109TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
1st Session } { 109–93

INTERNET SPYWARE (I-SPY) PREVENTION ACT OF 2005

MAY 23, 2005.—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. 744]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 744) to amend title 18, United States Code, to discourage spyware, and for other purposes, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

PURPOSE AND SUMMARY

H.R. 744, the "Internet Spyware (I-SPY) Prevention Act of 2005," clarifies and enhances existing fraud and computer crime law with criminal penalties targeting egregious abuses perpetrated upon Internet users by persons who maliciously employ various covert software applications, programs, applets, or computer code commonly known as "spyware." H.R. 744 also provides resources and

39–006

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. This legislation is substantially similar to H.R. 4661, which passed the House during the 108th Congress by a vote of 415–0.

BACKGROUND AND NEED FOR THE LEGISLATION

In recent years, the Internet has been transformed from an obscure academic research tool into a digital medium of unprecedented scope accessed by computers and people around the world. The rapid growth in both the usage and utility of the Internet has been facilitated by technologies designed to enhance the speed and efficiency of data transfer. New technologies and software applications that recognize return visitors to websites, store information on the consumer preferences of Internet users, and permit the secure transmission of personal data over the Internet have produced a degree of personalization that has enhanced consumer options and the overall potential of this medium. At the same time, software innovations that have enhanced and personalized usage of the Internet have also given rise to opportunities for abuse and illegal behavior.

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."[1] Examples of spyware include software that collects information about the use of the computer on which the software is installed, some of which 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 another third party. 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 the computer for the 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

[1] See *http://www.ftc.gov/bcp/workshops/spyware.*

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 by the National CyberSecurity Alliance found that over 90 percent 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 types of illegal behavior that are 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. These fraudulent websites and e-mails are designed to deceive Internet users into revealing personal information that can be used to defraud those same users. 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. Specifically, the schemes themselves, and the uses of the information by the criminals who obtain it are not unique to the Internet. In addition, almost all are illegal under existing Federal criminal laws dealing with wire fraud.

This scope of this problem was highlighted in a recent Department of Justice report on phishing. According to the report: 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. 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*) 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.[2]

GENERAL CHALLENGES ASSOCIATED WITH ADDRESSING THE PREVALENCE OF SPYWARE AND PHISHING

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. 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,

[2] See *http://www.usdoj.gov/criminal/fraud/Phishing.pdf*].

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, antivirus software, and various means of blocking unsolicited e-mail can address these other attendant ills and thwart most attacks.

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"), and lawmakers to deal with the problem of spyware and phishing not as particular technologies

but as types of behavior that make illegal 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. 744. 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 unwanted spyware to one user may be considered innocuous or marginally beneficial software to another. There is also a real risk that computer users will face so many Federally-mandated 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 enjoyment of computer users, then the solution must not diminish that experience more than the original problem. The approach of this bill is to focus on prosecuting companies engaged in criminal practices—not to impede legitimate companies from offering software that provides meaningful services in support of Internet commercial activity, such as market research, instant messaging, or security software.

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. Such a standard is at odds with the spirit of the Judiciary Committee's recent litigation reform efforts aimed at reducing liability barriers for American businesses. 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 hypothetically construct any phishing scheme that would not violate existing Federal wire fraud or identity theft laws. Likewise, some forms of spyware related behavior

would violate either Sec. 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. 744) 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 Sec. 1030A of Title 18 created by H.R. 744 is intended to provide new tools for prosecutors who may find it difficult to bring some spyware cases under current 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.

HEARINGS

No hearings were held on H.R. 744.

COMMITTEE CONSIDERATION

On May 18, 2005, the Committee met in open session and ordered favorably reported the bill H.R. 744, 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 consideration of H.R. 744.

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

H.R. 744, 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, May 23, 2005.

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. 744, the Internet Spyware (I-SPY) Prevention Act of 2005.

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) and Sarah Puro (for the state and local impact).

Sincerely,

DOUGLAS HOLTZ-EAKIN, *Director.*

Enclosure.

H.R. 744—Internet Spyware (I-SPY) Prevention Act of 2005

Summary: H.R. 744 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 2006–2009 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 2006 and $40 million over the 2006–2010 period. CBO expects that enacting the bill would have an insignificant effect on federal revenues and direct spending.

H.R. 744 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 ($62 million in 2005, 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. 744 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit).

	By fiscal year, in millions of dollars—				
	2006	2007	2008	2009	2010
CHANGES IN SPENDING SUBJECT TO APPROPRIATION					
Authorization Level	10	10	10	10	0
Estimated Outlays	9	10	10	10	1

For this estimate, CBO assumes the bill will be enacted near the start of the fiscal year 2006 and that the authorized amounts will be appropriated each year.

Enacting H.R. 744 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 pen-

alties 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. 744 would prohibit states from creating civil penalties that specifically reference the statue. 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 statues. 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 ($62 million in 2005, adjusted annually for inflation).

Estimated impact on the private sector: The bill contains no new private-sector mandates as defined in UMRA.

Estimate prepared by: Federal Costs: Melissa E. Zimmerman Impact on State, Local, and Tribal Governments: Sarah Puro Impact on the Private Sector: Paige Piper/Bach.

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.744 enhances existing fraud and computer crime law with strong criminal penalties targeting egregious abuses perpetrated upon Internet users by persons who maliciously employ various covert software applications, programs, applets, or computer code commonly known as "spyware" while enhancing penalties for "phishing."

CONSTITUTIONAL AUTHORITY STATEMENT

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

SECTION-BY-SECTION ANALYSIS AND DISCUSSION

Section 1. Short title

Section 1 provides that the Act may be cited as the "Internet Spyware (I-SPY) Prevention Act of 2005."

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 constitute an intentional illicit indirect use of a protected computer. Section 2 does this by adding a new Sec. 1030A to Title 18, of the U.S. Code. Subsection 2(a) amends Chapter 47 of Title 18 United States Code by inserting after Sec. 1030 the following new section:

Sec. 1030A Illicit indirect use of protected computers. New Sec. 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 com-

puter. New Sec. 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. New Sec. 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.

New subsection 1030A(c) of Title 18 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 Sec. 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 a 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.

New Sec. 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 Sec. 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 2006–FY 2009 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

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.

Subsection 4(b) offers guidance to the Department of Justice by setting forth Congress' 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 italic and exsting law in which no change is proposed is shown in roman):

CHAPTER 47 OF TITLE 18, UNITED STATES CODE

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 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 or bank account.

(e) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

* * * * * * *

MARKUP TRANSCRIPT

BUSINESS MEETING

MAY 18, 2005

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

The Committee met, pursuant to notice, at 10:07 a.m., in Room 2141, Rayburn House Office Building, Hon. F. James Sensenbrenner, Jr. [Chairman of the Committee] presiding.

Chairman SENSENBRENNER. The Committee will be in order. A working quorum is present.

Pursuant to notice, I now call up the bill H.R. 744, the "Internet Spyware (I-SPY) Prevention Act of 2005," 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. 744, follows:]

I

109TH CONGRESS
1ST SESSION

H. R. 744

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

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 10, 2005

Mr. GOODLATTE (for himself, Ms. ZOE LOFGREN of California, Mr. SMITH of Texas, Mr. JENKINS, Mr. HOSTETTLER, Ms. LINDA T. SÁNCHEZ of California, Mr NADLER, Mr. FORBES, Mr. HALL, and Mr. WOLF) 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.

. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Internet Spyware (I-SPY) Prevention Act of 2005".

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 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 or bank account.

"(e) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of

a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.".

(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 2006 through 2009, 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.

○

Chairman SENSENBRENNER. The Chair recognizes the gentleman from Virginia, Mr. Goodlatte, the sponsor of this bill, to tell us why it ought to pass.

Mr. GOODLATTE. Mr. Chairman, thank you for scheduling a markup of the Internet Spyware Prevention Act. This bipartisan legislation, which I introduced with my colleagues Zoe Lofgren, Lamar Smith, and many other Members of the Judiciary Committee, will impose tough criminal penalties on the truly bad actors without imposing a broad regulatory regime on legitimate online businesses. I believe that this targeted approach is the best way to combat spyware.

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, collecting 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 behaviors 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 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 penalties on these bad actors, this legislation will help deter the use of spyware and will thus help protect consumers from these aggressive attacks.

Enforcement is crucial in combating spyware. The I-SPY Prevention Act authorizes $10 million for fiscal years 2006 through 2009 to be devoted to prosecutors and expresses the sense of Congress that the Department of Justice should vigorously enforce the laws against spyware violations as well as against online phishing scams in which criminals spend fake e-mail messages to consumers on behalf of well-known companies and request account information that is later used to conduct criminal activities.

I believe that four overarching principles should guide the development of any spyware legislation. First, we must punish the bad actors while protecting legitimate online companies. Second, we must not overregulate but, rather, encourage innovative new services and the growth of the Internet. Third, we must not stifle the free market. Fourth, we must target the behavior, not the technology.

By imposing criminal penalties on those who use spyware to commit Federal crimes and other dangerous activities, the I-SPY Prevention Act will protect consumers by punishing the bad actors without imposing liability on those who act legitimately online. The targeted approach of the I-SPY Prevention Act also avoids excessive regulation and its repercussions, including the increased likelihood that an overly regulatory approach would have unintended consequences that could discourage the creation of new and excit-

ing technologies and services on the Internet. By encouraging innovation, the I-SPY Prevention Act will help ensure that consumers have access to cutting-edge products and services at lower prices.

In addition, the approach of the I-SPY Prevention Act does not interfere with the free market principle that a business should be free to react to consumer demand by providing consumers with easy access to the Internet's wealth of information and convenience. Increasingly, consumers want a seamless interaction with the Internet, and we must be careful not to interfere with business' ability to respond to this consumer demand by innovative services. The I-SPY Prevention Act will help ensure that consumers, not the Federal Government, define what their interaction with the Internet looks like.

Finally, by going after the criminal behavior associated with the use of spyware, the I-SPY Prevention Act recognizes that not all software is spyware and that the crime does not like in the technology itself but, rather, in actually using the technology for nefarious purposes. People commit crimes, not software.

The I-SPY Prevention Act is a targeted approach that protects consumers by imposing stiff penalties on the truly bad actors. I urge my colleagues to support this important legislation.

I yield back the balance of my time.

Chairman SENSENBRENNER. The gentleman from Michigan.

Mr. CONYERS. Mr. Chairman, may I yield to the author of this measure, the gentlelady from California, Zoe Lofgren?

Chairman SENSENBRENNER. The gentlewoman from California is recognized.

Ms. LOFGREN. Thank you, Mr. Chairman and Mr. Conyers. I am happy to have partnered with Mr. Goodlatte on this legislation to combat spyware.

Spyware actually is a growing problem to consumers on the Internet, and it is creating problems beyond just nuisance. Thieves are using spyware to harvest personal information from unsuspecting computer users. Criminals are even using spyware to track every keystroke that an individual makes. You can steal credit card and Social Security numbers that way.

Spyware also has an adverse impact on the business community because businesses are forced to spend money to block and remove spyware from their systems. In fact, Microsoft recently said that spyware is at least partially responsible for about one-half of all the application crashes that are reported to them, and experts estimate that 80 to 90 percent of all personal computers contain some form of spyware. In fact, last year, EarthLink identified more than 29 million spyware programs.

In short, spyware is a very real problem that is endangering consumers, damaging businesses, and creating millions of dollars of additional costs. H.R. 744, as Mr. Goodlatte has said, is a bipartisan measure that identifies the truly unscrupulous acts associated with spyware and subjects them properly to criminal punishment.

This bill is unique and it is the right approach because it focuses on behavior not on technology. As we have noted in the past, technology moves faster than legislation, and it is important that we target misbehavior without burdening technology innovation, and

this bill accomplishes that. As Mr. Goodlatte has noted, it also provides or authorized funding for the Attorney General so that prosecution, when appropriate, can be undertaken.

At the same time, I think it is important to note—and I do want to emphasize this because it was a point of discussion in the last Congress—H.R. 744 does not prevent existing or future State laws that prohibit spyware. This bill only preempts civil actions based on violations of this new Federal criminal law. It does not prevent a State from passing a similar law, nor does it prevent any lawsuits that are premised on existing State laws.

Last year, the House unanimously passed this bill, and I think it will do so again if we can report the bill out, and I hope that we will do so. And I thank the——

Mr. CONYERS. Would the gentlelady yield?

Ms. LOFGREN. Yes, I would.

Mr. CONYERS. I would like to just draw a small distinction between a similar measure coming out of another Committee in the House which we think the definitions are overly broad and it goes beyond criminal penalties and deals with civil sanctions and other matters that we think recommend this particular Judiciary measure to the entire Congress. And I want to thank the two authors of the measure.

Ms. LOFGREN. Reclaiming my time, I thank the Chairman—Mr. Conyers for that comment, and you're correct. There is a competing measure that Mr. Goodlatte—well, I don't want to speak for Mr. Goodlatte, but I believe has a more heavy-handed regulatory approach that is likely to chill technology innovation. This measure avoids that pitfall and is the sounder approach, and I think that's why it has such broad support in the technology community as well as the law enforcement community. And we're hopeful that if this Committee, if our Committee acts promptly, the wisdom of our ways as shown in this bill will prevail in the end and avoid an unfortunate technology burden that would have adverse impacts for the future. And I thank Mr. Conyers for allowing me to comment on this bill. And I yield back.

Mr. WATT. Mr. Chairman?

Chairman SENSENBRENNER. Does the gentleman yield back?

Without objection, opening statements will be placed in the record at this time.

[The prepared statement of Mr. Smith follows.]

PREPARED STATEMENT OF THE HONORABLE LAMAR SMITH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS, AND CHAIRMAN, SUBCOMMITTEE ON COURTS, THE INTERNET, AND INTELLECTUAL PROPERTY

Mr. Chairman, I am an original cosponsor of this bill and support its passage. And I thank Mr. Goodlatte for introducing such a much-needed piece of legislation.

Computer spyware is a growing problem that threatens the future of commerce over the Internet.

Yesterday, my staff performed a Google Internet search of the term "spyware"—it yielded over 20 million results. It's no wonder the problem is only getting worse.

In the first three quarters of 2004, more than three million scans for spyware were performed. These scans revealed over 83 million instances of spyware. That is obviously disturbing.

Spyware can be 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. But it's become much more than just a nuisance for computer users. It's a threat to information security. Some types of spyware help to facilitate identity theft and phishing.

HR 744 addresses spyware through the regulation of bad behavior rather than the regulation of technology. It provides strong penalties for those who engage in the illicit activities of spyware and phishing.

Rather than add to an already confusing regulatory structure, this bill takes a very narrow approach. It sets strong penalties for anyone who intentionally uses software to break into a computer to alter security settings or obtain personal information.

It further authorizes money for the DOJ to prosecute spyware and phishing crimes.

I urge my colleagues to put an end to spyware and support this bill.

Chairman SENSENBRENNER. Are there amendments?

Mr. WATT. Mr. Chairman?

Chairman SENSENBRENNER. The gentleman from North Carolina.

Mr. WATT. I move to strike the last word.

Chairman SENSENBRENNER. The gentleman is recognized for 5 minutes.

Mr. WATT. Solely for the purpose of asking a question. I don't think it will take 5 minutes, but I noticed that the gentlelady from California was about to run out of time, so I didn't want to put her in the position of running out of time while she was trying to answer the question.

She addressed the matter of preempting States from creating civil remedies based on violations of this act, and I'm just trying to figure out what the rationale for that is. If an individual is injured as a result of a violation of this act, and the purpose is to keep folks from using this spyware or doing whatever the bill prohibits, I'm not sure I understand what the rationale is for limiting personal actions which would be in my estimation a much, much more powerful deterrent to bad actors than possible criminal penalties, which very seldom will be used and will have a higher burden of proof.

So I guess I'm addressing the question to both Mr. Goodlatte and Ms. Lofgren. What is the rationale for that limitation? And are we once again being the Big Brother here by preempting the possibility of States doing something either more aggressive or making possible more effective enforcement of the law that we are about to pass here?

I would yield to either of them who wish to respond, or hopefully both of them will respond, and maybe I'll understand it from both perspectives.

Mr. GOODLATTE. Does the gentleman yield?

Mr. WATT. I yield to the gentleman from Virginia first.

Mr. GOODLATTE. Thank you. I thank the gentleman for his question. It's a good question. As you know, often when a Federal criminal statute is created, States create a civil liability action based on the Federal criminal statute. And the preemption language in the current bill would simply prohibit States from deriving new State tort actions based on violations of this new Federal criminal spyware statute so we didn't have 50 different approaches to something that is on the Internet where you have virtually interstate commerce by every single action that takes place on the Internet. The preemption language, however, in the current bill does not preempt other types of independent State computer fraud statutes.

Mr. WATT. I understand that. I summarized that. But your answer, your response hasn't added anything to the universe of knowledge about why that's—that's important. It seems to me

counterproductive to the objectives of the legislation to pass a Federal criminal statute and then say to States you can't even pass a civil law that will effectively allow individual claimants who have been injured as a result of this Federal criminal activity to redress their own rights.

Ms. LOFGREN. Would the gentleman yield?

Mr. WATT. So maybe I'll get a better response from Ms. Lofgren.

Ms. LOFGREN. If you look on page 3, line 1 of the bill, "No person may bring a civil action under the law of any State if such action is premised in whole or in part . . ." It does not preclude an action in Federal court of a civil major, and it does not preclude action under a different State statute.

So I think the goal here, number one, is to emphasize the criminal prosecution; number two, to have uniformity because it is—the Internet by its very nature is in interstate commerce; and, three, not to unduly disrupt the laws—the pre-existing laws of the States that—the most commonly used are trespass statutes. I mean, you could still do this, but the hope is that we would have uniformity both from a criminal law point of a view and a civil law point of view in the spyware arena.

Chairman SENSENBRENNER. The gentleman's time has expired.

Are there amendments?

[No response.]

Chairman SENSENBRENNER. If there are no amendments, a reporting quorum is not present. Without objection, the previous question is ordered on the motion to report the bill H.R. 744 favorably, and that question will be put when a reporting quorum appears.

[Intervening business.]

Chairman SENSENBRENNER. Are there amendments? Before we get to more amendments, a reporting quorum is present. The question is on reporting favorably the bill H.R. 744, the "I-SPY Prevention Act of 2005." Those in favor will say aye? Opposed, no?

The ayes appear to have it. The ayes have it, and the motion——

Ms. WATERS. Recorded vote, please.

Chairman SENSENBRENNER. A recorded vote is demanded.

Mr. CONYERS. She made a mistake.

Chairman SENSENBRENNER. Okay. The ayes have it on H.R. 744, and the motion to report favorably is agreed to. Without objection, the staff is directed to make technical and conforming changes, and all Members will be given 2 days as provided by the House rules in which to submit additional, dissenting, supplemental, or minority views.

[Intervening business.]

Chairman SENSENBRENNER. The Committee stands adjourned.

[Whereupon, at 11:41 a.m., the Committee adjourned.]

○