Science, Technology, Communications
Introduced: Mar 20, 2005
Current Status: Placed on Senate Legislative Calendar under General Orders. Calendar No. 467.
Latest Action: Placed on Senate Legislative Calendar under General Orders. Calendar No. 467. (Jun 12, 2006)
Official Text: https://www.congress.gov/bill/109th-congress/senate-bill/687

Sponsor

Name: Sen. Burns, Conrad R. [R-MT]
Party: Republican • **State:** MT • **Chamber:** Senate

Cosponsors (4 total)

Cosponsor	Party / State	Role	Date Joined
Sen. Boxer, Barbara [D-CA]	D · CA		Mar 20, 2005
Sen. Nelson, Bill [D-FL]	D · FL		Mar 20, 2005
Sen. Wyden, Ron [D-OR]	D · OR		Mar 20, 2005
Sen. Snowe, Olympia J. [R-ME]	R · ME		Jun 20, 2005

Committee Activity

Committee	Chamber	Activity	Date
Commerce, Science, and Transportation Committee	Senate	Reported By	Jun 12, 2006

Subjects & Policy Tags

Policy Area:

Science, Technology, Communications

Related Bills

No related bills are listed.

Summary (as of Jun 12, 2006)

Title I: Spyware - Software Principles Yielding Better Levels of Consumer Knowledge Act or the SPY BLOCK Act - (Sec. 102) Prohibits the installation of software on protected computers (a computer used in interstate or foreign commerce or communication) through unfair or deceptive acts or practices.

(Sec. 103) Prohibits a person who is not an authorized user of a protected computer from causing the installation of software that: (1) takes control of such computer through zombies, modem hijacking, denial of service attacks, or endless loop pop-up advertisements; (2) modifies the computer's settings to enable identity theft, to disable security in order to damage that or another computer, or to change, through unfair or deceptive means, the computer's Internet browser or bookmarks; or (3) prevents, without the user's authorization and by unfair or deceptive means, such user's reasonable efforts to block installation of, disable, or uninstall software.

(Sec. 104) Prohibits a person who is not an authorized user from causing the installation on a protected computer of software that collects sensitive personal information without first providing clear and conspicuous disclosure to the authorized user and obtaining the user's consent. Requires disclosure and consent to extract from the protected computer the user's: (1) social security number; (2) tax identification number; (3) driver's license number; (4) passport number; (5) any other government-issued identification number; (6) financial account, credit card, or debit card numbers; (7) account balances or overdraft history; or (8) other sensitive personal information.

Prohibits causing the installation on a computer of software that engages in any of the following practices without prior clear and conspicuous disclosure to, or with the knowledge of, the authorized user and for a purpose unrelated to the software purposes or service described to such user: (1) keystroke logging; (2) collection of personally identifying information that is correlated with the web sites visited, other than those operated by the person providing such software; and (3) extraction of substantive contents of files, data, software, or other information knowingly saved or installed by the authorized user or the substantive contents of communications sent to another computer. Exempts from such requirement a person that installs software that collects information for the provider of an online service or website knowingly used or subscribed to by an authorized user if the information collected is used only to affect the user's experience while using such service or website.

Prohibits, without first providing clear and conspicuous disclosure, causing the installation of such software that can not be uninstalled or disabled by an authorized user through a program removal function that is usual and customary with the computer's operating system. Exempts software that allows one authorized user of a computer to prevent other authorized users from unistalling or disabling the program if at least one authorized user retains the ability to uninstall or disable the software.

(Sec. 105) Prohibits causing the installation of software that causes advertising windows to appear on a protected computer regardless of whether any other non-advertising related functionality of the software is: (1) activated by the authorized user; or (2) conspicuously active on the computer. Exempts software that: (1) displays, each time the software causes an advertisement to appear, a clear and conspicuous label or other reasonable means of identifying the software that caused the advertisement to appear; (2) the authorized user is likely to identify as the main component of an installed software bundle; (3) contains a clear and conspicuous hypertext link that provides instructions concerning how the user may, through usual and customary means, uninstall the software causing the advertisement to appear; and (4) causes advertisements to be displayed without identification if those advertisements are displayed only when a user is gaining access to or using a website or online service owned or operated by the author or publisher of the software, or if the owner or operator authorized the author or publisher of the software to display such advertisements.

(Sec. 106) Exempts from such prohibitions any monitoring of or interaction with a subscriber's network connection or service, or a protected computer, by or at the direction of a telecommunications carrier, cable operator, computer hardware or software provider, financial institution or provider of information services, or interactive computer service for: (1) network or computer security purposes; (2) diagnostics; (3) technical support; (4) repair; (5) network management; (6) authorized updates of software or system firmware; (7) authorized remote system management; (8) authorized provision of protection for users from objectionable content; (9) authorized scanning for computer software used in violation of this Act for removal; or (10) detection or prevention of the unauthorized use of fraudulent software or other illegal activities. Exempts a computer manufacturer or retailer from liability for causing the installation of third-party branded software before the first retail sale and delivery of a computer, unless the manufacturer or retailer: (1) uses the software to collect information about a user or the use of the computer; or (2) knows that the software will cause advertisements for the manufacturer or retailer to be displayed or derives a direct financial benefit from other advertisements displayed.

States that it is not a violation of this Act for a multichannel video programming distributor to utilize, interact with, or install or use software on a navigation device in connection with the provision of programming or other services offered over a multichannel video programming system or the collection or disclosure of subscriber information, if the provision of such service or the collection or disclosure of such information is subject to provisions of the Communications Act of 1934 concerning notice to satellite subscribers.

(Sec. 107) Requires violations of this Act to be treated as unfair or deceptive acts or practices under the Federal Trade Commission Act. Provides for penalties for such violations. Allows the Federal Trade Commission (FTC) to increase the penalty to threefold the amount of penalty otherwise applicable. Authorizes the FTC to seek a civil penalty of no more than $3,000,000 for each violation. Authorizes the FTC to: (1) petition the court to order the seizure and forfeiture of assets attributable to the violation; and (2) require that violators disgorge any ill-gotten gains procured through unfair or deceptive acts or practices in violation of this Act. Requires the FTC to seize any such gains it has required to be disgorged.

(Sec. 108) Provides for enforcement of this Act by other agencies through the Federal Deposit Insurance Act, the Federal Credit Union Act, the Securities and Exchange Act of 1934, the Communications Act of 1934, provisions of law concerning transportation of air carriers, and state insurance law.

(Sec. 109) Authorizes states to bring civil actions in U.S. District Court to remedy violations of this Act on behalf of their citizens. Prohibits states from instituting an action against any defendant named in a complaint in an action instituted by or for the FTC for violation of this Act.

(Sec. 110) Authorizes a telecommunications carrier to bring a civil action to recover costs and charges incurred as a result of modem hijacking violations.

Precludes any person from bringing a civil action under state law for an action premised upon the defendant's violation of this Act.

(Sec. 111) Preempts state or local law that relates to, or confers a remedy for: (1) the installation or use of software to deliver advertisements to a protected computer to collect information about a user of a protected computer, or to allow a person other than an authorized user to direct or control a protected computer; or (2) the method or manner of unistalling or disabling software that performs any of these functions.

(Sec. 113) Prescribes penalties for intentionally gaining access to a protected computer without authorization, or exceeding authorized access to a protected computer by causing a computer program or code to be copied onto the computer, and: (1) intentionally using that program or code in furtherance of another federal criminal offense; or (2) intentionally impairing the security protection of the computer. Exempts people who solely provide: (1) a transmission or routing function through which software is delivered to a protected computer for installation; (2) the storage or hosting of software or a website through which software is made available for installation to a protected computer; or (3) an information location tool through which a user locates software available for installation. Exempts a provider of a network or online service that an authorized user uses or subscribes to for 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.

Title II: Increase in Certain Penalties - (Sec. 201) Increases civil penalties for violations involving an unfair or deceptive act or practice in a national emergency period or disaster period, or relating to an international disaster, if the act or practice exploits popular reaction to the emergency or disaster.

Actions Timeline

- **Jun 12, 2006:** Committee on Commerce, Science, and Transportation. Reported by Senator Stevens with an amendment in the nature of a substitute. With written report No. 109-262.
- **Jun 12, 2006:** Committee on Commerce, Science, and Transportation. Reported by Senator Stevens with an amendment in the nature of a substitute. With written report No. 109-262.
- **Jun 12, 2006:** Placed on Senate Legislative Calendar under General Orders. Calendar No. 467.
- **Nov 17, 2005:** Committee on Commerce, Science, and Transportation. Ordered to be reported with an amendment in the nature of a substitute favorably.
- **Mar 20, 2005:** Introduced in Senate
- **Mar 20, 2005:** Sponsor introductory remarks on measure. (CR S3105-3106)
- **Mar 20, 2005:** Read twice and referred to the Committee on Commerce, Science, and Transportation. (text of measure as introduced: CR S3106-3109)