

INTERNET SPYWARE (I-SPY) PREVENTION ACT OF 2004

SEPTEMBER 23, 2004.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. SENSENBRENNER, from the Committee on the Judiciary,  
submitted the following

R E P O R T

[To accompany H.R. 4661]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 4661) to amend title 18, United States Code, to discourage spyware, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

	Page
The Amendment .....	1
Purpose and Summary .....	3
Background and Need for the Legislation .....	3
Hearings .....	8
Committee Consideration .....	8
Vote of the Committee .....	8
Committee Oversight Findings .....	8
New Budget Authority and Tax Expenditures .....	8
Congressional Budget Office Cost Estimate .....	9
Performance Goals and Objectives .....	10
Constitutional Authority Statement .....	10
Section-by-Section Analysis and Discussion .....	11
Changes in Existing Law Made by the Bill, as Reported .....	12
Markup Transcript .....	14

THE AMENDMENT

The amendment is as follows:  
Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the “Internet Spyware (I-SPY) Prevention Act of 2004”.

**SEC. 2. PENALTIES FOR CERTAIN UNAUTHORIZED ACTIVITIES RELATING TO COMPUTERS.**

(a) **IN GENERAL.**—Chapter 47 of title 18, United States Code, is amended by inserting after section 1030 the following:

**“§ 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 not more than 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—

“(1) intentionally obtains, or transmits to another, personal information with the intent to defraud or injure a person or cause damage to a protected computer; or

“(2) 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) 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.

“(d) As used in this section—

“(1) the terms ‘protected computer’ and ‘exceeds authorized access’ have, respectively, the meanings given those terms in section 1030; and

“(2) the term ‘personal information’ means—

“(A) a first and last name;

“(B) a home or other physical address, including street name;

“(C) an electronic mail address;

“(D) a telephone number;

“(E) a Social Security number, tax identification number, drivers licence number, passport number, or any other government-issued identification number; or

“(F) a credit card or bank account number or any password or access code associated with a credit card or bank account.”.

(b) **CONFORMING AMENDMENT.**—The table of sections at the beginning of chapter 47 of title 18, United States Code, is amended by inserting after the item relating to section 1030 the following new item:

“1030A. Illicit indirect use of protected computers.”.

**SEC. 3. AUTHORIZATION OF APPROPRIATIONS.**

In addition to any other sums otherwise authorized to be appropriated for this purpose, there are authorized to be appropriated for each of fiscal years 2005 through 2008, the sum of \$10,000,000 to the Attorney General for prosecutions needed to discourage the use of spyware and the practice commonly called phishing.

**SEC. 4. FINDINGS AND SENSE OF CONGRESS CONCERNING THE ENFORCEMENT OF CERTAIN CYBERCRIMES.**

(a) **FINDINGS.**—Congress makes the following findings:

(1) Software and electronic communications are increasingly being used by criminals to invade individuals’ and businesses’ computers without authorization.

(2) Two particularly egregious types of such schemes are the use of spyware and phishing scams.

(3) These schemes are often used to obtain personal information, such as bank account and credit card numbers, which can then be used as a means to commit other types of theft.

(4) In addition to the devastating damage that these heinous activities can inflict on individuals and businesses, they also undermine the confidence that citizens have in using the Internet.

(b) **SENSE OF CONGRESS.**—Because of the serious nature of these offenses, and the Internet’s unique importance in the daily lives of citizens and in interstate commerce, it is the sense of Congress that the Department of Justice should use the amendments made by this Act, and all other available tools, vigorously to prosecute those who use spyware to commit crimes and those that conduct phishing scams.

## PURPOSE AND SUMMARY

H.R. 4661, the “Internet Spyware (I-SPY) Prevention Act of 2004,” enhances existing fraud and computer crime law with strong criminal penalties targeting egregious abuses perpetrated Internet users by persons who maliciously employ various covert software applications, programs, applets, or computer code commonly known as “spyware.” H.R. 4661, as amended, also provides resources and guidance to the Department of Justice for the dedicated prosecution of these offenses as well as fraudulent online identity theft (“phishing”) offenses and similar computer crimes.

## BACKGROUND AND NEED FOR THE LEGISLATION

## THE INTERNET—OPPORTUNITY AND PERIL

In little more than a decade, the Internet has grown from an obscure academic research tool into a digital medium of unprecedented scope accessed by computers and people around the world. The explosive growth of the Internet in terms of usage and utility has been facilitated by technologies designed to enhance the speed and efficiency of data transfer. Technologies that recognize return visitors to websites, store information on the consumer preferences of Internet users, and the development of software that permits the secure transmission of personal data have produced a degree of personalization that has enhanced consumer options and the overall potential of the Internet. At the same time, software innovations that have enhanced and personalized usage of the Internet have also given rise to software that presents opportunities for abuse and illegal behavior.

“SPYWARE” AND “PHISHING”—NEW PHENOMENA,  
PERVASIVE PROBLEMS*Spyware*

The Federal Trade Commission (“FTC”) loosely defines “spyware” as software that “aids in gathering information about a person or organization without their knowledge and which may send such information to another entity without the consumer’s consent, or asserts control over a computer without the consumer’s knowledge.”<sup>1</sup> In March 2004, testimony before the Senate Commerce Committee, Jerry Berman, President of the Center for Democracy and Technology, stated that spyware refers to “software ranging from ‘key-stroke loggers’ that capture every key typed on a particular computer; to advertising applications that track users’ web browsing; to programs that hijack users’ system settings.” He noted that what these various types of software programs “have in common is a lack of transparency and an absence of respect for users’ ability to control their own computers and Internet connections.”

Examples of spyware include software that collects information about the use of the computer on which the software is installed. Some products may collect personally identifiable information (“PII”). When the computer is connected to the Internet, the software periodically relays the information back to the software manufacturer, a marketing company, or a more nefarious third party.

<sup>1</sup> See <http://www.ftc.gov/bcp/workshops/spyware/>.

Another form of spyware commonly called “adware” traces a user’s Web activity and causes advertisements to suddenly appear on the user’s monitor—called “pop-up” ads—in response. Software programs that include spyware functionality may be pre-installed on a new computer, can be sold or provided for free on a disk (or other media), or downloaded from the Internet, often without the knowledge of the Internet user. The greatest security and privacy challenges posed by spyware relate to technologies that are specifically intended to capture a user’s personal information or take control of his computer for the spyware purveyor’s purposes without the knowledge or consent of the user. These include keystroke logging programs that capture a user’s passwords, Social Security, or account numbers. This information can then be captured and redirected for criminal purposes including fraud, larceny, identity theft, or other cybercrimes. Perhaps even worse is the use of spyware that allows computer hackers to hijack a user’s computer and turn it to their own purposes rendering the computer a “zombie” capable of being directed remotely to send spam, viruses, help hack other computers, or allow others access to engage in copyright piracy.

According to the FTC, a survey of broadband users released last summer by the National CyberSecurity Alliance found that over 90% of consumers had some form of spyware on their computers, and most consumers were not aware of it. Spyware presents privacy, security, and functionality concerns for both Internet users and legitimate commercial activity on the Internet. It has created opportunities for illegal behavior that is often difficult to detect and even more difficult to prosecute under existing law. In addition, the proliferation of spyware threatens to undermine consumer confidence in the integrity and security of the Internet and stifle the enormous commercial and communications potential of the information superhighway.

### *Phishing*

“Phishing” is a general term for using what appear to be either the websites of, or e-mails that appear to be sent from, well known legitimate businesses to deceive Internet users into revealing personal information that can be used to defraud those same users. The Committee notes that in some respects, phishing is only distinguished from traditional identity theft and fraud because it involves employing the Internet as a means to obtain the wanted information. But the schemes themselves, and the uses of the information by the criminals who obtain it are not unique to the Internet, and almost all are illegal under existing Federal criminal laws dealing with wire fraud. According to a recent Department of Justice special report on “phishing”<sup>2</sup>:

- During 2003 and early 2004, law enforcement authorities, businesses, and Internet users have seen a significant increase in the use of “phishing”;
- Criminals create and use such e-mails and websites to deceive Internet users into disclosing their bank and financial account information or other personal data like usernames and passwords;

<sup>2</sup> See <http://www.usdoj.gov/criminal/fraud/Phishing.pdf>

- The “phishers” then take that information and use it for criminal purposes, like identity theft and fraud. A growing number of phishing schemes exploit for illegal purposes the names and logos of legitimate financial institutions, businesses, and government agencies in North America, Europe, and the Asia-Pacific region;
- One industry organization, the Anti-Phishing Working Group ([www.antiphishing.org](http://www.antiphishing.org)) has reported that in January 2004, there were 176 unique phishing attacks reported to it—an increase of more than 50 percent over the number of reported phishing attacks in December 2003.

#### NO EASY SOLUTIONS BUT MANY ANSWERS

##### *General Challenges*

The Committee notes that one difficulty in solving the problems of both spyware and phishing is that average computer users are not aware of the steps they can take to protect themselves from both. Most computer users today have access to security features that are either part of their operating system or web browser or that can be obtained through additional software available at little or no cost, features which can stop most spyware from ever being installed on a user’s computer. Unfortunately, many computer users fail to take advantage of these features, such as firewalls, anti-spyware programs, cookie-blockers, etc. or use them properly. Likewise, most phishing scams require the willing participation of the recipient to either visit a website or reply to an email and give out personal information. As in earlier forms of fraud using the mail or telephones, common sense and a healthy level of suspicion go a long way toward not becoming a victim of phishing. Users can protect themselves against many phishing predators by exercising heightened scrutiny and undertaking verification measures whenever they are asked for passwords, credit card numbers, banking information, or other personal information by someone online. To the extent that spyware, phishing, hacking, and spam now sometimes intersect in attacks on computers, the proper use of a firewall, anti-virus software, and various means of blocking unsolicited email can address these other attendant ills and thwart most attacks. There is no silver bullet to end spyware or phishing but greater consumer awareness and use of available technological countermeasures clearly hold the greatest promise for curbing these abusive practices.

A second major difficulty in solving both spyware and phishing is that many of those who are the beneficiaries of information gleaned from these practices are difficult to track and locate, and the most egregious abusers are seldom legitimate businesses or individuals who might be responsive to government regulation or civil penalties. Annoying but less harmful forms of spyware, particularly adware, are used by a number of legitimate companies that could be found and could be expected to comply with regulations. However, the worst spyware abuses and the vast majority of phishing would likely be unaffected by government regulation or civil enforcement.

A third difficulty in solving the spyware problem is that many legitimate and beneficial tools for making a user’s computing and

Internet experience more enjoyable are technologically indistinguishable from spyware that is used to harm users and computers. For example, a “cookie” is a small text file typically downloaded when a person visits a website, it stores personal information and information about the user’s preferences to make navigation of the site easier and typically is only accessible and active when the user is visiting that website. Another example of a benevolent cookie would be the “shopping cart” cookie on many retail websites that allows the user to “carry” their purchases through the virtual store and to the virtual checkout. However some cookies that are technologically similar in most respects could be used for less benevolent purposes, such as intentionally targeting the user with ads, or tracking the user’s visits to other websites and communicating this information to the originating website upon a return visit. A cookie could also be used for even more malicious purposes to give a criminal access to personal information that would allow them to defraud or otherwise harm the user. Other programs that make use of “spying” capabilities such as parental monitoring software or technical support system monitoring software are clearly beneficial in the hands of authorized users but if installed on a computer by the wrong hands, could be used maliciously. These similarities in technological terms but differences in use exemplify why it is imperative for consumers, Internet Service Providers (“ISPs”), or lawmakers to deal with the problem of spyware and phishing not as particular technologies but as types of behavior that make use of the Internet and various codes, programs, and software.

#### *Alternative Legislative Approaches to Spyware*

Several other legislative approaches to the problem of spyware have been offered in Congress. These approaches establish new regulatory regimes revolving around notice and consent requirements so that computer users would be notified and could either “opt in” or “opt out” of installing spyware at the time of installation. To varying degrees these approaches attempting to define proper notice and consent would not only proscribe bad spyware behavior but would define in detail the online experience of computer users via regulatory requirements. Certainly the concept of consumer consent is critical, and is implicit in the term “authorized access” contained in H.R. 4661. The Committee is concerned, however, that Congress is ill-suited to fix in place a particular notice and consent regime by statute that would be at best a snap shot in time in the constantly evolving area of how computer users interface with the Internet and software. There is a subjective element in computer user expectations that may not square with a comprehensive one-size-fits-all regulatory regime. What is malicious spyware to one user may be innocuous or marginally beneficial software to another. There is also a real risk that computer users will face so many federally required multiple notices that they will be overwhelmed and ignore them or have their Internet experience degraded. Furthermore, regulatory approaches designed to stop spyware unavoidably sweep legitimate uses of technology into the regulatory regime which must then be carved out via exceptions that often fall short. If the chief rationale for Congressional action on spyware is the harm being done to the expectations and enjoy-

ment of computer users, then the solution must not diminish that experience more than the original problem.

The Committee is also concerned that a notice and consent regulatory approach to spam is unlikely to stop bad actors, but it will likely impose additional costs and burdens on legitimate products and services that consumers depend upon. Moreover, it would impose strict liability on the companies least likely to engage in the worst forms of spyware. Legislation reported by the House Committee on Energy and Commerce exemplifies this concern. It contains no requirement for a showing of materiality or willfulness for the prohibited deceptive practices but contains severe per computer civil fines for violations. The net effect is to expose companies who make a one time mistake to strict liability at potentially bankrupting fine levels. Such a standard is at odds with the spirit of the Judiciary Committee's recent litigation reform efforts aimed at reducing catastrophic liability barriers for American businesses. The civil penalties in the Energy and Commerce reported bill go far beyond those currently available to the FTC, and the fines are oddly capped for a person who engages in a pattern or practice of violations but NOT for a person who does not engage in a pattern of such behavior. Finally, the Committee is concerned that this legislative approach goes beyond spyware and represents a more sweeping regulation of Internet privacy than any effort previously passed by Congress. While Internet privacy legislation may be worthy of consideration, it is inappropriate to cloak such comprehensive legislation as a "spyware bill."

The Committee maintains that the pernicious effects of spyware can be most effectively addressed through defining prohibited behavior rather than regulating how technology is used and accessed by consumers.

#### *Problems under Current Law*

The Committee believes that some current spyware and phishing practices are already illegal under existing Federal criminal law. For instance, it is difficult to construct any phishing scheme hypothetical that would not violate existing Federal wire fraud or identity theft laws. Likewise, some forms of spyware related behavior would violate either §§ 1030 and 1037, of Title 18, United States Code. There may, however, be insufficient emphasis upon and enforcement of such crimes by Federal prosecutors to have the desired deterrent value. The Committee believes that additional guidance to, and resources for, the Department of Justice are necessary to ensure that such spyware and phishing related acts already illegal under existing law (as well as the new provisions of H.R. 4661) are vigorously prosecuted by the Department. Therefore, sections authorizing appropriations and setting forth the sense of Congress on the practice of phishing were included in the legislation and the Committee expects that the Department of Justice will take notice and act accordingly.

The Committee also finds that some spyware related behavior may not be easily prosecuted under existing Federal criminal laws that were not designed to explicitly deal with the relatively new phenomenon of spyware. Therefore the new § 1030A of Title 18 created by H.R. 4661 is intended to provide new tools for prosecutors who may find it difficult to bring some spyware cases under cur-

rent law. Section 1030A should not be read in any way to supersede or displace current §§ 1030 and 1037 of Title 18 nor in any way to limit the ability of prosecutors to continue bringing actions for spyware or phishing related crimes under these or other existing statutes.

#### *Amendment*

The Committee reported version of the bill includes an amendment that added a section authorizing appropriations to the Department of Justice for prosecution of spyware and related computer crimes, and also a section concerning the views of Congress on the practice of deceptive online identity theft commonly known as “phishing.”

Because much spyware and phishing related behavior is already prohibited under Federal law, the Committee believes that narrow legislation such as H.R. 4661 updating necessary criminal law provisions and emphasizing increased enforcement is the correct approach. Because of the attendant harm to the Internet that could result from imposing an overly broad regulatory regime to address problems still in their infancy, the Committee also believes legislation focused on the worst spyware and phishing behaviors is the only course without significant unintended consequences available to Congress at this time.

#### HEARINGS

No hearings were held in the Committee on the Judiciary on H.R. 4661.

#### COMMITTEE CONSIDERATION

On September 8, 2004, the full Committee on the Judiciary met in open session and ordered favorably reported the bill H.R. 4661, with an amendment by a voice vote, a quorum being present.

#### VOTE OF THE COMMITTEE

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee notes that there were no recorded votes during the committee’s consideration of H.R. 4661.

#### COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee reports that the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

#### NEW BUDGET AUTHORITY AND TAX EXPENDITURES

Clause 3(c)(2) of rule XIII of the Rules of the House of Representatives is inapplicable because this legislation does not provide new budgetary authority or increased tax expenditures.



## CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 4661, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,  
CONGRESSIONAL BUDGET OFFICE,  
*Washington, DC, September 17, 2004.*

Hon. F. JAMES SENSENBRENNER, Jr., *Chairman,*  
*Committee on the Judiciary,*  
*House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4661, the Internet Spyware (I-SPY) Prevention Act of 2004.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Melissa E. Zimmerman (for federal costs), who can be reached at 226-2860, and Sarah Puro (for the state and local impact), who can be reached at 225-3220.

Sincerely,

DOUGLAS HOLTZ-EAKIN.

Enclosure

cc: Honorable John Conyers, Jr.  
Ranking Member

*H.R. 4661—Internet Spyware (I-SPY) Prevention Act of 2004.*

## SUMMARY

H.R. 4661 would establish new federal crimes for the use of certain computer software—known as spyware—to collect personal information or to commit a federal criminal offense. The bill would authorize the appropriation of \$40 million over the 2005–2008 period for the Attorney General to prosecute violations of the new law. Assuming appropriation of the authorized amounts, CBO estimates that implementing the bill would cost \$9 million in 2005 and \$40 million over the 2005–2009 period. CBO expects that enacting the bill would have an insignificant effect on federal revenues and direct spending.

H.R. 4661 contains an intergovernmental mandate 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 contains no new private-sector mandates as defined in UMRA.

## ESTIMATED COST TO THE FEDERAL GOVERNMENT

The estimated budgetary impact of H.R. 4661 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

	2005	2006	2007	2008	2009
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Authorization Level	10	10	10	10	0
Estimated Outlays	9	10	10	10	1

For this estimate, CBO assumes the bill will be enacted this fall and that the authorized amounts will be appropriated each year.

Enacting H.R. 4661 could increase federal revenues and direct spending as a result of additional criminal penalties assessed for violations of law relating to spyware. Collections of criminal penalties are recorded in the budget as revenues, deposited in the Crime Victims Fund, and later spent. CBO estimates, however, that any additional revenues and direct spending that would result from enacting the bill would not be significant because of the relatively small number of cases likely to be involved.

#### ESTIMATED IMPACT ON STATE, LOCAL, AND TRIBAL GOVERNMENTS

Section 1030A (c) of H.R. 4661 would prohibit states from creating civil penalties that specifically reference the statute. This prohibition would constitute a mandate as defined in UMRA, but it is narrow and would not prohibit states from passing similar criminal and civil statutes. Therefore, CBO estimates that any costs to state, local, or tribal governments would be minimal and would fall significantly below the threshold established in UMRA (\$60 million in 2004, adjusted annually for inflation).

#### ESTIMATED IMPACT ON THE PRIVATE SECTOR

H.R. 4661 contains no new private-sector mandates as defined in UMRA.

#### ESTIMATE PREPARED BY:

Federal Costs: Melissa E. Zimmerman (226–2860)

Impact on State, Local, and Tribal Governments: Sarah Puro (225–3220)

Impact on the Private Sector: Paige Piper/Bach (226–2940)

#### ESTIMATE APPROVED BY:

Peter H. Fontaine

Deputy Assistant Director for Budget Analysis

#### PERFORMANCE GOALS AND OBJECTIVES

The Committee states that pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, H.R. 4661 will deter criminal use of spyware and phishing against American computer users, punish criminals who engage in such conduct, and provide additional tools and resources to prosecutors.

#### CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representative Committee finds the authority for this legislation in article I, § 8 of the Constitution.

## SECTION-BY-SECTION ANALYSIS AND DISCUSSION

The following discussion describes the bill as reported by the Committee.

*Section 1—Short Title*

Section 1 provides that the Act may be cited as the “Internet Spyware (I-SPY) Prevention Act of 2004.”

*Section 2—Penalties for Certain Unauthorized Activities Relating to Computers*

Section 2 provides new criminal offenses and penalties for certain types of spyware activity that constitutes an intentional illicit indirect use of a protected computer. Section 2 does this by adding a new § 1030A to Title 18, of the U.S. Code.

Subsection 2(a) amends Chapter 47 of Title 18 United States Code by inserting after § 1030 the following new section:

§ 1030A Illicit indirect use of protected computers

New § 1030A makes it a crime to intentionally access a protected computer without authorization or exceed authorized access by causing a computer program or code to be copied on to the protected computer.

(a) New § 1030A(a) provides that anyone who uses that program or code in furtherance of another Federal criminal offense shall be fined under this title or imprisoned for up to 5 years, or both

(b) New § 1030A(b) provides fines under this title or imprisonment up to 2 years or both for anyone who by means of that program or code—

(1) intentionally obtains, or transmits to another, personal information with the intent to defraud or injure a person or cause damage to a protected computer; or

(2) intentionally impairs the security protection of the protected computer;

(c) New subsection 1030A(c) added to Title 18 by the bill, clarifies that the preceding provisions are intended only to create a new Federal criminal cause of action as an additional tool to be used by prosecutors combating the worst types of spyware. Because some states generally allow for civil tort actions premised on a violation of Federal criminal statutes, the Committee believes the language of § 1030A(c) is necessary. The Committee does not intend this legislation to create new state civil causes of action merely by passage of this new Federal criminal law, nor is the legislation intended to preempt existing or future state laws that may prohibit conduct similar or identical to the conduct prohibited in new § 1030A. The plain meaning of the bill language should be clear on its face since the text of § 1030A(c) reads: “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.” This text specifically does not use typical language for broader preemption that might read: “. . . if such action is premised ON THE DEFENDANT’S

ENGAGING IN CONDUCT THAT WOULD VIOLATE THIS SECTION.” The language of this subsection therefore should not be interpreted to prevent a state from later passing anti-spyware legislation that mirrors this Federal statute providing it did not use violation of the Federal statute as a predicate for recovery. Likewise, it follows that this subsection could not be interpreted to affect any existing state law that prohibits similar or identical conduct because such a law would not reference or be predicated upon the more recently enacted provisions of this legislation.

(d) New § 1030A(d) provides definitions of terms used in this section, including:

(1) “protected computer” and “exceeds authorized access” have the meanings given to those terms in § 1030 of Title 18.

(2) the term “personal information” means: (A) a first and last name; (B) a home or other physical address, including street name; (C) an electronic mail address; (D) a telephone number; (E) a Social Security number, tax ID number, driver’s license number, passport number, or any other government issued identification number; or (F) a credit card or bank account number or any password or access code associated with a credit card number or bank account.

Section 2(b) makes a conforming amendment to the table of sections at the beginning of Title 18.

#### *Section 3—Authorization of Appropriations*

Section 3 authorizes appropriations to the Department of Justice for fiscal years FY 2005-FY 2008 of \$10 million per fiscal year for dedicated prosecutions needed to discourage the use of spyware and the practice commonly called “phishing.” This sum authorized is in addition to any sums otherwise authorized to be appropriated for this purpose.

#### *Section 4—Findings and Sense of Congress Concerning the Enforcement of Certain Cybercrimes*

(a) FINDINGS—Subsection 4(a) sets forth findings on the impact of cybercrimes involving spyware and “phishing” and the effects of such crimes on the confidence of Internet users.

(b) SENSE OF CONGRESS—Subsection 4(b) offers guidance to the Department of Justice by setting forth Congress’s view of the gravity of these crimes and their effects, and declares that it is the sense of Congress that the Department of Justice use the amendments made by this Act and all other available tools to vigorously prosecute those who utilize spyware or phishing software to engage in criminal activity.

#### CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italics)

and 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

Sec.  
1001. Statements or entries generally.

\* \* \* \* \*

1030A. *Illicit indirect use of protected computers.*

\* \* \* \* \*

#### **§ 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 not more than 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—*

*(1) intentionally obtains, or transmits to another, personal information with the intent to defraud or injure a person or cause damage to a protected computer; or*

*(2) 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) *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.*

(d) *As used in this section—*

*(1) the terms "protected computer" and "exceeds authorized access" have, respectively, the meanings given those terms in section 1030; and*

*(2) the term "personal information" means—*

*(A) a first and last name;*

*(B) a home or other physical address, including street name;*

*(C) an electronic mail address;*

*(D) a telephone number;*

*(E) a Social Security number, tax identification number, drivers licence number, passport number, or any other government-issued identification number; or*

*(F) a credit card or bank account number or any password or access code associated with a credit card or bank account.*

\* \* \* \* \*

MARKUP TRANSCRIPT

**BUSINESS MEETING**

**WEDNESDAY, SEPTEMBER 8, 2004**

HOUSE OF REPRESENTATIVES,  
COMMITTEE ON THE JUDICIARY,  
*Washington, DC.*

The Committee met, pursuant to notice, at 10:00 a.m., in Room 2141, Rayburn House Office Building, Hon. F. James Sensenbrenner, Jr., [Chairman of the Committee] Presiding.

[Intervening business.]

Chairman SENSENBRENNER. Now, pursuant to notice, I call up the bill H.R. 4661, the "Internet Spyware Prevention Act of 2004," for purposes of markup and move its favorable recommendation to the House. Without objection, the bill will be considered as read and open for amendment at any point.

[The bill, H.R. 4661, follows:]

108TH CONGRESS  
2D SESSION

# H. R. 4661

To amend title 18, United States Code, to discourage spyware, and for other purposes.

---

## IN THE HOUSE OF REPRESENTATIVES

JUNE 23, 2004

Mr. GOODLATTE (for himself, Ms. LOFGREN, and Mr. SMITH of Texas) introduced the following bill; which was referred to the Committee on the Judiciary

---

## A BILL

To amend title 18, United States Code, to discourage spyware, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*  
2 *tives of the United States of America in Congress assembled,*

### 3 SECTION 1. SHORT TITLE.

4 This Act may be cited as the “Internet Spyware (I-  
5 SPY) Prevention Act of 2004”.

### 6 SEC. 2. PENALTIES FOR CERTAIN UNAUTHORIZED ACTIVITIES RELATING TO COMPUTERS.

8 (a) IN GENERAL.—Chapter 47 of title 18, United  
9 States Code, is amended by inserting after section 1030  
10 the following:

1 **“§ 1030A Illicit indirect use of protected computers**

2 “(a) Whoever intentionally accesses a protected com-  
3 puter without authorization, or exceeds authorized access  
4 to a protected computer, by causing a computer program  
5 or code to be copied onto the protected computer, and in-  
6 tentiously uses that program or code in furtherance of  
7 another Federal criminal offense shall be fined under this  
8 title or imprisoned 5 years, or both.

9 “(b) Whoever intentionally accesses a protected com-  
10 puter without authorization, or exceeds authorized access  
11 to a protected computer, by causing a computer program  
12 or code to be copied onto the protected computer, and by  
13 means of that program or code—

14 “(1) intentionally obtains, or transmits to an-  
15 other, personal information with the intent to de-  
16 fraud or injure a person or cause damage to a pro-  
17 tected computer; or

18 “(2) intentionally impairs the security protec-  
19 tion of the protected computer;  
20 shall be fined under this title or imprisoned not more than  
21 2 years, or both.

22 “(c) No person may bring a civil action under the  
23 law of any State if such action is premised in whole or  
24 in part upon the defendant’s violating this section. For  
25 the purposes of this subsection, the term ‘State’ includes



1 the District of Columbia, Puerto Rico, and any other terri-  
2 tory or possession of the United States.

3 “(d) As used in this section—

4 “(1) the terms ‘protected computer’ and ‘ex-  
5 ceeds authorized access’ have, respectively, the  
6 meanings given those terms in section 1030; and

7 “(2) the term ‘personal information’ means—

8 “(A) a first and last name;

9 “(B) a home or other physical address, in-  
10 cluding street name;

11 “(C) an electronic mail address;

12 “(D) a telephone number;

13 “(E) a Social Security number, tax identi-  
14 fication number, drivers licence number, pass-  
15 port number, or any other government-issued  
16 identification number; or

17 “(F) a credit card or bank account number  
18 or any password or access code associated with  
19 a credit card or bank account.”.

20 (b) CONFORMING AMENDMENT.—The table of sec-  
21 tions at the beginning of chapter 47 of title 18, United  
22 States Code, is amended by inserting after the item relat-  
23 ing to section 1030 the following new item:

“1030A. Illicit indirect use of protected computers.”.

○

Chairman SENSENBRENNER. The Chair recognizes the gentleman from Virginia, Mr. Goodlatte, for 5 minutes to explain the bill.

Mr. GOODLATTE. Thank you, Mr. Chairman; and I will not use the full 5 minutes.

I thank you for holding a markup of this important legislation. Spyware is a growing and serious problem. The Federal Trade Commission has testified that spyware appears to be a new and rapidly growing practice that poses a risk of serious harm to consumers. Spyware is software that provides a tool for criminals to crack into computers to conduct nefarious activities such as altering a user's security settings, collect the personal information to steal a user's identity, or to commit other crimes.

The I-SPY Prevention Act would impose criminal penalties on the most egregious behavior associated with spyware. Specifically, this legislation would impose up to a 5-year prison sentence on anyone who uses software to intentionally break into a computer and uses that software in furtherance of another Federal crime. In addition, it would impose up to a 2-year prison sentence on anyone who uses spyware to intentionally break into a computer and either alter the computer's security settings or obtain personal information with the intent to defraud or injure a person or with the intent to damage a computer.

By imposing stiff penalty on these bad actors, this legislation will help deter the use of spyware and will thus help protect consumers from these aggressive attacks. In addition, this legislation would not interfere with the development of technological solutions to block spyware. Many technologies are currently available to help consumers detect and rid their computers of spyware. These—as these technologies progress, we must be careful not to impose unnecessary burdens on these innovators who are helping to fight against spyware.

By imposing stiff penalties on the truly bad actors and leaving the spyware—leaving the door open for the development of anti-spyware technologies, H.R. 4661 provides an important step in the fight against spyware. I was pleased to introduce this bipartisan legislation, along with my colleague from California, Ms. Lofgren, and I urge the Members of the Committee to support this important legislation.

Yield back.

Chairman SENSENBRENNER. Anybody wish—the gentlewoman from California, Ms. Lofgren, is recognized for 5 minutes.

Ms. LOFGREN. Thank you, Mr. Chairman; and thanks for holding this markup.

The I-SPY bill I think is an important answer to spyware which is increasingly causing problems for computer users around the world. Spyware can cause problems all the way from businesses that are forced to sustain costs to block and remove spyware, to criminals who are using spyware to track key strokes to steal identity or credit card information or Social Security numbers, to those of us who just use our personal computers and find spyware and are bothered by it. Further, there are estimates that at least 25 percent of all the computer crashes that occur on home computers are really caused by spyware that the owners are unaware of.

So I think that this legislation is not only important but quite necessary. Because the issue of spyware and also phishing—that is

going to be addressed in the manager's amendment, which I also support—is not a static problem. It is a growing problem and one that we should get ahead of.

Now there are other bills that have been introduced in the Congress and they take an approach that I think is not as clean and useful as the one in the bill before us. This measure goes after wrongdoing. It goes after criminal activity. It does not attempt to freeze technology or to try and define technology in a way that would limit or impair the development of technology, and I think that is the exact right approach and why I am so happy to be the principal cosponsor of the bill with Mr. Goodlatte.

I am aware and several persons have contacted me to express at least an issue that I think is very clear and that is why I want to address it here today on the preemption issue. In order to have an effective measure at the Federal level for computer use, you have to have a preemption or else—I mean, the Internet is an international technology, which is why you need an important Federal response.

However, if you look at page two, line 22, it says 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 defendants violating this section. So, really, we are preempting for Federal purposes.

I think the other side of that coin is that there is a State law—clearly, one can bring an action under State law, and it is not my intention nor Mr. Goodlatte's intention to preempt that. And I think several people have said we should clarify the language. I think it is very clear, and just by creating this legislative history hopefully we will resolve whatever issue exists on that score. So that is why I wanted to specifically outline it.

With that, I support the manager's amendment that will be offered later. I, as always, enjoy working with Mr. Goodlatte on these technology issues; and I yield back, or I yield to Mr. Scott.

Mr. SCOTT. On the section—the preemption that you just mentioned, if someone violates a section and causes harm, a criminal act, why shouldn't you be able to bring a civil action?

Ms. LOFGREN. Under the law of any State. It preempts State law.

Mr. SCOTT. And so if the action is premised in whole or in part upon the defendants violation of this section, if the defendant can say that your trespassing into his computer was implicated in this bill, you get thrown out of State court.

Ms. LOFGREN. No. Because you are not premising it on this Federal act. If you have a State trespass action and you bring a trespass action under State law, we are not preempting a trespass action. But if you utilize this statute as the basis for your State action, then, yes, you are preempted.

Mr. GOODLATTE. If the gentlewoman would yield.

Ms. LOFGREN. I would yield.

Mr. GOODLATTE. I would simply add we don't want to create 50 new State court actions based upon a Federal statute when there are already independent State actions that we do not preempt.

Mr. SCOTT. Well, will the gentlelady yield?

Ms. LOFGREN. Yes, I would yield.

Mr. SCOTT. Is there any other criminal action that you can commit that would not trigger civil remedies? If you cause somebody

harm by committing a criminal act that you can't get civil remedies for the damage caused by the criminal act?

Ms. LOFGREN. I don't have a photographic memory of the title 18, but—I don't know the answer to that question.

Chairman SENSENBRENNER. The gentlewoman's time has expired.

Without objection, all Members may place opening statements into the record at this point.

Are there amendments?

And the Chair recognizes the gentleman from Virginia, Mr. Goodlatte, for purposes of offering an amendment in the nature of a substitute.

Mr. GOODLATTE. Thank you, Mr. Chairman. That amendment is at the desk.

Chairman SENSENBRENNER. The clerk will report the amendment.

The CLERK. Amendment in the nature of a substitute to H.R. 4661 offered by Mr. Goodlatte.

Chairman SENSENBRENNER. Without objection, the amendment is considered as read and open for amendment at any point.

[The amendment follows:]

**AMENDMENT IN THE NATURE OF A SUBSTITUTE**  
**TO H.R. 4661**  
**OFFERED BY MR. Goodlatte**

Strike all after the enacting clause and insert the following:

**1 SECTION 1. SHORT TITLE.**

2 This Act may be cited as the "Internet Spyware (I-  
 3 SPY) Prevention Act of 2004".

**4 SEC. 2. PENALTIES FOR CERTAIN UNAUTHORIZED ACTIVI-**  
**5 TIES RELATING TO COMPUTERS.**

6 (a) In General- Chapter 47 of title 18, United States  
 7 Code, is amended by inserting after section 1030 the fol-  
 8 lowing:

**9 "§ 1030A Illicit indirect use of protected computers**

10 "(a) Whoever intentionally accesses a protected com-  
 11 puter without authorization, or exceeds authorized access  
 12 to a protected computer, by causing a computer program  
 13 or code to be copied onto the protected computer, and in-  
 14 tentiously uses that program or code in furtherance of  
 15 another Federal criminal offense shall be fined under this  
 16 title or imprisoned not more than 5 years, or both.

17 "(b) Whoever intentionally accesses a protected com-  
 18 puter without authorization, or exceeds authorized access

1 to a protected computer, by causing a computer program  
2 or code to be copied onto the protected computer, and by  
3 means of that program or code—

4 “(1) intentionally obtains, or transmits to an-  
5 other, personal information with the intent to de-  
6 fraud or injure a person or cause damage to a pro-  
7 tected computer; or

8 “(2) intentionally impairs the security protec-  
9 tion of the protected computer;

10 shall be fined under this title or imprisoned not more than  
11 2 years, or both.

12 “(c) No person may bring a civil action under the  
13 law of any State if such action is premised in whole or  
14 in part upon the defendant’s violating this section. For  
15 the purposes of this subsection, the term ‘State’ includes  
16 the District of Columbia, Puerto Rico, and any other terri-  
17 tory or possession of the United States.

18 “(d) As used in this section—

19 “(1) the terms ‘protected computer’ and ‘ex-  
20 ceeds authorized access’ have, respectively, the  
21 meanings given those terms in section 1030; and

22 “(2) the term ‘personal information’ means—

23 “(A) a first and last name;

24 “(B) a home or other physical address, in-  
25 cluding street name;

1 “(C) an electronic mail address;

2 “(D) a telephone number;

3 “(E) a Social Security number, tax identi-  
 4 fication number, drivers licence number, pass-  
 5 port number, or any other government-issued  
 6 identification number; or

7 “(F) a credit card or bank account number  
 8 or any password or access code associated with  
 9 a credit card or bank account.”.

10 (b) Conforming Amendment- The table of sections at  
 11 the beginning of chapter 47 of title 18, United States  
 12 Code, is amended by inserting after the item relating to  
 13 section 1030 the following new item:

“1030A. Illicit indirect use of protected computers.”.

14 **SEC. 3. AUTHORIZATION OF APPROPRIATIONS.**

15 In addition to any other sums otherwise authorized  
 16 to be appropriated for this purpose, there are authorized  
 17 to be appropriated for each of fiscal years 2005 through  
 18 2008, the sum of \$10,000,000 to the Attorney General  
 19 for prosecutions needed to discourage the use of spyware  
 20 and the practice commonly called phishing.

21 **SEC. 4. FINDINGS AND SENSE OF CONGRESS CONCERNING**

22 **THE ENFORCEMENT OF CERTAIN**  
 23 **CYBERCRIMES.**

24 (a) FINDINGS.—Congress makes the following find-  
 25 ings:

1           (1) Software and electronic communications are  
2           increasingly being used by criminals to invade indi-  
3           viduals' and businesses' computers without authoriza-  
4           tion.

5           (2) Two particularly egregious types of such  
6           schemes are the use of spyware and phishing scams.

7           (3) These schemes are often used to obtain per-  
8           sonal information, such as bank account and credit  
9           card numbers, which can then be used as a means  
10          to commit other types of theft.

11          (4) In addition to the devastating damage that  
12          these heinous activities can inflict on individuals and  
13          businesses, they also undermine the confidence that  
14          citizens have in using the Internet.

15          (b) SENSE OF CONGRESS.—Because of the serious  
16          nature of these offenses, and the Internet's unique impor-  
17          tance in the daily lives of citizens and in interstate com-  
18          merce, it is the sense of Congress that the Department  
19          of Justice should use the amendments made by this Act,  
20          and all other available tools, vigorously to prosecute those  
21          who use spyware to commit crimes and those that conduct  
22          phishing scams.



Chairman SENSENBRENNER. Are there any second degree amendments to the amendment in the nature of a substitute offered by the gentleman from Virginia?

Mr. GOODLATTE. Mr. Chairman, I can explain the amendment.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. GOODLATTE. Thank you, Mr. Chairman.

This amendment would make two changes to the underlying bill which could call attention to two dangerous types of activities that pose serious threats to consumers and threaten to undermine the confidence that consumers have in using the Internet.

First, the amendment authorizes \$10 million to the Department of Justice to combat spyware and phishing scams. Phishing scams typically involve the use of fake e-mail messages and Web sites to lure consumers into providing bank account information, credit card numbers and other personal information. These fake e-mail messages and Web sites are often indistinguishable from the real ones and often request account information from consumers. However, once consumers provide their account information they often find that they are the victims of identity theft.

Phishing is not just a nuisance anymore. In April of this year, the anti-phishing working group reported a 180 percent increase in phishing scams over the previous month. Another recent report showed that Internet users are losing confidence in Internet communications. Specifically, the report stated that Internet users are 63 percent less trusting of e-mail. In June 2003, that number was 52 percent.

With consumers' credit records and life savings as well as public confidence in Internet communications at stake, we must focus attention on this serious criminal development. By authorizing additional resources to the Department of Justice, this amendment would send the message that prosecuting these criminals should be a top priority.

In addition, this amendment would express the sense of Congress that the Department should vigorously enforce the laws that punish spyware and phishing scams. By calling on the Department to aggressively prosecute these Internet-related crimes this amendment will help protect users' account information and help restore the confidence that citizens have in using the Internet to obtain information, shop on-line, and do business with governmental and private entities.

This amendment strengthens the underlying bill, and I urge the Members of this Committee to support its adoption.

Chairman SENSENBRENNER. Are there any second degree amendments to the amendment in the nature of substitute?

The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Mr. Chairman, I have an amendment at the desk.

Chairman SENSENBRENNER. The clerk will report the amendment.

The CLERK. Amendment to the amendment in the nature of a substitute to H.R. 4661 offered by Mr. Scott of Virginia.

On page two, line 12, strike subsection "(c)", and renumber succeeding subsections accordingly.

[The amendment follows:]

**AMENDMENT TO THE AMENDMENT IN THE NATURE OF A SUBSTITUTE  
TO H.R. 4661  
OFFERED BY MR. SCOTT OF VIRGINIA**

On page 2, line 12, strike subsection “(c)”, and renumber succeeding subsections accordingly.

Chairman SENSENBRENNER. The gentleman from Virginia is recognized for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman.

Mr. Chairman, I think the provision in section (c) just sets up a bad policy. Here you have got a criminal act and then say that the damage that occurs as a proximate cause of someone committing a criminal act is not the—you are not able to bring a civil action in State law—I mean, in State court, after they have committed a criminal act. I am not aware of any Federal criminal act that you can commit causing somebody harm that you can’t bring an action against them to recoup damages. So I think we ought to just eliminate section (c).

Yield back.

Chairman SENSENBRENNER. Gentleman from Virginia.

Mr. GOODLATTE. Move to strike the last word.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. GOODLATTE. Thank you, Mr. Chairman.

Mr. Chairman, I strongly oppose this amendment. We have been careful in crafting this legislation not to preempt other State law causes of action that already exist should these types of scams take place. But we are having a problem with State laws being crafted around the country that do interfere with the ability to have one national policy related to the Internet, and I think that to adopt this amendment would be to expose the process to 50 new different State court types of actions, and I think we ought to limit this to a new Federal procedure to criminally prosecute those who violate these conditions and not expand the area beyond that.

Ms. LOFGREN. Would the gentleman yield?

Mr. GOODLATTE. I would yield to the gentlewoman from California.

Ms. LOFGREN. I agree with you at this time. But one of the things I think that we need to monitor is how the legislation we pass actually works.

And I support this bill. I think that the criminal activity that is occurring is sufficiently grave that it will attract the enforcement attention of Federal prosecutors, and I think it should. And I think we should monitor how many prosecutions are brought and how it works. But we may find in a period of several years that it didn’t actually result in prosecutions, in which case we might want to take another look at civil remedies.

I have prepared—I think at this point we should try this. But I think also—and I don’t have an amendment to this effect, but—nor do I think we need to put it in here. I think we ought to promise ourselves to have a hearing next year or in about 18 months and

get a report from the Justice Department on how this has actually worked.

Because we know, for example, with the spam bill that the House passed and has signed into law, it hasn't reduced—I voted against it because I didn't think it would work. It hasn't worked. Now maybe that will change, but we need to monitor this stuff because it is a new area of law, and I would hope that we could address whether or not we should have the amendment that Mr. Scott is proposing at that time, after we see this—how this works. And I would oppose it at this time, although I think the intentions are admirable and honest.

And I yield back.

Mr. SCOTT. Would the gentleman yield?

Mr. GOODLATTE. Reclaiming my time, I yield to the gentleman from Virginia.

Mr. SCOTT. Thank you.

Let me just get this straight. There is no—under existing State law, there is no prohibition for bringing a State action under State law so long as you don't implicate this law, is that right?

Mr. GOODLATTE. That is correct.

Mr. SCOTT. And there is no prohibition against coming from the Federal court to vindicate your rights under this bill, is that right?

Mr. GOODLATTE. That is correct.

Mr. SCOTT. Thank you.

Mr. GOODLATTE. Reclaiming my time. I endorse the observations of the gentlewoman from California. This is a totally new area, and I think we should proceed with caution in terms of expanding legal actions. And I think this approach is a good one, but if we find if that is not the case we can review it later.

I yield back.

Chairman SENSENBRENNER. The question is on the amendment to the amendment in the nature of a substitute offered by the gentleman from Virginia, Mr. Scott. Those in favor will say aye. Opposed, no.

The no appears to have it. The no has it, and the amendment is not agreed to.

Are there further second degree amendments to the amendment in the nature of a substitute?

Mr. SMITH. Mr. Chairman, I move to strike the last word.

Chairman SENSENBRENNER. Gentleman from Texas is recognized for 5 minutes.

Mr. SMITH. Thank you, Mr. Chairman; and I will only take a couple of minutes.

Now, Mr. Chairman, I simply wanted to thank Representative Goodlatte and Representative Lofgren for offering this substitute amendment which makes a good bill even better.

I support the substitute amendment because it gets to the heart of the problem we face with spyware, the regulation of bad behavior rather than technology. It provides strong penalties for those who engage in the illicit activities of spyware and phishing. Spyware enables someone to gather and transmit information about a computer user without his or her knowledge. It can range from software that tracks every key typed to programs that hijack a user's system settings. Even with the significant security provided for computer systems in the House of Representatives, com-

puters in my own office and others have been infected with spyware.

Spyware is often a confusing problem for consumers. Many don't know they have it or, if they do, they don't know how to get rid of it. A Yahoo Internet search of the term spyware yields over 8 million results. It is no wonder the problem is only getting worse.

Likewise, phishing, which occurs when a consumer is deceived and gives up personal information, is a common problem that must be addressed.

Rather than add to an already confusing regulatory structure, this bill rightly takes a very narrow approach. It sets strong penalties for anyone who intentionally uses software to break into a computer in order to alter security settings or obtain personal information. It further authorizes money for the DOJ to prosecute spyware and phishing crimes.

It is a good substitute amendment, Mr. Chairman; and I will yield back the balance of my time.

Chairman SENSENBRENNER. The questions occurs on the amendment in the nature of a substitute offered by the gentleman from Virginia. All in favor will say aye. Opposed, no.

The ayes appear to have it. The ayes have it. The amendment in the nature of a substitute is agreed to.

The question now occurs on the motion——

Mr. GOODLATTE. Mr. Chairman, very briefly I ask unanimous consent to add several letters that we have in support of H.R. 4661 into the record.

Chairman SENSENBRENNER. Without objection, so ordered.

Mr. GOODLATTE. Thank you, Mr. Chairman.

[The material referred to follows:]



1250 Eye Street NW Suite 200  
Washington, DC 20005  
202-737-8888 www.itic.org

**CHAIRMAN**  
Nancy Heiman  
Apple  
**PAST CHAIRMAN**  
Dennis Roberson  
Motorola

**OFFICERS**  
Rhett Dawson  
President  
Ralph Hullmann  
Senior Vice President  
Helga Sayadian  
Vice President

September 7, 2004

The Honorable Bob Goodlatte  
2240 Rayburn House Office Building  
Washington, D.C. 20515

Dear Chairman Goodlatte:

I am writing to thank you for introducing H.R. 4661, the "Internet Spyware Prevention Act." Your legislation will help protect consumers by ensuring that a crime committed using information collected through unauthorized access to a computer carries additional criminal penalties. The use of simple software programs to collect information in order to steal, defraud, or otherwise break the law is the type of "spyware" behavior consumers fear most. By targeting this behavior, H.R. 4661 will not only ensure greater penalties for perpetrators of computer crimes but will also inspire greater consumer confidence online.

The Information Technology Industry Council is proud to offer its strong support to H.R. 4661, and we look forward to working with you as this legislation continues through the Judiciary Committee process and beyond.

If you have any questions, please contact Scott Corley at (202) 626-5722.

Best Regards,

Rhett Dawson  
President

*The association of leading IT companies*

Accenture • Agilent • Apple • Canon USA • Cisco • Corning • Dell • Eastman Kodak • eBay  
EMC Corporation • Hewlett Packard • Honeywell • IBM • Intel • Lexmark • Microsoft • National Semiconductor  
NCR • Oracle • Panasonic • SAP • Sony Electronics • Sun Microsystems • Symbol Technologies • Teletronics • Time Warner • Unisys

CHAMBER OF COMMERCE  
OF THE  
UNITED STATES OF AMERICA

R. BRUCE JOSTEN  
EXECUTIVE VICE PRESIDENT  
Government Affairs

1615 H STREET, N.W.  
WASHINGTON, D.C. 20062-2000  
202/462-5310

September 8, 2004

TO THE MEMBERS OF THE HOUSE JUDICIARY COMMITTEE:

On behalf of the U.S. Chamber of Commerce, the world's largest business federation representing more than three million businesses of every size, sector and region, I am writing to express our support for H.R. 4661, the Internet Spyware Prevention Act (I-SPY Act).

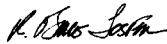
Computer crime is a serious problem, draining millions of dollars from our nation's economy every year. The most serious privacy and security concerns are associated with surreptitious programs that capture a user's personal information without their knowledge or consent. These programs include keystroke logging software that records the user's information and "phishing" or false webpages that capture passwords and other private financial data from consumers, both of which can lead to theft of one's identity.

The types of practices identified above are deplorable and companies that utilize them should be held accountable. However, defining "spyware" is very difficult, as there are many downloadable software applications that help to strengthen computer security and advance e-commerce. For example, web beacons are used by many websites to create a secure online marketplace and cookies can improve the user experience by allowing people to more easily traverse multiple pages on a single site.

Computer security is an issue that affects any business that operates in the online world, including the technology, telecommunications, financial services, travel and tourism, and retail industries. The I-SPY Act identifies the truly unscrupulous acts associated with spyware and uses the appropriate criminal legal standards to bring bad actors to justice. In addition, the bill is narrowly written to avoid the creation of unintended consequences, including subjecting businesses to frivolous lawsuits when they use otherwise legitimate software applications.

For these reasons, I urge you to pass H.R. 4661 and to support language expressing the "Sense of Congress" that this is an issue of vital importance to our nation.

Sincerely,



R. Bruce Josten



September 7, 2004

The Honorable Bob Goodlatte  
2240 Rayburn House Office Building  
Washington, DC 20515

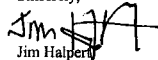
Re: Support for H.R. 4661

Dear Representative Goodlatte:

The Internet Commerce Coalition, whose members include AT&T, BellSouth, Comcast, eBay, MCI, SBC Communications and Verizon, writes to express our strong support for H.R. 4661, which would aim criminal penalties at the egregious uses of spyware. This bill appropriately targets the greatest threats to consumers posed by spyware—obtaining personal information to perpetrate harm against a computer user or undermining the security of computers.

We congratulate you on the introduction of H.R. 4661 and look forward to its passage through the Judiciary Committee, and to working with you and the Commerce Committee on balanced, effective legislation to address the harms caused by use of spyware.

Sincerely,

  
Jim Halpert  
General Counsel  
202.861.3938

**Software & Information  
Industry Association**  
1090 Vermont Ave NW Sixth Floor  
Washington, DC 20005-4095



September 8, 2004

The Honorable James Sensenbrenner, Chairman  
Committee on the Judiciary  
U.S. House of Representatives  
Washington, DC 20515

Dear Chairman Sensenbrenner:

I am writing on behalf of the members of the Software & Information Industry Association (SIIA) to commend Cong. Bob Goodlatte, Cong. Zoe Lofgren, and Cong. Lamar Smith for their leadership in introducing H.R. 4661, the "Internet Spyware (I-SPY) Prevention Act of 2004". We urge the Committee to mark-up this important legislation as soon as possible, as we continue to work with the Congress on meaningful legislation to combat the pernicious effects of spyware.

Our interest in legislation in this area stems from two perspectives related to our role as the principal trade association of the software code and information content industry. The more than 600 members of SIIA develop and market software and electronic content for business, education, consumers and the Internet. SIIA's members are software companies, ebusinesses, and information service companies, as well as many electronic commerce companies. Our membership consists of some of the largest and oldest technology enterprises in the world as well as many smaller and newer companies.

First, many of our member companies are adversely affected by abusive behaviors perpetrated by unscrupulous actors on the Internet. These bad actors use a variety of tools and mechanisms to carry out their activities, and we are interested in stopping this bad behavior. Second, any policy response in this area may directly affect the ability of our members to develop and manage products that meet the expectations of consumer, business and enterprise users for seamless and unburdensome experiences on the Internet and in the use of software and services to meet their needs.

We have appreciated the outreach by the Sponsors of H.R. 4661 and Committee staff, and as a result believe the legislation has significant benefits in the fight against spyware. We look forward to working with you and the entire Committee as the bill moves its way through the House. In particular, SIIA looks forward to working with the Committee to ensure that the pre-emption section is carefully crafted and does not preempt state laws that are essential to combating fraud and promoting computer security. Please do not hesitate to contact me if you have any questions.

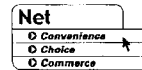
Sincerely,

A handwritten signature in black ink, appearing to read 'Mark Bohannon'.

Mark Bohannon  
General Counsel &  
Senior Vice President Public Policy

Tel: +1.202.289.7442  
Fax: +1.202.289.7097  
[www.sii.net](http://www.sii.net)





## Press Release

September 8, 2004  
 Media Contact:  
 Mark Blafkin  
 202-331-2130 x104  
[mblafkin@actonline.org](mailto:mblafkin@actonline.org)

### NetChoice Commends I-SPY Bill

Washington, DC – Today, the House Judiciary Committee is marking up H.R. 4661, the Internet Spyware (I-SPY) Prevention Act. The bill was sponsored by Congressman Goodlatte (R-VA), Congresswoman Zoe Baird (D-CA) and Lamar Smith (R-TX). NetChoice Executive Director, Steve DeBianco, made the following comments in support of the bill's approach:

"The proliferation of spyware has become a critical problem for consumers and e-commerce businesses and deserves the attention of Congress. Spyware is surreptitiously added to computers, secretly collects information about users and their Internet use, and is often nearly impossible to remove.

I-SPY specifically targets malicious spyware, and focuses attention on phishing, an old-economy criminal scam that has migrated to the internet. The bill's sponsors have taken the right approach by targeting criminal behavior that occurs online.

Unfortunately, some states are considering laws to regulate technologies instead of bad behavior. And to make matters worse, the patchwork quilt of conflicting state regulations being created would throw a wet blanket on e-commerce."

*NetChoice is a coalition of trade associations, eCommerce businesses, and online consumers who share the goal of promoting convenience, choice and commerce on the Net. Founding members of NetChoice include the Association for Competitive Technology, Information Technology Association of America, the Electronic Retailing Association, eBay, 1-800 Contacts, eRealty.com, and Orbitz. More information about NetChoice can be found at [www.netchoice.org](http://www.netchoice.org).*

###

Chairman SENSENBRENNER. The question now occurs on the motion to report the bill H.R. 4661 favorably as amended. A reporting quorum is present. All in favor, say aye. Opposed, no.

The ayes appear to have it. The ayes have it. The motion to report favorably is adopted.

Without objection, the bill will be reported favorably to the House in the form of a single amendment in the nature of a substitute incorporating the amendment adopted here today. Without objection, the Chairman is authorized to move to go to conference pursuant to House rules. Without objection, the staff is directed to make any technical and conforming changes; and then all Members will be given 2 days as provided by House rules in which to submit additional dissenting supplemental or minority views.

