Calendar No. 425

109TH CONGRESS *2d Session*	SENATE	REPORT 109–253

PROTECTING CONSUMER PHONE RECORDS ACT

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 2389

together with

ADDITIONAL VIEWS

MAY 9, 2006—Ordered to be printed

U.S. GOVERNMENT PRINTING OFFICE
49–010 WASHINGTON : 2006

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

TED STEVENS, Alaska, *Chairman*
DANIEL K. INOUYE, Hawaii, *Co-Chairman*

JOHN MCCAIN, Arizona
CONRAD BURNS, Montana
TRENT LOTT, Mississippi
KAY BAILEY HUTCHISON, Texas
OLYMPIA J. SNOWE, Maine
GORDON H. SMITH, Oregon
JOHN ENSIGN, Nevada
GEORGE ALLEN, Virginia
JOHN E. SUNUNU, New Hampshire
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA SUTHERLAND, *Staff Director*
CHRISTINE KURTH, *Deputy Staff Director*
KENNETH NAHIGIAN, *Chief Counsel*
MARGARET CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL WHITEHORN, *Democratic Deputy Staff Director and General Counsel*

Calendar No. 425

109TH CONGRESS *2d Session* | SENATE | REPORT 109–253

PROTECTING CONSUMER PHONE RECORDS ACT

MAY 9, 2006.—Ordered to be printed

Mr. STEVENS, from the Committee on Commerce, Science, and Transportation, submitted the following

REPORT

together with

ADDITIONAL VIEWS

[To accompany S. 2389]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 2389) to amend the Communications Act of 1934 to prohibit the unlawful acquisition and use of confidential customer proprietary network information, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

The purpose of S. 2389 is to make it illegal to acquire, use, sell, or solicit a third party to unlawfully obtain a person's confidential phone records without that person's consent. The Federal Communications Commission (FCC) would be required to enhance the confidentiality procedures of telecommunications carriers and IP-enabled voice providers with access to such information to the extent existing protections are inconsistent with standards set forth in the Gramm-Leach-Bliley Act (P.L. 106–102) (GLBA). The bill also would provide the FCC and the Federal Trade Commission (FTC)

with strengthened enforcement authority to ensure that confidential phone records are not accessible by bad actors. Under the bill, a carrier or an IP-enabled voice provider would be required to notify a customer if someone without authorization gains access to a customer's phone records. The bill's provisions would cover wireless, wireline, and IP telephone services. Furthermore, the bill would require the FCC and FTC to educate the public on various protections and enforcement efforts used to prevent unauthorized access of consumers' phone records.

BACKGROUND AND NEEDS

Personal phone records are confidential consumer information, but have recently become targets of data brokers who buy and sell customer phone records for a fee over the Internet. Data brokers sometimes use what is called "pretexting," whereby a person impersonates a phone customer to obtain confidential customer phone records from a carrier. The broker then sells the records on a website to anyone willing to pay a small fee. Certain websites, like "www.locatecell.com," have offered for sale to the public a full cell phone record of a consumer's incoming and outgoing calls for $110.00. In a recent stunt by an online blogger, the cell phone records of former Presidential candidate, Wesley Clark, were purchased from "www.celltolls.com" for $89.95. The relative ease by which individuals can obtain and sell these records has led to public calls for government action to prevent such personal information from becoming public.

Investigations currently are underway by both the FCC and the FTC as to how phone records are being divulged to third party data brokers without a customer's consent. Several methods are possible, but the use of pretexting likely is a primary method through which phone records are obtained by impersonating the authorized user. Pretexting is made even easier if unauthorized third parties obtain personal information such as a customer's password, Social Security number, or identifying information that can be used to convince the carrier that release of the true customer's phone records is legitimate and appropriate.

Other methods and means by which unauthorized third parties obtain and sell personal phone records in the public domain include hacking and compromised employees.

In addition to recent actions taken by Federal regulators against pretexters, the FCC also issued a Notice of Proposed Rulemaking in February to consider what additional steps, if any, should be taken by the Commission to further protect the confidentiality of customer proprietary network information (CPNI).

Telecommunications carriers are already under an affirmative obligation to protect and safeguard a customer's proprietary information, and to refrain from distributing this information to a third party without the customer's consent or as permitted by law (e.g., emergency purposes, law enforcement purposes) (47 U.S.C. §1A222). CPNI includes such data as quantity of phone calls by a customer, destination of the phone call, location, and amount of use of a telecommunications service. For example, if a customer purchases basic local telephone service, the local telephone company and its affiliates do not need the customer's approval to use CPNI to try to sell voice mail or caller ID services to the customer. The

local telephone company, however, may not use or share CPNI with an affiliate to try to sell wireless service without the customer's approval, because wireless telephone service is a different category of service than local telephone service.

With such an affirmative obligation regime in place, the carrier must still be able to provide a customer with personal account information upon request. Carriers, therefore, are required to balance a customer's expectation of privacy that phone records remain closed to public inquiry, while concurrently providing a level of service that does not impede access for a customer in obtaining the customer's own information.

Currently, under rules adopted pursuant to GLBA, specific prohibitions on prextexting are limited to cases where pretexting is used to obtain financial records. Current law does not specifically outlaw pretexting for phone records. (15 U.S.C. §1A45(a) and §1A6801–09). The FTC has taken the position that it has the power to pursue actions against phone record pretexters based on its general authority to prevent deceptive and unfair business practices, but without this explicit ban, such practices may be more difficult to prosecute. Even if FTC's authority to pursue actions against pretexters of phone records is assumed, the Federal Trade Commission Act (FTC Act) does not authorize the immediate imposition of civil penalties against third party data brokers. An action filed in a Federal district court against the accused party would be the only way for the FTC to obtain injunctive or equitable relief.

SUMMARY OF PROVISIONS

The bill, S. 2389, would make it illegal to acquire or use a person's phone records without that person's written consent; to acquire a person's phone records by misrepresenting that person's consent to such acquisition; to obtain unauthorized access to data; or to sell or solicit data that was or will be obtained without authorization. The bill would provide exceptions for phone companies using customer information for legitimate uses not currently prohibited by section 222 of the Communications Act. IP-enabled voice providers, which are not currently covered by law, would be specifically treated as phone companies for the purpose of allowing them to benefit from the same course of business exemption.

The bill would require the FCC to issue rules enhancing confidentiality procedures for phone companies or IP-enabled voice service providers to the extent the FCC determines that changes in its rules are necessary to bring confidentiality protections in line with these regulations adopted by the FTC under GLBA, taking into consideration the differences between financial information and CPNI.

The bill would increase penalties and extend the FCC's statute of limitations under section 509 of the Communications Act from one year to two years. The bill also would extend phone record protection requirements under section 222 of the Communications Act of 1934 (1934 Act) to IP-enabled voice service providers. Within 14 calendar days of a breach, phone companies and IP-enabled service providers would be required to notify a customer whose records were improperly given out.

The bill also would provide for service provider enforcement as if the violations of the bill were an unfair or deceptive act or prac-

tice, and would give the FCC concurrent jurisdiction with the FTC in that respect to enforce the illegal acquisition provisions of the bill. The bill would provide that venue for any action shall be in the place of business of the service provider rather than the bad actor. It would preempt State laws regulating the treatment of CPNI by telecommunications carriers and IP-enabled voice service providers except those of general applicability, tort or contract law, and other fraud or computer crime laws. It also would require the FTC and the FCC to jointly establish and implement a public education campaign.

LEGISLATIVE HISTORY

The Protecting Consumer Phone Records Act was introduced by Senator Allen on March 8, 2006, and is cosponsored by Senators Stevens, Inouye, Burns, Dorgan, Hutchison, Bill Nelson, Pryor, Vitter, Coleman, Martinez, Santorum, Talent, Thune, and Warner. On Wednesday, February 8, 2006, the Subcommittee on Consumer Affairs, Product Safety, and Insurance held a hearing to examine privacy implications arising from the distribution of personal phone records without a customer's prior authorization. The subsequent sale of these phone records over the Internet by third party data brokers/website operators was the focus of the hearing. The Subcommittee heard testimony on available methods for preventing third parties from obtaining consumers' phone records without consent.

On March 30, 2006, the Committee held an Executive Session during which S. 2389 was considered. Chairman Stevens and Senator Inouye offered an amendment in the nature of a substitute that would clarify that consent to acquire phone records may be granted electronically; clarify that the general prohibitions against the acquisition, use or sale of CPNI do not extend to the current business practices by voice providers (including IP-enabled voice service providers), or third parties that lawfully obtain CPNI from a carrier or provider that are not prohibited by section 222; and maintain the status quo with respect to the acquisition and use of CPNI for law enforcement, homeland security, or similar purposes already authorized by law. The substitute amendment was adopted by voice vote.

An amendment to the substitute was offered by Senators Stevens and Burns that would expand the group of entities that may carry out State enforcement to include State Public Utility Commissions or other State agencies in States, which have delegated enforcement of such matters to such officials. The amendment to the substitute was adopted by voice vote.

Senator Boxer offered an amendment to the substitute that would preclude wireless telephone companies from including customer numbers in any wireless directory assistance database without providing prior notice to customers of their right not to be listed and without obtaining express prior authorization from the customer to include his or her number in such database. The amendment also would prohibit wireless companies from charging customers for the removal of their number from a wireless directory and would preempt inconsistent State and local laws. The amendment to the substitute was adopted by voice vote.

Senator Pryor offered an amendment to the substitute that would allow a consumer harmed by a violation of section 2 to bring a civil action in a Federal district court or other court of competent jurisdiction against the person who caused the harm. The consumer would be able to obtain damages of up to $11,000 per violation or treble damages if it is proven that the defendant knowingly or willfully violated section 2 of this bill. The Court would be permitted to assess against any party the costs of such an action, including reasonable attorney's fees. Although the Committee has not recently adopted a private right of action in other consumer legislation, the amendment was offered in this case because of the special type of physical and psychological harm that potentially could be caused if a consumer's CPNI is inappropriately obtained and used. Senator Pryor's amendment was adopted by a rollcall vote of 11 to 10 (Senator Rockefeller was recorded as necessarily absent).

The Committee, without objection, ordered that S. 2389 be reported with amendments.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

MAY 8, 2006.

Hon. TED STEVENS,
Chairman, Committee on Commerce, Science, and Transportation, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 2389, the Protecting Consumer Phone Records Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contacts are Melissa Z. Petersen (for federal costs), Sarah Puro (for the impact on state, local, and tribal governments), and Fatimot Ladipo (for the impact on the private sector).

Sincerely,

DONALD B. MARRON,
Acting Director.

Enclosure.

S. 2389—Protecting Consumer Phone Records Act

Summary: S. 2389 would prohibit obtaining or selling the personal information of telecommunications customers—including phone records—without the consumer's consent. The bill also would require telecommunications carriers to take precautions to safeguard customers' personal information and to notify customers whenever there is a breach in the security of this information. Under S. 2389, the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) would enforce restrictions and requirements related to the security of this information, including assessing and collecting civil penalties for violations of the bill's provisions. Finally, the FCC and the FTC would conduct an outreach campaign to inform consumers of the security issues

involving telecommunications information. Assuming appropriation of the necessary amounts, CBO estimates that implementing the bill would cost less than $500,000 in 2006 and about $10 million over the 2007–2011 period.

Enacting S. 2389 could increase federal revenues and direct spending as a result of the collection of additional civil, criminal, and forfeiture penalties assessed for violations of the new laws and regulations. Collections of civil penalties and forfeiture penalties are recorded in the budget as revenues. Collections of criminal penalties are recorded in the budget as revenues, deposited in the Crime Victims Fund, and later spent. CBO estimates, however, that any additional revenues and direct spending that would result from enacting the bill would not be significant because of the relatively small number of cases likely to be involved.

S. 2389 contains intergovernmental mandates as defined in the Unfunded Mandates Reform Act (UMRA), but CBO estimates costs to state, local, and tribal governments, if any, would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted annually for inflation).

S. 2389 would impose new private-sector mandates, as defined in UMRA, on telecommunications carriers and providers of Internet protocol (IP)-enabled voice service. The bill would require the FCC to prescribe more stringent confidentiality requirements for customer proprietary network information and require telecommunications carriers and IP-enabled voice service providers to certify on an annual basis that they are in compliance with those regulations. Additionally, the bill would require such providers to notify customers on a timely basis if their customer information has been disclosed, and prohibit wireless telephone providers from listing subscribers' numbers in any directory assistance database or written directory without prior authorization. The costs of several mandates depend on regulations that have not been established; therefore, CBO cannot determine whether the costs of the mandates in the bill would exceed the 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 S. 2389 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 appropriated for each year. Based on information from the FTC and the FCC, CBO estimates that implementing the bill would cost each agency less than $250,000 in 2006 and about $5 million over the 2007–2011 period. In total, CBO estimates that implementing the bill would cost less than $500,000 in 2006 and about $10 million over the 2007–2011 period for the FCC and the FTC to enforce the bill's provisions regarding the personal information of telecommunications customers.

	By fiscal year, in millions of dollars—					
	2006	2007	2008	2009	2010	2011
CHANGES IN SPENDING SUBJECT TO APPROPRIATION						
Estimated Authorization Level	*	2	2	2	2	2
Estimated Outlays	*	2	2	2	2	2

Note: *=Less than $500,000.

Estimated impact on State, local, and tribal governments: Provisions in section 7 would require State Attorneys General to notify the FTC and the FCC of any action taken under the bill, allow either federal agency to intervene in those actions, and limit the actions that Attorneys General may take in certain circumstances. Also, provisions in sections 4 and 8 would preempt state laws regarding the protection and disclosure of certain phone records. Those provisions constitute intergovernmental mandates as defined in UMRA. CBO estimates that the aggregate costs, if any, to state, local, and tribal governments of complying with the mandates in the bill would be small and would not exceed the threshold established in UMRA ($64 million in 2006, adjusted for inflation).

Estimated impact on the private sector: S. 2389 would impose new private-sector mandates, as defined in UMRA, on telecommunications carriers and IP-enabled voice service providers. As the cost of many of the provisions in the bill depend on the rules to be prescribed by the FCC, CBO cannot determine whether the costs of the mandates in the bill would exceed the annual threshold for private-sector mandates ($128 million in 2006, adjusted annually for inflation).

Section 3 of the bill would require the FCC to prescribe regulations adopting more stringent confidentiality procedures for protecting customer proprietary network information. The FCC regulations would require telecommunications carriers and IP-enabled voice service providers to:

- Protect the security and confidentiality of customer proprietary network information;
- Certify annually that they are in compliance with the current FCC regulations on protecting customer proprietary information; and
- Notify a customer within 14 days if their information was disclosed in violation of FCC regulations.

According to government sources, some of the requirements are currently practiced by the telecommunications industry. In addition, according to industry sources the direct cost for carriers to comply with these new notification requirements would be nominal. The cost of providing such 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 those mandates.

Additionally, the bill would prohibit wireless communications providers from including their customers' wireless phone numbers in any wireless directory assistance service database or written directory without prior authorization. According to industry sources, wireless communications providers have not made this service available, however, some carriers may be exploring this service for their business subscribers. Those carriers have indicated that the cost of complying with this mandate would be small.

Previous CBO estimates: On March 15, 2006, CBO transmitted a cost estimate for H.R. 4943, the Prevention of Fraudulent Access to Phone Records Act, as ordered reported by the House Committee on Energy and Commerce on March 8, 2006. The two bills contain similar provisions related to the security of the personal information of telecommunications customers. CBO estimates that both bills would have similar costs for the FCC, but that S. 2389 would

have slightly higher costs for the FTC to enforce the new laws and regulations and to conduct the media campaign in conjunction with the FCC.

H.R. 4943 is similar in scope to S. 2389 but does not contain any preemptions of state and local laws. The intergovernmental mandates statements reflect that difference.

The private-sector mandates contained in H.R. 4943 are very similar to some of the mandates in S. 2389. Both bills require telecommunications carriers to increase the protection of customer proprietary network information, provide timely notice to each customer upon breach of customer proprietary network information. Because the cost of mandates in both bills depends on rules to be prescribed by the FCC, CBO could not determine whether those costs would exceed UMRA's annual threshold for private-sector mandates.

Estimate prepared by: Federal Costs: Melissa Z. Petersen; Impact on State, Local, and Tribal governments: Sarah Puro; Impact on the Private Sector: Fatimot Ladipo.

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

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

The FCC may issue regulations to implement the requirement set forth in the reported bill that it be illegal to acquire, use, sell, or solicit a person's confidential phone records without that person's consent. The reported bill also would require the FCC to promulgate rules to the extent it determines necessary, to require regulated entities to enhance their procedures for protecting consumer records and ensure that its rules regarding the security of confidential phone records are consistent with those protections adopted under GLBA, taking into account the differences between financial information and CPNI. The FCC would be required to develop regulations to implement these requirement, so individuals or businesses that handle relevant consumer records subject to the legislation would become subject to new or modified regulations.

ECONOMIC IMPACT

S. 2389 would not have an adverse economic impact on the nation's economy. The Act would require that the FCC impose additional safeguards and procedures on phone companies if they are determined to be necessary.

PRIVACY

The reported bill would enhance the personal privacy of U.S. citizens.

PAPERWORK

The reported bill should not increase paperwork requirements significantly for individuals and businesses.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title; Table of contents

This section sets forth the short title "Protecting Consumer Phone Records Act" and the table of contents.

Section 2. Unauthorized acquisition, use, or sale of confidential customer proprietary network telephone information

Subsection (a) would make it unlawful for any person to acquire, use, or sell another person's customer proprietary network information or CPNI, which is already defined in section 222(i)(1) of the 1934 Act and includes phone records and certain other information made available to carriers based on the customer's use of the service, without that person's affirmative written consent (which may be given electronically). This subsection would outlaw the sale of CPNI and specifically would outlaw misrepresenting that a person has given authorization to another person to obtain their phone records, often referred to as pretexting.

Subsection (b) would ensure that prohibitions under subsection 2(a) do not apply to legitimate business practices currently not prohibited by section 222 of the 1934 Act. This subsection would preserve law enforcement's ability to obtain phone records, require that IP-enabled voice service providers be treated like telecommunications carriers for purposes of section 2 of this bill, and clarify continued legality of using caller ID to identify calls received. Nothing in subsection 2(b)(4) prohibits the use of caller identification services to identify the originator of telephone calls or requirements enabling a person to conceal their telephone number from caller ID devices and services. In addition, the Committee is aware that under current law telecommunications carriers and IP-enabled voice service providers engage third parties in activities that involve CPNI in the normal course of business. For instance, a carrier or provider might contract out its billing functions, which necessarily involves CPNI, or may allow a company that is considering purchasing it to review its books and assets, including CPNI. In other examples, aggregate data containing phone numbers may be provided to third parties in a secure manner. Under each of these sharing scenarios, third parties agree via contract to be bound in their handling of such data by the laws applicable to carriers handling and use of such information. In still other cases, call data may be shared in connection with the provision of in-vehicle emergency communications in order to provide emergency services to consumers. Thus, to the extent that certain disclosures of CPNI data are permitted under current law, the Committee does not intend that anything in this Act would change the permissiveness of such practices. The Committee drafted the exception for legitimate business practices in subsection 2(b) with the intent of preserving such business practices that currently are not prohibited under section 222 of the 1934 Act or under the FCC's rules. The Committee does not intend for the exception to extend beyond normal business practices related to provisioning voice service. For instance, acquiring CPNI from another carrier in violation of section 2 is not intended to be covered by this exception.

Subsection (c) would allow phone companies to initiate a private right of action against data brokers or others who illegally acquire,

use, sell, or solicit phone records. This subsection would boost enforcement because a carrier may be in a better position than consumers to figure out who is obtaining this information and also may have more resources to litigate such claims. Similar authority has been helpful with respect to enforcing the anti-spam law. This subsection would provide for treble damages and for inflation adjustment.

Subsection (d) would allow a consumer who was harmed by a violation of section 2 to bring a civil action in a Federal district court or other court of competent jurisdiction, but would not allow a consumer to bring a civil action against a telecommunications carrier. The consumer would be able to obtain damages of up to $11,000 per violation or treble damages if the defendant is proved to have knowingly or willfully violated section 2. The district court would be permitted to assess against any party the costs of such an action, including reasonable attorney's fees.

Subsection (e) would provide for civil penalty of $11,000 for each violation or each day of a continuing violation, but caps penalty for single act or failure to act at $11,000,000.

Subsection (f) would clarify that nothing under this Act or section 222 of the 1934 Act authorizes a customer to bring a private right of action against a telecommunications carrier or an IP-enabled voice service provider.

Subsection (g) would provide definitions for the terms "Customer Proprietary Network Information," "IP-enabled voice service," and "Telecommunications Carrier."

Section 3. Enhanced confidentiality procedures

Subsection (a) would require the FCC to review its regulations and revise them, if necessary, to ensure that the regulations meet the three directives set forth in GLBA for financial institutions. To the extent the FCC revises its regulations, the Commission is directed to adopt rules similar in scope and structure to the regulations adopted by the FTC pursuant to GLBA. This is intended to help standardize industry practices for protecting consumer information.

Subsection (b) would require phone companies to annually certify that such carriers are in compliance with section 222 of the 1934 Act, as well as any regulations issued pursuant to this section.

Section 4. Penalties; Extension of confidentiality requirements to other entities

Subsection (a) would establish a $30,000 penalty per violation for any person found to have violated section 2 of this Act, with a limit of $90,000 per day for any continuing violation, and a cap of $3 million for any single act or failure to act. This section also would add additional criminal penalties under the 1934 Act of $30,000 per violation or $90,000 per day for any continuing violation.

Subsection (b) would extend FCC's phone record and CPNI rules to IP-enabled voice services. As a result, all wireline, wireless and IP based phone companies would be covered by comparable rights and obligations.

Subsection (c) would define IP-enabled voice service. The Committee notes that the definition of IP-enabled voice service provider is different in this bill than the definition used in the context of

911 calls over IP-enabled voice services. This bill would propose a definition that would capture one-way services that only allow calls to or from the public switched telephone network. In the context of 911, the Committee believed that consumers who purchase a voice service with limited capabilities and features would not necessarily expect to be able to call 911, so the definition in that context only included two-way services. However, the Committee believes that consumers still would have an expectation of privacy relative to the records of any phone calls they make or receive even in connection with a one-way service.

Subsection (d) would require telecommunications carriers and IP-enabled voice service providers to notify customers within 14 calendar days if they realize that the customers information has been provided to unauthorized third parties. This section also would provide an exception for delay consistent with law enforcement or homeland security determinations.

Subsection (e) would provide for a two-year statute of limitations for FCC enforcement under title V of the 1934 Act.

Subsection (f) would exempt cable VOIP service from the privacy requirements of title VI to the extent such service is covered by the Protecting Consumer Phone Records Act to provide competitive neutrality and to prevent conflicting regulatory requirements.

Subsection (g) prohibits commercial mobile service providers from including the wireless telephone number information of any customer in a wireless directory assistance service database unless the provider first provides notice to the customer of the right not to be listed, and then obtains separate, express authorization from the customer to be included in the directory upon request on a cost-free basis. Finally, this subsection preempts any State or local laws that are inconsistent with its requirements.

Section 5. Enforcement by the FTC

This section would provide authority for FTC enforcement of section 2 of the Protecting Consumer Phone Records Act as if a violation of that section were a violation of the FTC Act.

Section 6. Concurrent enforcement by the FCC

This section would give the FCC concurrent jurisdiction with the FTC to enforce section 2, and would provide that for enforcement purposes a violation of section 2 would be deemed a violation of the 1934 Act.

Section 7. Enforcement by States

Subsection 7(a) would allow States to sue in Federal district court to enforce section 2 or to impose civil penalties if State has reason to believe its citizens are threatened or adversely affected.

Subsection 7(b) would require that before initiating a civil action under subsection 7(a), a State must serve written notice on the FTC and the FCC.

Subsection 7(c) would allow the FTC and the FCC to intervene in a civil action under subsection 7(a) and to be heard on all matters therein and to file petitions for appeal of a decision in such civil action.

Subsection 7(d) would clarify that subsection 7(a) would not prevent a State from conducting investigations or administering oaths

or affirmations, or compelling the attendance of witnesses or the production of documentary and other evidence.

Subsection 7(e) would provide that venue for an action brought under subsection 7(a) lies in Federal district court pursuant to 28 U.S.C. 1391, and that process may be served without regard to territorial limits of the district or State where the action is instituted. Subsection 7(e) also would provide that a person who participated in an alleged violation may be joined in the civil action without regard to the residence of that person.

Subsection 7(f) would provide that if either the FTC or the FCC has instituted a proceeding for violation of section 2, the State in which the violation has occurred may not bring an action under section 2 against the same alleged violator during pendency of such proceeding.

Section 8. Preemption of State law

Section 8 would provide that sections 2 and any regulations prescribed pursuant to section 3 of this bill and section 222 of the 1934 Act shall preempt (1) any State or local statute, regulation or rule that requires a telecommunications carrier or provider of IP-enabled voice service to develop, implement, maintain, or restrict customer proprietary network information or other individually identifiable customer information held by that telecommunications carrier or provider of IP-enabled voice service, and (2) any such statute, regulation, or rule, or judicial precedent of any State court under which liability is imposed on a telecommunications carrier or provider of IP-enabled voice service for failure to comply with the requirements of section 2 or 3 of this Act, or section 222 of the 1934 Act. The Committee intends that Federal preemption under this section will extend to State laws that are inconsistent with the provisions of sections 2 or 3 of this Act and section 222 of the 1934 Act.

Section 9. Consumer outreach and education

Section 9 would require that within 180 days after the date of enactment of this Act, the FTC and the FCC shall jointly establish and implement a campaign to educate the public about the protection afforded under this Act as well as under the FTC Act and the 1934 Act. Subsection 9(b) would require such public education campaign to inform the public about the theft and misuse of customer proprietary network information, methods to protect such information, and Federal prevention and enforcement efforts. In carrying out this education requirement, the FTC and FCC must explore the use of various distribution platforms.

ROLLCALL VOTES IN COMMITTEE

Senator Pryor offered an amendment to the substitute that would allow a consumer who was harmed by a violation of section 2 to bring a civil action in a Federal district court or other court of competent jurisdiction. By a rollcall vote of 11 yeas and 10 nays as follows (Senator Rockefeller was recorded as necessarily absent), the amendment was adopted.

YEAS—11	NAYS—10
Ms. Snowe	Mr. McCain [1]
Mr. Smith	Mr. Burns [1]
Mr. Inouye	Mr. Lott
Mr. Kerry [1]	Mrs. Hutchison [1]
Mr. Dorgan[1]	Mr. Ensign[1]
Mrs. Boxer	Mr. Allen
Mr. Nelson of Florida [1]	Mr. Sununu
Ms. Cantwell	Mr. DeMint [1]
Mr. Lautenberg	Mr. Vitter[1]
Mr. Nelson of Nebraska[1]	Mr. Stevens
Mr. Pryor	

[1]By proxy

ADDITIONAL VIEWS OF SENATOR PRYOR

Private Right of Action for Consumers

As the Committee considered the difficult issue of protecting consumers' private phone records, I felt that it was extremely important that consumers be given the tools they need to protect themselves from fraudulent and unscrupulous behavior. In this legislation, we have provided a litany of enforcement protections for consumers-including enforcement by the Federal Trade Commission, Federal Communications Commission, and State Attorneys General. I believe that these enforcement protections are valuable and necessary to helping end the practice of fraudulently obtaining and selling consumers' phone records without authorization from the consumer. I support them wholeheartedly. However, these enforcement protections do not provide any recourse for the consumer-the person or persons most likely to be harmed by unauthorized disclosures of phone records. Furthermore, FTC, FCC, and State Attorney General enforcement actions do not provide adequate protections for those whose phone records are used for stalking and domestic violence. For this reason, I offered an amendment to the committee bill that would authorize consumers who have been harmed by a person fraudulently obtaining or selling their phone records to file suit against the person who caused the harm through a violation of this act.

The Committee also did adopt, as a part of this legislation, a providers' private right of action. Other recent consumer protection legislation has not included a consumers' private right of action. The inclusion of this amendment in this legislation does not lead me to believe that the committee will include a consumer private right of action in every circumstance. In the SPAM legislation, the committee provided Internet service providers a right of action. In S. 1408, the Identity Theft Protection Act, there is no consumer or provider private right of action. I believe that the exclusions of private rights of action in these pieces of legislation are not a good reason to exclude a consumer private right of action in this case. In both cases of identity theft and SPAM, the nature of the harm caused and the entity causing the harm are fundamentally different than is the case with phone records. Harm caused by SPAM is at worst an inconvenience, and legitimate businesses could have a breach due to an honest mistake in the case of identity theft. In those instances, we have not allowed consumers to sue businesses performing legitimate business practices. In the case of phone records, the nature of the harm that can be caused is dramatically different than in SPAM or identity theft because the harm can be physical-it can literally endanger someone's life. Individuals, rogue Internet operators, and fraudsters are deliberately trying to cause harm, and as the committee heard in testimony, this harm can sometimes lead to death. Because of the special type of harm that

can be caused by an unauthorized disclosure of phone records, I believe a consumer private right of action is a needed additional protection for consumers.

Several of my colleagues are concerned that the inclusion of this amendment will create a precedent for future committee consumer protection legislation. I believe that any future consideration of a private right of action for consumers should be done on a case by case basis. In this case of protecting phone records, I felt that a consumer private right of action was a common sense improvement to the bill, and a majority of my colleagues agreed. I don't expect my colleagues to always agree that this is an additional needed protection.

The purpose of this legislation is to protect consumers' phone records. They are the ones most likely to be harmed through an unauthorized release of their phone records, and they have as much of a legally protectable interest as their providers. The intention of my amendment is to provide recourse for consumers who might not have any other place to go for help, especially in the case of domestic violence. I feel they should be allowed to pursue action, independent of the government, against the criminals who intentionally steal their information with the intent to cause harm. The unauthorized disclosure, sale, or use of consumers' phone records are practices we are trying to eliminate through this legislation. I believe that more enforcement is always preferable to less enforcement. My amendment is an attempt to make this bill stronger for consumers.

CHANGES IN EXISTING LAW

SEC. 222. PRIVACY OF CUSTOMER INFORMATION.

[47 U.S.C. 222]

(a) IN GENERAL.—Every telecommunications carrier *or IP-enabled voice service provider* has a duty to protect the confidentiality of proprietary information of, and relating to, other [telecommunication carriers] *telecommunications carriers or IP-enabled voice service providers,* equipment manufacturers, and customers, including [telecommunication carriers] *telecommunications carriers or IP-enabled voice service providers* reselling telecommunications services provided by a telecommunications carrier *or IP-enabled voice service provider*.

(b) CONFIDENTIALITY OF CARRIER *AND IP-ENABLED VOICE SERVICE PROVIDER* INFORMATION.—A telecommunications carrier *or IP-enabled voice service provider* that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.

(c) CONFIDENTIALITY OF CUSTOMER PROPRIETARY NETWORK INFORMATION.—

(1) PRIVACY REQUIREMENTS FOR TELECOMMUNICATIONS CARRIERS *AND IP-ENABLED VOICE SERVICE PROVIDERS*.—Except as required by law or with the approval of the customer, a telecommunications carrier *or IP-enabled voice service provider* 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.

(2) DISCLOSURE ON REQUEST BY CUSTOMERS.—A telecommunications carrier *or IP-enabled voice service provider* shall disclose customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.

(3) AGGREGATE CUSTOMER INFORMATION.—A telecommunications carrier *or IP-enabled voice service provider* 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.

(d) EXCEPTIONS.—Nothing in this section prohibits a telecommunications carrier *or IP-enabled voice service provider* from using, disclosing, or permitting access to customer proprietary network information obtained from its customers, either directly or indirectly through its agents—

(1) to initiate, render, bill, and collect for telecommunications services;

(2) to protect the rights or property of the carrier *or provider*, or to protect users of those services and other carriers *or providers* 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 such call was initiated by the customer and the customer approves of the use of such information to provide such service; and

(4) to provide call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d))—

(A) to a public safety answering point, emergency medical service provider or emergency dispatch provider, public safety, fire service, or law enforcement official, or hospital emergency or trauma care facility, in order to respond to the user's call for emergency services;

(B) to inform the user's legal guardian or members of the user's immediate family of the user's location in an emergency situation that involves the risk of death or serious physical harm; or

(C) to providers of information or database management services solely for purposes of assisting in the delivery of emergency services in response to an emergency.

(e) SUBSCRIBER LIST INFORMATION.—Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service shall provide subscriber list information gathered in its capacity as a provider of such service on a timely and unbundled basis, under nondiscriminatory and reasonable rates, terms, and conditions, to any person upon request for the purpose of publishing directories in any format.

(f) AUTHORITY TO USE WIRELESS LOCATION INFORMATION.—For purposes of subsection (c)(1), without the express prior authorization of the customer, a customer shall not be considered to have approved the use or disclosure of or access to—

(1) call location information concerning the user of a commercial mobile service (as such term is defined in section 332(d)), other than in accordance with subsection (d)(4); or

(2) automatic crash notification information to any person other than for use in the operation of an automatic crash notification system.

(g) SUBSCRIBER LISTED AND UNLISTED INFORMATION FOR EMERGENCY SERVICES.—Notwithstanding subsections (b), (c), and (d), a telecommunications carrier that provides telephone exchange service *or IP-enabled voice service provider* shall provide information

described in subsection (i)(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) NOTICE OF VIOLATIONS.—

(1) IN GENERAL.—The Commission shall by regulation require each telecommunications carrier or IP-enabled voice service provider to notify a customer within 14 calendar days after the carrier or provider is notified of, or becomes aware of, an incident in which customer proprietary network information relating to such customer was disclosed to someone other than the customer in violation of this section or section 2 of the Protecting Consumer Phone Records Act.

(2) LAW ENFORCEMENT AND HOMELAND SECURITY RELATED DELAYS.—Notwithstanding paragraph (1), a telecommunications carrier or IP-enabled voice service provider may delay the required notification for a reasonable period of time if—

(A) a Federal or State law enforcement agency determines that giving notice within the 14-day period would materially impede a civil or criminal investigation; or

(B) a Federal national security agency or the Department of Homeland Security determines that giving notice within the 14-day period would threaten national or homeland security.

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

(1) CUSTOMER PROPRIETARY NETWORK INFORMATION.—The term "customer proprietary network information" means—

(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service *or IP-enabled voice service* subscribed to by any customer of a telecommunications carrier *or IP-enabled voice service provider*, and that is made available to the carrier *or provider* by the customer solely by virtue of the carrier-customer *or provider-customer* relationship; and

(B) information contained in the bills pertaining to **[**telephone exchange service or telephone toll service**]** *telephone exchange service, telephone toll service, or IP-enabled voice service* received by a customer of a carrier *or provider*;

except that such term does not include subscriber list **[**information.**]** *information nor does it include information that is related to non-voice service features bundled with IP-enabled voice service.*

(2) AGGREGATE INFORMATION.—The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

(3) SUBSCRIBER LIST INFORMATION.—The term "subscriber list information" means any information—

(A) identifying the listed names of subscribers of a carrier *or provider* and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and

(B) that the carrier *or provider* or an affiliate has published, caused to be published, or accepted for publication in any directory format.

(4) PUBLIC SAFETY ANSWERING POINT.—The term "public safety answering point" means a facility that has been designated to receive emergency calls and route them to emergency service personnel.

(5) EMERGENCY SERVICES.—The term "emergency services" means 9–1–1 emergency services and emergency notification services.

(6) EMERGENCY NOTIFICATION SERVICES.—The term "emergency notification services" means services that notify the public of an emergency.

(7) EMERGENCY SUPPORT SERVICES.—The term "emergency support services" means information or data base management services used in support of emergency services.

(8) 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 classes 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 interconnection capability such that the service can originate traffic to, or terminate traffic from, the public switched telephone network.

(j) WIRELESS CONSUMER PRIVACY PROTECTION.—

(1) IN GENERAL.—A provider of commercial mobile services, or any direct or indirect affiliate or agent of such a provider, may not include the wireless telephone number information of any subscriber in any wireless directory assistance service database unless the mobile service provider—

(A) provides a conspicuous, separate notice to the subscriber informing the subscriber of the right not to be listed in any wireless directory assistance service; and

(B) obtains express prior authorization for listing from such subscriber, separate from any authorization obtained to provide such subscriber with commercial mobile service, or any calling plan or service associated with such commercial mobile service, and such authorization has not been subsequently withdrawn.

(2) COST-FREE DE-LISTING.—A provider of commercial mobile services, or any direct or indirect affiliate or agent of such a provider, shall remove the wireless telephone number information of any subscriber from any wireless directory assistance service database upon request by that subscriber and without any cost to the subscriber.

(3) PUBLICATION OF DIRECTORIES PROHIBITED.—A provider of commercial mobile services, or any direct or indirect affiliate or

agent of such a provider, may not publish, in printed, electronic, or other form, or sell or otherwise disseminate, the contents of any wireless directory assistance service database, or any portion or segment thereof unless the mobile service provider—

(A) provides a conspicuous, separate notice to the subscriber informing the subscriber of the right not to be listed; and

(B) obtains express prior authorization for listing from such subscriber, separate from any authorization obtained to provide such subscriber with commercial mobile service, or any calling plan or service associated with such commercial mobile service, and such authorization has not been subsequently withdrawn.

(4) NO CONSUMER FEE FOR RETAINING PRIVACY.—A provider of commercial mobile services may not charge any subscriber for exercising any of the rights described under this subsection.

(5) STATE AND LOCAL LAWS PRE-EMPTED.—To the extent that any State or local government imposes requirements on providers of commercial mobile services, or any direct or indirect affiliate or agent of such providers, that are inconsistent with the requirements of this subsection, this subsection preempts such State or local requirements.

(6) DEFINITIONS.—In this subsection:

(A) WIRELESS TELEPHONE NUMBER INFORMATION.—The term "wireless telephone number information" means the telephone number, electronic address, and any other identifying information by which a calling party may reach a subscriber to commercial mobile services, and which is assigned by a commercial mobile service provider to such subscriber, and includes the name and address of such subscriber.

(B) WIRELESS DIRECTORY ASSISTANCE SERVICE.—The term "wireless directory assistance service" means any service for connecting calling parties to a subscriber of commercial mobile service when such calling parties themselves do not possess the wireless telephone number information of such subscriber.

* * * * * * *

SEC. 503. FORFEITURES IN CASES OF REBATES AND OFFSETS.

[47 U.S.C. 503]

(a) Any person who shall deliver messages for interstate or foreign transmission to any carrier, or for whom as sender or receiver, any such carrier shall transmit any interstate or foreign wire or radio communication, who shall knowingly by employee, agent, officer, or otherwise, directly or indirectly, by or through any means or device whatsoever, receive or accept from such common carrier any sum of money or any other valuable consideration as a rebate or offset against the regular charges for transmission of such messages as fixed by the schedules of charges provided for in this Act, shall in addition to any other penalty provided by this Act forfeit to the United States a sum of money three times the amount of money so received or accepted and three times the value of any

other consideration so received or accepted, to be ascertained by the trial court; and in the trial of said action all such rebates or other considerations so received or accepted for a period of six years prior to the commencement of the action, may be included therein, and the amount recovered shall be three times the total amount of money, or three times the total value of such consideration, so received or accepted, or both, as the case may be.

(b)(1) Any person who is determined by the Commission, in accordance with paragraph (3) or (4) of this subsection, to have—

(A) willfully or repeatedly failed to comply substantially with the terms and conditions of any license, permit, certificate, or other instrument or authorization issued by the Commission;

(B) willfully or repeatedly failed to comply with any of the provisions of this Act or of any rule, regulation, or order issued by the Commission under this Act or under any treaty, convention, or other agreement to which the United States is a party and which is binding upon the United States;

(C) violated any provision of section 317(c) or 508(a) of this Act; or

(D) violated any provision of section 1304, 1343, or 1464 of title 18, United States Code;

shall be liable to the United States for a forfeiture penalty. A forfeiture penalty under this subsection shall be in addition to any other penalty provided for by this Act; except that this subsection shall not apply to any conduct which is subject to forfeiture under title II, part II or III of title III, or section 506 of this Act.

(2)(A) If the violator is (i) a broadcast station licensee or permittee, (ii) a cable television operator, or (iii) an applicant for any broadcast or cable television operator license, permit, certificate, or other instrument or authorization issued by the Commission, the amount of any forfeiture penalty determined under this section shall not exceed $25,000 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $250,000 for any single act or failure to act described in paragraph (1) of this subsection.

(B) If the violator is a common carrier subject to the provisions of this Act or an applicant for any common carrier license, permit, certificate, or other instrument of authorization issued by the Commission, the amount of any forfeiture penalty determined under this subsection shall not exceed $100,000 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $1,000,000 for any single act or failure to act described in paragraph (1) of this subsection.

(C) In any case not covered in subparagraph (A) or (B), the amount of any forfeiture penalty determined under this subsection shall not exceed $10,000 for each violation or each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $75,000 for any single act or failure to act described in paragraph (1) of this subsection.

(D) The amount of such forfeiture penalty shall be assessed by the Commission, or its designee, by written notice. In determining the amount of such a forfeiture penalty, the Commission or its designee shall take into account the nature, circumstances, extent, and

gravity of the violation and, with respect to the violator, the degree of culpability, any history of prior offenses, ability to pay, and such other matters as justice may require.

(3)(A) At the discretion of the Commission, a forfeiture penalty may be determined against a person under this subsection after notice and an opportunity for a hearing before the Commission or an administrative law judge thereof in accordance with section 554 of title 5, United States Code. Any person against whom a forfeiture penalty is determined under this paragraph may obtain review thereof pursuant to section 402(a).

(B) If any person fails to pay an assessment of a forfeiture penalty determined under subparagraph (A) of this paragraph, after it has become a final and unappealable order or after the appropriate court has entered final judgment in favor of the Commission, the Commission shall refer the matter to the Attorney General of the United States, who shall recover the amount assessed in any appropriate district court of the United States. In such action, the validity and appropriateness of the final order imposing the forfeiture penalty shall not be subject to review.

(4) Except as provided in paragraph (3) of this subsection, no forfeiture penalty shall be imposed under this subsection against any person unless and until—

(A) the Commission issues a notice of apparent liability, in writing, with respect to such person;

(B) such notice has been received by such person, or until the Commission has sent such notice to the last known address of such person, by registered or certified mail; and

(C) such person is granted an opportunity to show, in writing, within such reasonable period of time as the Commission prescribes by rule or regulation, why no such forfeiture penalty should be imposed.

Such a notice shall (i) identify each specific provision, term, and condition of any Act, rule, regulation, order, treaty, convention, or other agreement, license, permit, certificate, instrument, or authorization which such person apparently violated or with which such person apparently failed to comply; (ii) set forth the nature of the act or omission charged against such person and the facts upon which such charge is based; and (iii) state the date on which such conduct occurred. Any forfeiture penalty determined under this paragraph shall be recoverable pursuant to section 504(a) of this Act.

(5) No forfeiture liability shall be determined under this subsection against any person, if such person does not hold a license, permit, certificate, or other authorization issued by the Commission, and if such person is not an applicant for a license, permit, certificate, or other authorization issued by the Commission, unless, prior to the notice required by paragraph (3) of this subsection or the notice of apparent liability required by paragraph (4) of this subsection, such person (A) is sent a citation of the violation charged; (B) is given a reasonable opportunity for a personal interview with an official of the Commission, at the field office of the Commission which is nearest to such person's place of residence; and (C) subsequently engages in conduct of the type described in such citation. The provisions of this paragraph shall not apply,

however, if the person involved is engaging in activities for which a license, permit, certificate, or other authorization is required, or is a cable television system operator, if the person involved is transmitting on frequencies assigned for use in a service in which individual station operation is authorized by rule pursuant to section 307(e), or in the case of violations of section 303(q), if the person involved is a nonlicensee tower owner who has previously received notice of the obligations imposed by section 303(q) from the Commission or the permittee or licensee who uses that tower. Whenever the requirements of this paragraph are satisfied with respect to a paricular person, such person shall not be entitled to receive any additional citation of the violation charged, with respect to any conduct of the type described in the citation sent under this paragraph.

(6) No forfeiture penalty shall be determined or imposed against any person under this subsection if—

(A) such person holds a broadcast station license issued under title III of this Act and if the violation charged occurred—

(i) more than 1 year prior to the date of issuance of the required notice or notice of apparent liability; or

(ii) prior to the date of commencement of the current term of such license,

whichever is earlier; or

[(B) such person does not hold a broadcast station license issued under title III of this Act and if the violation charged occurred more than 1 year prior to the date of issuance of the required notice or notice of apparent liability.]

(B) such person does not hold a broadcast station license issued under title III of this Act and—

(i) the person is charged with violating section 222 and the violation occurred more than 2 years prior to the date of issuance of the required notice or notice of apparent liability; or

(ii) the person is charged with violating any other provision of this Act and the violation occurred more than 1 year prior to the date of issuance of the required notice or notice of apparent liability.

For purposes of this paragraph, "date of commencement of the current term of such license" means the date of commencement of the last term of license for which the licensee has been granted a license by the Commission. A separate license term shall not be deemed to have commenced as a result of continuing a license in effect under section 307(c) pending decision on an application for renewal of the license.

SEC. 509. PENALTIES FOR CONFIDENTIAL CUSTOMER PROPRIETARY NETWORK INFORMATION VIOLATIONS.

(a) CIVIL FORFEITURE.—

(1) IN GENERAL.—Any person determined by the Commission, in accordance with paragraphs (3) and (4) of section 503(b), to have violated section 2 of the Protecting Consumer Phone Records Act shall be liable to the United States for a forfeiture penalty. A forfeiture penalty under this subsection shall be in addition to any other penalty provided for by this Act. The

amount of the forfeiture penalty determined under this subsection shall not exceed $30,000 for each violation, or 3 times that amount for each day of a continuing violation, except that the amount assessed for any continuing violation shall not exceed a total of $3,000,000 for any single act or failure to act.

(2) RECOVERY.—Any forfeiture penalty determined under paragraph (1) shall be recoverable pursuant to section 504(a) of this Act.

(3) PROCEDURE.—No forfeiture liability shall be determined under paragraph (1) against any person unless such person receives the notice required by section 503(b)(3) or section 503(b)(4) of this Act.

(4) 2-YEAR STATUTE OF LIMITATIONS.—No forfeiture penalty shall be determined or imposed against any person under paragraph (1) if the violation charged occurred more than 2 years prior to the date of issuance of the required notice or notice or apparent liability.

(b) CRIMINAL FINE.—Any person who willfully and knowingly violates section 2 of the Protecting Consumer Phone Records Act shall upon conviction thereof be fined not more than $30,000 for each violation, or 3 times that amount for each day of a continuing violation, in lieu of the fine provided by section 501 for such a violation. This subsection does not supersede the provisions of section 501 relating to imprisonment or the imposition of a penalty of both fine and imprisonment.

* * * * * * *

PART IV—MISCELLANEOUS PROVISIONS

SEC. 631. PROTECTION OF SUBSCRIBER PRIVACY.

[47 U.S.C. 551]

(a)(1) At the time of entering into an agreement to provide any cable service or other service to a subscriber and at least once a year thereafter, a cable operator shall provide notice in the form of a separate, written statement to such subscriber which clearly and conspicuously informs the subscriber of—

(A) the nature of personally identifiable information collected or to be collected with respect to the subscriber and the nature of the use of such information;

(B) the nature, frequency, and purpose of any disclosure which may be made of such information, including an identification of the types of persons to whom the disclosure may be made;

(C) the period during which such information will be maintained by the cable operator;

(D) the times and place at which the subscriber may have access to such information in accordance with subsection (d); and

(E) the limitations provided by this section with respect to the collection and disclosure of information by a cable operator and the right of the subscriber under subsections (f) and (h) to enforce such limitations.

In the case of subscribers who have entered into such an agreement before the effective date of this section, such notice shall be

provided within 180 days of such date and at least once a year thereafter.

(2) For purposes of this section, other than subsection (h)—

(A) the term "personally identifiable information" does not include any record of aggregate data which does not identify particular persons;

(B) the term "other service" includes any wire or radio communications service provided using any of the facilities of a cable operator that are used in the provision of cable service; and

(C) the term "cable operator" includes, in addition to persons within the definition of cable operator in section 602, any person who (i) is owned or controlled by, or under common ownership or control with, a cable operator, and (ii) provides any wire or radio communications service.

(b)(1) Except as provided in paragraph (2), a cable operator shall not use the cable system to collect personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned.

(2) A cable operator may use the cable system to collect such information in order to—

(A) obtain information necessary to render a cable service or other service provided by the cable operator to the subscriber; or

(B) detect unauthorized reception of cable communications.

(c)(1) Except as provided in paragraph (2), a cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator.

(2) A cable operator may disclose such information if the disclosure is—

(A) necessary to render, or conduct a legitimate business activity related to, a cable service or other service provided by the cable operator to the subscriber;

(B) subject to subsection (h), made pursuant to a court order authorizing such disclosure, if the subscriber is notified of such order by the person to whom the order is directed;

(C) a disclosure of the names and addresses of subscribers to any cable service or other service, if—

(i) the cable operator has provided the subscriber the opportunity to prohibit or limit such disclosure, and

(ii) the disclosure does not reveal, directly or indirectly, the—

(I) extent of any viewing or other use by the subscriber of a cable service or other service provided by the cable operator, or

(II) the nature of any transaction made by the subscriber over the cable system of the cable operator; or

(D) to a government entity as authorized under chapters 119, 121, or 206 of title 18, United States Code, except that such disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator.

(d) A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator. Such information shall be made available to the subscriber at reasonable times and at a convenient place designated by such cable operator. A cable subscriber shall be provided reasonable opportunity to correct any error in such information.

(e) A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information under subsection (d) or pursuant to a court order.

(f)(1) Any person aggrieved by any act of a cable operator in violation of this section may bring a civil action in a United States district court.

(2) The court may award—

(A) actual damages but not less than liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is higher;

(B) punitive damages; and

(C) reasonable attorneys' fees and other litigation costs reasonably incurred.

(3) The remedy provided by this section shall be in addition to any other lawful remedy available to a cable subscriber.

(g) Nothing in this title shall be construed to prohibit any State or any franchising authority from enacting or enforcing laws consistent with this section for the protection of subscriber privacy.

(h) Except as provided in subsection (c)(2)(D), a governmental entity may obtain personally identifiable information concerning a cable subscriber pursuant to a court order only if, in the court proceeding relevant to such court order—

(1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and

(2) the subject of the information is afforded the opportunity to appear and contest such entity's claim.

(i) CUSTOMER PROPRIETARY NETWORK INFORMATION.—This section does not apply to customer proprietary network information (as defined in section 222(i)(1) of this Act) as it relates to the provision of IP-enabled voice service (as defined in section 222(i)(8) of this Act) by a cable operator to the extent that section 222 of this Act and section 2 of the Protecting Consumer Phone Records Act applies to such information.

○