110TH CONGRESS
1st Session
HOUSE OF REPRESENTATIVES
REPORT
110–159

INTERNET SPYWARE (I–SPY) PREVENTION ACT OF 2007

MAY 21, 2007.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

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

R E P O R T

[To accompany H.R. 1525]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 1525) to amend title 18, United States Code, to discourage spyware, and for other purposes, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

CONTENTS

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 2007".

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 with the intent to defraud or injure a person or damage a 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) CLERICAL 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 2008 through 2011, the sum of $10,000,000 to the Attorney General for prosecutions needed to discourage the use of spyware and the practices commonly called phishing and pharming.

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.

(5) The continued development of innovative technologies in response to consumer demand is crucial in the fight against spyware.

(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 and pharming scams.

PURPOSE AND SUMMARY

H.R. 1525, the "Internet Spyware (I–SPY) Prevention Act of 2007," amends title 18 of the United States Code to clarify and enhance criminal penalties when spyware is used for the purpose of perpetrating identity theft and other privacy intrusions against innocent Internet users. In addition, H.R. 1525 provides resources and guidance to the Department of Justice for the prosecution of spyware, as well as for phishing and pharming, which involve other types of fraudulent activities. This legislation is substantially similar to H.R. 744, the "Internet Spyware (I–SPY) Prevention Act of 2005," which passed the House during the 109th Congress by a vote of 395–1.

BACKGROUND AND NEED FOR THE LEGISLATION

The proliferation of spyware and phishing threatens to undermine consumer confidence in the integrity and security of the Internet. Software and electronic communications are increasingly being used by criminals to invade individuals' and businesses' computers without authorization. Two particularly egregious examples involve the use of spyware and phishing scams.

Spyware presents privacy, security, and functionality concerns for both Internet users and legitimate commercial activity on the Internet. The Federal Trade Commission has defined "spyware" as software that "aids in gathering information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge."[1] For example, one type of spyware is placed on a user's system to steal confidential information such as user names, passwords, and credit card details. Adware, another form of spyware, in its worst form traces a user's Web activity and causes "pop-up" advertisements to suddenly appear on the user's monitor in response, which in many instances cannot be closed by the user.

The greatest security and privacy challenges posed by spyware relate to technologies such as keystroke logging programs that capture a user's passwords, Social Security number, or bank or credit account numbers. This information can then be captured and redirected for criminal purposes including fraud, larceny, identity theft, or other cybercrimes. Recent studies estimate that 80 percent of computers are infected with some form of spyware and that 89 percent of consumers are unaware of the fact that they have spyware.[2]

---

[1] Federal Trade Commission, Public Workshop: Monitoring Software on Your PC: Spyware, Adware, and Other Software, 69 Fed. Reg. 8538 (Feb. 24, 2004), at *http://www.ftc.gov/os/2004/02/0402l7spywareworkshopfrn.pdf.*

[2] Patricia Moloney Figliola, Spyware: Background and Policy Issues for Congress, Congressional Research Service Report to Congress, at 4 (July 17, 2006); *see also* Pew Internet & American Life Project, *Spyware: The threat of unwanted software programs is changing the way peo-*

Continued

A difficulty in combating spyware 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 data about the user's preferences to make navigation of the site easier. A cookie typically is only accessible and active when the user is visiting that website.

Nevertheless, a cookie can be used for less benevolent purposes, such as intentionally targeting the user with ads, or tracking the user's visits to other web sites and communicating this information to the originating website upon a return visit. A cookie can also be used for even more malicious purposes, such as, to give a criminal access to a user's personal information so that the criminal can then defraud or otherwise harm the user.

Similarities in technological aspects of various cookies, yet differences in their use, exemplify why it is imperative to address the problem of spyware with appropriate care. The problem concerns the illegal use of the Internet and various codes, programs, and software, rather than particular technologies. Shortsighted regulatory approaches designed to stop spyware may unavoidably capture legitimate uses of technology. Accordingly, the Committee has concluded that the pernicious effects of spyware are most effectively addressed through defining prohibited criminal behavior, rather than regulating how technology is used and accessed by consumers.

H.R. 1525, the "Internet Spyware (I–SPY) Prevention Act of 2007," amends title 18 of the United States Code to clarify and enhance criminal penalties when spyware is used for the purpose of perpetrating identity theft and other privacy intrusions against innocent Internet users. Specifically, it prohibits an individual from intentionally accessing a protected computer without authorization, or exceeding authorized access, by causing a computer program or code to be copied onto the protected computer, and intentionally using that program or code: (1) in furtherance of another Federal criminal offense; (2) to obtain or transmit personal information (including a Social Security number or other Government-issued identification number, a bank or credit card number, or an associated password or access code) with intent to defraud or injure a person or cause damage to a protected computer; or (3) to impair the security protection of that computer.

H.R. 1525, in addition, addresses other types of fraudulent activities, such as online identity theft known as "phishing." Phishing refers to the artifice of using websites that closely emulate those of legitimate businesses or other entities. It also includes the use of e-mails that appear to be sent from legitimate businesses.[3] These fraudulent web sites and e-mails are designed to deceive Internet users into revealing personal information that can then be used to

---

ple use the Internet, at 3 (July 5, 2005), at *http://www.pewInternet.org/pdfs/PIP_SpywareReport_July_5.pdf (2005).*

[3] *See The Internet Spyware (I–SPY) Prevention Act of 2007: Hearing on H.R. 1525 Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary,* 110th Cong. (2007) (testimony of Representative Zoe Lofgren (D–CA)).

defraud these users.[4] While phishing is adequately addressed by existing Federal wire fraud or identity theft statues, additional funds are needed to prosecute the crime.[5] Pharming is a version of phishing that involves the fraudulent use of domain names. In pharming, hackers hijack a legitimate website's domain name, and redirect traffic intended for that website to their own. The computer user sees the intended website's address in the browser's address line, but instead, he or she is connected to the hacker's site and may unknowingly provide personal information to the hacker.[6]

To address these fraudulent activities, H.R. 1525 would authorize $10 million to be appropriated for each of fiscal years 2008 through 2011 to the Attorney General for prosecutions needed to discourage the unlawful use of spyware as well as phishing and pharming.

HEARINGS

The Committee's Subcommittee on Crime, Terrorism, and Homeland Security held 1 day of hearings on H.R. 1525 on May 1, 2007. Testimony was received from Representative Zoe Lofgren (D–CA) and Representative Bob Goodlatte (R–VA).

COMMITTEE CONSIDERATION

On May 2, 2007, the Committee met in open session and ordered the bill, H.R. 1525, favorably reported with an amendment, by voice vote, a quorum being present.

COMMITTEE VOTES

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that there were no recorded votes during the Committee's consideration of H.R. 1525.

COMMITTEE OVERSIGHT FINDINGS

In compliance with clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee advises 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.

---

[4] The Anti-Phishing Working Group, an industry organization, reported that in January 2007 alone there were 29,930 incidents of phishing reported. *See http://www.antiphishing.org.*

[5] Some forms of spyware-related behavior may arguably violate sections 1030 and 1037 of title 18 of the United States Code. There may, however, be insufficient emphasis upon, guidance to, and enforcement of such crimes by Federal prosecutors.

[6] *See* Marcia Smith, Internet Privacy: Overview and Legislation in the 109th Congress, Congressional Research Service Report for Congress (Jan. 26, 2006).

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. 1525, 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 17, 2007.

Hon. John Conyers, 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. 1525, the Internet Spyware (I–SPY) Prevention Act of 2007.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Mark Grabowicz (for federal costs), and Melissa Merrell (for the State and local impact).

Sincerely,

PETER R. ORSZAG,
Director.

Enclosure.

H.R. 1525—Internet Spyware (I–SPY) Prevention Act of 2007.

Summary: H.R. 1525 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 2008–2011 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 2008 and $40 million over the 2008–2012 period. CBO expects that enacting the bill would have an insignificant effect on federal revenues and direct spending.

H.R. 1525 contains an intergovernmental mandate as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates that any costs to State, local, and tribal governments would be minimal and would not exceed the threshold established in UMRA ($66 million in 2007, 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. 1525 is shown in the following table. The costs of this legislation fall within budget function 750 (administration of justice).

	By fiscal year, in millions of dollars—				
	2008	2009	2010	2011	2012
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 that the bill will be enacted near the start of the fiscal year 2008 and that the authorized amounts will be appropriated each year.

Enacting H.R. 1525 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. 1525 would prohibit States from creating civil penalties that specifically reference the federal statute. This prohibition would constitute a mandate as define in UMRA, but it is narrow and would not prohibit States from passing similar criminal and civil statutes. CBO estimates that any costs to State, local, or tribal governments would be minimal and would fall significantly below the threshold established in UMRA ($66 million in 2007, 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: Mark Grabowicz; Impact on state, local, and tribal governments: Melissa Merrell; 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. 1525 enhances existing fraud and computer crime law with strong criminal penalties targeting egregious abuses perpetrated upon Internet users by persons who use spyware, and provides additional resources to combat spyware and 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 3 of the Constitution.

ADVISORY ON EARMARKS

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 1525 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9(d), 9(e), or 9(t) of rule XXI.

SECTION-BY-SECTION ANALYSIS

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

Sec. 1. Short title

Section 1 sets forth the short title of the bill as the "Internet Spyware (I–SPY) Prevention Act of 2007."

Sec. 2. Penalties for certain unauthorized activities relating to computers.

Section 2 establishes new criminal offenses and penalties for certain types of spyware activity. It amends title 18 of the United States Code to add a new provision, section 1030A. New section 1030A makes it a crime to intentionally access a protected computer without authorization or to exceed authorized access by causing a computer program or code to be copied onto the protected computer. It should be noted that section 1030A is not intended to supersede or displace sections 1030 and 1037 of title 18, nor is it intended to limit in any respect the ability of prosecutors to continue bringing actions for spyware- or phishing-related crimes under these or other existing statutes.

Section 1030A(a) provides that anyone who uses that program or code in furtherance of another Federal criminal offense shall be fined under title 18 or imprisoned for up to 5 years, or both.

Section 1030A(b) authorizes the imposition of fines under title 18 or imprisonment up to 2 years, or both, for anyone who by means of such 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.

Section 1030A(c) provides that 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 violation of this section. This provision does not preempt cases brought in State court based on independent State law causes of action, nor is the provision intended to preempt existing or future State laws that may prohibit conduct similar or identical to the conduct prohibited in the Act. The provision simply provides that violation of the Act itself cannot supply the basis for a State civil action. As some States permit civil tort actions premised on a violation of Federal criminal statutes, the Committee believes the clarifying language of section 1030A(c) is necessary. In addition, because much of the power and promise of the Internet comes from its ability to transcend geographic and political boundaries, it is important to avoid having Internet commerce become mired in potentially inconsistent State application of Federal law. Section 1030A(c) ensures that this does not happen.

Section 1030A(d) defines certain terms used in this section. The terms "protected computer" and "exceeds authorized access" have the same meanings as set forth in section 1030 of title 18. The term "personal information" means: (1) a first and last name; (2) a home or other physical address, including street name; (3) an electronic mail address; (4) a telephone number; (5) a Social Security number, tax ID number, driver's license number, passport number, or any other Government-issued identification number; or (6) 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) of the Act makes a conforming amendment to the table of sections in title 18 of the United States Code.

Sec. 3. Authorization of appropriations

Section 3 authorizes $10 million to be appropriated for each of fiscal years 2008 through 2011 to the Attorney General for prosecutions needed to discourage the use of spyware as well as phishing and pharming.

Sec. 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 utilize 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 with the intent to defraud or injure a person or damage a 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.

* * * * * * *

○