AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

109TH CONGRESS
*2d Session*
HOUSE OF REPRESENTATIVES
REPORT
109–398

# PREVENTION OF FRAUDULENT ACCESS TO PHONE RECORDS ACT

MARCH 16, 2006.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Mr. BARTON of Texas, from the Committee on Energy and Commerce, submitted the following

# R E P O R T

[To accompany H.R. 4943]

[Including cost estimate of the Congressional Budget Office]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 4943) to prohibit fraudulent access to telephone records, having considered the same, report favorably thereon without amendment and recommend that the bill do pass.

CONTENTS

| | Page |
|---|---|
| Purpose and Summary | 1 |
| Background and Need for Legislation | 2 |
| Hearings | 3 |
| Committee Consideration | 3 |
| Committee Votes | 4 |
| Committee Oversight Findings | 4 |
| Statement of General Performance Goals and Objectives | 4 |
| New Budget Authority, Entitlement Authority, and Tax Expenditures | 4 |
| Committee Cost Estimate | 4 |
| Congressional Budget Office Estimate | 4 |
| Federal Mandates Statement | 7 |
| Advisory Committee Statement | 7 |
| Constitutional Authority Statement | 7 |
| Applicability to Legislative Branch | 7 |
| Section-by-Section Analysis of the Legislation | 7 |
| Changes in Existing Law Made by the Bill, as Reported | 11 |

## PURPOSE AND SUMMARY

The purpose of H.R. 4943, the "Prevention of Fraudulent Access to Phone Records Act," is to make pretexting for telephone records

illegal and to strengthen the security measures taken by telecommunications carriers to protect such records.

## BACKGROUND AND NEED FOR LEGISLATION

Since the advent of the Internet, there has been growing public discomfort with the availability of sensitive personal information that can be found through the Internet. Nearly any kind of personal data can be located on the Internet, both for free and for a price. One of the growing markets for personal information is the sale of phone records, and in particular, mobile phone records.

For a nominal fee, there are dozens of online companies that offer to sell telephone records, both mobile and wireline. In the Electronic Privacy and Information Center's August 30, 2005, letter filed with the Federal Trade Commission (FTC) there are 40 different data broker companies listed that offer for sale telephone calling records and other confidential information. These services cost as little as $100. These data brokers advertise the availability of information relating to calls to and from a particular phone number, the duration of the calls, and the date and time of the calls. Some Internet brokers offer to sell information relating to the location from which mobile phone calls were made.

The Committee received testimony about the scope and the dangers related to the sale of these sensitive phone records. For instance, on January 6, 2006, a Chicago police official used locatecell.com to obtain the call records of an undercover narcotics officer's telephone number, and received accurate call records within four hours of the request. In 1999, law enforcement authorities discovered that an information broker sold a Los Angeles detective's pager number to an Israeli mafia member who was trying to determine the identity of the detective's confidential informant. In a separate incident in California on September 8, 2005, according to a Cingular court-filed affidavit, certain defendants or their agents posed as an employee/agent of Cingular and as a customer of the carrier to induce Cingular's customer service representative to provide them with the call records of a targeted consumer. These records can also be used by criminals, such as stalkers or abusive spouses trying to find victims.

Unlike other types of personal information which can be found in many public documents that data brokers mine, the only repositories of telephone call records are the telephone companies. Under section 222 of the Communications Act of 1934 (47 U.S.C. § 222), the telephone carriers are under a legal duty to protect customer call records, known as Confidential Proprietary Network Information (CPNI), which is defined as "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service" as well as "information contained in the bills pertaining to telephone exchange service or telephone toll service." (47 U.S.C. § 222(h)(1)).

Despite the protections in existing law, there is a healthy Internet market for the sale of telephone records. The primary method of obtaining such records is through "pretexting," by which the data broker pretends to be the telephone account holder to access customer account information. A "pretexter" can place a call to the telecommunications carrier, and with a few pieces of personal information, such as a social security number or phone number, per-

suade an employee to release the secured information. A "pretexter" can also take advantage of situations in which a consumer has not set up an online account for a given phone number. With those same personal identifiers, a "pretexter" can set up the online account and access all of the targeted customer's personal information. In other instances, a data broker will pose as an executive within the telecommunications company calling a more junior employee demanding the information. A telecommunications carrier may also have an employee on the inside willing to sell the data. Additionally, there are questions surrounding the effectiveness of the current security procedures used by telecommunication carriers since sensitive information is being accessed by data brokers, even if such access is achieved through fraudulent means.

Congress expressly prohibited pretexting for financial data under the Gramm-Leach-Bliley Act (GLBA) (P.L. 106–102), but that law did not cover telephone records. The FTC has successfully brought "pretexting" cases under its Section 5 authority, which prohibits "unfair or deceptive acts or practices in or affecting commerce." (15 U.S.C. § 45(a)) Before the GLBA became a public law, the FTC used its Section 5 authority to enforce against financial "pretexting." However, a specific prohibition against pretexting for telephone record information will give the FTC authority to seek civil penalties against the pretexters.

H.R. 4943, the "Prevention of Fraudulent Phone Records Act," is designed to stop the sale of sensitive customer telephone records by expressly prohibiting pretexting for telephone records and strengthening the security requirements for proprietary customer information held by telephone carriers.

## HEARINGS

On February 1, 2006, the Committee on Energy and Commerce held a hearing on the fraudulent sale of telephone records. The Committee received testimony from: the Honorable Kevin Martin, Chairman, Federal Communications Commission; the Honorable Jon Leibowitz, Commissioner, Federal Trade Commission; the Honorable Lisa Madigan, Attorney General, State of Illinois; the Honorable Steve Largent, President and Chief Executive Officer, Cellular Telecommunications and Internet Association; Mr. Edward Merlis, Senior Vice President, Law & Policy, United States Telecom Association; Mr. Marc Rotenberg, Executive Director, Electronic Privacy and Information Center; and Mr. Robert Douglas, Chief Executive Officer, PrivacyToday.com.

## COMMITTEE CONSIDERATION

On Wednesday, March 8, 2006, the Full Committee met in open markup session and ordered a Committee Print favorably reported to the House, amended, by a voice vote, a quorum being present. A request by Mr. Barton to allow a report to be filed on a bill to be introduced by Mr. Barton, and that the actions of the Committee be deemed as actions on that bill, was agreed to by unanimous consent.

## COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the motion to report legislation and amendments thereto. There were no record votes taken in connection with ordering H.R. 4943 reported. A motion by Mr. Barton to order the Committee Print reported to the House, amended, was agreed to by a voice vote.

## COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c)(1) of rule XIII of the Rules of the House of Representatives, the Committee held an oversight hearing and made findings that are reflected in this report.

## STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

The goal of H.R. 4943, the "Prevention of Fraudulent Access to Phone Records Act" is to make pretexting for telephone records illegal and to strengthen the security measures taken by telecommunications carriers to protect such records.

## NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

In compliance with clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee finds that H.R. 4943, the "Prevention of Fraudulent Access to Phone Records Act," would result in changes to budget authority, entitlement authority, and tax expenditures and revenues to the extent stated below in the Committee Cost Estimate.

## COMMITTEE COST ESTIMATE

The Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974.

## CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
*Washington, DC, March 15, 2006.*

Hon. JOE BARTON,
*Chairman, Committee on Energy and Commerce,*
*House of Representatives, Washington, DC.*

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 4943, the Prevention of Fraudulent Access to Phone Records Act.

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. 4943—Prevention of Fraudulent Access to Phone Records Act*

Summary: H.R. 4943 would prohibit deceitfully obtaining or selling the personal information of telecommunications customers, including customers' phone records. The bill also would require telecommunications carriers to take precautions to safeguard customers' personal information and to notify customers and the Federal Communications Commission (FCC) whenever there is a breach in the security of this information. The FCC and the Federal Trade Commission (FTC) would enforce these restrictions and requirements. The bill also would direct the FCC to write regulations regarding security precautions for carriers, periodically audit the security practices of telecommunication carriers, and prepare reports on the assessment of the new regulations and requirements.

Assuming appropriation of the necessary amounts, CBO estimates that implementing the bill would cost the FCC less than $500,000 in 2006 and about $5 million over the 2007–2011 period to enforce the bill's provisions regarding the personal information of telecommunications customers. write regulations, audit security systems, and prepare reports. We estimate that implementing the bill would not have a significant effect on FTC spending.

Enacting the bill could increase federal revenues as a result of the col1ection of additional civil penalties assessed for violations of the new laws and regulations. Collections of civil penalties are recorded in the budget as revenues. CBO estimates, however, that any additional revenues that would result from enacting the bill would not be significant because of the relatively small number of cases likely to be involved. Enacting the bill would not affect direct spending.

H.R. 4943 contains no intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would not affect the budgets of state, local, or tribal governments. H.R. 4943 would impose new private-sector mandates, as defined in UMRA, on telecommunications carriers. The bill would require such carriers to expand certain privacy requirements relating to phone records and would require the FCC to prescribe more stringent security requirements for customer proprietary network information including phone records. Since the regulations have not been established, CBO cannot estimate the direct cost to comply with those mandates. Consequently, CBO cannot determine whether the costs of the mandates would exceed UMRA's annual threshold for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

Estimated cost to the Federal Government: The estimated budgetary impact of H.R. 4943 is shown in the following table. The costs of this legislation fall within budget function 370 (commerce and housing credit). For this estimate, CBO assumes that the bill will be enacted in 2006 and that the necessary amounts will be appro-

priated for each year. Based on information from the FCC, CBO estimates that implementing the bill would cost less than $500,000 in 2006 and about $5 million over the 2007–2011 period for the agency to enforce the bill's provisions regarding the personal information of telecommunications customers, issue regulations, audit the security practices of telecommunication carriers, and prepare reports on the assessment of the new regulations and requirements.

| | By fiscal year, in millions of dollars— | | | | | |
|---|---|---|---|---|---|---|
| | 2006 | 2007 | 2008 | 2009 | 2010 | 2011 |
| CHANGES IN SPENDING SUBJECT TO APPROPRIATION | | | | | | |
| Estimated Authorization Level | * | 1 | 1 | 1 | 1 | 1 |
| Estimated Outlays | * | 1 | 1 | 1 | 1 | 1 |

Note.— * = Less than $500,000.

Estimated impact on State, local, and tribal governments: H.R. 4943 contains no intergovernmental mandates as defined in UMRA and would not affect the budgets of state, local, or tribal governments.

Estimated impact on the private sector: H.R. 4943 would impose new private-sector mandates, as defined in UMRA, by expanding the customer privacy requirements for telecommunications carriers. The bill would require such carriers to receive express prior authorization from the customer before using, accessing or disclosing their phone records to joint venture partners, independent contractors or others. Based on information from government sources, the direct cost for carriers to comply with this new requirement could be nominal. Section 203 would require the FCC to prescribe regulations adopting more stringent security standards for customer proprietary network information. The FCC regulations would require telecommunications carriers to:

- Provide timely notice to each customer and the commission upon breach of the regulations;
- Submit to periodic audits by the commission;
- Maintain certain records;
- Establish a security policy; and
- Prohibit the disclosure of customer phone information by an employee or agent of the carrier.

According to government sources, some of the requirements would be satisfied by current practices within the telecommunications industry. The cost of providing additional security would depend on the rules to be prescribed by the FCC. Since the regulations have not been established, CBO cannot estimate the direct cost to comply with the new mandates. Consequently, CBO cannot determine whether the costs of those mandates would exceed the annual threshold for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

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

Estimate approved by: Peter H. Fontaine, Deputy Assistant Director for Budget Analysis.

## FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

## ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

## CONSTITUTIONAL AUTHORITY STATEMENT

Pursuant to clause 3(d)(1) of rule XIII of the Rules of the House of Representatives, the Committee finds that the Constitutional authority for this legislation is provided in Article I, section 8, clause 3, which grants Congress the power to regulate commerce with foreign nations, among the several States, and with the Indian tribes.

## APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

## SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

*Section 1. Short title*

Section 1 establishes the short title of the bill as the "Prevention of Fraudulent Access to Phone Records Act."

*Section 101. Fraudulent access to customer telephone records*

Section 101 prohibits the fraudulent access to customer telephone records. The section contains three distinct prohibitions. Section 101(a) makes it unlawful for any person to obtain or attempt to obtain, or disclose or cause to be disclosed, customer proprietary network information (CPNI) relating to another person by making fraudulent statements or representations to a telecommunications carrier or by providing documentation to a carrier that the person knows or should know to be forged, counterfeit, lost, stolen, or fraudulently obtained, or known to contain fraudulent statements or representations.

Section 101(b) prohibits soliciting a person to obtain from a telecommunications carrier CPNI relating to a third person, if the person making the solicitation knew or should have known that the solicited person will obtain or attempt to obtain the information in a manner that violates section (a).

Section 101(c) prohibits the sale or other disclosure of CPNI relating to any other person if the person selling or disclosing the information obtained such information in a manner that violates section (a).

*Section 102. Exemption*

Section 102 provides an exemption from the prohibitions in section 101 for any action by a law enforcement agency in connection with the performance of the official duties of the agency. The provi-

sion makes clear that all activity must be in accordance with other applicable laws.

*Section 103. Enforcement by the Federal Trade Commission*

Section 103 provides enforcement authority to the FTC. The section provides that a violation of section 101 shall be treated as a violation of a rule defining an unfair or deceptive act or practice prescribed under section 18(a)(1)(B) of the FTC Act.

*Section 104. Definitions*

Section 104 defines the terms "customer proprietary network information" and "telecommunications carrier," as those terms are defined in the Communications Act of 1934.

*Section 201. Findings*

Section 201 contains findings for Title II.

*Section 202. Expanded protection for detailed customer records*

Section 202(a) governs how telecommunications carriers can share CPNI with their agents, joint venture partners, contractors and other third parties under section 222 of the Communications Act. Section 202(a)(1)(A) sets out the general rule that, except as required by law or under the specific language of the paragraph, a carrier that receives or obtains individually identifiable CPNI, including detailed customer telephone records, shall only use, disclose, or permit access to such information or records in the provision of (i) the telecommunications service from which such information is derived; or (ii) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.

Section 202(a)(1)(B) allows a telecommunications carrier to use, disclose, or permit access to detailed customer telephone records to a joint venture partner, independent contractor, or other third party (other than an affiliate) only if the customer has given express prior authorization for that use, disclosure, or access, and that authorization has not been withdrawn.

Section 202(a)(1)(C) allows a telecommunications carrier to use, disclose, or permit access to CPNI, including detailed customer telephone records, to affiliates for the services described in clause (i) or (ii) of section 202(a)(1)(A), with the approval of the customer.

Section 202(a)(1)(D) allows a telecommunications carrier to use, disclose, or permit access to CPNI, excluding detailed customer telephone records, to joint venture partners or independent contractors for the services described in clause (i) or (ii) of section 202(a)(1)(A), with the approval of the customer.

In deciding how CPNI can be shared with the carrier's business partners, in its 1998 rulemaking, the Federal Communications Commission (FCC or Commission) adopted the "total service approach" which divides the term "telecommunications service" into three service categories: local, interexchange, and commercial mobile radio service. (47 C.F.R. §64.2005(b)) This approach permits a telecommunications carrier to use, disclose, or provide access to CPNI for the purpose of marketing products within a category of service to customers, provided the customer already subscribes to that category of service. For example, a carrier could use CPNI ob-

tained through the provision of local service to market other local service products, but not mobile service.

Under the total service approach, the sharing of CPNI must be modified in light of the changes relating to the sharing of detailed customer telephone records with joint venture partners and independent contractors. Telecommunications carriers and their affiliates can continue to use CPNI, including detailed customer telephone records, to market communications-related services with the approval of the customer, and the carrier's joint venture partners and independent contractors may continue to use CPNI, excluding detailed customer telephone records, to market communications-related services with the approval of the customer. Under this bill, however, the carrier will need the express prior authorization of the customer to use, disclose, or provide access to detailed customer telephone records to its joint venture partners and independent contractors.

Section 202(a)(1)(E) requires the prior express authorization from a customer before a telecommunications carrier may disclose or permit access to a wireless telephone number. This language is intended to limit the ability of carriers to create a telephone directory of wireless telephone numbers without obtaining the express consent of its customers.

Section 202(b) incorporates the term of "detailed customer telephone record" into section 222(c)(2) of the Communications Act as it relates to the disclosure of CPNI at the request of the customer.

Section 202(c) treats third party aggregators of CPNI as the carrier for purposes of section 222(c)(3) of the Communications Act if the aggregation is done in a secure manner and under the control or supervision of the carrier. The Committee is aware that there are a number of innovative new applications being developed that rely on aggregated CPNI. This language is intended to allow such data to more easily be aggregated for third party applications and services as long as such aggregation occurs in a secure environment.

Section 202(d) adds a new paragraph to section 222(c) of the Communications Act that prohibits any person from selling, renting, leasing, or otherwise making available for remuneration or other consideration customer telephone records. Therefore, regardless of how the CPNI is obtained, anyone trading in such data for profit will be subject to liability.

Currently, the exemptions in section 222(d) of the Communications Act flow only to the carriers and their "agents." The exemptions contained in section 222(d) include: (1) to initiate, render, bill, and collect for telecommunications services; (2) to protect the rights or property of the carriers, or to protect the users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services; (3) to provide any inbound telemarketing, referral, or administrative services to the customer for the duration of the call, if the call was initiated by the customer and the customer approves of the use of such information to provide the service; and (4) to provide call location information concerning a mobile service user to certain entities in the event of an emergency. Section 202(e)(1) expands the availability of the exemptions to joint venture partners and independent contractors. Additionally, the existing exemption to "initiate, render, bill, and collect

for telecommunications services" in section 222(d)(1) of the Communications Act is expanded by section 202(e)(2) of the bill to include the provision of customer service with respect to telecommunications services to which the customer subscribes.

*Section 203. Prevention by telecommunications carriers of fraudulent access to phone records*

Section 203 creates a new section 222(h) of the Communications Act that directs the Commission to complete a rulemaking within 180 days of enactment of H.R. 4943, the "Prevention of Fraudulent Access to Phone Records Act," that adopts more stringent security standards for CPNI.

In section 203(h)(A), the Commission must prescribe regulations that: (1) require telecommunications carriers to provide timely notice to affected customers upon learning of a breach of CPNI regulations; (2) require telecommunications carriers to provide timely notice to the FCC when the carriers learn of a breach of CPNI regulations; (3) require the Commission to conduct periodic audits of telecommunications carriers and their agents to determine compliance with section 222 of the Communications Act; (4) require telecommunications carriers and their agents to maintain records of each time CPNI is requested or accessed by, or disclosed to, a person purporting to be the customer or acting at the request of the customer, and if such access or disclosure is granted, how the identity of the person was verified; (5) require telecommunications carriers to establish a security policy that includes appropriate standards relating to administrative, technical, and physical safeguards to ensure the security and confidentiality of CPNI; (6) prohibit any telecommunications carrier from obtaining or disclosing, or attempting to obtain or disclose, CPNI relating to any customer of another carrier by using false, fictitious, or fraudulent statements to an officer, employee, or agent of another carrier, or to a customer of another carrier; and (7) only for purposes of section 222 of the Communications Act, to treat as a telecommunications service provided by a telecommunications carrier any real-time Internet Protocol-enabled voice communications offered by any person to the public, or such classes of users as to be effectively available to the public, that allows a user to originate traffic to, or terminate traffic from, the public switched telephone network. The Committee intends the definition of Internet Protocol-enabled voice communications to only be applicable to section 222 of the Communications Act and shall not have any precedential effect for any other part of the Communications Act or for the FCC in any future proceedings.

Section 203(h)(B) requires the Commission to consider prescribing regulations that: (1) require telecommunications carriers to institute customer-specific identifiers in order for customers to access CPNI; (2) require encryption of CPNI to secure such data; or (3) require deletion of CPNI after a reasonable period of time if such data is no longer necessary for the purpose for which it was collected, or for an exception contained in section 222(d) of the Communications Act, and there are no pending requests for access to such information. The Committee strongly suggests that if the FCC decides to adopt customer-specific identifiers that such identifiers not utilize social security numbers.

Section 203(h)(2) requires the Commission to, within 12 months after the Commission's regulations are prescribed, and again not later than 3 years thereafter, the Commission shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate, a report containing (i) an assessment of the efficacy and adequacy of the regulations and remedies provided to protect CPNI in H.R. 4943, the "Prevention of Fraudulent Access to Phone Records Act," (ii) an assessment of the efficacy and adequacy of telecommunications carriers' safeguards to secure such data, security plans, and notification procedures; and (iii) any recommendations for additional legislative or regulatory action to protect CPNI. Additionally, the Commission is directed to submit to Congress an annual report detailing its enforcement activities of section 222 of the Communications Act.

Section 203(h)(3) prevents dual regulation of any entity offering Internet Protocol-enabled voice communications. Any person that is treated as a telecommunications carrier providing a telecommunications service with respect to the offering of real-time Internet Protocol-enabled voice communications by the new regulations required under section 203(1)(A)(vii) shall not be subject to the provisions of section 631 of the Communications Act with respect to such communications.

Section 203(i)(1) increases the FCC forfeiture penalties available under section 503(b)(1) of the Communications Act for section 222 violations from a maximum of $100,000 to a maximum of $300,000 per violation, and increases the maximum forfeiture penalty for continuing violations from $1,000,000 to $3,000,000. Section 203(i)(2) eliminates the first warning requirement under section 503(b) for violations of section 222 of the Communications Act by any telecommunications carrier or agent of such carrier.

*Section 204. Definitions*

Section 204 defines "detailed customer telephone record" as CPNI that contains the specific and detailed destinations, locations, duration, time, and date of telecommunications to or from a customer, as typically contained in bills for such service. This term does not mean aggregate data or subscriber list information.

The term "real-time Internet Protocol-enabled voice communications" is defined in section 203(h) of this bill. This definition shall only be applicable to section 222 of the Communications Act and shall not have any precedential effect for any other part of the Communications Act or for the FCC in any future proceedings.

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 (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman)

**COMMUNICATIONS ACT OF 1934**

* * * * * * *

## TITLE II—COMMON CARRIERS

* * * * * * *

# PART I—COMMON CARRIER REGULATION

* * * * * * *

**SEC. 222. PRIVACY OF CUSTOMER INFORMATION.**

(a) * * *

* * * * * * *

(c) CONFIDENTIALITY OF CUSTOMER PROPRIETARY NETWORK INFORMATION.—

[(1) PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS.—Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.]

*(1) PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS.—*

*(A) IN GENERAL.—Except as required by law or as permitted under the following provisions of this paragraph, a telecommunications carrier that receives or obtains individually identifiable customer proprietary network information (including detailed customer telephone records) by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to such information or records in the provision by such carrier of—*

*(i) the telecommunications service from which such information is derived; or*

*(ii) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories.*

*(B) REQUIREMENTS FOR DISCLOSURE OF DETAILED INFORMATION.——A telecommunications carrier may only use detailed customer telephone records through, or disclose such records to, or permit access to such records by, a joint venture partner, independent contractor, or any other third party (other than an affiliate) if the customer has given express prior authorization for that use, disclosure, or access, and that authorization has not been withdrawn.*

*(C) REQUIREMENTS FOR AFFILIATE USE OF BOTH GENERAL AND DETAILED INFORMATION.—A telecommunications carrier may not, except with the approval of a customer, use individually identifiable customer proprietary network information (including detailed customer telephone records) through, or disclose such information or records to, or permit access to such information or records by, an affiliate of*

*such carrier in the provision by such affiliate of the services described in clause (i) or (ii) of subparagraph (A).*

*(D) REQUIREMENTS FOR PARTNER AND CONTRACTOR USE OF GENERAL INFORMATION.—A telecommunications carrier may not, except with the approval of the customer, use individually identifiable customer proprietary network information (other than detailed customer telephone records) through, or disclose such information to, or permit access to such information by, a joint venture partner or independent contractor in the provision by such partner or contractor of the services described in clause (i) or (ii) of subparagraph (A).*

*(E) ACCESS TO WIRELESS TELEPHONE NUMBERS.—A telecommunications carrier may not, except with prior express authorization from the customer, disclose the wireless telephone number of any customer or permit access to the wireless telephone number of any customer.*

(2) DISCLOSURE ON REQUEST BY CUSTOMERS.—A telecommunications carrier shall disclose customer proprietary network information *(including a detailed customer telephone record)*, upon affirmative written request by the customer, to any person designated by the customer.

(3) AGGREGATE CUSTOMER INFORMATION.—A telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service may use, disclose, or permit access to aggregate customer information other than for the purposes described in paragraph (1). A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in paragraph (1) only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor. *Aggregation of data that is conducted by a third party may be treated for purposes of this subsection as aggregation by the carrier if such aggregation is conducted in a secure manner under the control or supervision of the carrier.*

*(4) PROHIBITION OF SALE OF GENERAL OR DETAILED INFORMATION.—Except for the purposes for which use, disclosure, or access is permitted under subsection (d), it shall be unlawful for any person to sell, rent, lease, or otherwise make available for remuneration or other consideration the customer proprietary network information (including the detailed customer telephone records) of any customer.*

(d) EXCEPTIONS.—Nothing in this section prohibits a telecommunications carrier from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through [its agents] *its joint venture partners, contractors, or agents*—

(1) to initiate, render, bill, and collect for telecommunications services*, or provide customer service with respect to telecommunications services to which the customer subscribes*;

* * * * * * *

(g) SUBSCRIBER LISTED AND UNLISTED INFORMATION FOR EMERGENCY SERVICES.—Notwithstanding subsections (b), (c), and (d), a

telecommunications carrier that provides telephone exchange service shall provide information described in [subsection (i)(3)(A)] *subsection (j)(3)(A)* (including information pertaining to subscribers whose information is unlisted or unpublished) that is in its possession or control (including information pertaining to subscribers of other carriers) on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions to providers of emergency services, and providers of emergency support services, solely for purposes of delivering or assisting in the delivery of emergency services.

*(h) PREVENTION OF FRAUDULENT ACCESS TO PHONE RECORDS.—*

*(1) REGULATIONS.—Within 180 days after the date of enactment of the Prevention of Fraudulent Access to Phone Records Act, the Commission shall prescribe regulations adopting more stringent security standards for customer proprietary network information (including detailed customer telephone records) to detect and prevent violations of this section. The Commission—*

*(A) shall prescribe regulations—*

*(i) to require timely notice (written or electronic) to each customer upon breach of the regulations under this section with respect to customer proprietary network information relating to that customer;*

*(ii) to require timely notice to the Commission upon breach of the regulations under this section with respect to customer proprietary network information relating to any customer;*

*(iii) to require periodic audits by the Commission of telecommunication carriers and their agents to determine compliance with this section;*

*(iv) to require telecommunications carriers and their agents to maintain records—*

*(I) of each time customer proprietary network information is requested or accessed by, or disclosed to, a person purporting to be the customer or to be acting at the request or direction of the customer; and*

*(II) if such access or disclosure was granted to such a person, of how the person's identity or authority was verified;*

*(v) to require telecommunications carriers to establish a security policy that includes appropriate standards relating to administrative, technical, and physical safeguards to ensure the security and confidentiality of customer proprietary network information;*

*(vi) to prohibit any telecommunications carrier from obtaining or attempting to obtain, or causing to be disclosed or attempting to cause to be disclosed to that carrier or its agent or employee, customer proprietary network information relating to any customer of another carrier—*

*(I) by using a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of another telecommunications carrier; or*

*(II) by making a false, fictitious, or fraudulent statement or representation to a customer of another telecommunications carrier; and*

*(vii) only for the purposes of this section, to treat as a telecommunications service provided by a telecommunications carrier any real-time Internet protocol-enabled voice communications offered by any person to the public, or such classes of users as to be effectively available to the public, that allows a user to originate traffic to, or terminate traffic from, the public switched telephone network; and*

*(B) shall consider prescribing regulations—*

*(i) to require telecommunications carriers to institute customer-specific identifiers in order to access customer proprietary network information;*

*(ii) to require encryption of customer proprietary network information data or other safeguards to better secure such data; and*

*(iii) to require deletion of customer proprietary network information data after a reasonable period of time if such data is no longer necessary for the purpose for which it was collected or for the purpose of an exception contained in section (d), and there are no pending requests for access to such information.*

*(2) REPORTS.—*

*(A) ASSESSMENT AND RECOMMENDATIONS.—Within 12 months after the date on which the Commission's regulations under paragraph (1) are prescribed, and again not later than 3 years later, the Commission shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report containing—*

*(i) an assessment of the efficacy and adequacy of the regulations and remedies provided in accordance with this subsection in protecting customer proprietary network information;*

*(ii) an assessment of the efficacy and adequacy of telecommunications carriers' safeguards to secure such data, security plans, and notification procedures; and*

*(iii) any recommendations for additional legislative or regulatory action to address threats to the privacy of customer information.*

*(B) ANNUAL REPORT.—The Federal Communications Commission shall submit to Congress an annual report containing—*

*(i) the number and disposition of all enforcement actions taken pursuant to this subsection; and*

*(ii) the number and type of notifications received under paragraph (1)(A)(ii) and the methodology, including the basis for the selection of carriers to be audited, and the results of each audit conducted under paragraph (1)(A)(iii).*

*(3) DUAL REGULATION PROHIBITED.—Any person that is treated as a telecommunications carrier providing a telecommunications service with respect to the offering of real-time Internet*

*protocol-enabled voice communications by the regulations prescribed under paragraph (1)(A)(vii) shall not be subject to the provisions of section 631 with respect to the offering of such communications.*

*(i) FORFEITURE PENALTIES.—*

*(1) INCREASED PENALTIES.—In any case in which the violator is determined by the Commission under section 503(b)(1) to have violated this section or the regulations thereunder, section 503(b)(2)(B) shall be applied—*

*(A) by substituting "$300,000" for "$100,000"; and*

*(B) by substituting "$3,000,000" for "$1,000,000".*

*(2) NO FIRST WARNINGS.—Paragraph (5) of section 503(b) shall not apply to the determination of forfeiture liability under such section with respect to a violation of this section or the regulations thereunder by any telecommunications carrier or any agent of such a carrier.–*

**[**(h)**]** *(j)* DEFINITIONS.—As used in this section:

(1) * * *

* * * * * * *

*(8) DETAILED CUSTOMER TELEPHONE RECORD.—The term "detailed customer telephone record" means customer proprietary network information that contains the specific and detailed destinations, locations, duration, time, and date of telecommunications to or from a customer, as typically contained in the bills for such service. Such term does not mean aggregate data or subscriber list information.*

*(9) WIRELESS TELEPHONE NUMBER.—The term "wireless telephone number" means the telephone number of a subscriber to a commercial mobile service.*

* * * * * * *

○