Calendar No. 811

108TH CONGRESS *2d Session*	SENATE	REPORT 108–424

THE SPY BLOCK ACT

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 2145

DECEMBER 7, 2004.—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE

39–010 WASHINGTON : 2004

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JOHN MCCAIN, Arizona, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina
CONRAD BURNS, Montana	DANIEL K. INOUYE, Hawaii
TRENT LOTT, Mississippi	JOHN D. ROCKEFELLER IV, West Virginia
KAY BAILEY HUTCHISON, Texas	JOHN F. KERRY, Massachusetts
OLYMPIA J. SNOWE, Maine	JOHN B. BREAUX, Louisiana
SAM BROWNBACK, Kansas	BYRON L. DORGAN, North Dakota
GORDON SMITH, Oregon	RON WYDEN, Oregon
PETER G. FITZGERALD, Illinois	BARBARA BOXER, California
JOHN ENSIGN, Nevada	BILL NELSON, Florida
GEORGE ALLEN, Virginia	MARIA CANTWELL, Washington
JOHN E. SUNUNU, New Hampshire	FRANK LAUTENBERG, New Jersey

JEANNE BUMPUS, *Staff Director and General Counsel*
ROB FREEMAN, *Deputy Staff Director*
SAMUEL WHITEHORN, *Democratic Staff Director and Chief Counsel*
MARGARET SPRING, *Democratic Senior Counsel*

Calendar No. 811

108TH CONGRESS *2d Session* | SENATE | REPORT 108–424

THE SPY BLOCK ACT

DECEMBER 7, 2004.—Ordered to be printed

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

REPORT

[To accompany S. 2145]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 2145) 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 deceptive software and online practices that may result in spyware or other unwanted software being placed on consumers' computers. Specifically, the legislation would prohibit (1) deceptive software installation and removal practices; (2) software that collects information about consumers or their computer usage and transmits it to others automatically without consent or notice of such features to consumers prior to the collection of the information; (3) software delivering advertisements on consumers' computers without identifying itself as the source of the ads; and (4) various other practices that may frustrate a consumer's control of his or her computer.

BACKGROUND AND NEEDS

The term "spyware" commonly refers to software that secretly monitors a computer user's activities, or collects his or her personal information, and shares it with others via the Internet without that user's knowledge or consent. Spyware may be downloaded onto

a consumer's computer in several different forms: as self-executing programs contained in unsolicited e-mail messages (spam); as advertisement-serving software (adware); as keystroke-logging software (key-loggers); or as what appears to be a harmless program or data file a user downloads from a website or obtains through a file-sharing program that actually contains malicious, self-executing software code much like a virus (Trojan horses).[1] Spyware may be used for many criminal, deceptive, and privacy-intrusive purposes, including: to record a user's keystroke data and transmit to others his or her captured log-in account names, passwords and e-mail addresses; to steal a user's financial and other personally identifiable information (PII); to barrage users with pop-up advertisements; to change a computer's dial-up connection to dial a "900 number" pay-per-minute call instead of the user's Internet service provider; and to redirect browser home pages to promotional or pornographic sites. According to a 2004 online safety study of home computer users conducted jointly by the National Cyber Security Alliance and America Online, Inc., eighty percent of those surveyed had spyware or adware programs on their home computer.[2]

As further discussed below, the legislation addresses deceptive practices and information collection with respect to two types of software: "spyware" and "adware".

SPYWARE

The term spyware could be applied to software that does any number of monitoring activities without a consumer's knowledge or consent. However, most proponents of spyware legislation agree that certain practices are clearly anti-consumer practices that should be either prohibited because of privacy concerns (i.e., spyware) or regulated for other consumer protection purposes (i.e., deceptive trade practices). Taken together, these illegal or, at the very least, unacceptable practices typically are based on three types of problems: (1) threats to the privacy and security of a user's computer without his or her knowledge or consent; (2) the transparency of the process used in distributing the programs, including downloading and installing software on a consumer's computer; and (3) the availability of easy-to-understand user controls to remove any unwanted software. For example, most distributors of legitimate software would agree that the following practices should be, or are already, prohibited by law: reconfiguring a consumer's operating system or other software on the computer without the consumer's knowledge or consent; installing software on a consumer's computer without permission, through deceptive means, or by coercion; and preventing a consumer—by either software design or by artificially creating an unnecessarily complicated procedure—from easily removing unwanted software from his or her computer.

In the prototypical case of spyware, a computer user is unaware that a software program has been installed on his or her computer, and if the user does becomes aware of it, he or she often has a dif-

[1] Internet industry experts differ in how they define the term "spyware." For some, the terms "spyware", "adware", "sneakware", and "malware" are all used interchangeably. For others, especially Internet advertising companies, there are significant differences between spyware and adware, which will be further discussed below.

[2] Press Release, National Cyber Security Alliance, October 25, 2004 (see www.staysafeonline.info).

ficult time uninstalling it. In some cases, spyware programs piggyback on other applications or trick users into authorizing their download and installation through deceptive "pop-up" ads. Additionally, some forms of spyware spread themselves by exploiting security vulnerabilities in e-mail attachments or browsers. Most often, consumers unknowingly get spyware on their computer while downloading free applications such as screensavers, games, basic utility programs (e.g., calendars or calculators), or peer-to-peer (P2P) file-sharing programs. Even if some actual notice of the software's purpose is provided at the time of download, it is often buried in the complexities of an End User License Agreement (EULA) that obfuscates the warning. The usual result is that consumers typically do not know that spyware is being downloaded on their computer nor appreciate the level of permission that they are unwittingly giving others to access their computers, obtain their PII, or monitor their Internet browsing habits.

By unintentionally allowing access to their computers, consumers run the risk, among other things, of having their credit card numbers and account passwords stolen, which may ultimately result in the crime of identity theft being perpetrated against them. Additionally, if a consumer gets enough spyware on his or her computer, important resources such as virtual memory and processing power may become over-burdened, hindering the normal operation of the computer and preventing the consumer from doing other tasks. Disturbingly, a consumer in such situations normally experiences increasingly sluggish computer performance, and in some cases inoperability, without any clear indication to him or her of either the nature of the problem, the responsible software, or the solution by which to remedy it.

These performance issues are compounded by the inherent characteristic of most spyware programs to not only be difficult to find, but also difficult to remove. Often a user will not be aware, even after the fact, that spyware has been installed and is running because the software automatically operates in the background. Additionally, most spyware programs will not list themselves in the operating system's installed program list, which is the most common way consumers would find software that they wanted to remove from their computer. Instead, the software code that runs spyware is often intentionally dispersed into many separate file folders throughout the computer, which usually makes it difficult for even professional computer technicians to remove it completely once installed. Some spyware programs also use separate stand-alone features, such as a "tickler", which can reinstall the program after a user has attempted to remove it. Other spyware programs, dubbed "burrower" programs, implant themselves so deeply into a computer's operating system that they cannot be found because they effectively hide behind standard operating system filenames.

ADWARE

One type of software program that some may refer to as spyware is more accurately described as "adware". Adware is software that resides on consumers' computers and serves advertisements to them based upon their Internet browsing habits. The ads are usually displayed in the form of pop-up graphical message boxes (or

"windows") separate from the web browser.[3] Advertising executives typically refer to this more targeted means of advertising as "contextual advertising" because it is based on an individual consumer's preferences derived from the context of the webpages he or she actually views. For example, when a computer user types a search term into a browser or clicks on a link indicating some interest in a type of commercial activity, an adware program will typically cause a pop-up window—containing an advertisement, coupon, or both—to be displayed on the user's screen until he or she either acts on it (i.e., by clicking on a link in the ad) or otherwise closes the pop-up window (if possible). Like telemarketing, this type of advertising and the methods companies employ to deliver it have raised privacy concerns for consumers who do not wish to receive the ads.

Adware is normally bundled with free software that a consumer downloads to his or her computer. Adware distributors often describe the adware as pop-up ad or coupon programs that make the free distribution of the other software economically viable in the first place. Adware company executives also argue that their companies do not distribute "spyware" because they provide consumers with clear and concise notices about the nature of their software and require a consumer's affirmative consent (i.e., opt-in consent) before any adware programs are downloaded or installed. Additionally, some adware companies have provided testimony to the Committee explaining that their programs do not collect PII nor share any information about a user's computer with third parties. Rather, they testified, the ad-serving software resident on a computer is used only to monitor that user's web-browsing patterns in order to request a highly contextual ad to be served to the computer that is targeted to that user's known preferences.[4]

Adware companies maintain that these advertising practices are not only legal and consistent with good software practices, but that they are also consistent with traditional advertising practices in other mediums as well. For example, adware companies point out that this business model of receiving advertisements in return for free content is similar to many other legal, advertising-supported business models such as free over-the-air television supported by TV commercials, free Internet services like online e-mail supported by banner ads, and free Internet access provided by ISPs that serve advertisements through a proprietary browser that the user is required to use to obtain Internet access. In each of these other models, adware companies claim that consumers have no control over the content, frequency, or length of time they are forced to view ads. In addition, they argue that in each of these other models, consumers face a stark choice: either receive the free content with the ads, or not at all. Adware companies therefore defend their model as no different than the others—you may remove the adware, but when you do, the free software with which it was bundled will also be removed. For these reasons, adware companies argue that soft-

[3] These windows may appear on top of the current webpage a user is viewing ("pop-over" ads), or underneath a webpage being viewed so that the user will not see them until they close their browser window ("pop-under" ads).

[4] Additionally, other kinds of advertisement-serving software may operate in real time and have no need to store or transmit PII that might be ephemerally collected in the process of serving an advertisement to a computer.

ware operating as their programs do should not be prohibited or regulated like spyware.

Consumer advocacy groups and privacy experts argue in response, however, that the other forms of advertising are mass market advertising, and traditionally do not involve the collection of PII or the monitoring of users' off-site viewing habits in order to serve ads.[5] Furthermore, these observers argue that adware practices raise privacy concerns that are not raised by traditional one-way, mass market advertising practices, a key difference which justifies closer scrutiny and regulation by the government. Finally, some commercial websites contend that adware programs have enabled their competitors' pop-over ads to be displayed on top of their webpages' content, raising concerns of unfair trade practices, consumer deception, and trademark infringement. Companies concerned about the competitive fairness of contextual advertising claim that customers are being confused by the pop-up ads, and that the adware distributors are unjustly enriching themselves by selling advertising space to companies on their competitors' websites without authorization. Industry observers who support adware-based business models counter that these issues of competitive fairness should be addressed in traditional forums, such as the courts, the Federal Trade Commission and the Department of Justice, and that these developing business models should not be prohibited preemptively by legislation.

CURRENT EFFORTS TO ADDRESS CONSUMER CONCERNS

Anti-spyware Software. In response to the growing proliferation of spyware and adware, manufacturers of privacy and security software are now offering anti-spyware software to consumers. Some of these companies have extensive previous experience creating firewall, anti-virus, or anti-spam software, and have begun including new anti-spyware features in their existing titles as they release the latest versions. Other companies have launched targeted anti-spyware programs specifically designed to address the more complex tasks associated with spyware. These programs may include features such as detecting, removing, and preventing users from unwittingly downloading spyware and other unknown malicious software that may threaten the user's privacy, or the security or operational integrity of the user's computer system.

Operationally, anti-spyware applications act much like anti-virus software in that these programs are only able to find and remove spyware and other programs that have been identified by their programmers. The increasing proliferation of malicious programs, however, creates an overwhelming problem for anti-spyware programmers who have a difficult time keeping up with the onslaught of new variations of spyware. For example, PestPatrol, a leading anti-spyware program, only recognized six types of spyware programs at the beginning of 2003, but within six months the company had identified over forty different types of spyware.[6] These anti-spyware companies are facing an uphill battle very similar to

[5] For example, when browsing a financial website, you may see ads for mortgage loans. However, the financial website typically will not serve you ads for herbal medicines (even if you normally browse medical sites) because the website typically does not track your viewing habits on webpages not hosted by that financial website.

[6] PC Magazine, "Special Report: Spyware and Identity Theft," March 2, 2004.

the one fought by spam-filtering companies in their fight to keep spam out of users' e-mail inboxes. As more investment dollars flow to privacy and security software developers, consumers can expect the release of many more titles of anti-spyware software that employ the latest technological means to combat spyware creators' ever-evolving techniques.

Operating System and Internet Browser Upgrades. Microsoft recently released an operating system upgrade to its popular Windows XP system that contains the code for an enhanced-security Windows Internet browser. This latest release, Service Pack 2 (or SP2), has been widely reported as a significant step in resolving numerous security issues found with previous versions of XP. It is expected that a number of the new features contained in SP2 will alleviate some of the problems experienced by consumers that have been attributable to spyware. In particular, SP2 provides a new firewall program for users. Unlike XP's earlier firewall, this one is automatically enabled as a default and protects every connection on a computer, even if a user already has third-party software firewalls running on the computer. The new system also monitors the activities of all computer programs that are running—if one of them attempts to open up a new channel of communication with the Internet, the user is prompted to first approve the action. This latter feature may help prevent the type of spyware that collects personal information and, unbeknownst to the user, surreptitiously transmits it through an open Internet connection to a destination where it may be stored. In addition to Microsoft's efforts, other developers of operating systems and Internet browsers are working to update their systems to provide better security from all Internet threats including spyware.

Consumer Awareness of Safe Browsing Practices. Many public interest organizations and consumer advocacy groups that monitor Internet practices have begun initiatives to educate consumers about the proliferation and harmfulness of spyware. The Center for Democracy and Technology (CD&T), in particular, released a report in November 2003 entitled *Ghosts in Our Machines: Background and Policy Proposals on the "Spyware" Problem*.[7] Much of the information on the spyware practices reported by CD&T has been previously summarized in the background section above, but the report also provides tips for computer users about what steps they can take today to protect their personal information and programs from spyware. For example, in addition to running spyware detection and removal utilities, CD&T recommends that consumers avoid installing free, ad-supported applications unless they are from a trusted party, particularly if the advertising component is provided by an unknown third party. CD&T also advises consumers to diligently monitor their Internet browsing, being mindful of webpages or pop-up ads with automated download procedures that may start running without their consent or active input. As suggest by the report, Internet users who wish to prevent spyware on their computers should raise the security level of their Internet

[7] Copies of this report may be obtained at http://www.cdt.org/privacy/spyware.

browsers so that automated, self-executing downloads are prohibited.[8]

In addition to consumer advocacy groups, government officials at the Federal Trade Commission and the Organization for Economic Co-operation and Development (OECD) have spearheaded efforts at both organizations to develop a set of understandable Internet security principles that should be publicly promoted and voluntarily adopted in order to keep consumers safe online.[9] The spread of spyware and the proliferation of computer viruses are greatly aided by computer users' lack of awareness of the risks of such harmful programs. Through government and private efforts to strengthen consumer awareness of the potential risks arising from indiscriminately downloading unfamiliar software, the spread of spyware and malicious programs could potentially be reduced.

Software Industry Efforts. One of the concerns raised by business software companies with respect to proposed spyware legislation is that the definition of spyware must be narrowly tailored. If not, they explain, important business software relied on by corporate America will be unintentionally pulled into a web of burdensome regulatory practices that may not only prevent the software's most efficient use, but also limit its future innovation and development. Software industry efforts have therefore focused on identifying a set of industry best practices for the download, installation, and removal of software programs on consumers' computers in order to define legitimate practices that should remain free of regulation. Likewise, the industry's help in identifying "unacceptable" or deliberately criminal or deceptive trade practices will not only aid policymakers, but also will help consumer advocacy groups shape the message to consumers as to the type of suspicious software practices they should be mindful of while using a computer. Many spyware experts suggest that policymakers, consumer groups, and software developers should work cooperatively together to identify areas ripe for legislation, to improve consumer awareness of spyware-related problems, and to encourage safe online browsing and downloading practices.

State Legislation. In 2004, several State legislatures considered, and in some cases passed, spyware legislation to address many of the deceptive practices outlined above. Industry representatives opposed to State legislation have argued that many of these spyware practices already violate existing Federal and State civil laws and regulations governing computer fraud and abuse, electronic privacy, and consumer protection, as well as criminal fraud laws. Industry observers supporting Federal legislation, however, contend that one uniform national law regulating spyware is necessary to preempt States from enacting 50 different laws in the future that may create uncertainty for business models or unintentionally capture legitimate software practices within the scope of their regulations.

---

[8] Using a browser's highest security setting, however, may cause the loss of some functionality, particularly on webpages that contain significant amounts of graphic or video content, or interactive features.

[9] The Federal Trade Commission's "Stay Safe Online" initiative and related resources can be viewed at http://www.ftc.gov/infosecurity.

LEGISLATIVE HISTORY

On February 27, 2004, Senator Burns introduced S. 2145, the "SPY BLOCK Act of 2004," which was referred to the Committee on Commerce, Science, and Transportation for consideration. The bill was originally cosponsored by Senators Wyden and Boxer, and is also cosponsored by Senator Clinton. Additionally, spyware legislation was introduced in the House of Representatives by Rep. Bono on July 25, 2003 (H.R. 2929), and by Rep. Goodlatte on June 23, 2004 (H.R. 4661).

On March 23, 2004, the Committee's Communications Subcommittee held a hearing on S. 2145 at which Subcommittee Chairman Burns presided. Witnesses at the hearing included a diverse group of representatives from a company, an industry association, a public interest group, and a private party, each of whom had expertise on spyware, adware, and other Internet matters raising consumer protection concerns.

On September 22, 2004, the Committee met in open executive session to consider an amendment in the nature of a substitute to S. 2145 offered by Senator Burns that made several substantive changes to the bill's provisions as introduced. Additionally, Senator Allen offered an amendment to add criminal penalties for using unauthorized software installations on a computer to engage in federal criminal activities or impair the computer's security protections. The amendments were adopted by voice vote and 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:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, October 5, 2004.

Hon. JOHN MCCAIN,
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. 2145, the SPY BLOCK Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Susanne S. Mehlman (for federal costs), and Sarah Puro (for the impact on state, local, and tribal governments).

Sincerely,

ELIZABETH ROBINSON,
(For Douglas Holtz-Eakin, Director).

Enclosure.

S. 2145—SPY BLOCK Act

Summary: S. 2145 would prohibit the use of computer software (known as spyware) to collect personal information and to monitor the behavior of computer users without permission. Enacting S. 2145 could affect direct spending and receipts because those indi-

viduals who violate the provisions under this legislation could be subject to civil and criminal penalties. Based on information provided by the Federal Trade Commission (FTC), CBO estimates that implementing S. 2145 would not have a significant effect on revenues, direct spending, or spending subject to appropriation.

S. 2145 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 ($60 million in 2004, adjusted annually for inflation).

The bill would impose mandates on the private sector. CBO's analysis of the cost of those mandates will be provided later in a separate report.

Estimated cost to the Federal Government: Enacting S. 2145 could increase federal direct spending and revenues from the criminal and civil penalties assessed for violations under the bill's provisions, but CBO estimates that any new collections and subsequent spending would be less than $500,000 a year.

Implementing the bill also could increase spending by the FTC and other federal agencies for law enforcement, subject to the availability of appropriated funds. However, due to the relatively small number of cases likely to be involved, CBO expects that any such increase would be insignificant.

Estimated impact on state, local, and tribal governments: Section 8 would require the Attorney General of a state who files a civil suit against a person engaging in activities prohibited by this bill 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 9(b) would preempt state laws that prohibit the use of certain types of computer software and would establish penalties for violators. Section 1030A would prohibit states from creating civil penalties that specifically reference the provisions of this bill. Those preemptions and prohibitions are mandates as defined in UMRA but would specifically preserve state authority to pursue fraud, trespass, contract, and tort cases under state law. They also would not prohibit states from enacting similar criminal and civil statutes.

CBO estimates that any costs to state, local, or tribal governments would be insignificant and would fall significantly below the threshold established in UMRA ($60 million in 2004, adjusted annually for inflation).

Estimated impact on the private sector: The bill would impose mandates on the private sector. CBO's analysis of the cost of those mandates will be provided later in a separate report.

Previous CBO estimates: On July 8, 2004, CBO transmitted a cost estimate for H.R. 2929, the Securely Protect Yourself Against Cyber Trespass Act, as ordered reported by the House Committee on Energy and Commerce on June 24, 2004. In addition, on September 28, 2004, CBO transmitted a cost estimate for H.R. 4661, the Internet Spyware (I–SPY) Prevention Act of 2004, as ordered reported by the House Committee on the Judiciary on September 8, 2004. All three pieces of legislation are similar, although H.R. 4661 would authorize the appropriation of funds to enforce its pro-

visions. The intergovernmental mandates in S. 2145 also were contained in H.R. 2929 and H.R. 4661.

Estimate prepared by: Federal Costs: Susanne S. Mehlman. Impact on State, Local, and Tribal Governments: Sarah Puro.

Estimate approved by: Robert A. Sunshine, 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. 2145 would establish Federal regulations for certain practices that may result in spyware or other unwanted software being placed on consumers' computers without their consent. The bill would therefore cover every person or entity that causes the installation of software or the delivery of advertisements in a proscribed manner on consumers' computers, subject to certain limitations set forth in the legislation.

ECONOMIC IMPACT

S. 2145 would require software distributors, websites, Internet service providers, and other online entities involved in the distribution, download, installation, operation, or removal of software, or in the delivery of advertisements in a certain manner, to comply with notice, consent, and removal requirements when causing the installation of software or delivery of advertisements in such manner on consumers' computers. Although such entities may already voluntarily provide notice, consent, and other protections for consumers, the legislation could nonetheless create compliance costs on such providers in the form of equipment 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 and the software distribution or online advertising industries in general, and the costs may be passed on to Internet users through increased costs of software, Internet access, website premium fees, or other charges.

PRIVACY

S. 2145 would likely increase consumer privacy by imposing limitations on the installation of software that may collect and transmit information about a user, a user's web-browsing habits, or other use of a computer without the user's consent or prior notice. Such restrictions should result in a reduced likelihood of Internet users having unwanted software installed on their computer and personal information shared without their consent. In this regard, the legislation is similar to online privacy legislation which the Committee has previously considered.

PAPERWORK

S. 2145 is expected to have minimal or no impact on current paperwork levels.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

Section 1 would set forth the short title of the legislation as the "Software Principles Yielding Better Levels of Consumer Knowledge Act" or the "SPY BLOCK Act".

Section 2. Prohibited practices in relation to software installation in general

Section 2 would prohibit certain installation and removal practices for computer software. Subsection (a) would prohibit the surreptitious installation of software by persons other than the authorized user of a computer. For purposes of this subsection, surreptitious installation would mean the installation of software in a manner that is designed either to conceal from the computer user the fact that the software is being installed or to prevent the user from having an opportunity to knowingly grant or withhold his or her consent to the installation.

Subsection (b) would prohibit third parties wishing to install software on users' computers from using misleading inducements to achieve that result. For purposes of this subsection, misleading inducements to install would be inducing an authorized user of a computer to consent to the installation of software by making false representations about any of the following: the identity of an operator of an Internet website or online service at which the software is made available for download from the Internet; the identity of the author or publisher of the software; the nature or function of the software; or the consequences of not installing the software.

Subsection (c) would prohibit the installation of software on a computer if such software could not be uninstalled or disabled by the reasonable efforts of the user. This prohibition would not, however, require that individual features or functions of a software program, updates to a previously installed software program, or software programs that were installed on a bundled basis be separately capable of being uninstalled or disabled on an individual basis.

Section 3. Installing surreptitious information collection features on a user's computer

Section 3 would prohibit software having surreptitious information collection features from being installed on a user's computer without first informing and obtaining the consent of the user.

Specifically, this section would prohibit a person who is not an authorized user of a computer to cause the installation of software on that computer that collects and transmits information about an authorized user of the computer, or an authorized user's Internet browsing behavior or other use of the computer, to any other person, on an automatic basis or at the direction of a person other than the authorized user of the computer, if—

(1) the software's collection and transmission of such information is not functionally related to or in support of a software capability or function that an authorized user of the computer has chosen or consented to execute or enable, and

(2) either—

(A) there has been no notification to an authorized user of the computer, prior to the collection of such information, explaining the type or manner of information collection, or

(B) if notice has been provided—

(i) it was not provided in a manner reasonably calculated to provide actual notice to an authorized user of the computer, or

(ii) it occurred at a time or in a manner that did not enable an authorized user of the computer to consider the information contained in the notification before choosing whether to permit the collection or transmission of information.

This section also provides an exception to these requirements for software that is reasonably necessary to determine whether a user of a computer is licensed or authorized to use the software.

Section 4. Adware that conceals its operation

Section 4 would prohibit adware that conceals its operation by delivering ads to a computer at a time or in a manner such that a reasonable user of the computer may not understand that the software is responsible for delivering the advertisements, and the ads do not contain a label or other reasonable means of identifying which software is responsible for its delivery.

Section 5. Other practices that thwart user control of computer

Section 5 would prohibit certain practices that thwart user control of a computer. Under the provisions of this section, it would be unlawful for any person who is not the authorized user of a computer knowingly and without authorization—

- to utilize the computer to send unsolicited information or material from the computer to other computers;
- to divert the Internet browser of the computer away from the website the user intended to view to one or more other websites, unless such diversion has been authorized by the website the user intended to view;
- to display an advertisement, series of advertisements, or other content through windows in the computer's Internet browser in such a manner that the user of the computer cannot end the display of such advertisements or content without turning off the computer or closing the Internet browser;
- to covertly modify settings relating to the use of the computer or to the computer's access to or use of the Internet, including—
  - altering the default webpage that initially appears when a user of the computer launches an Internet browser;
  - altering the default provider or web proxy used to access or search the Internet;
  - altering bookmarks used to store favorite Internet website addresses; or
  - altering settings relating to security measures that protect the computer and the information stored on the computer against unauthorized access or use;

• to use software installed in violation of section 3 to collect information about the user or the user's Internet browsing behavior; or

• to remove, disable, or render inoperative a security or privacy protection technology installed on the computer.

Section 6. Limitations on liability

Section 6 would limit the liability of any person who may inadvertently provide services, such as Internet access or web hosting services, over which prohibited software practices are conducted without their active participation in such practices. Under this section, a person would not be liable for violations of the Act solely because the person provided the Internet connection, telephone connection, or other transmission or routing function through which software was delivered to a protected computer for installation. Additionally, a person would not be liable for violations of the Act solely for providing storage for software or for hosting an Internet website through which such software was made available for installation to a computer. Finally, a person would not be liable for violations of the Act solely for providing an information location tool (i.e., a directory, index, reference, pointer, or hypertext link) through which a user of a protected computer located software available for installation.

This section would also ensure that providers of a network or online service shall not be deemed to have violated sections 3 or 5 of the Act for any installation, monitoring or use of software for the purposes of (1) protecting the security of the network, service, or computer, (2) facilitating diagnostics, technical support, maintenance, network management, or repair of the network or services, or (3) preventing or detecting unauthorized, fraudulent, or otherwise unlawful uses of the network or service.

Section 7. Administration and enforcement

Section 7 would provide that the Act be enforced by the Federal Trade Commission (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 FTC Act (15 U.S.C. 57a(a)(1)(B)). The FTC would be required to prevent persons from violating this legislation in the same manner, by the same means, and with the same jurisdiction, powers, and duties as though all applicable terms and provisions of the FTC Act were incorporated and made a part of this legislation.

This section would also 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 8. Actions by States

Section 8 would grant State attorneys general the right to bring a civil action for violations of the Act. 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

damage, 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, this section 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 rights to be heard with respect to any matter that arises in that action and to file a petition for appeal.

Section 9. Effect on other laws

Section 9 would clarify the effect the legislation would have on current Federal and State law. This section would set forth 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.

Additionally, this section would provide a general rule preempting any State statute, regulation, or rule that expressly limits or restricts the installation or use of software (1) to collect information about the user of the computer, or the user's Internet browsing behavior or other use of the computer, or (2) to cause advertisements to be delivered to the user of the computer. Exceptions to this general rule of preemption would be provided for State laws that prohibit deception in connection with the installation or use of such software and any other State laws not specific to software, including State trespass, contract, tort, or anti-fraud law.

Section 10. Penalties for certain unauthorized activities relating to computers

Section 10 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 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 in furtherance of another federal criminal offense. Such conduct would be punishable by fine or imprisonment for up to 5 years. 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 2 years.

Section 10 would also provide the same limitations on liability for purposes of this section's provisions that are provided under section 6 for purposes of the bill's civil provisions. Specifically, under these limitations on liability, providers of certain services, such as Internet access, website hosting, website indexing, or network monitoring services, would not be criminally liable under this section solely for providing those services through which software may be used in violation of this section. This section would also

prohibit the bringing of State civil actions under the law of any State where the action is premised in whole or in part on the defendant's violating this section. For purposes of this section, then term "State" would include the District of Columbia, Puerto Rico, and any other territory or possession of the United States.

Section 11. Definitions

Section 11 would define 10 terms used throughout the Act. The following definitions included in the Act are of particular importance to understanding the legislation and the explanation of the Act's provisions provided in this section-by-section analysis:

Software. The term "software" would mean any program designed to cause a computer to perform a desired function or functions. Such term would not include a cookie, as defined in this section.

Cookie. The term "cookie" would mean a text file that is placed on a computer by an ISP, an interactive computer service, or Internet website, the sole function of which is to record information that can be read or recognized when the user of the computer subsequently accesses particular websites or online locations or services.

Install. The term "install" would mean to write computer software to a computer's persistent storage medium, such as the computer's hard disk, in such a way that the computer software is retained on the computer after the computer is turned off and subsequently restarted. The term "install" would also mean to write computer software to a computer's temporary memory, such as random access memory, in such a way that the software is retained and continues to operate after the user of the computer turns off or exits the Internet service, interactive computer service, or Internet website from which the computer software was obtained.

Cause the installation. The term "cause the installation" would mean to knowingly provide the technical means by which the software is installed, or to knowingly induce or pay or provide other consideration to another person to do so.

Section 12. Effective date

Section 12 would provide that the provisions of this legislation would take effect 180 days after the date of enactment.

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):

TITLE 18, UNITED STATES CODE

PART I. CRIMES

CHAPTER 47. FRAUD AND FALSE STATEMENTS

* * * * * * *

§ 1030A Illicit indirect use of protected computers

(a) 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 5 years, or both.

(b) 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 protected computer shall be fined under this title or imprisoned not more than 2 years, or both.

(c) 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) 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 of, 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) No person may bring a civil action under the law of any State if such action is premised in whole or in part upon the defendant's violating this section. For the purposes of this subsection, the term 'State' includes the District of Columbia, Puerto Rico, and any other territory or possession of the United States.

○