In the context of discussing H.R. 3632, I cited a situation in Texas in which a crime ring was implicated for the import of over 100 million counterfeit cigarettes by mislabeling shipping documents and indicating that they were importing toys or plastic parts. That crime threatened the copyright royalties of property owners.

However, this legislation extrapolates that aspect of criminal activity by inserting the possibility that unsafe products as well as counterfeit products could be circulated in the flow of interstate commerce.

Last year, U.S. Immigration and Customs Enforcement officials seized fake goods valued at $22 million in the Houston area alone. Federal inspectors now work to curtail the flow of fake Louis Vuitton and Coach handbags and other items coming from Houston, which lags behind only New York and Los Angeles in supplying counterfeit products to the rest of the nation. Furthermore, during Super Bowl XXXVIII that was held in Houston this past year, NFL investigators seized about 1,000 counterfeit products in Houston that were peddled by two vendors.

Therefore, the subject matter of this bill is of great importance to me. This bill is largely bipartisan; however, we have a duty to ensure that its provisions are narrowly tailored before passing them into law.

At the Committee level, I had questions regarding the intended scope of search and seizure law and how H.R. 32 proposes to change it. One question that I posed relates to the property forfeiture provision found on page 3, line 21 of the bill as drafted. Subparagraphs (A) and (B) are conjunctive so as to require both findings before a forfeiture would follow—how proposes to prevent law enforcement from seizing the property of an innocent person (assuming it is in possession or use by the perpetrator of the underlying offense). I hope that this legislation is clear in its provisions to jurists in order to prevent future appellate litigation that can be both costly and time consuming—to the detriment of bona fide claimants.

Another question I posed goes to the matter of restitution. Section 2, page 4, lines 15–16 would require one convicted of the offense in question to pay restitution damages to the ''victim'' as defined in Title 18, Section 3663(A)(2):

a person directly and *proximately harmed* as a result of the commission of an offense for which restitution may be ordered including, in the case of an offense that involves as an element a scheme, conspiracy, or pattern of criminal activity, any person directly harmed by the defendant's criminal conduct in the course of the scheme, conspiracy, or pattern.

(emphasis added). I queried whether the drafter of this bill contemplate those proximately harmed by the perpetration of the crimes enumerated to include state governments. As I cited earlier in my statement, criminals trafficked over 1,000 counterfeit products in the stream of commerce and caused the State of Texas, among others, to lose significant revenues.

I believe that H.R. 32 can provide much needed legislative protection of the American consumer and of the owners of intellectual and licensed property.

Ms. ZOE LOFGREN of California. Mr. Speaker, I yield back the balance of my time.

Mr. SENSENBRENNER. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. RADANOVICH). The question is on the motion offered by the gentleman from Wisconsin (Mr. SENSENBRENNER) that the House suspend the rules and pass the bill, H.R. 32, as amended.

The question was taken; and (two-thirds having voted in favor thereof) the rules were suspended and the bill, as amended, was passed.

A motion to reconsider was laid on the table.

## INTERNET SPYWARE (I–SPY) PREVENTION ACT OF 2005

Mr. SENSENBRENNER. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 744) to amend title 18, United States Code, to discourage spyware, and for other purposes, as amended.

The Clerk read as follows:

H.R. 744

*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, 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) CONFORMING AMENDMENT.—The table of sections at the beginning of chapter 47 of title 18, 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 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.

The SPEAKER pro tempore. Pursuant to the rule, the gentleman from Wisconsin (Mr. SENSENBRENNER) and the gentlewoman from California (Ms. ZOE LOFGREN) each will control 20 minutes.

The Chair recognizes the gentleman from Wisconsin (Mr. SENSENBRENNER).

GENERAL LEAVE

Mr. SENSENBRENNER. Mr. Speaker, I ask unanimous consent that all Members may have 5 legislative days within which to revise and extend their remarks and include extraneous material on H.R. 744, the bill currently under consideration.

The SPEAKER pro tempore. Is there objection to the request of the gentleman from Wisconsin?

There was no objection.

Mr. SENSENBRENNER. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I rise today in support of H.R. 744, the Internet Spyware Prevention Act of 2005. This legislation clarifies and enhances criminal penalties and provides additional tools to prosecute and deter those who utilize spyware and phishing schemes to engage in illegal behavior online.

Since its inception, the Internet has been transformed from an obscure research tool into an electronic medium of unprecedented reach. The impressive growth of the Internet has been facilitated by technology that has customized the online experience of Internet users. However, the same software and technology innovations that have enhanced and personalized usage of the Internet can also provide opportunities for privacy violations and criminal behavior.

This bill establishes strong criminal penalties for those who engage in online criminal behavior using spyware programs and phishing schemes. This legislation enhances criminal penalties for those who obtain personally identifiable information, including a Social Security number or other government-issued identification number or a bank or credit card number with the intent to defraud or injure a person or cause damage to a protected computer.

The bill also authorizes appropriations for the Justice Department to crack down on spyware, phishing, and other online schemes.

As we consider this legislation, Congress must be mindful that there is no single legal regulatory or technological silver bullet to end spyware or phishing. Greater consumer awareness and utilization of commercially available countermeasures are part of the solution. Congressional efforts to curb spyware and phishing are most likely to succeed if we focus on deterring and prosecuting illegal and abusive online behavior, rather than imposing burdensome requirements upon a medium whose growth can largely be attributed to the refusal of the Federal Government to heavily regulate it.

H.R. 744 does not impose a new statutory or regulatory regime that dictates the appearance of a computer's user screen, nor does it degrade the online experience by requiring that Internet users be bombarded with incessant notices. Most importantly, it does not represent a heavy-handed government mandate that may present a greater danger to the Internet than it seeks to correct. Rather, the bill preserves and promotes the integrity of the Internet by increasing criminal penalties for those who employ it to engage in abusive and illegal online activities.

Targeted legislation tailored to address illegal online activity rather than an invasive regulatory regime with unknown consequences represents the right approach to addressing the problems associated with spyware and phishing. Congress ratified this approach by passing substantially similar legislation last Congress by a vote of 415–0.

I would like to thank the gentleman from Virginia (Mr. GOODLATTE), the author and lead proponent of H.R. 744 for his leadership on this issue. I urge my colleagues to support this legislation.

Mr. Speaker, I reserve the balance of my time.

Ms. ZOE LOFGREN of California. Mr. Speaker, I yield myself such time as I may consume.

Mr. Speaker, I am proud to have partnered with the gentleman from Virginia (Mr. GOODLATTE) on this legislation, H.R. 744, the Goodlatte-Lofgren I–SPY bill. Spyware is quickly becoming one of the biggest threats to consumers on the Internet. It is one of the reasons why we have an identity theft epidemic in this country. Thieves are using spyware to harvest personal information from unsuspecting Americans. Criminals are even using spyware to track every keystroke an individual makes, including credit and Social Security numbers.

Spyware also adversely affects the business community, who are forced to spend money to block and remove it from their systems. In fact, Microsoft has stated that spyware is at least partially responsible for approximately one-half of all application crashes reported to them. Experts estimate that as many as 80 to 90 percent of all personal computers contain some form of spyware.

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. I am proud to be a party to H.R. 744, this bipartisan measure, because it identifies the truly unscrupulous acts associated with spyware and subjects them to criminal punishment.

This bill is unique, however, because it focuses on behavior rather than technology. It targets the worst forms of spyware without unduly burdening technological innovation. Why is this important? We know that innovation goes faster than legislation. It is important that we not try to fix the development of legislation in time. Instead, we need to focus on misbehavior, not technology, so that technology innovation can continue to move as rapidly as it does and yet the American consumer and businesses can be protected.

It is important, and this is an issue that there was some question about and I think we can answer quite easily, it is important to note that H.R. 744 does not prevent existing or future State laws which prohibit spyware. This bill only preempts civil actions that are based on violations of this new Federal criminal law in State courts. It does not prevent a State from passing a similar law, nor does it prevent any lawsuits that are premised on existing State laws.

□ 1430

H.R. 744 also gives the Attorney General the money he needs to find and prosecute spyware offenders. And, finally, it expresses the sense of Congress that the Department of Justice should vigorously pursue online phishing scams in which criminals send fake e-mail messages to consumers on behalf of famous companies and request personal information that is later used to conduct criminal activities.

Phishing and spyware are not just an inconvenience to consumers. They represent a direct threat to the vitality of the Internet itself because if people cannot trust the Internet, they will not utilize Internet commerce.

I would like to note that I also serve on the Committee on Homeland Security, and we are well aware that phishing to the extent that it yields identity theft information is of great concern as we seek to protect the Nation from terrorism. So what we are doing here today is important for consumers, it is important for business, it is important for the future of our high-tech economy, and it is important for the security of the Nation. I would urge my colleagues to strike a blow for the continued vitality of the Internet and again pass this bill unanimously.

Mr. Speaker, I reserve the balance of my time.

Mr. SENSENBRENNER. Mr. Speaker, I yield 4 minutes to the gentleman from Virginia (Mr. GOODLATTE), the principal author of the bill.

Mr. GOODLATTE. Mr. Speaker, I rise in strong support of the Internet Spyware I–SPY Prevention Act and thank the gentleman from Wisconsin, the chairman of the committee, for moving this legislation to the floor. This bipartisan legislation which I was pleased to introduce with the gentlewoman from California (Ms. ZOE LOFGREN) 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.

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.

In addition to strong penalties, enforcement is crucial in combating spyware. The I–SPY Prevention Act authorizes $10 million for fiscal years 2006

through 2009 to be devoted to prosecutions and expresses the sense of Congress that the Department of Justice should vigorously enforce the law against spyware violations as well as against online phishing scams in which criminals send fake e-mail messages to consumers on behalf of well-known companies and request account information that is later used to conduct criminal activities.

The bill also directs resources to the Department of Justice to combat pharming scams in which hackers intercept Internet traffic and redirect unknowing Internet users to fake Web sites where they often trick consumers into giving their account information and passwords.

I believe that four overarching principles should guide the consideration 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; and, fourth, we must target the behavior, not the technology.

The targeted approach of the I–SPY Prevention Act will protect consumers by punishing the bad actors without imposing liability on those that act legitimately online. In addition, this legislation will avoid excessive regulation such as one-size-fits-all notice and consent requirements prescribed by the Federal Government. A targeted approach will avoid red tape that hampers the creation of new and exciting 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. Increasingly, consumers want a seamless interaction with the Internet, and we must be careful to not interfere with businesses' ability to respond to this consumer demand with 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.

As we move forward, I look forward to continuing to work with all stakeholders to further ensure that bad actors are punished while legitimate businesses are protected including working with the Department of Justice which has expressed an interest in working with our office on this issue. In addition, technological solutions are crucial in winning the fight against spyware. As the spyware debate continues, I look forward to working to ensure that antispyware technologies are fostered and that they are not subjected to frivolous lawsuits from spyware providers.

I urge my colleagues to support this important legislation.

Ms. ZOE LOFGREN of California. Mr. Speaker, I yield myself such time as I may consume.

I would just note that the House will be considering at least two items having to do with spamming and phishing and the like today. Certainly we hope to move this issue forward. I strongly believe that the approach that this bill takes, which is targeting behavior instead of technology, puts us on the soundest footing; and I hope that in the end as we sort through the various approaches that that will be our guide to protect technology innovation.

Ms. JACKSON-LEE of Texas. Mr. Speaker, I support the legislation before us that has been introduced by my colleague from California, Representative LOFGREN as well as the Gentleman from Virginia, Representative GOODLATTE. It amends the federal computer fraud and abuse statute to make it a clear offense to access a computer without authorization or to intentionally exceed authorized access by causing a computer program or code to be copied onto the computer and using that program or code to transmit or obtain personal information (for example, first and last names, addresses, e-mail addresses, telephone numbers, Social Security numbers, drivers license numbers, or bank or credit account numbers).

Furthermore, H.R. 744 authorizes appropriations for these crimes and discourages the practice of 'phishing.' As we all know too well, spyware is quickly becoming one of the biggest threats to consumers on the information superhighway. Spyware encompasses several potential risks including the promotion of identity theft by harvesting personal information from consumer's computers. Additionally, it can adversely affect businesses, as they are forced to sustain costs to block and remove spyware from employees' computers, in addition to the potential impact on productivity.

Spyware has been defined as ''software that aids in gathering information about a person or organization without their knowledge and which may send such information to another entity with the consumer's consent, or asserts control over a computer with the consumer's knowledge.'' Among other things, criminals can use spyware to track every keystroke an individual makes, including credit card and social security numbers.

Some estimates suggest 25 percent of all personal computers contain some kind of spyware while other estimates show that spyware afflicts as many as 80–90 percent of all personal computers. Businesses are reporting several negative effects of spyware. Microsoft says evidence shows that spyware is ''at least partially responsible for approximately one-half of all application crashes'' reported to them, resulting in millions of dollars of unnecessary support calls.

Mr. Speaker, again, I am strongly in support of the legislation.

Ms. ZOE LOFGREN of California. Mr. Speaker, I yield back the balance of my time.

Mr. SENSENBRENNER. Mr. Speaker, I yield back the balance of my time.

The SPEAKER pro tempore (Mr. RADANOVICH). The question is on the motion offered by the gentleman from Wisconsin (Mr. SENSENBRENNER) that the House suspend the rules and pass the bill, H.R. 744, as amended.

The question was taken.

The SPEAKER pro tempore. In the opinion of the Chair, two-thirds of those present have voted in the affirmative.

Mr. SENSENBRENNER. Mr. Speaker, on that I demand the yeas and nays.

The yeas and nays were ordered.

The SPEAKER pro tempore. Pursuant to clause 8 of rule XX and the Chair's prior announcement, further proceedings on this motion will be postponed.

## SECURELY PROTECT YOURSELF AGAINST CYBER TRESPASS ACT

Mr. BARTON of Texas. Mr. Speaker, I move to suspend the rules and pass the bill (H.R. 29) to protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes, as amended.

The Clerk read as follows:

H.R. 29

*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 ''Securely Protect Yourself Against Cyber Trespass Act'' or the ''Spy Act''.

**SEC. 2. PROHIBITION OF [UNFAIR OR] DECEPTIVE ACTS OR PRACTICES RELATING TO SPYWARE.**

(a) PROHIBITION.—It is unlawful for any person, who is not the owner or authorized user of a protected computer, to engage in unfair or deceptive acts or practices that involve any of the following conduct with respect to the protected computer:

(1) Taking control of the computer by—

(A) utilizing such computer to send unsolicited information or material from the computer to others;

(B) diverting the Internet browser of the computer, or similar program of the computer used to access and navigate the Internet—

(i) without authorization of the owner or authorized user of the computer; and

(ii) away from the site the user intended to view, to one or more other Web pages, such that the user is prevented from viewing the content at the intended Web page, unless such diverting is otherwise authorized;

(C) accessing, hijacking, or otherwise using the modem, or Internet connection or service, for the computer and thereby causing damage to the computer or causing the owner or authorized user or a third party defrauded by such conduct to incur charges or other costs for a service that is not authorized by such owner or authorized user;

(D) using the computer as part of an activity performed by a group of computers that causes damage to another computer; or

(E) delivering advertisements that a user of the computer cannot close without undue effort or knowledge by the user or without turning off the computer or closing all sessions of the Internet browser for the computer.

(2) Modifying settings related to use of the computer or to the computer's access to or use of the Internet by altering—

(A) the Web page that appears when the owner or authorized user launches an Internet browser or similar program used to access and navigate the Internet;

(B) the default provider used to access or search the Internet, or other existing Internet connections settings;

(C) a list of bookmarks used by the computer to access Web pages; or

(D) security or other settings of the computer that protect information about the owner or authorized user for the purposes of