109TH CONGRESS } HOUSE OF REPRESENTATIVES { REPORT
2d Session } { 109–395

LAW ENFORCEMENT AND PHONE PRIVACY PROTECTION ACT OF 2006

MARCH 16, 2006.—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. 4709]

[Including cost estimate of the Congressional Budget Office]

The Committee on the Judiciary, to whom was referred the bill (H.R. 4709) to amend title 18, United States Code, to strengthen protections for law enforcement officers and the public by providing criminal penalties for the fraudulent acquisition or unauthorized disclosure of phone records, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

	Page
The Amendment	1
Purpose and Summary	1
Background and Need for Legislation	2
Hearings	3
Committee Consideration.	3
Vote of the Committee	3
Committee Oversight Findings	3
New Budget Authority and Tax Expenditures	4
Congressional Budget Office Cost Estimate	4
Performance Goals and Objectives	5
Constitutional Authority Statement	5
Section-by-Section Analysis and Discussion	5
Changes in Existing Law Made by the Bill, as Reported	6

PURPOSE AND SUMMARY

The purpose of H.R. 4709, the "Law Enforcement and Phone Privacy Protection Act of 2006" is to provide explicit protection for the privacy of confidential telephone records, including call logs, and to

establish specific criminal penalties for the fraudulent acquisition or disclosure of such records without the consent of the consumer.

The bill targets "pretexting" and other fraudulent tactics by unscrupulous businesses that operate in a gray area of the law. It prohibits unauthorized access or trafficking in confidential phone records. The bill also provides enhanced criminal penalties for anyone who engages in large-scale operations to violate its provisions or who discloses or uses such fraudulently obtained records in furtherance of crimes of violence, including domestic violence and stalking, or to kill, injure, or intimidate a witness, juror, confidential informant, or law enforcement officer.

BACKGROUND AND NEED FOR THE LEGISLATION

Recent investigations by law enforcement authorities, including the Chicago Police Department and the Federal Bureau of Investigation (FBI), and numerous media reports have documented the ease with which any party, without proper authorization, may obtain the confidential calling records of consumers.[1] Services that operate under a variety of names have advertised the ability to retrieve the recent calling history of any telephone number, often within a matter of hours, to anyone willing to pay a fee of approximately $100.[2] Many of these companies have operated on the Internet, but some experts believe there may be thousands of other companies and investigators who provide this service that have not been subject to public and media scrutiny.[3] These companies typically do not inquire about the customers' reason for seeking confidential calling records. In addition, these enterprises often only request readily available public information such as the name and telephone number of the person whose records their customer wishes to obtain.[4]

The Committee is aware of reports that many of these services employ a variety of fraudulent schemes and devices to obtain these records.[5] More often than not, these frauds are perpetrated directly on phone service providers, whose business operations require them to maintain detailed individual calling records and who need to be able to respond in a timely manner to legitimate consumer requests for the release of their own personal account information.[6] Experts believe the most common method of obtaining these records from telephone companies is the practice of "pretexting." Pretexting occurs when an unauthorized individual calls the phone company posing as someone who is authorized to receive the information lawfully, such as the actual phone service subscriber or another employee of the target phone company.[7]

---

[1] Frank Main, Anyone Can Buy Cell Phone Records: Online Services Raise Security Concerns for Law Enforcement, Chi. Sun-Times, January 5, 2006, at A3.

[2] Frank Main, Foreign Internet Services Selling U.S. Phone Records: Congress Bids to Make it Illegal Because of Privacy Concerns, Chi. Sun-Times, February 9, 2006, at A6.

[3] Jonathan Krim, Online Data Gets Personal: Cell Phone Records for Sale, Wash. Post, July 13, 2005, at B1.

[4] Id.

[5] Sheryl Harris, Your Private Data Fuels Entire Online Industry, Clev. Pl. Dealer, March 9, 2006, at C1.

[6] Dave Gussow, Verizon Lawsuit Says Phony Callers Are Committing Fraud, St. Pete. Times, January 30, 2006, at 1D.

[7] Id.

Once in possession of these private consumer calling records, these services, which some have dubbed "data bandits,"[8] deliver them, often by e-mail or fax to their customer with no concern for how the information will be used.[9] By scrutinizing the records of whom one chooses to call and for how long one converses, criminals and unscrupulous individuals can obtain a great deal of useful and potentially sensitive personal information. A careful examination of these records can reveal much about a person's business and personal relationships, including details that may involve their medical, financial, professional, or family life. In some instances, calling records may even be used to identify the physical location of the caller. This raises particular concerns for undercover law enforcement officers, and victims of stalking and domestic violence.

Armed with this knowledge and alarmed at the widespread availability and easy accessibility of these records, the Chicago Police Department and the FBI have reportedly warned their personnel to take steps to safeguard their personal information, including their home and cell phone numbers.[10] Law enforcement officials are particularly troubled by the potential danger that these activities pose to undercover operatives and confidential informants.[11] Law enforcement investigations and the lack of any identifiable prosecutions for this fraudulent conduct under existing Federal criminal statutes have clearly demonstrated the need to move expeditiously to enact an explicit Federal criminal statute that prohibits the fraudulent acquisition or transfer of confidential personal calling records. The Committee considers this legislation to be urgently needed to preserve consumers privacy rights and to protect the personal safety of domestic violence victims, confidential informants, witnesses, jurors, and law enforcement personnel.

HEARINGS

The House Committee on the Judiciary held no hearings on H.R. 4709.

COMMITTEE CONSIDERATION

On March 2, 2006, the Committee met in open session and ordered favorably reported the bill H.R. 4709 without an amendment by 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. 4709.

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 Rep-

[8] Patricia Sabatini, Calling for Privacy, Pitt. Post-Gaz., January 22, 2006, at D1.
[9] Peter Sensson, Call May Be Private, But Record of It Isn't, Char. Obs., January 19, 2006, at 1D.
[10] Main, Anyone Can Buy Cell Phone Records, supra note 1.
[11] Id.

resentatives, are incorporated in the descriptive portions of this report.

NEW BUDGET AUTHORITY AND TAX EXPENDITURES

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

CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

In compliance with clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the Committee sets forth, with respect to the bill, H.R. 4709, the following estimate and comparison prepared by the Director of the Congressional Budget Office under section 402 of the Congressional Budget Act of 1974:

MARCH 16, 2006.

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. 4709, the Law Enforcement and Phone Privacy Protection Act of 2006.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Melissa Z. Petersen.

Sincerely,

DONALD B. MARRON, *Acting Director.*

Enclosure.

H.R. 4709—Law Enforcement and Phone Privacy Protection Act of 2006

CBO estimates that implementing H.R. 4709 would not have a significant cost to the federal government. Enacting the bill could affect direct spending and revenues, but CBO estimates that any such effects would not be significant. H.R. 4709 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

H.R. 4709 would establish a new federal crime for fraudulently obtaining, purchasing, or selling confidential phone records. The bill also would specify enhanced penalties for using such records to commit a crime. Because the bill would establish a new offense, the government would be able to pursue cases that it otherwise would not be able to prosecute. We expect that H.R. 4709 would apply to a relatively small number of offenders, however, so any increase in costs for law enforcement, court proceedings, or prison operations would not be significant. Any such costs would be subject to the availability of appropriated funds.

Because those prosecuted and convicted under H.R. 4709 could be subject to criminal fines, the federal government might collect additional fines if the legislation is enacted. Criminal fines are recorded in the budget as revenues, deposited in the Crime Victims Fund, and later spent. CBO expects that any additional revenues and direct spending would not be significant because of the small number of cases likely to be affected.

On March 9, 2006, CBO transmitted a cost estimate for S. 2178, the Consumer Telephone Records Protection Act of 2006, as reported by the Senate Committee on the Judiciary on March 2, 2006. The two pieces of legislation are similar, and our cost estimates are the same.

The CBO staff contact for this estimate is Melissa Z. Petersen. This estimate was 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. 4709 will help to provide additional protections for confidential phone records information.

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 art. I, § 8 of the Constitution.

SECTION-BY-SECTION ANALYSIS AND DISCUSSION

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

Section 1. Short title

This section establishes the short title of this legislation as the "Law Enforcement and Phone Privacy Protection Act of 2006."

Sec. 2. Findings

This section makes various findings with regard to the need and purpose of the legislation.

Sec. 3. Fraud and related activity in connection with obtaining confidential phone records information of a covered entity

This provision adds a new 18 U.S.C. § 1039 that provides explicit criminal penalties for fraudulently obtaining or providing confidential phone records information of a consumer held by a telephone company or IP-enabled voice service.

Specifically, the legislation would make it a crime to knowingly and intentionally obtain, or attempt to obtain, confidential phone records of a company that provides telephone service (a "covered entity") using a fraudulent scheme or device, including "pretexting," or without authorization from the customer via the Internet. A person convicted under this section would be subject to a fine up to $250,000 (individuals) or $500,000 (organizations), or imprisonment up to 20 years, or both.

In addition to creating a crime for obtaining confidential information of a covered entity by fraud, the legislation criminalizes the sale, transfer, or attempts to sell or transfer, such records without authorization, allowing fines up to $250,000 (individuals) or $500,000 (organizations), imprisonment up to five years, or both. This provision is intended to act as a deterrent for those who are in a position that requires access to this type of information from taking advantage of such access to compromise the private infor-

mation of consumers. The legislation also includes criminal penalties for individuals who purchase confidential phone records information knowing the records were obtained without authorization. This provision allows for a fine up to $250,000 (individuals) or $500,000 (organizations) and imprisonment up to five years, or both.

In addition to the penalties for the underlying crimes, the legislation allows for enhanced penalties for cases in which the information is used to commit further crimes, is used to further a crime of violence, or causes substantial financial harm. Specifically, it allows a judge to add up to five years and up to one million dollars in fines to a sentence for violations of this act while violating another U.S. law or as part of a pattern of illegal activity that meets specified thresholds. Additionally, anyone who violates or attempts to violate any of the provisions of this Act in connection with either a Federal crime of domestic violence or crimes that relate to the safety of law enforcement officers, their families, or persons involved in the judicial process, may be fined up to an additional $250,000 (individuals) or $500,000 (organizations), imprisoned up to an additional 5 years, or both.

This section makes it clear that the Committee intends for the law to apply to offenses that occur beyond U.S. territorial and maritime borders. The Committee recognizes that many of the companies may operate overseas; however, if these companies are in violation of this law and the result harms U.S. citizens, they should be prosecuted under U.S. laws.

This section makes it clear that nothing in the Act is to be construed to impede compliance with a lawful request by a law enforcement agency to produce such records. It is the view of this Committee that this provision is not intended to prohibit any lawfully authorized investigative, protective or intelligence activity of a law enforcement or intelligence agency.

Finally, this section provides definitions that are intended to apply only to the activities specified in this Act and should not be construed to affect other laws or statutes. The intent of H.R. 4709 is to prevent unauthorized or fraudulent use of consumer telephone records. The Committee does not intend that H.R. 4709 be construed to prevent legitimate, legally authorized use of such information by covered entities for business purposes. For purposes of this bill, the Committee intends that the exceptions contained in 47 U.S.C. 222(d) apply to uses of information by both telecommunications carriers and Internet Protocol-enabled voice service providers.

Sec. 4. Sentencing guidelines

This section requires the United States Sentencing Commission to review and, if appropriate, amend the Federal sentencing guidelines and policy statements that will apply to any persons convicted under 18 U.S.C. § 1039 18 not later than 180 days after date of enactment.

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, 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

* * * * * * *

§ 1039. Fraud and related activity in connection with obtaining confidential phone records information of a covered entity

(a) CRIMINAL VIOLATION.—Whoever knowingly and intentionally obtains, or attempts to obtain, confidential phone records information of a covered entity, by—

(1) making false or fraudulent statements or representations to an employee of a covered entity;

(2) making such false or fraudulent statements or representations to a customer of a covered entity;

(3) providing a document to a covered entity knowing that such document is false or fraudulent; or

(4) accessing customer accounts of a covered entity via the Internet without prior authorization from the customer to whom such confidential records information relates;

shall be fined under this title, imprisoned for not more than 20 years, or both.

(b) PROHIBITION ON SALE OR TRANSFER OF CONFIDENTIAL PHONE RECORDS INFORMATION.—Except as otherwise provided by applicable law, any person, including any employee of a covered entity or any data broker, who knowingly and intentionally sells, transfers, or attempts to sell or transfer, confidential phone records information of a covered entity, without authorization from the customer to whom such confidential phone records information relates, shall be fined under this title, imprisoned for not more than 5 years, or both.

(c) PROHIBITION ON PURCHASE OF PHONE RECORDS INFORMATION.—Except as otherwise provided by applicable law, any person who purchases confidential phone records information of a covered entity, knowing such information was obtained fraudulently or without prior authorization from the customer to whom such confidential records information relates, shall be fined under this title, imprisoned not more than 5 years, or both.

(d) ENHANCED PENALTIES FOR AGGRAVATED CASES.—Whoever violates, or attempts to violate, subsection (a) while violating another law of the United States or as part of a pattern of any illegal activity involving more than $100,000, or more than 50 customers of a covered entity, in a 12-month period shall, in addition to the penalties provided for in subsection (a), be fined twice the amount provided in subsection (b)(3) or (c)(3) (as the case may be) of section 3571 of this title, imprisoned for not more than 5 years, or both.

(e) ENHANCED PENALTIES FOR USE OF INFORMATION IN FURTHERANCE OF CERTAIN CRIMINAL OFFENSES.—

(1) Whoever, violates, or attempts to violate, subsection (a), (b), or (c) knowing that such information may be used in furtherance of, or with the intent to commit, an offense described in section 2261, 2261A, 2262, or any other crime of violence shall, in addition to the penalties provided for in subsection (a), (b), or (c), be fined under this title and imprisoned not more than 5 years.

(2) Whoever, violates, or attempts to violate, subsection (a), (b), or (c) knowing that such information may be used in furtherance of, or with the intent to commit, an offense under section 111, 115, 1114, 1503, 1512, 1513, or to intimidate, threaten, harass, injure, or kill any Federal, State, or local law enforcement officer shall, in addition to the penalties provided for in subsection (a), (b) or (c), be fined under this title and imprisoned not more than 5 years.

(f) EXTRATERRITORIAL JURISDICTION.—There is extraterritorrial jurisdiction over an offense under this section.

(g) NONAPPLICABILITY TO LAW ENFORCEMENT AGENCIES.—Nothing in this Act shall be construed to prevent, hinder, or otherwise delay the production of confidential phone records information from a covered entity upon receipt of a lawful request from a law enforcement agency, or any officer, employee, or agent of such agency, in accordance with other applicable laws.

(h) DEFINITIONS.—In this section:

(1) CONFIDENTIAL PHONE RECORDS INFORMATION.—The term "confidential phone records information" means—

(A) information that—

(i) relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity subscribed to by any customer of that covered entity; and

(ii) is made available to a covered entity by a customer solely by virtue of the relationship between the covered entity and the customer; or

(B) information contained in any bill, itemization, or account statement related to a product or service provided by a covered entity to any customer of the covered entity.

(2) COVERED ENTITY.—The term "covered entity"—

(A) has the same meaning given the term "telecommunications carrier" in section 3 of the Communications Act of 1934 (47 U.S.C. 153); and

(B) includes any provider of IP-enabled voice service.

(3) CUSTOMER.—The term "customer" means, with respect to a covered entity, any individual, partnership, association, joint stock company, trust, or corporation, or authorized representative of such customer, to whom the covered entity provides a product or service.

(4) IP-ENABLED VOICE SERVICE.—The term "IP-enabled voice service" means the provision of real-time 2-way voice communications offered to the public, or such class of users as to be effectively available to the public, transmitted through customer premises equipment using TCP/IP protocol, or a successor protocol, for a fee (whether part of a bundle of services or sepa-

rately) with 2-way interconnection capability such that the service can originate traffic to, and terminate traffic from, a public switched telephone network.

* * * * * * *

MARKUP TRANSCRIPT

BUSINESS MEETING

THURSDAY, MARCH 2, 2005

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

The Committee met, pursuant to notice, at 10:00 a.m., in Room 2141, Rayburn House Office Building, the Honorable F. James Sensenbrenner, Jr. (Chairman of the Committee) presiding.

[Intervening business.]

Chairman SENSENBRENNER. Pursuant to notice, I now call up the bill H.R. 4709, the "Law Enforcement and Phone Privacy Protection Act of 2006," 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. 4709, follows:]

I

109TH CONGRESS
2D SESSION

H. R. 4709

To amend title 18, United States Code, to strengthen protections for law enforcement officers and the public by providing criminal penalties for the fraudulent acquisition or unauthorized disclosure of phone records.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 8, 2006

Mr. SMITH of Texas (for himself, Mr. CONYERS, Mr. GOODLATTE, Mr. SCOTT of Virginia, Mr. CANNON, Ms. ZOE LOFGREN of California, Mr. WILSON of South Carolina, Ms. HERSETH, and Mr. REICHERT) introduced the following bill; which was referred to the Committee on the Judiciary

---

A BILL

To amend title 18, United States Code, to strengthen protections for law enforcement officers and the public by providing criminal penalties for the fraudulent acquisition or unauthorized disclosure of phone records.

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 ''Law Enforcement and Phone Privacy Protection Act of 2006''.

SEC. 2. FINDINGS.

Congress finds that—

(1) telephone records can be of great use to criminals because the information contained in call logs may include a wealth of personal data;

(2) call logs may reveal the names of telephone users' doctors, public and private relationships, business associates, and more;

(3) call logs are typically maintained for the exclusive use of phone companies, their authorized agents, and authorized consumers;

(4) telephone records have been obtained without the knowledge or consent of consumers through the use of a number of fraudulent methods and devices that include but are not limited to—

(A) telephone company employees selling data to unauthorized data brokers;

(B) ''pretexting'', whereby a data broker or other person represents they are an authorized consumer and convinces an agent of the telephone company to release the data; or

(C) gaining unauthorized Internet access to account data by improperly activating a consumer's account management features on a phone company's webpage or contracting with an Internet-based data broker who trafficks in such records; and

(5) the unauthorized disclosure of telephone records not only assaults individual privacy but, in some instances, may further acts of domestic violence, compromise the personal safety of law enforcement officers, their families, or confidential informants, and undermine the integrity of law enforcement investigations.

SEC. 3. FRAUD AND RELATED ACTIVITY IN CONNECTION WITH OBTAINING CONFIDENTIAL PHONE RECORDS INFORMATION OF A COVERED ENTITY.

Chapter 47 of title 18, United States Code, is amended by inserting after section 1038 the following:

"§ 1039. Fraud and related activity in connection with obtaining confidential phone records information of a covered entity

''(a) CRIMINAL VIOLATION.—Whoever knowingly and intentionally obtains, or attempts to obtain, confidential phone records information of a covered entity, by—

''(1) making false or fraudulent statements or representations to an employee of a covered entity;

''(2) making such false or fraudulent statements or representations to a customer of a covered entity;

"(3) providing a document to a covered entity knowing that such document is false or fraudulent; or

"(4) accessing customer accounts of a covered entity via the Internet without prior authorization from the customer to whom such confidential records information relates;

shall be fined under this title, imprisoned for not more than 20 years, or both.

"(b) PROHIBITION ON SALE OR TRANSFER OF CONFIDENTIAL PHONE RECORDS INFORMATION.—Except as otherwise provided by applicable law, any person, including any employee of a covered entity or any data broker, who knowingly and intentionally sells, transfers, or attempts to sell or transfer, confidential phone records information of a covered entity, without authorization from the customer to whom such confidential phone records information relates, shall be fined under this title, imprisoned for not more than 5 years, or both.

"(c) PROHIBITION ON PURCHASE OF PHONE RECORDS INFORMATION.—Except as otherwise provided by applicable law, any person who purchases confidential phone records information of a covered entity, knowing such information was obtained fraudulently or without prior authorization from the customer to whom such con-

fidential records information relates, shall be fined under this title, imprisoned not more than 5 years, or both.

''(d) ENHANCED PENALTIES FOR AGGRAVATED CASES.—Whoever violates, or attempts to violate, subsection (a) while violating another law of the United States or as part of a pattern of any illegal activity involving more than $100,000, or more than 50 customers of a covered entity, in a 12-month period shall, in addition to the penalties provided for in subsection (a), be fined twice the amount provided in subsection (b)(3) or (c)(3) (as the case may be) of section 3571 of this title, imprisoned for not more than 5 years, or both.

''(e) ENHANCED PENALTIES FOR USE OF INFORMATION IN FURTHERANCE OF CERTAIN CRIMINAL OFFENSES.—

''(1) Whoever, violates, or attempts to violate, subsection (a), (b), or (c) knowing that such information may be used in furtherance of, or with the intent to commit, an offense described in section 2261, 2261A, 2262, or any other crime of violence shall, in addition to the penalties provided for in subsection (a), (b), or (c), be fined under this title and imprisoned not more than 5 years.

''(2) Whoever, violates, or attempts to violate, subsection (a), (b), or (c) knowing that such infor-

mation may be used in furtherance of, or with the intent to commit, an offense under section 111, 115, 1114, 1503, 1512, 1513, or to intimidate, threaten, harass, injure, or kill any Federal, State, or local law enforcement officer shall, in addition to the penalties provided for in subsection (a), (b) or (c), be fined under this title and imprisoned not more than 5 years.

''(f) EXTRATERRITORIAL JURISDICTION.—There is extraterritorrial jurisdiction over an offense under this section.

''(g) NONAPPLICABILITY TO LAW ENFORCEMENT AGENCIES.—Nothing in this Act shall be construed to prevent, hinder, or otherwise delay the production of confidential phone records information from a covered entity upon receipt of a lawful request from a law enforcement agency, or any officer, employee, or agent of such agency, in accordance with other applicable laws.

''(h) DEFINITIONS.—In this section:

''(1) CONFIDENTIAL PHONE RECORDS INFORMATION.—The term 'confidential phone records information' means—

''(A) information that—

''(i) relates to the quantity, technical configuration, type, destination, location,

or amount of use of a service offered by a covered entity subscribed to by any customer of that covered entity; and

''(ii) is made available to a covered entity by a customer solely by virtue of the relationship between the covered entity and the customer; or

''(B) information contained in any bill, itemization, or account statement related to a product or service provided by a covered entity to any customer of the covered entity.

''(2) COVERED ENTITY.—The term 'covered entity'—

''(A) has the same meaning given the term 'telecommunications carrier' in section 3 of the Communications Act of 1934 (47 U.S.C. 153); and

''(B) includes any provider of IP-enabled voice service.

''(3) CUSTOMER.—The term 'customer' means, with respect to a covered entity, any individual, partnership, association, joint stock company, trust, or corporation, or authorized representative of such customer, to whom the covered entity provides a product or service.

''(4) IP-ENABLED VOICE SERVICE.—The term 'IP-enabled voice service' means the provision of real-time 2-way voice communications offered to the public, or such class of users as to be effectively available to the public, transmitted through customer premises equipment using TCP/IP protocol, or a successor protocol, for a fee (whether part of a bundle of services or separately) with 2-way interconnection capability such that the service can originate traffic to, and terminate traffic from, a public switched telephone network.''.

SEC. 4. SENTENCING GUIDELINES.

(a) REVIEW AND AMENDMENT.—Not later than 180 days after the date of enactment of this Act, the United States Sentencing Commission, pursuant to its authority under section 994 of title 28, United States Code, and in accordance with this section, shall review and, if appropriate, amend the Federal sentencing guidelines and policy statements applicable to persons convicted of any offense under section 1039 of title 18, United States Code.

(b) AUTHORIZATION.—The United States Sentencing Commission may amend the Federal sentencing guidelines in accordance with the procedures set forth in section 21(a) of the Sentencing Act of 1987 (28 U.S.C. 994 note)

as though the authority under that section had not expired.

○

Chairman SENSENBRENNER. The Chair recognizes the sponsor of the legislation, the gentleman from Texas, Mr. Smith, for 5 minutes to explain the bill briefly.

Mr. SMITH. Thank you, Mr. Chairman. First of all, I would like to thank the original cosponsors of the legislation, the Ranking Member, Mr. Conyers, and Mr. Goodlatte and Mr. Scott, for their help in drafting H.R. 4709, the "Law Enforcement and Phone Privacy Protection Act of 2006."

This bipartisan legislation provides new protections for the privacy of confidential telephone records, including calling logs. It establishes specific criminal penalties for the fraudulent acquisition or disclosure of these records without consumer consent.

Few things are more personal and potentially more revealing than our phone records. The records of whom we call can reveal much about our business and personal lives. These records can reveal details of our medical or financial life and also disclose our physical location.

Millions of Americans already voluntarily list their phone numbers in the National Do-Not-Call Registry. Others keep their telephone number unlisted. Federal law recognizes the right of Americans to maintain this kind of privacy by providing some limited protections for the confidential information contained in calling logs. Phone companies and others who have a legitimate interest in having this information may not release it without either consumer consent or a determination that certainly narrowly prescribed conditions exist.

Unfortunately, current Federal statutes are inadequate to protect these records. Numerous companies and individuals offer to sell confidential phone records information, both cell and land line, to virtually anyone with no questions asked. This is data burglary. For an average of $100, these companies sell the confidential personal information of American citizens as a commodity. Many of these companies have operated on the Internet under a variety of names.

In recent weeks, several States have taken civil enforcement action against these kinds of companies, filing suits that allege violations of various State deceptive trade practices statutes. However, civil enforcement alone is not enough. New Federal criminal penalties are needed to deter and penalize dishonest individuals and businesses, and put them out of business.

The Law Enforcement and Phone Privacy Protection Act imposes serious criminal penalties on anyone who knowingly and intentionally obtains or attempts to obtain the confidential phone records of a telephone company using a fraudulent scheme or device.

This legislation is urgently needed to preserve consumers' privacy rights and to protect the personal safety of law enforcement personnel and victims of domestic violence.

Mr. Chairman, enactment of this bill will send a clear signal that these breaches of privacy will no longer be tolerated.

Also, Mr. Chairman, let me note that I understand that the Senate Judiciary Committee considered a companion bill this morning, and passed it under unanimous consent. The Senate bill was cosponsored by Senator Specter, the Chairman of the Senate Judiciary Committee, and the Senator from New York, Mr. Schumer, so

this legislation is on a fast track, and much needed, and I encourage my colleagues to support it.

Chairman SENSENBRENNER. The gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Mr. Chairman, and I am proud to support this along with the gentleman from Texas, Mr. Smith. I ask unanimous consent that my statement in support of the bill as an original sponsor be included in the record at this time.

Chairman SENSENBRENNER. Without objection. And without objection, all Members may put opening statements in the record at this point.

[The prepared statement of Mr. Conyers follows:]

PREPARED STATEMENT OF THE HONORABLE JOHN CONYERS, JR., A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN, AND RANKING MEMBER, COMMITTEE ON THE JUDICIARY

I am pleased to join Lamar Smith as an original sponsor of this bill.

Recent investigations undertaken by law enforcement officials have documented the ease with which an individual can obtain the confidential calling records of a third party. By simply contacting one of the many online data brokers, within a matter of hours, and after a small fee of approximately $100 dollars, the private records of anyone sitting in this room could be filtered into the public domain.

Of course, it goes without saying, that if put into the wrong hands such information could be used to commit countless crimes of violence, including domestic violence offenses; or alternatively could be used to kill, injure, or intimidate witnesses, jurors, confidential informants, or law enforcement officers.

Our bill seeks to stop these potential abuses from becoming a reality. It does so by making several important changes to current law. First, it establishes a new criminal offense against anyone who knowingly and intentionally obtains, or attempts to obtain, the confidential phone records of a third party through one of several enumerated schemes or devices to defraud. Penalties for violating this prohibition include a fine or a term of imprisonment of not more than 20 years, or both.

Second, the bill establishes a new set of criminal penalties for anyone who knowingly and intentionally sells or purchases the confidential phone records of a third party, without proper authorization or knowing that such records were obtained through fraud. Violators of either of these provisions are subjected to a maximum term of imprisonment of up to 5 years, in addition to whatever other criminal penalty that may apply.

Finally, in an effort to offer increased protection to the likely victims of such activities, the legislation includes a series of enhanced criminal penalties against any individual who engages in any one of the aforementioned crimes knowing that such information was sought in furtherance of, or with the intent to commit a crime of violence or any one of nearly a dozen enumerated offenses. Individuals specifically protected under this provision, include potential victims of domestic-violence related offenses, jurors, criminal witnesses, confidential informants and law enforcement officers.

I strongly urge my colleagues to vote yes on this worthwhile measure.

[The prepared statement of Mr. Goodlatte follows:]

PREPARED STATEMENT OF THE HONORABLE BOB GOODLATTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

MR. CHAIRMAN, THANK YOU FOR HOLDING A MARKUP OF THIS IMPORTANT LEGISLATION. I WAS PLEASED TO JOIN WITH REPRESENTATIVES SMITH, CONYERS AND SCOTT TO INTRODUCE THIS IMPORTANT LEGISLATION WHICH WILL HELP PROTECT PHONE RECORDS FROM THIEVES AND OPPORTUNISTS.

THE SALE OF CONFIDENTIAL PHONE RECORDS IS A SERIOUS PROBLEM. FOR APPROXIMATELY $100, ANYONE CAN BUY AN INDIVIDUAL'S PRIVATE CELL PHONE CALL HISTORY. THESE HISTORIES CATALOUGE EVERY OUTGOING AND INCOMING CALL A CUSTOMER MAKES OR RECIEVES. THIS INFORMATION SHOULD NOT BE AVAILABLE FOR UNAUTHORIZED SALE ON THE INTERNET.

THE PRIMARY METHOD THIEVES USE TO OBTAIN THIS INFORMATION IS KNOWN AS "PRETEXTING". THIS INVOLVES AN INDIVIDUAL WITH SOME KEY INFORMATION—A CELL PHONE NUMBER OR POSSIBLY A SOCIAL SECURITY NUMBER—PRETENDING TO BE THE SUBSCRIBER TO GET INFORMATION ABOUT AN ACCOUNT. THE LAW ENFORCEMENT AND PHONE PRIVACY PROTECTION ACT PUTS A STOP TO THIS BY IMPOSING CRIMINAL PENALTIES FOR "PRETEXTING," AS WELL AS OTHER METHODS OF SEEKING TO OBTAIN SUCH RECORDS THROUGH THE USE OF FRAUD.

FURTHERMORE, THE LAW ENFORCEMENT AND PHONE PRIVACY PROTECTION ACT WILL PROVIDE ADDITIONAL PUNISHMENT FOR THOSE WHO ILLEGALLY OBTAIN OR SELL PHONE RECORDS KNOWING THEY WILL BE USED IN A CRIMINAL ACT. THIS IS EXTREMELY IMPORTANT FOR THE PROTECTION OF LAW ENFORCEMENT OFFICERS AND VICTIMS OF DOMESTIC VIOLENCE WHOSE CALL HISTORIES MAY BE PARTICULARLY DESIREABLE TO THOSE WHO WISH TO DO THEM HARM.

WE ALL USE TELEPHONES AND CELL PHONES WITH THE ASSUMPTION THAT INFORMATION ABOUT WHO WE RECEIVE CALLS FROM AND MAKE CALLS TO WILL NOT FALL INTO THE WRONG HANDS. I URGE THE MEMBERS OF THIS COMMITTEE TO SUPPORT THIS LEGISLATION TO ENSURE THAT PHONE RECORDS ARE ACTUALLY PROTECTED.

THANK YOU AGAIN, MR. CHAIRMAN FOR HOLDING THIS IMPORTANT MARKUP.

[The prepared statement of Ms. Lofgren follows:]

PREPARED STATEMENT OF THE HONORABLE ZOE LOFGREN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

I am pleased to be an original cosponsor of this bill. I believe it provides critical privacy protections to the more than 180 million Americans who use cell phones. It will also protect the privacy of more than 100 million American homes with wired telephones. And it will protect Voice over IP users, now more than 2 million Americans and rapidly rising.

I think we've heard too many stories of how easy it is to fraudulently obtain cell phone call records and even cell phone locations. We've heard of how one political blog bought Wesley Clark's cell phone records, but the fact is lots of ordinary Americans have reason to be concerned about the privacy of their phone records. Imagine what a criminal organization could do with the cell phone call records of an undercover law enforcement agent, or what an abuser could do with a spouse's cell phone location. No one should be able to get another person's phone records through fraud, and this bill makes it a crime to purchase or use phone records obtained through fraud.

I want to thank Chairman Smith of the IP Subcommittee and Ranking Member Conyers for their leadership in drafting this legislation, which I believe represents a sensible, bipartisan solution to a growing problem. I urge my colleagues to join me in voting to report this bill favorably.

Mr. CONYERS. And I noticed that we not only seek to curb these abuses of personal telephone called from data brokers, but we are also attempting to punish those who sell these confidential records without proper authorization. So we are trying to hamper this activity both ways, and I think that it's incredibly important that we protect people in the way that we're doing by putting criminal penalties to the selling of confidential calling records to others.

In the Judiciary Committee, it never stops—does it?—that we are constantly coming across new schemes to avert and avoid the legal consequences of activity. There are new plans being hatched almost every month. And this is an important one. I can't help but feel that every Member of this Committee will feel very strongly about the steps that we are taking today. And I return any unused time——

Ms. LOFGREN. Would the gentleman yield?

Mr. CONYERS. Of course.

Ms. LOFGREN. I would just like to—I will put my statement in the record, but I am happy to be a cosponsor of this legislation. I think it is an important issue, but it also approaches the solution in the proper way. And I hope that we will get unanimous support for the measure, and I thank the gentleman for yielding.

Mr. CONYERS. I return my time.

Chairman SENSENBRENNER. The gentleman's time has expired.

Are there amendments?

[No response.]

Chairman SENSENBRENNER. If there are no amendments, a reporting quorum is present. The question occurs on the motion to report the bill favorably. All in favor, say aye? Opposed, no?

The ayes appear to have it. The ayes have it, and the motion to report favorably is agreed to.

Without objection, the staff is directed to make any 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.]

The business noticed on today's schedule having been concluded, without objection, the Committee stands adjourned.

[Whereupon, at 11:01 a.m., the Committee was adjourned.]

○