COMBATING PRETEXTING: PREVENTION OF FRAUDULENT ACCESS TO PHONE RECORDS ACT

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

ON

H.R. 936

MARCH 9, 2007

Serial No. 110–16

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

39–361 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON ENERGY AND COMMERCE

JOHN D. DINGELL, Michigan, *Chairman*

HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
DIANA DeGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
DARLENE HOOLEY, Oregon
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana

JOE BARTON, Texas
Ranking Minority Member
RALPH M. HALL, Texas
J. DENNIS HASTERT, Illinois
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee

PROFESSIONAL STAFF

DENNIS B. FITZGIBBONS, *Chief of Staff*
GREGG A. ROTHSCHILD, *Chief Counsel*
SHARON E. DAVIS, *Chief Clerk*
BUD ALBRIGHT, *Minority Staff Director*

C O N T E N T S

	Page
Hon. John D. Dingell, a Representative in Congress from the State of Michigan, opening statement	1
Hon. Hon. Fred Upton, a Representative in Congress from the State of Michigan, opening statement	3
Hon. Edward J. Markey, a Representative in Congress from the Commonwealth of Massachusetts, opening statement	4
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement	5
Hon. Bobby L. Rush, a Representative in Congress from the State of Illinois, opening statement	6
Hon. Joe Barton, a Representative in Congress from the State of Texas, opening statement	6
Hon. Rick Boucher, a Representative in Congress from the Commonwealth of Virginia, opening statement	7
Hon. J. Dennis Hastert, a Representative in Congress from the State of Illinois, opening statement	7
Hon. Albert R. Wynn, a Representative in Congress from the State of Maryland, opening statement	8
Hon. Joseph R. Pitts, a Representative in Congress from the Commonwealth of Pennsylvania, opening statement	8
Hon. Gene Green, a Representative in Congress from the State of Texas, opening statement	9
Hon. Greg Walden, a Representative in Congress from the State of Oregon, opening statement	9
Hon. Anthony D. Weiner, a Representative in Congress from the State of New York, opening statement	10
Hon. Diana DeGette, a Representative in Congress from the State of Colorado, opening statement	10
Hon. Edolphus Towns, a Representative in Congress from the State of New York, opening statement	11
Hon. Jay Inslee, a Representative in Congress from the State of Washington, opening statement	12
Hon. Tammy Baldwin, a Representative in Congress from the State of Wisconsin, opening statement	12
Hon. Barbara Cubin, a Representative in Congress from the State of Colorado, opening statement	13
Hon. Jan Schakowsky, a Representative in Congress from the State of Illinois, opening statement	13
H.R. 936, To prohibit fraudulent access to telephone records.	14

WITNESSES

Lydia Parnes, Director, Bureau of Consumer Protection, U.S. Federal Trade Commission	32
Prepared statement	34
Thomas Navin, Chief, Wireline Bureau, Federal Communications Commission	45
Prepared statement	47
Marc Rotenberg, executive director, Electronic Privacy Information Center	56
Prepared statement	56
Hon. Steve Largent, president, chief executive officer, CTIA-the Wireless Association	67
Prepared statement	69
Walter McCormick, president and chief executive officer, United States Telecom Association	79

Page

Walter McCormick, president and chief executive officer, United States Telecom Association—Continued
Prepared statement 81
David Einhorn, president, Greenlight Capital, Incorporated, ... 84
Prepared statement 86

COMBATING PRETEXTING: PREVENTION OF FRAUDULENT ACCESS TO PHONE RECORDS ACT

FRIDAY, MARCH 9, 2007

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
Washington, DC.

The committee met, pursuant to call, at 10:30 a.m., in room 2123 of the Rayburn House Office Building, Hon. John D. Dingell (chairman) presiding.

Members present: Representatives Markey, Boucher, Towns, Rush, Stupak, Wynn, Green, DeGette, Schakowsky, Gonzalez, Inslee, Baldwin, Hooley, Weiner, Barrow, Barton, Hall, Hastert, Upton, Stearns, Cubin, Shimkus, Shadegg, Pickering, Radanovich, Pitts, Walden, Terry, Ferguson, Rogers, Sullivan, Murphy, and Burgess.

OPENING STATEMENT OF HON. JOHN D. DINGELL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

The CHAIRMAN. The hearing will come to order.

I thank you all for coming here to be with us and discuss these matters, our views on H.R. 936, the Prevention of Fraudulent Access to Phone Records Act.

A certain major telecommunications company allegedly turned over detailed call records of millions of Americans to the National Security Agency. These phone customers were not informed that NSA had their records. Apparently, this may have been done without proper process. At least one company found it illegal and refused to comply.

We also learned about pretexting, which occurs when a person obtains phone records through fraudulent means. Apparently, some of the largest companies in America, such as Hewlett-Packard Corporation, did not see any problems in using this deceptive practice. One of our witnesses discovered 40 Web sites that offered to sell phone records to anyone online.

Last Congress, this committee's Subcommittee on Oversight and Investigations held several hearings on pretexting abuses and scandals, and I want to commend our two friends, Mr. Stupak and Mr. Whitfield for their extraordinary leadership in building a strong record on these matters.

In a bipartisan manner, this committee passed the same legislation that we are discussing today. The legislation is bipartisan, and I intend to see that it remains so.

We also commend Ranking Member Barton for his distinguished leadership and for his willingness to work to produce sound legislation.

Unfortunately, after the committee reported the bill, for some strange reason, it mysteriously disappeared from the House floor schedule, and the House took no action before the 109th Congress adjourned, so today, we will continue our effort to ensure that call record information held by phone companies remains secure.

In that regard, I am pleased that we have before us representatives of the Federal Communications Commission and the Federal Trade Commission to discuss these matters. The FCC is charged with ensuring that phone companies protect our calling records. And the FTC has the ability to crack down on fraudulent practices, such as pretexting. This legislation will provide more specific authority to both the FCC and the FTC to take appropriate action.

We need to hear from the FCC what they are doing to protect these records. Every telecommunications company under the Communications Act has a duty to protect the sensitive, personal information of customers. Given the well-publicized breaches of customer privacy, we must address whether the statute adequately empowers the FCC to protect those records. I am aware that the FCC had expected to issue new rules governing phone record security by the end of the year. And we are encouraged that that is so, and we encourage the FCC to issue these new rules as quickly as they are able.

Likewise, we need to hear from the FTC on whether or not they believe they have the authority, under existing law, to pursue those who engage in pretexting. The FTC has been aggressive in using section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive acts and practices in interstate commerce to bring enforcement actions against pretexters. But last year, they testified that more specific prohibitions were needed against pretexting soliciting and selling customer phone records. The agency also seeks enhanced authority to impose civil penalties.

The Chair also looks forward to the testimony of the other distinguished members of our panel, the landline and wireless companies. And last, but, by no means, least, we will hear important testimony from a victim of pretexting. This is not a faceless crime, and it is not a crime that has no consequences. Mr. Einhorn, the committee thanks you for coming before us, and I am sorry, indeed, about what has happened to you and your family, and I pledge the best efforts of myself and the committee to make this kind of event less likely to happen to anyone else.

In the interest of fairness, the committee will leave the record open for 30 days in case Allied Capital wants to submit a statement.

This measure passed this committee in a bipartisan fashion last Congress. Just as Mr. Barton did last Congress so effectively well, I will work to address this issue in the same bipartisan manner. And as always, the committee will conduct the oversight necessary

to ensure that the American people are protected in the privacy of their phone records.

The Chair will follow the usual practices of the committee, and we will recognize the members for 3 minutes. And if the members choose to waive that 3-minute opening statement, they will be recognized for an additional 3 minutes at the time of the questioning.

The Chair recognizes now the distinguished gentleman from Michigan, Mr. Upton, who has done a superb job on this legislation. Mr. Upton for 3 minutes.

OPENING STATEMENT OF HON. FRED UPTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MICHIGAN

Mr. UPTON. Well, thank you, Mr. Chairman. I know Mr. Barton is on the way as well.

There have been great advances in technology since the days of the little black rotary phone. But the unfortunate reality is that, along with great advances in technology, there have been great advances in fraud as well.

Over the last year, pretexting has garnered the national spotlight. Nearly a year ago, to the day, we marked up similar legislation in this committee, but hit a few minor bumps along the way. And I am hopeful that we will have a little more success this time, and consumers will, in fact, be the better for it.

On the surface, pretexting seems harmless enough, but it is a violation of one's basic rights that can have grave consequences. Someone with bad intentions and a few bucks can get a hold of almost anyone cell phone record. It is alarming that our cell phone bills, a score sheet for our daily lives, can fall into the wrong hands with a simple phone call or even a click of the mouse.

The consequences of firms trying to make a quick buck on the Internet are terrifying. Records can be used to track down someone's location, such as a woman in hiding from an abusive partner or stalker. Gangs and drug runners have been known to obtain phone records to determine if anyone in their group, in their gang, has been in contact with rival groups or even with the police.

It doesn't matter what the motive is, no matter how barbaric or innocent the intentions, pretexting is wrong and a violation of an individual's basic right to privacy. Carriers do have a duty to protect their customers, and we have a duty to close the loophole once and for all.

We have a quality piece of bipartisan legislation that will bring an end to this practice, once and for all. And the Nation's 190 million cell phone users will all be safer for it. And while we continue to make great advances in technology, one thing that will continue to remain constant is the consumer's right to privacy.

I yield back my time.

Thank you, Mr. Chairman.

The CHAIRMAN. I thank the gentleman.

The Chair recognizes now the distinguished gentleman from Massachusetts, Mr. Markey, for 3 minutes.

OPENING STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. MARKEY. I thank the chairman very much.

Mr. Chairman, personal privacy is the cornerstone of individual freedom. A person's telephone records can disclose some of the most intimate details of a person's life. information about who you call, when you call, how long you are on the phone can reveal a lot about a person, their relationships, their business dealings, their family members, their children. The public sale of this information can be embarrassing, awkward, and uncomfortable for a consumer. It can be dangerous when it is in the hands of stalkers, thieves, abusers, and others who intend to do harm.

More troubling, in my mind, is the fact that last year this committee discovered that pretexting is not solely the province of individual, low-rent fraudsters who prey on vulnerable citizens. In a shocking revelation last September, Hewlett-Packard, a Fortune 500 company, agreed to pay a $14 million penalty for illegal pretexting. Likewise, Washington hedge fund manager, David Einhorn, who is testifying here today, fell victim to pretexting when a financial service's firm hired someone to illegally obtain his phone records.

In the last Congress, this committee passed this important bill to ensure that consumer phone records are not for sale in some cyberspace bizarre and to take action to shut down these practices. Last session's bill, however, mysteriously disappeared from the House suspension calendar prior to House floor consideration, reportedly due to concerns from the intelligence community. These concerns implicated the alleged disclosure of phone records by certain telephone companies to the National Security Agency or others. The pretexting bill's sudden disappearance represented a case of extraordinary legislative rendition.

Under the Telecommunications Act, telephone companies are legally obligated to safeguard the confidentiality of phone records. After the scandals of last year, many phone companies certainly responded by tightening internal controls to prevent unauthorized disclosure of phone records. While the fraudsters may be acting illegally by using pretexting, the fact that these records are apparently so easily obtained on the Internet and elsewhere makes it self-evident that enforcement and security needs to be stepped up.

The FCC has been developing new rules to do just that for several months, and we are eager for the Commission to finalize its action. Doing so may obviate the need to legislate portions of the bill before us. I also continue to believe it is important for the Commission, as an independent, regulatory agency, to investigate media reports regarding disclosure of consumer phone records by phone companies without legal process and in violation of the Communications Act. This is still timely, as this morning's newspapers indicate. There is still a lack of respect of a law of our country that privacy of Americans be protected and that only a judge, ultimately, can authorize the compromise of these important communications records.

I look forward to working with you, Mr. Chairman, Mr. Barton, Mr. Upton, with Chairman Rush, and Mr. Stearns, and our other committee colleagues on this important legislation.

I thank you.

The CHAIRMAN. The Chair thanks the distinguished gentleman.

The Chair recognizes now our good friend from Florida, Mr. Stearns, for 3 minutes.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Mr. Chairman, thank you very much. This is deja vu all over again. I mean, we have been talking about this bill. We have had the hearings on it in my subcommittee that I chaired in the last Congress, Commerce, Consumer Protection and Trade with the Federal Trade Commission having jurisdiction over this. Unfortunately, the Telecom Act of 1996 exempted common carriers, which allowed this to be under the jurisdiction of the FCC rather than the Federal Trade Commission. I think many of us on this side were sorely disappointed that we couldn't have reached a compromise and had this bill on the floor under suspension, perhaps with amendment, and got this through. I think we all realize, no matter what we talk about, the stark reality is that there is always going to be con artists and cyber thieves to keep us busy. And so we have got to pass this bill. We must recognize the importance of securing and protecting personal data from exploitation by fraudsters, whether the preferred technique is pretexting, hacking, or good old-fashioned fraud. Likewise, ensuring the public is informed about the need to protect personal data will also help thwart the fastest-growing criminal enterprise in America, which is identity theft.

So, Mr. Chairman, our subcommittee that I chaired and now that Mr. Rush chairs are eagerly looking forward to passing this. And I think under your leadership, Mr. Dingell, hopefully, we will have this on the floor in short order. I think it is an issue that, for a long time, has been in agreement that it should pass. I am a cosponsor of this bill, this H.R. 936. As we all know, it is not perfect. Perhaps as it works its way through the process out of our committee and to the House floor and to the Senate, we will have that opportunity to improve it. Hopefully, the intelligence community will come on board and not thwart and prevent this from passing. I think the good of this is overwhelming, and we must not restrict legitimate marketing practices that can benefit consumers, but we also might understand that there is a need to identify and protect the consumers' privacy.

So I look forward to working with you, Mr. Chairman, and obviously Mr. Upton, who is chairman of the Telecommunications Committee, and the ranking member of our full committee, Mr. Barton.

Thank you.

The CHAIRMAN. The Chair recognizes now the distinguished gentleman from Illinois, Mr. Rush, for 3 minutes.

OPENING STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. RUSH. Thank you, Chairman Dingell, for conducting this hearing. And I want to commend you and Ranking Member Barton for your continued bipartisan leadership on this issue.

Mr. Chairman, pretexting is a serious problem that can have devastating effects on the average consumer. And I am sure Mr. Einhorn's testimony will further illustrate the devastating effects that pretexting can have.

Mr. Chairman, H.R. 936, the Prevention of Fraudulent Access to Phone Records Act, is a hard-hitting but deliberative response to this widespread crime. Most of today's discussion in our hearing will center around title 2 of the bill. But as chairman of the Subcommittee on Commerce, Trade, and Consumer Protection, I want to highlight the provisions of title 1.

Title 1 of the bill grants the FTC specific authority to crack down on pretexters by explicitly declaring the practice of fraudulently obtaining or selling customer proprietary network information as an unlawful conduct and an unlawful act. The FTC will enforce this provision as a violation of the Federal Trade Commission Act and its prohibition on unfair or deceptive practices. The Commission is to be lauded for its past and ongoing enforcement actions under its existing authority under Section 5 of the FTC Act. But last year, in hearings, we heard testimony that the Commission needed more specific statutory authority to better protect the public. title 1 fulfills this need.

Mr. Chairman, every returning member of this committee voted for this bill in the last Congress, and it is my sincere hope that every member of this committee will repeat that vote.

Too many consumers remain vulnerable to pretexting and its devastating effects, and H.R. 936 will go a long way in addressing this basic consumer protection issue. Last Congress, we did our job. We reported a good bill out of our committee for consideration on the House floor only to see it go nowhere and die. I hope this year's bill won't meet the same fate. Let us make sure that today's hearing is the 110th Congress's first step toward eventually enacting this important measure into law.

Thank you, Mr. Chairman. I yield back the balance of my time.

The CHAIRMAN. Thanks to the distinguished gentleman from Illinois.

It is with great pleasure that the Chair recognizes my good friend and colleague, the ranking member of the committee, Mr. Barton, who provided such extraordinary leadership in this matter last year. The gentleman is recognized for 5 minutes.

OPENING STATEMENT OF HON. JOE BARTON, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. BARTON. Thank you, Mr. Chairman.

I won't take very much time. I am submitting my full statement for the record. Suffice it to say that we worked together on this in the last Congress and didn't quite get over the finish line. I am proud to be an original sponsor with you and several other members in this Congress. Pretexting is something that we need to combat. And as we all know, pretexting is pretending to be someone

you are not to get something you shouldn't have to use in a way that is probably wrong.

So I am sure, on a bipartisan basis, we can move this bill and move it to the floor and move it to the Senate and put it on the President's desk and strike a blow for individual privacy in this Congress.

And with that, I would yield back.

The CHAIRMAN. The Chair thanks the gentleman, and without objection, his full statement will appear in the record, as will the statements of our other colleagues, who so desire.

The Chair recognizes now our good friend and colleague, the gentleman from Virginia, Mr. Boucher, for 1 minute. Mr. Boucher.

OPENING STATEMENT OF HON. RICK BOUCHER, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF VIRGINIA

Mr. BOUCHER. Well, thank you very much, Mr. Chairman.

It is my pleasure to join with you and other members of the committee in cosponsoring this measure. And I commend the bipartisan process that has produced this bill. Pretexting was rendered unlawful by action in the last Congress, but there is an ongoing need to make sure that the integrity of customer proprietary information is protected by local exchange carriers and by the wireless industry. That information should never be sold, and there should be ongoing steps taken by the carrier to make sure that that information is appropriately safeguarded.

That said, I think it is also important that we carefully evaluate the exemptions to make sure that none of the provisions about sharing information with third parties would prohibit normal and effective operations by the telecommunications carrier. They need to contract out certain information to third parties, including engineers and information technology specialists of various kinds. And the ability to do that is absolutely essential to the effective functioning of their operations. And so I would simply urge the committee to take care, as we have this hearing, to listen to the representatives of the telecommunications industry and heed their recommendations with regard to what the scope of those exemptions should be.

Thank you, Mr. Chairman, and I yield back.

Ms. DEGETTE [presiding]. The Chair is now delighted to recognize Mr. Hastert for 1 minute.

OPENING STATEMENT OF HON. J. DENNIS HASTERT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. HASTERT. Well, thank you, Madame Chairwoman.

I would like to thank the witnesses for coming this morning to speak about pretexting and the sale of phone records. Since the development of the Internet, our personal information has been more readily available and increasingly easier to obtain. In fact, there is a growing market for the sale of phone records. These records provide detailed information about who and what and when we call and how long we spend on the phone. Fraudulently obtaining this information is an invasion to our personal privacy, and it cannot be allowed to continue.

But at the same time, we need to provide for equal treatment for all those who collect that data. As we move forward, we should ensure that this bill will not hamper lawful and necessary means to protect our country from foreign terrorism. I look forward to hearing from each witness as we address these concerns.

And I thank you, and I yield back my time.

Ms. DEGETTE. The Chair now recognizes the distinguished gentleman from Maryland, Mr. Wynn, for 1 minute.

OPENING STATEMENT OF HON. ALBERT R. WYNN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF MARYLAND

Mr. WYNN. Thank you, Madame Chairman, for holding this hearing on an issue of such importance to American consumers. Pretexting, the unlawful, false, fictitious or fraudulent statements or representations in order to obtain the personal proprietary information of a consumer poses serious threats to the privacy of consumers and to the integrity of the telecommunications industry. The ease with which one can obtain private information on other individuals concerns me, especially when we know the harm that can be done with such records. The improper use of customer propriety network information, CPNI, have been used in the past by suspected mobsters to intimidate police officers and by stalking in the murder of Amy Boyer in 1999.

As a matter of public policy, we must ensure that this type of information cannot be easily bought over the Internet. We need to pass legislation to make sure that those who illegally purchase CPNI are aggressively prosecuted, but, at the same time, we need to make sure this bill does not hamstring telecommunication providers who use CPNI in a responsible manner to better target their consumers for new products or services and ultimately pass savings along to them.

I look forward to this hearing and hearing from the witnesses. It is critical that we safeguard individuals from pretexting. I thank you for this time, and I yield back.

Ms. DEGETTE. The Chair now recognizes the distinguished gentleman from Illinois, Mr. Shimkus, for 1 minute.

Mr. SHIMKUS. I will waive.

Ms. DEGETTE. The gentleman waives.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Pitts.

OPENING STATEMENT OF HON. JOSEPH R. PITTS, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF PENNSYLVANIA

Mr. PITTS. Thank you, Madame Chairman.

I am looking forward to hearing what our witnesses have to say this morning. Everyone agrees that pretexting needs to be stopped, but we need to do it in a way that does not ensnare legitimate business practices. We have a good bill before us, and I will be interested to hear what our witnesses have to say about how we can improve it when we mark it up.

I am also grateful to the sponsors of this bill for including the wireless directory assistance language that I and my friend Chair-

man Markey worked so hard on over the last two Congresses. While telephone numbers are not, strictly speaking, considered customer proprietary network information, wireless telephone numbers are definitely considered personal information by the vast majority of consumers, and I expect this language will become law this year, and I am very happy about that. This hearing will also be a chance for us to make sure that that part of the bill is written the best way possible and will not have any unintended consequences.

Thank you, Madame Chairman.

Ms. DEGETTE. The Chair now recognizes the distinguished gentleman from Texas, Mr. Green, for 1 minute.

OPENING STATEMENT OF HON. GENE GREEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. GREEN. Madame Chairman, I am glad we are considering H.R. 936, and I am a proud cosponsor of it. Our committee has a history of privacy protections, going back to the legislation on banking in the last decade, and we are concerned about the privacy of our own information, whether it is good banking records or our cell phones and our own hard lines. And pretexting should have passed last time, as most of my colleagues said. I think there is an issue we are going to have to deal with on the contracting out, as I heard our chair of the Energy Subcommittee talk about. I would just hope that whatever we do about contracting out would have the same restrictions as the person who is doing the contracting.

And I yield back my time.

Ms. DEGETTE. The gentleman yields back.

The Chair now recognizes the distinguished gentleman from Oregon, Mr. Walden, for 1 minute.

OPENING STATEMENT OF HON. GREG WALDEN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OREGON

Mr. WALDEN. Thank you, Madame Chair.

I am looking forward to this hearing, and while I supported this legislation last year and certainly participated in the oversight hearings on pretexting, I want to make sure that, as we move forward, that we aren't doing something that has unintended consequences when it comes to legitimate marketing issues so that consumers can get access to information for offers and things they may want to take advantage of. And so I am going to raise a few of those questions. I think there have been some points raised since this bill was passed out of this committee last year and sent to the full House, which never took it up, that need to be addressed to make sure we are doing the right thing, which is protecting the rights of consumers, not to be ripped off and not to be abused, as we witnessed in our hearings. And there are some very serious legitimate problems out there that we need to address. In doing so, let us make sure that we don't go overboard.

So thank you for this hearing and for your work on the Oversight Committee as well, and I look forward to the testimony of our witnesses.

Ms. DEGETTE. The gentleman yields back.

The Chair now recognizes the gentleman from Texas, Mr. Gonzalez, for 1 minute.

Mr. GONZALEZ. I waive.

Ms. DEGETTE. The gentleman waives.

The Chair now recognizes the distinguished gentle lady from Oregon, Ms. Hooley, for 1 minute.

The gentle lady waives.

The gentleman from New York, Mr. Weiner.

OPENING STATEMENT OF HON. ANTHONY D. WEINER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. WEINER. Thank you, Madame Chair. And I look forward to this hearing, and I want to commend the committee for the work that they have done last year.

There are some foundational principles that we should keep in mind. One is there has to be a reasonable understanding that consumers expect the information to be shared. In this case, I think most, as Mr. Markey said, consumers don't even realize this information is available to be shared. And this is not like some other data in our lives that we kind of sense maybe someone else is going to get a hold of.

And second, if the administration has concerns about national security, concerns about the legislation, let us hope this year they confront it in a more forthright fashion, rather than in the dark of night, simply killing a bill that should have been on the suspension calendar, as many of us would agree with. If a court gets an opportunity to view these concerns, I am convinced that they will make the right decisions. But simply making these privacy decisions in the dark of night by security officials, we have learned over and over again, this administration cannot be trusted with that much authority.

And I yield back my time.

Ms. DEGETTE. The gentleman yields back.

The Chair now recognizes the gentleman from Nebraska, Mr. Terry, for 1 minute.

Mr. TERRY. Waive.

Ms. DEGETTE. The gentleman waives.

The Chair now recognizes the gentleman from Texas, Mr. Hall, for 1 minute.

Mr. HALL. Chairman, there is nothing I can add to this. I voted for it the last time. I don't know why we don't run it on through now and pull our hat down over our ears and try to get it out of the Senate and listen to these five young men and this lovely lady to tell us what they think about this, and especially to welcome Mr. Largent, a former member here.

I yield back.

Ms. DEGETTE. The Chair recognizes herself for 1 minute.

OPENING STATEMENT OF HON. DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

Ms. DEGETTE. Last year, we had a series of hearings in the Oversight and Investigations Subcommittee on pretexting, and really, what we learned was disturbing. Your personal data is out there for sale, and, as we have heard, it just takes a few minutes

and a little money for someone to get access to your telephone records and other pieces of private information.

What seemed worse to me, though, was there are a number of prominent citizens in this country and lawyers who don't seem to understand that this is, at best, unethical, in many situations, and, at worst, and probably, in many States, illegal. And that is why we need to clarify the Federal law. That is what H.R. 936 was intended to do.

Last year, this committee passed that bill unanimously, and somehow between this committee and the House floor, it got lost. And we never did find it. But this year, it is a new year. It is a new Congress. And it is going to be a new fate for H.R. 936.

I look forward to hearing the witnesses about this bill. And most importantly, I look forward to passing this bill through the committee and through the House of Representatives.

With that, the Chair now recognizes Mr. Burgess from Texas for 1 minute.

Mr. BURGESS. Thank you, Madame Chairman. I think, in the interest of time, I will submit my statement for the record and reserve time for questions.

Ms. DEGETTE. Without objection.

The Chair now recognizes Mr. Sullivan from Oklahoma.

Mr. SULLIVAN. Madame Chairman, I, too, shall submit mine for the record.

Ms. DEGETTE. The chairman now recognizes the gentleman from New York, Mr. Towns, for 1 minute.

OPENING STATEMENT OF HON. EDOLPHUS TOWNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEW YORK

Mr. TOWNS. Thank you very much, Madame Chair.

Let me thank all of the witnesses for coming. And I especially want to thank my former colleague, Steve Largent for being here.

Also, what I would like for these fine witnesses to do for me is to clarify the issues that the industry has with the bill and to show us how companies use customer proprietary network information to assist them in providing better choices and products to our constituents.

Although consumers enjoy all the new options they have, they want to believe that their personal details will not be abused. And of course, I would like to hear. Some of that makes me feel comfortable in that regard, and at the same time, we recognize that we do not want to eliminate progress, but we also have to be concerned about fraud.

On that note, I yield back, Madame Chair.

Ms. DEGETTE. The gentleman yields back.

The Chair now recognizes the gentleman from Mississippi, Mr. Pickering.

Mr. PICKERING. Thank you, Madame Chairman.

In the interest of time, I will yield back.

Ms. DEGETTE. The Chair now recognizes Mr. Inslee from Washington State.

OPENING STATEMENT OF HON. JAY INSLEE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WASHINGTON

Mr. INSLEE. Thank you. I think it is about time to do it since I first heard about people stealing your personal records over the Internet a couple of days after Christmas 2005. So I am glad to finally be here.

I want to note the opt-in provision of this bill that I think is important to give consumers the right to opt in rather than have to opt out so their records will be protected unless they specifically give advanced approval for their information to be divulged. But I think I am interested in looking at how we do that without interfering with the legitimate operational activities of the carriers. What my vision is we could have an opt-in requirement for any marketing purposes, and the like. But let us get this job done this year. Thanks.

Ms. DEGETTE. The Chair now recognizes the gentle lady from Wisconsin, Ms. Baldwin, for 1 minute.

OPENING STATEMENT OF HON. TAMMY BALDWIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WISCONSIN

Ms. BALDWIN. Thank you, Madame Chairwoman.

I hope that hearings like this will generate enough momentum to actually move the bill through Congress this year, and I echo my colleagues' concerns that pretexting not only violates a person's right to privacy, but it poses serious risks to people's safety, such as some of the high-profile cases that we have heard of victims of domestic violence and stalking and police officers who are doing undercover work.

Furthermore, last fall's revelations at that corporate sector has been using pretexting to obtain personal records of employees, board members, journalists and critics further injected a renewed sense of urgency in addressing this issue. Imposing penalties on the actions of pretexters is certainly a necessary component of stemming the problem, but it is not the only one. That is why I am particularly pleased that this bill not only makes pretexting to obtain, solicit, sell, or disclose customer proprietary network information illegal, but it also gives the FTC the enforcement power, and it also amends section 222 of the Telecommunications Act to cover joint venture partners, et cetera. I do hope that we will promptly get about to the task of passing this legislation.

Thank you, Madame Chairwoman.

Ms. DEGETTE. The Chair now is pleased to recognize the distinguished gentle lady from Wyoming, Ms. Cubin.

OPENING STATEMENT OF HON. BARBARA CUBIN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF WYOMING

Ms. CUBIN. Thank you, Madame Chairman.

I cosponsored this legislation, because I have no doubt that it, excuse me, takes the right approach in banning the practice of pretexting and giving the FTC enforcement authority to halt this practice. And I am looking forward to hearing the Commission's enforcement efforts today.

However, I do have some concerns regarding how this legislation will affect rural carriers. Often, important, well-meaning legislation, such as this, affects rural areas in ways that Congress may not have anticipated, and I am very interested in hearing from the panel about how this legislation will impact rural carriers and rural customers. And I do appreciate the Commission's efforts to enforce section 222 of the Telecommunications Act. And I believe this bill takes positive steps to do so.

However, I would not like to see rural companies face unnecessary, and I would like to underline, disproportionate costs as a result of enforcement of this.

So I would appreciate remarks from the panel on that.

So thank you, Madame Chairman.

Ms. DEGETTE. The Chair now recognizes the distinguished gentle lady from Illinois, Ms. Schakowsky, for 1 minute.

OPENING STATEMENT OF HON. JAN SCHAKOWSKY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Ms. SCHAKOWSKY. I thank you, Madame Chairman.

As has been mentioned before, our committee passed an identical bill by unanimous vote in the last Congress, and I hope that we can get this bill, which would allow the FTC to assess civil penalties for pretexting for phone records and require phone companies to better secure customer records, and that we will get it signed into law.

A number of States, including my own State, and our attorney general, Lisa Madigan, was here at the first hearing we had last session and actually was invited today, but her schedule didn't permit, have used their general consumer protection and consumer fraud statutes to file lawsuits against the practice, but because there was not a clear Federal statute outlining this anti-consumer practice, there were those who still chose to dabble in what they claim was a gray area of the law. Last year, a bill that would allow for criminal penalties for pretexting was signed into law, but we still need to give the FTC the extra authority it needs to impose civil penalties.

But another important concern goes to the reason that con artists who pretext are so successful, when we started our investigation into pretexting in February 2006, there were over 40 sites selling other's phone records. And in the most infamous case to date—let me just conclude with this, the quick and easy access to phone records raises the question of what phone companies are doing or not doing to protect our consumers' records, and that is a very important piece of this.

So I look forward to passing this important legislation. Thank you.

Ms. DEGETTE. The Chair recognizes the distinguished gentleman from Louisiana, Mr. Melancon.

The gentleman waives. Are there any other Members who wish to make an opening statement?

Statements will be accepted for the record as well as the text of H.R. 936.

[H.R. 936 follows:]

I

110TH CONGRESS
1ST SESSION

H. R. 936

To prohibit fraudulent access to telephone records.

IN THE HOUSE OF REPRESENTATIVES

FEBRUARY 8, 2007

Mr. DINGELL (for himself, Mr. BARTON of Texas, Mr. MARKEY, Mr. UPTON, Mr. RUSH, Mr. STEARNS, Ms. SCHAKOWSKY, Mr. BOUCHER, Mr. GORDON of Tennessee, Ms. ESHOO, Mr. STUPAK, Mr. GENE GREEN of Texas, Ms. DEGETTE, Mrs. CAPPS, Mr. DOYLE, Ms. SOLIS, Mr. GONZALEZ, Mr. INSLEE, Ms. BALDWIN, Ms. HOOLEY, Mr. MATHESON, Mr. BUTTERFIELD, Mr. FOSSELLA, Mr. TERRY, Mr. BURGESS, and Mr. ENGEL) introduced the following bill; which was referred to the Committee on Energy and Commerce

---

A BILL

To prohibit fraudulent access to telephone records.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Prevention of Fraudulent Access to Phone Records Act".

TITLE I—FEDERAL TRADE COMMISSION PROVISIONS

SEC. 101. FRAUDULENT ACCESS TO CUSTOMER TELEPHONE RECORDS.

(a) PROHIBITION ON OBTAINING CUSTOMER INFORMATION BY FALSE PRETENSES.—It shall be unlawful for any person to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, customer proprietary network information relating to any other person by—

(1) making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a telecommunications carrier; or

(2) providing any document or other information to an officer, employee, or agent of a telecommunications carrier that the person knows or should know to be forged, counterfeit, lost, stolen, or fraudulently obtained, or to contain a false, fictitious, or fraudulent statement or representation.

(b) PROHIBITION ON SOLICITATION OF A PERSON TO OBTAIN CUSTOMER INFORMATION UNDER FALSE PRETENSES.—It shall be unlawful to request a person to obtain from a telecommunications carrier customer proprietary network information relating to any third person, if the person making such a request knew or should have

1 known that the person to whom such a request is made
2 will obtain or attempt to obtain such information in the
3 manner described in subsection (a).

4 (c) PROHIBITION ON SALE OR OTHER DISCLOSURE
5 OF CUSTOMER INFORMATION OBTAINED UNDER FALSE
6 PRETENSES.—It shall be unlawful for any person to sell
7 or otherwise disclose to any person customer proprietary
8 network information relating to any other person if the
9 person selling or disclosing obtained such information in
10 the manner described in subsection (a).

11 **SEC. 102. EXEMPTION.**

12 No provision of section 101 shall be construed so as
13 to prevent any action by a law enforcement agency, or any
14 officer, employee, or agent of such agency, from obtaining
15 or attempting to obtain customer proprietary network in-
16 formation from a telecommunications carrier in connection
17 with the performance of the official duties of the agency,
18 in accordance with other applicable laws.

19 **SEC. 103. ENFORCEMENT BY THE FEDERAL TRADE COM-**
20 **MISSION.**

21 A violation of section 101 shall be treated as a viola-
22 tion of a rule defining an unfair or deceptive act or prac-
23 tice prescribed under section 18(a)(1)(B) of the Federal
24 Trade Commission Act (15 U.S.C. 57a(a)(1)(B)). The
25 Federal Trade Commission shall enforce this title in the

same manner, by the same means, and with the same jurisdiction as though all applicable terms and provisions of the Federal Trade Commission Act were incorporated into and made a part of this title.

SEC. 104. DEFINITIONS.

As used in this title—

(1) the term "customer proprietary network information" has the meaning given such term in section 222(j)(1) of the Communications Act of 1934 (47 U.S.C. 222(j)(1)) (as redesignated by section 203 of this Act);

(2) the term "telecommunications carrier"—

(A) has the meaning given such term in section 3(44) of the Communications Act of 1934 (47 U.S.C. 153(44)); and

(B) includes any provider of real-time Internet protocol-enabled voice communications; and

(3) the term "real-time Internet protocol-enabled voice communications" means any service that is treated by the Federal Communications Commission as a telecommunications service provided by a telecommunications carrier for purposes of section 222 of the Communications Act of 1934 (47 U.S.C.

222) under regulations promulgated pursuant to subsection (h) of such section.

TITLE II—FEDERAL COMMUNICATIONS COMMISSION PROVISIONS

SEC. 201. FINDINGS.

The Congress finds the following:

(1) As our Nation's communications networks become more ubiquitous and increasingly sophisticated, more individuals and industries will be using such networks in greater amounts to communicate and conduct commercial transactions.

(2) The ease of gathering and compiling sensitive personal information as a result of such communications is becoming more efficient and commonplace due to advances in digital technology and the widespread use of the Internet.

(3) Ensuring the privacy of sensitive individual telephone calling records, both wireline and wireless, is of utmost importance. The information gathered and retained by communications providers can convey details about intimate aspects of an individual's life, including who they call, when they call, the duration of such calls, the frequency of their communications, information about their purchases, infor-

1 mational inquiries, political or religious interests, or
2 other affiliations.
3 (4) Disclosure of personal telephone records can
4 also lead to harassment, intimidation, physical harm,
5 and identity theft.
6 (5) The government has a compelling interest
7 in protecting sensitive personal information con-
8 tained in customer telephone records and ensuring
9 that commercial interests adequately protect such
10 records in order to preserve individual freedom, safe-
11 guard personal privacy, and ensure trust in elec-
12 tronic commerce.
13 (6) Because customers have a proprietary inter-
14 est in their sensitive personal information, customers
15 should have some control over the use and disclosure
16 of telephone calling records.
17 (7) A telecommunications carrier may use ag-
18 gregated data it has obtained from its customer
19 databases to improve services, solicit new business,
20 or market additional services to its customers.
21 (8) A telecommunications carrier may commu-
22 nicate to all consumers in order to broadly solicit
23 new business, and may also target specific commu-
24 nications to its own existing customers, without use
25 or disclosure of detailed customer calling records

1 and thus without the threat of compromising cus-
2 tomer privacy.
3 (9) The risk of compromising customer privacy
4 is raised and increased whenever additional entities
5 or persons are permitted use of, or access to, or re-
6 ceive disclosure of, customer calling records beyond
7 the carrier with which the customer has an estab-
8 lished business relationship.
9 (10) A telecommunications carrier which ob-
10 tains or possesses a customer's calling records has a
11 duty to safeguard the confidentiality of such cus-
12 tomer's personal information. Detailed customer
13 calling records describing the customer's use of tele-
14 communications services should not be publicly avail-
15 able or offered for commercial sale.

16 **SEC. 202. EXPANDED PROTECTION FOR DETAILED CUS-**
17 **TOMER RECORDS.**

18 (a) CONFIDENTIALITY OF CUSTOMER INFORMA-
19 TION.—Paragraph (1) of section 222(c) of the Commu-
20 nications Act of 1934 (47 U.S.C. 222(c)(1)) is amended
21 to read as follows:
22 "(1) PRIVACY REQUIREMENTS FOR TELE-
23 COMMUNICATIONS CARRIERS.—
24 "(A) IN GENERAL.—Except as required by
25 law or as permitted under the following provi-

1 sions of this paragraph, a telecommunications
2 carrier that receives or obtains individually
3 identifiable customer proprietary network infor-
4 mation (including detailed customer telephone
5 records) by virtue of its provision of a tele-
6 communications service shall only use, disclose,
7 or permit access to such information or records
8 in the provision by such carrier of—
9 "(i) the telecommunications service
10 from which such information is derived; or
11 "(ii) services necessary to, or used in,
12 the provision of such telecommunications
13 service, including the publishing of direc-
14 tories.
15 "(B) REQUIREMENTS FOR DISCLOSURE OF
16 DETAILED INFORMATION.—A telecommuni-
17 cations carrier may only use detailed customer
18 telephone records through, or disclose such
19 records to, or permit access to such records by,
20 a joint venture partner, independent contractor,
21 or any other third party (other than an affil-
22 iate) if the customer has given express prior au-
23 thorization for that use, disclosure, or access,
24 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).

1 "(E) ACCESS TO WIRELESS TELEPHONE
2 NUMBERS.—A telecommunications carrier may
3 not, except with prior express authorization
4 from the customer, disclose the wireless tele-
5 phone number of any customer or permit access
6 to the wireless telephone number of any cus-
7 tomer.".

8 (b) DISCLOSURE OF DETAILED INFORMATION ON
9 REQUEST BY CUSTOMER.—Section 222(c)(2) of such Act
10 is amended by inserting "(including a detailed customer
11 telephone record)" after "customer proprietary network
12 information".

13 (c) AGGREGATE DATA.—Section 222(c)(3) of such
14 Act is amended by adding at the end the following new
15 sentence: "Aggregation of data that is conducted by a
16 third party may be treated for purposes of this subsection
17 as aggregation by the carrier if such aggregation is con-
18 ducted in a secure manner under the control or super-
19 vision of the carrier.".

20 (d) PROHIBITION OF SALE OF GENERAL OR DE-
21 TAILED INFORMATION.—Section 222(c) of such Act is fur-
22 ther amended by adding at the end the following new para-
23 graph:

24 "(4) PROHIBITION OF SALE OF GENERAL OR
25 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.".

(e) EXCEPTIONS TO LIMITATIONS ON DISCLOSURES OF DETAILED INFORMATION.—Section 222(d) of such Act is amended—

(1) by striking "its agents" and inserting "its joint venture partners, contractors, or agents"; and

(2) in paragraph (1), by inserting after "telecommunications services" the following: ", or provide customer service with respect to telecommunications services to which the customer subscribes".

SEC. 203. PREVENTION BY TELECOMMUNICATIONS CARRIERS OF FRAUDULENT ACCESS TO PHONE RECORDS.

Section 222 of the Communications Act of 1934 (47 U.S.C. 222) is further amended—

(1) by redesignating subsection (h) as subsection (j);

(2) by inserting after subsection (g) the following new subsections:

1 "(h) PREVENTION OF FRAUDULENT ACCESS TO
2 PHONE RECORDS.—
3 "(1) REGULATIONS.—Within 180 days after the
4 date of enactment of the Prevention of Fraudulent
5 Access to Phone Records Act, the Commission shall
6 prescribe regulations adopting more stringent secu-
7 rity standards for customer proprietary network in-
8 formation (including detailed customer telephone
9 records) to detect and prevent violations of this sec-
10 tion. The Commission—
11 "(A) shall prescribe regulations—
12 "(i) to require timely notice (written
13 or electronic) to each customer upon
14 breach of the regulations under this section
15 with respect to customer proprietary net-
16 work information relating to that cus-
17 tomer;
18 "(ii) to require timely notice to the
19 Commission upon breach of the regulations
20 under this section with respect to customer
21 proprietary network information relating to
22 any customer;
23 "(iii) to require periodic audits by the
24 Commission of telecommunication carriers

1 and their agents to determine compliance
2 with this section;
3 "(iv) to require telecommunications
4 carriers and their agents to maintain
5 records—
6 "(I) of each time customer pro-
7 prietary network information is re-
8 quested or accessed by, or disclosed
9 to, a person purporting to be the cus-
10 tomer or to be acting at the request
11 or direction of the customer; and
12 "(II) if such access or disclosure
13 was granted to such a person, of how
14 the person's identity or authority was
15 verified;
16 "(v) to require telecommunications
17 carriers to establish a security policy that
18 includes appropriate standards relating to
19 administrative, technical, and physical
20 safeguards to ensure the security and con-
21 fidentiality of customer proprietary net-
22 work information;
23 "(vi) to prohibit any telecommuni-
24 cations carrier from obtaining or attempt-
25 ing to obtain, or causing to be disclosed or

1 attempting to cause to be disclosed to that
2 carrier or its agent or employee, customer
3 proprietary network information relating to
4 any customer of another carrier—
5 "(I) by using a false, fictitious,
6 or fraudulent statement or representa-
7 tion to an officer, employee, or agent
8 of another telecommunications carrier;
9 or
10 "(II) by making a false, ficti-
11 tious, or fraudulent statement or rep-
12 resentation to a customer of another
13 telecommunications carrier; and
14 "(vii) only for the purposes of this
15 section, to treat as a telecommunications
16 service provided by a telecommunications
17 carrier any real-time Internet protocol-en-
18 abled voice communications offered by any
19 person to the public, or such classes of
20 users as to be effectively available to the
21 public, that allows a user to originate traf-
22 fic to, or terminate traffic from, the public
23 switched telephone network; and
24 "(B) shall consider prescribing regula-
25 tions—

"(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 Com-

1 mittee on Commerce, Science, and Transpor-
2 tation of the Senate a report containing—
3 "(i) an assessment of the efficacy and
4 adequacy of the regulations and remedies
5 provided in accordance with this subsection
6 in protecting customer proprietary network
7 information;
8 "(ii) an assessment of the efficacy and
9 adequacy of telecommunications carriers'
10 safeguards to secure such data, security
11 plans, and notification procedures; and
12 "(iii) any recommendations for addi-
13 tional legislative or regulatory action to ad-
14 dress threats to the privacy of customer in-
15 formation.
16 "(B) ANNUAL REPORT.—The Federal
17 Communications Commission shall submit to
18 Congress an annual report containing—
19 "(i) the number and disposition of all
20 enforcement actions taken pursuant to this
21 subsection; and
22 "(ii) the number and type of notifica-
23 tions received under paragraph (1)(A)(ii)
24 and the methodology, including the basis
25 for the selection of carriers to be audited,

1 and the results of each audit conducted
2 under paragraph (1)(A)(iii).
3 "(3) DUAL REGULATION PROHIBITED.—Any
4 person that is treated as a telecommunications car-
5 rier providing a telecommunications service with re-
6 spect to the offering of real-time Internet protocol-
7 enabled voice communications by the regulations
8 prescribed under paragraph (1)(A)(vii) shall not be
9 subject to the provisions of section 631 with respect
10 to the offering of such communications.
11 "(i) FORFEITURE PENALTIES.—
12 "(1) INCREASED PENALTIES.—In any case in
13 which the violator is determined by the Commission
14 under section 503(b)(1) to have violated this section
15 or the regulations thereunder, section 503(b)(2)(B)
16 shall be applied—
17 "(A) by substituting '$300,000' for
18 '$100,000'; and
19 "(B) by substituting '$3,000,000' for
20 '$1,000,000'.
21 "(2) NO FIRST WARNINGS.—Paragraph (5) of
22 section 503(b) shall not apply to the determination
23 of forfeiture liability under such section with respect
24 to a violation of this section or the regulations there-

1 under by any telecommunications carrier or any
2 agent of such a carrier."; and
3 (3) in subsection (g), by striking "subsection
4 (i)(3)(A)" and inserting "subsection (j)(3)(A)".

5 **SEC. 204. DEFINITIONS.**

6 Subsection (j) of section 222 of the Communications
7 Act of 1934 (47 U.S.C. 222(j)), as redesignated by section
8 203(1) of this Act, is amended by adding at the end the
9 following new paragraphs:
10 "(8) DETAILED CUSTOMER TELEPHONE
11 RECORD.—The term 'detailed customer telephone
12 record' means customer proprietary network infor-
13 mation that contains the specific and detailed des-
14 tinations, locations, duration, time, and date of tele-
15 communications to or from a customer, as typically
16 contained in the bills for such service. Such term
17 does not mean aggregate data or subscriber list in-
18 formation.
19 "(9) WIRELESS TELEPHONE NUMBER.—The
20 term 'wireless telephone number' means the tele-
21 phone number of a subscriber to a commercial mo-
22 bile service.".

○

Ms. DEGETTE. I would like to welcome our panel today of distinguished witnesses, most especially our former colleague, Mr. Largent, who we are delighted to have appear in front of the committee. The witnesses are now recognized, and we will start with Ms. Lydia Parnes.

Ms. Parnes.

STATEMENT OF LYDIA PARNES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, U.S. FEDERAL TRADE COMMISSION

Ms. PARNES. Good morning, Madame Chairman, Ranking Member Barton, members of the committee.

I appreciate your invitation to appear today to discuss the privacy and security of consumers' telephone records.

Although my written statement is that of the Commission, my oral testimony and responses to questions reflect my own views and not necessarily those of the Commission or any individual commissioner.

Protecting the privacy and security of consumer-sensitive personal information is one of the Commission's highest priorities, and aggressive law enforcement is at the center of our efforts to protect consumers' telephone call records from pretexting.

Last May, the Commission announced five lawsuits against 12 defendants who obtained and sold consumers' telephone records without their knowledge or authorization. The Commission alleged that these practices were unfair and prohibited by section 5 of the FTC Act. In each of these cases, the defendant advertised on its Web site that it could obtain confidential, customer phone records from telecommunications carriers for fees ranging from $65 to $180.

To date, the Commission has settled two of these cases, obtaining strong, permanent injunctions that bar the defendants from selling phone records or personal information taken from those records. In addition, the settlements require the defendants to disgorge their profits. The remaining three cases are still in active litigation.

These five cases were the culmination of extensive investigations of this industry. Commission staff surfed the Internet for companies that offer to sell consumers' phone records, sent warning letters, and then identified appropriate targets for investigation and completed undercover purchases of these records. The Commission worked closely with the Federal Communications Commission in developing these cases. We are committed to coordinating our work on this issue, as we have done successfully in other areas.

Last month, the Commission filed a sixth case against six defendants that allegedly conducted or directed actual pretexting. Again, the FTC alleged that the defendants obtained and sold consumers' confidential phone records without their knowledge or consent. This case connects the actual pretexters to the middlemen who sell the records to third parties. In addition to alleging that the unauthorized sale of phone records is an unfair practice, the FTC's complaint alleges that the defendants engaged in deception by obtaining the records through the use of fraud and misrepresentations.

These telephone-pretexting cases follow a long line of actions against defendants charged with the pretexting of financial records.

We filed our first financial pretexting case in 1999 against a company that offered to provide consumers' bank account numbers and balances for a fee. Congress later enacted the Gramm-Leach-Bliley Act, which expressly prohibits pretexting for financial records. The FTC has followed up with more than a dozen cases.

Let me turn briefly to the subject of legislation.

The proposed Phone Records Act contains several important provisions that would assist the Commission in combating phone pretexting.

First, it applies not only to pretexters, but to those who solicit their services and know, or should know, that the records are obtained through false pretenses. Second, it grants the FTC the power to seek civil penalties against violators. And third, it contains an important exemption for law enforcement. These provisions would provide the Commission with useful, additional tools for combating telephone records pretexting.

In addition to the Phone Records Act, two recently-passed statutes will assist in the fight against phone pretexting.

First, in December 2006, Congress enacted the U.S. Safe Web Act, which allows greater cooperation and information sharing between the Commission and its counterparts in other countries. The U.S. Safe Web Act will assist the Commission in pursuing data brokers, who are operating outside the United States. Second, Congress passed the Telephone Records and Privacy Protection Act, which criminalizes obtaining confidential records by making false statements to a telephone service provider. In light of this new law, we anticipate developing criminal law enforcement referrals to our sister agency, the Department of Justice.

Again, thank you for the opportunity to testify today. We look forward to working with the committee and its staff on this very important issue, and I would be happy to answer any questions you may have.

[The prepared statement of Ms. Parnes follows:]

PREPARED STATEMENT OF THE FEDERAL TRADE COMMISSION

Before the

COMMITTEE ON ENERGY AND COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

on

"Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act"

March 9, 2007

I. Introduction

Chairman Dingell, Ranking Member Barton, and members of the Committee, I am Lydia Parnes, Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to discuss the practice of obtaining unauthorized access to consumers' sensitive information through fraud, a practice known as "pretexting," as well as the Commission's significant work to protect the privacy and security of telephone records and other types of sensitive consumer information. I also appreciate the opportunity to comment on the proposed Prevention of Fraudulent Access to Phone Records Act, H.R. 936. The Committee's work in this area has been important in protecting consumers.

Ensuring the privacy and security of consumers' personal information is one of the Commission's highest priorities. Individuals or companies that procure through pretexting or sell on the open market confidential consumer information without the consumer's knowledge or consent not only violate the law, but they undermine consumers' confidence in the marketplace and in the security of their sensitive data. Accordingly, the Commission has used its full arsenal of tools to attack the pretexters and the brokers who sell pretexted information. Since 2006, the Commission initiated a half dozen law enforcement actions against online data brokers and pretexters of confidential consumer telephone records. The Commission also has developed and disseminated a variety of new online and written materials to educate consumers about protecting their sensitive personal information in general and from pretexting in particular.

Today, I will first discuss the FTC's efforts to protect consumers from the sale of phone

---

[1] The views expressed in this statement represent the views of the Commission. My oral testimony and responses to questions reflect my own views and do not necessarily represent the views of the Commission or any individual Commissioner.

records obtained through pretexting. Next, I will provide a brief history of the FTC's enforcement efforts in the area of pretexting for financial information. I will then address the provisions of H.R. 936.

II. FTC Enforcement Efforts Against Firms Selling Telephone Records

Aggressive law enforcement is at the center of the FTC's efforts to protect consumers' telephone call records from pretexting. The acquisition of such records by unauthorized third parties is a serious intrusion into consumers' privacy that presents a significant risk of harm. Evidence obtained in the Commission's law enforcement actions reveals truly horrifying incidents of stalking and harassment of consumers whose call records were pretexted.[2]

Last May, the Commission announced an initial wave of five lawsuits in federal courts across the country against online data brokers, alleging that the defendants had engaged in unfair practices, prohibited by Section 5 of the FTC Act,[3] when they obtained and sold consumer

---

[2] Several consumers whose phone records were obtained and sold by the defendants in one of the FTC's pending phone pretexting cases have submitted signed declarations, attesting that they have been stalked and physically threatened by, for example, a former co-worker, an ex-spouse. and an ex-boyfriend. In addition to the real threat posed to their safety, these consumers have spent significant time and hundreds of dollars changing phone numbers or service providers. *See Br. of Pl. FTC in Supp. of Mot. for Summ. J.* at 8-14, *FTC v. AccuSearch, Inc.*, No. 06-CV-0105 (D. Wyo. Jan. 22, 2007).

In addition, there have been media reports of other incidents of pretexting that led to harm. One data broker reportedly sold home phone numbers and addresses of Los Angeles Police Department detectives to suspected mobsters, who then used the information in an apparent attempt to intimidate the detectives and their families. *See, e.g.,* Peter Svensson, *Calling Records Sales Face New Scrutiny,* Wash. Post, Jan. 18, 2006, *available at* www.washingtonpost.com/wp-dyn/content/ article/2006/01/18/AR2006011801659.html.

[3] 15 U.S.C. § 45(a). An act or practice is unfair if it: (1) causes or is likely to cause consumers substantial injury; (2) the injury is not reasonably avoidable by consumers; and (3) the injury is not outweighed by countervailing benefits to consumers or competition. *Id.* at § 45(n). Under Section 13(b) of the FTC Act, 15 U.S.C. § 53(b), the Commission has the authority to file actions in federal district court to obtain injunctions and other equitable relief against those

telephone records without the consumer's knowledge or authorization.[4] In each of these cases, the defendant advertised on its website that it could obtain confidential customer phone records from telecommunications carriers for fees ranging from $65 to $180. The complaints alleged that the defendants, or persons they hired, obtained this information by using false pretenses, including posing as the carrier's customer, to induce the carrier's employees to disclose the records.

To date, the Commission has settled two of these cases, obtaining permanent injunctions that bar the defendants from selling customer phone records or consumer personal information derived from such records.[5] In addition, the settlements require the defendants to disgorge the profits they derived from the alleged illegal operations.[6] The remaining three cases are still in active litigation.

The FTC's first wave of phone pretexting cases was the culmination of extensive investigations of this industry. Commission staff surfed the Internet for companies that offered to sell consumers' phone records, then identified appropriate targets for investigation and

---

engaged in violations of Section 5.

[4] *FTC v. Info. Search, Inc.*, No. 1:06-CV-01099-AMD (D. Md. filed May 1, 2006); *FTC v. AccuSearch, Inc.*, No. 06-CV-0105 (D. Wyo. filed May 1, 2006); *FTC v. CEO Group, Inc.*, No. 06-60602 (S.D. Fla. filed May 1, 2006); *FTC v. 77 Investigations, Inc.*, No. EDCV06-0439 VAP (C.D. Cal. filed May 1, 2006); *FTC v. Integrity Sec. and Investigation Servs., Inc.*, No. 2:06-CV-241-RGD-JEB (E.D. Va. filed May 1, 2006).

[5] *FTC v. Integrity Sec. and Investigation Servs., Inc., supra* note 4 (final judgment entered Oct. 30, 2006) *available at* www.ftc.gov/os/caselist/pretextingsweep/061005isisstipfinalord.pdf; and *FTC v. Info. Search, Inc., supra* note 4 (final judgment entered Feb. 22, 2007).

[6] The FTC does not have authority to obtain civil penalties in these cases, and therefore is limited to the equitable remedy of disgorgement. As currently drafted, H.R. 936 would authorize the Commission to seek civil penalties.

completed undercover purchases of the records. For some of these companies, staff sent warning letters and followed up later to ensure that they were no longer selling consumer phone records. Other companies became targets for enforcement action, as described above.

The Commission has been assisted greatly in its efforts by the Federal Communications Commission, which has jurisdiction over telecommunications carriers subject to the Telecommunications Act.[7] Our two agencies are committed to coordinating our work on this issue, as we have done successfully in enforcing the "National Do Not Call" implementation legislation.

Building upon evidence gathered in its initial cases, last month the Commission filed a sixth case in federal district court in Florida against several defendants that allegedly conducted or directed the actual pretexting and obtained consumers' phone records on behalf of others.[8]

---

[7] Consumer telephone records are considered "customer proprietary network information" under the Telecommunications Act of 1996 ("Telecommunications Act"), which amended the Communications Act, and accordingly are afforded privacy protections by the regulations under that Act. *See* 42 U.S.C. § 222; 47 C.F.R. §§ 64.2001- 64.2009. The Telecommunications Act requires telecommunications carriers to secure the data, but does not specifically address pretexting to obtain telephone records. The FTC's governing statute exempts from Commission jurisdiction common carrier activities that are subject to the Communications Act. 15 U.S.C. § 46(a). The Commission recommended that Congress remove this exemption at its two most recent reauthorization hearings and in testimony on FTC jurisdiction over broadband Internet access service before the Senate Judiciary Committee in June 2006. *See* http://www.ftc.gov/os/2003/06/030611reauthhr.htm; http://www.ftc.gov/os/2003/06/030611reauthsenate.htm; *see also* http://www.ftc.gov/os/203/06/030611learysenate.htm; http://www.ftc.gov/os/2002/07/sfareauthtest.htm; http://www.ftc.gov/os/2006/06/p052103CommissionTestimonyReBroadbandInternetAcess Services06142006Senate.pdf.

[8] *FTC v. Action Research Group, Inc.*, No. 6:07-cv-227-Orl-22JGG, (M.D. Fla. filed Feb. 14, 2007). Several of the defendants named in the FTC's complaint are also the subject of federal and state criminal actions in California, stemming from the well-publicized phone records pretexting of Hewlett-Packard board members and journalists. *See, e.g.,* Matt Richtel, *With a Little Stealth, Just About Anyone Can Get Phone Records,* NY Times, Sep. 7,

The FTC alleged that Action Research Group and its principals and agents obtained and sold consumers' confidential phone records without their knowledge or consent. This case connects the phone records pretexters to the middlemen who sell the records to third parties. In addition to alleging that the unauthorized sale of phone records is an unfair practice, the FTC's complaint alleges that the defendants engaged in deceptive practices by obtaining the records through the use of fraud and misrepresentations. The agency has asked the court to stop the conduct and to order the defendants to give up their ill-gotten gains.

III. FTC's History of Combating Financial Pretexting

In addition to the recent cases involving telephone records pretexting, the Commission has brought actions under Section 5 of the FTC Act and Section 521 of the Gramm-Leach-Bliley Act ("GLBA") against businesses and individuals who used false pretenses to obtain and sell financial information without consumer consent.

The Commission filed its first pretexting case against a company that offered to provide consumers' financial records to anybody for a fee.[9] According to the complaint, the company's employees allegedly obtained these records from financial institutions by posing as the consumer whose records were being sought. The complaint charged that this practice was both deceptive and unfair under Section 5 of the FTC Act.

In 1999, Congress passed the GLBA, which provided another tool to attack the

---

2006, *available at* http://www.nytimes.com/2006/09/07/technology/07phone.html?ex=1158465600&en=2f20498c7fcc7e5b&ei=5070.

[9] *FTC v. James J. Rapp*, No. 99WM-783 (D. Colo. final judgment entered June 22, 2000), *available at* http://www.ftc.gov/os/2000/06/touchtoneorder.

unauthorized acquisition of consumers' financial information.[10] Section 521 of the GLBA prohibits "false, fictitious, or fraudulent statement[s] or representation[s] to an officer, employee, or agent of a financial institution" to obtain customer information from a financial institution.[11]

To ensure awareness of and compliance with the then-new anti-pretexting provisions of the GLBA, the Commission launched Operation Detect Pretext in 2001.[12] Operation Detect Pretext combined a broad monitoring program, the widespread dissemination of industry warning notices, consumer education, and aggressive law enforcement.

In the initial monitoring phase of Operation Detect Pretext, FTC staff conducted a "surf" of more than 1,000 websites and a review of more than 500 advertisements in print media to identify firms offering to conduct searches for consumers' financial data. The staff found approximately 200 firms that offered to obtain and sell consumers' asset or bank account information to third parties. The staff then sent notices to these firms, advising them that their practices were subject to the FTC Act and the GLBA and providing information about how to comply with the law.[13]

The Commission followed its education campaign with aggressive law enforcement,

---

[10] 15 U.S.C. §§ 6821-6827

[11] *Id.* at § 6821.

[12] FTC press release, "As Part of Operation Detect Pretext, FTC Sues to Halt Pretexting" (Apr. 18, 2001), *available at* http://www.ftc.gov/opa/2001/04/pretext.htm.

[13] FTC press release, "FTC Kicks Off Operation Detect Pretext" (Jan. 31, 2001), *available at* http://www.ftc.gov/opa/2001/01/pretexting.htm. In conjunction with the warning letters, the Commission released a consumer alert, *Pretexting: Your Personal Information Revealed,* describing how pretexters operate and advising consumers on how to avoid having their information obtained through pretexting, *available at* http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm.

including a trio of law enforcement actions filed in 2001 against information brokers.[14] In each of these cases, the defendants advertised that they could obtain non-public, confidential financial information, including information on checking and savings account numbers and balances, stock, bond, and mutual fund accounts, and safe deposit box locations, for fees ranging from $100 to $600. Based on evidence obtained in undercover investigations, the FTC alleged that the defendants or persons they hired called banks and posed as customers to obtain balances on checking accounts. The defendants in each of the cases ultimately agreed to settlements that barred them from further violations of the law and required them to surrender ill-gotten gains.[15] Since GLBA's passage, the FTC has brought over a dozen cases alleging violations of Section 521 in various contexts.[16]

Because the anti-pretexting provisions of the GLBA provide for criminal penalties, the Commission also may refer financial pretexters to the U.S. Department of Justice for criminal prosecution, as appropriate. Following one such referral, an individual pled guilty to one count of pretexting under the GLBA.[17]

IV. FTC Education and Outreach

---

[14] *FTC v. Victor L. Guzzetta*, No. CV-01-2335 (E.D.N.Y. final judgment entered Feb. 25, 2002); *FTC v. Info. Search, Inc.*, No. AMD-01-1121 (D. Md. final judgment entered Mar. 15, 2002); *FTC v. Paula L. Garrett*, No. H 01-1255 (S.D. Tex. final judgment entered Mar. 25, 2002).

[15] *See* www.ftc.gov/opa/2002/03/pretextingsettlements.htm.

[16] *See* www.ftc.gov/privacy/privacyintiatives/pretexting_enf.htm.

[17] *United States v. Peter Easton*, No. 05 CR 0797 (S.D.N.Y. final judgment entered Nov. 17, 2005).

In addition to its law enforcement efforts, the Commission has an extensive program to teach consumers and businesses better ways to protect sensitive data. For example, in February 2006, the Commission released a consumer alert, *Pretexting: Your Personal Information Revealed,* describing how pretexters operate and advising consumers on how to avoid having their information obtained through pretexting.

The FTC also recently launched a nationwide identity theft education program, "Avoid ID Theft: Deter, Detect, Defend," which broadly advises consumers on how to avoid becoming victims of identity theft. The message for consumers is that they can (1) deter identity thieves by safeguarding their personal information; (2) detect suspicious activity by routinely monitoring their financial accounts, billing statements, and credit reports; and (3) defend against ID theft as soon as they suspect it. The Deter, Detect, Defend campaign has been very popular. The FTC has distributed more than 1.5 million brochures to consumers and 30,000 kits to employers, community groups, members of Congress, and others to educate their constituencies. The kits contain a victim recovery guide, a training booklet, a guide to talking about identity theft, presentation slides, an easy-to-read brochure, and a 10-minute video that organizations can use to educate their employees, customers, and communities about identity theft.

The FTC also sponsors an innovative multimedia website, OnGuardOnline, designed to educate consumers about basic computer security.[18] The website provides information on specific topics such as phishing, spyware, and identity theft. Since its launch in late 2005, OnGuardOnline has attracted more than 3.5 million visits. All of these materials are part of the

---

[18] *See* www.onguardonline.gov.

Commission's comprehensive library on consumer privacy, data security, and identity theft.[19]

V. The Prevention of Fraudulent Access to Phone Records Act, H.R. 936

As described above, the Commission has used its jurisdiction under Section 5 of the FTC Act to take action against individuals and business engaged in the pretexting or sale of confidential phone records obtained through pretexting. Although Section 5 is a powerful tool, the Commission continues to support the enactment of more specific prohibitions against phone pretexting that provide additional remedies for violations.[20]

The proposed Prevention of Fraudulent Access to Phone Records Act (the "Phone Records Act") contains several important components that would assist the Commission in combating phone pretexting. First, in addition to prohibiting pretexting itself, the Phone Records Act would extend liability to individuals who solicit such records and knew or should have known that the records would be obtained through false pretenses. The Commission agrees that those who solicit pretexting should be held responsible, and that the knowledge standard contained in the Phone Records Act is the appropriate one, because it would prevent data brokers from turning a "blind eye" to the manner in which their sources obtain phone records.

The Phone Records Act also would allow the FTC to recover civil penalties from violators. Often, monetary penalties can be the most effective civil remedy in privacy-related actions and, as noted earlier, the Commission currently is unable to obtain this remedy in phone pretexting cases brought under the FTC Act. Finally, the Phone Records Act contains an important exemption for law enforcement agencies in connection with their official duties.

---

[19] *See* www.ftc.gov/privacy/index.html.

[20] *See* Commission Testimony from the 109th Congress before this Committee, *available at* http://www.ftc.gov/opa/2006/09/houseenergy.htm.

In addition to the Phone Records Act, two recently passed statutes will assist in the fight against phone pretexting. First, in December 2006, Congress passed and the President signed the "US SAFE WEB Act" into law.[21] This Act allows greater cooperation and information sharing between law enforcers in the United States and their counterparts in other countries. In developing the Commission's phone pretexting cases, FTC staff learned that some websites offering consumer telephone records were registered to foreign addresses. The US SAFE WEB Act will assist the Commission in pursuing data brokers who are operating outside the United States.

Second, Congress recently approved and, on January 12, 2007, President Bush signed into law the Telephone Records and Privacy Protection Act,[22] which criminalizes obtaining confidential records by making false statements to a telephone service provider. The Commission anticipates that its ongoing actions against phone records pretexting will lead to criminal law enforcement referrals to our sister agency, the Department of Justice.

VI. Conclusion

Protecting the privacy of consumers' telephone records requires a multi-faceted approach: coordinated law enforcement by government agencies against the pretexters; efforts by the telephone carriers to protect their records from intrusion; and outreach to educate consumers on actions they can take to protect themselves. The Commission has been at the forefront of efforts to safeguard consumer information and is committed to continuing its work in this area. The Commission looks forward to continuing to work with this Committee to protect the privacy and security of sensitive consumer information.

[21] The Undertaking Spam, Spyware, and Fraudulent Enforcement with Enforcers Across Borders Act of 2006, Pub. L. No. 109-455, 120 Stat. 3372.

[22] Telephone Records and Privacy Protection Act, Pub. L. No: 109-476.

Ms. DEGETTE. Thank you.

Mr. Navin.

STATEMENT OF THOMAS NAVIN, CHIEF, WIRELINE BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Mr. NAVIN. Thank you.

Good morning, Madame Chairman, Ranking Member Barton, and members of the committee.

I appreciate the opportunity to speak with you today about the ongoing work of the Federal Communications Commission to ensure the privacy of American consumers' sensitive telephone call records.

Section 222 of the Communications Act requires telecommunications carriers to protect the confidentiality of their customers' personal information collected in the course of providing telephone service. This information is commonly referred to as "customer proprietary network information" or CPNI. As you are aware, third parties, known as "data brokers" or "pretexters", had invaded consumers' privacy by gaining unauthorized access to this very personal data for profit.

The Commission has taken several steps to curb the unauthorized disclosures and sale of consumers' personal telephone records. Specifically, FCC Chairman Martin has proposed imposing stricter security standards for CPNI for all providers of telephone service, including mandatory passwords for accessing customer call records. Further, the Commission has investigated, and will continue to investigate, this unlawful activity and take strong enforcement action to address any violations by telecommunications carriers of their obligations to protect CPNI.

The Commission began its investigation of the data broker problem in late summer 2005. In August 2005, the Electronic Privacy Information Center, or EPIC, filed a petition for rulemaking at the FCC to address the sufficiency of carrier privacy practices in light of the fact that online data brokers were selling consumers' private telephone data. In early 2006, the Commission issued a Notice of Proposed Rulemaking, inviting comment on the EPIC petition and whether additional Commission rules are necessary to strengthen the carriers' safeguards for customers' records.

Based on the evidence submitted in its rulemaking proceeding, and gathered in its enforcement investigations, the Commission has learned about the methods that data brokers routinely use to seek to obtain unauthorized access to CPNI. The Commission also has learned of a variety of steps carriers can take to further protect the privacy of customer account information.

Significantly, we also recognize the importance of this issue to law enforcement, particularly in light of the new Telephone Records and Privacy Protection Act of 2006, which makes pretexting a criminal offense. The Commission has an item for consideration before it which would address these issues by requiring providers to adopt additional safeguards to protect customers' phone record information from unauthorized access and disclosure.

The chairman has circulated an order that, for example, proposes prohibiting providers from releasing call detail information except when the customer provides a password, or by sending it to an ad-

dress of record or by calling the customer at the telephone of record. To protect against possible efforts to circumvent these requirements, the order proposes to require carriers to notify the customer immediately when information such as passwords or the address of record is created or changed. The chairman also proposed a notification process for both law enforcement and customers in the event of a breach of CPNI.

In addition, Chairman Martin proposed to modify our current rules to require providers to obtain affirmative customer consent before disclosing any of that customer's phone record information to a provider's joint venture partner or independent contractor for marketing purposes. Further, the order proposes to extend all CPNI obligations to interconnected voice over Internet protocol, or VoIP, providers. These additional privacy safeguards should sharply limit pretexters' ability to obtain unauthorized access to CPNI.

The Commission also has used its enforcement authority to help address this problem. The Commission has issued subpoenas to a number of data brokers seeking information about how companies obtained phone record information and then sold it.

Additionally, the Commission has investigated telecommunications carriers' practices to fulfill section 222's duty to protect customer information through numerous meetings with the carriers, a review of the carriers' annual section 222 compliance certifications, and through formal letters of inquiries that have been issued to nearly 20 carriers.

Throughout these investigations, the Commission closely coordinated with the Federal Trade Commission staff. In addition, the Commission has offered assistance to State attorneys general in their efforts to combat pretexting. The Commission takes very seriously any breach of consumers' privacy, as well as carriers' statutory duty to protect the customer information that they collect. The Commission also remains committed to strengthening its rules as warranted to help ensure that carriers implement adequate practices to protect their customers' privacy, as required by the Communications Act. We, likewise, will continue to coordinate with the Federal Trade Commission, State and Federal attorneys general, and other law enforcement authorities about our findings, and work with them in any way we can to take legal action against data brokers and pretexters. We look forward to working collaboratively with the members of this committee and other Members of Congress to ensure that consumers' personal phone data remains confidential.

Thank you for the opportunity to testify, and I would be pleased to respond to your questions.

[The prepared statement of Mr. Navin follows:]

Written Statement

of

Thomas J. Navin
Chief, Wireline Competition Bureau
Federal Communications Commission

Before the

Committee on Energy and Commerce
U.S. House of Representatives

On

"Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act"

March 9, 2007

Good morning, Chairman Dingell, Ranking Member Barton, and members of the Committee. I appreciate the opportunity to speak with you today about the ongoing work of the Federal Communications Commission to ensure the privacy of American consumers' sensitive telephone call records.

Section 222 of the Communications Act of 1934, as amended, requires telecommunications carriers to protect the confidentiality of their customers' personal information collected in the course of providing telephone service. This information is commonly referred to as customer proprietary network information or CPNI. As you are aware, third parties, known as "data brokers" and "pretexters," have invaded consumers' privacy by gaining unauthorized access to this very personal data for profit.

The Commission has taken several steps to curb the unauthorized disclosures and sale of consumers' personal telephone records. Specifically, FCC Chairman Martin has proposed imposing stricter security standards for CPNI for all providers of telephone service, including mandatory passwords for accessing customer call records. Further, the Commission has investigated, and will continue to investigate, this unlawful activity and take strong enforcement action to address any violations by telecommunications carriers of their obligations to protect CPNI.

Background

Congress enacted section 222 of the Act, as part of the Telecommunications Act of 1996 amendments, for the express purpose of protecting consumers' privacy. Specifically, section 222 of the Act provides that telecommunications carriers have a duty to protect the confidentiality of CPNI, which includes, among other things, customers'

calling activities and history, and billing records. The Act limits carriers' ability to use customer phone records even for their own marketing purposes without appropriate consumer approval and safeguards. Furthermore, unless otherwise required by law, the Act prohibits carriers from using, disclosing, or permitting access to this information without customer approval if the use or disclosure is not in connection with the service being provided. The Commission's rules also provide that a telecommunications carrier "must have an officer, as an agent of the carrier, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established operating procedures that are adequate to ensure compliance" with the Commission's CPNI rules.

The Commission began its investigation of the data broker problem in late Summer 2005, and in August 2005, the Electronic Privacy Information Center ("EPIC") filed a petition for rulemaking to address the sufficiency of carrier privacy practices in light of the fact that online data brokers were selling consumers' private telephone data. As described in the petition, numerous websites were advertising the sale of personal telephone records, including records of calls to and from a particular phone number and the duration of such calls, for wireless and wireline customers. Following the filing of EPIC's petition, the Commission moved to consider rules that impose stricter security standards on all providers of telephone service concerning sensitive customer information. The Commission also took action to investigate these activities under the existing CPNI rules.

On February 1, 2006, Chairman Martin testified before this Committee and in response to a request by several members on how best to combat this problem, suggested

that Congress make illegal the commercial availability of consumers' phone records. In addition, Chairman Martin suggested that a more stringent "opt-in" approval method for protection of consumer phone record information could be implemented, and also proposed that Congress could strengthen the Commission's enforcement tools.

In the last session, Congress adopted legislation called the Telephone Records and Privacy Protection Act of 2006, which made pretexting a criminal offense subject to fines and imprisonment, and on January 12, 2007, the President signed this legislation.

On February 8, 2007, Chairman Dingell, Ranking Member Barton, and several members of the Committee introduced H.R. 936 to further prohibit fraudulent access to telephone records. I note that, among other things, the bill would make pretexting unlawful and would expressly extend "opt-in" approval requirements to the sharing of certain information with joint venture partners, independent contractors, and other third parties. Further, H.R. 936 would expand the penalties for CPNI violations and make it easier for the Commission to bring enforcement actions against non-common carriers, such as data brokers.

Commission Efforts to Strengthen Existing CPNI Rules

In response to the problem of pretexting, the Commission currently is considering new rules to ensure that carriers adequately protect their customers' private information. Specifically, the Commission issued a Notice of Proposed Rulemaking ("Notice") inviting comment on the EPIC petition and whether additional Commission rules are necessary to strengthen the carriers' safeguards for customer records.

Based on the evidence submitted in its rulemaking proceeding, and gathered in its enforcement investigations, the Commission learned that data brokers routinely seek to obtain unauthorized access to CPNI by impersonating an authorized user, the account holder or another company employee either when speaking with a carrier's customer service representative or via online access. There also has been evidence of some limited instances of employee misconduct. And while we consider it a positive development that numerous carriers (as well as the FTC and numerous states) have filed lawsuits seeking to enjoin pretexting activity, unfortunately it is also an indication of the success pretexters have had.

As we have met with parties regarding the strengthening of our CPNI rules and conducted investigations, we have learned of a variety of steps carriers can take to further protect the privacy of customer account information, some of which certain carriers are implementing today. These steps include, among other things, using better security and authentication measures in call centers and with respect to setting up online accounts; notifying customers of account changes; providing notice of unauthorized access to CPNI; and greater employee training and monitoring. Significantly, we also recognize the importance of this issue to law enforcement, particularly in light of the new Telephone Records and Privacy Protection Act of 2006, which makes pretexting a criminal offense.

The Commission has an item for consideration which would address these issues by requiring providers to adopt additional safeguards to protect customers' phone record information from unauthorized access and disclosure. The Chairman has circulated an order that, for example, proposes prohibiting providers from releasing call detail

information except when the customer provides a password, or by sending it to an address of record or calling the customer at the telephone of record. To protect against possible efforts to circumvent these requirements, the order proposes to require carriers to notify the customer immediately when information such as passwords or the address of record is created or changed. The Chairman also proposed a notification process for both law enforcement and customers in the event of a CPNI breach.

In addition, Chairman Martin proposed to modify our current rules to require providers to obtain affirmative customer consent before disclosing any of that customer's phone record information to a provider's joint venture partner or independent contractor for marketing purposes. Further, the order proposes to extend all CPNI obligations to interconnected voice over Internet protocol (VoIP) providers. These additional privacy safeguards should sharply limit pretexters' ability to obtain unauthorized access to CPNI.

Commission Enforcement Action

The Commission also has taken a hard look into the world of data brokerage and has used its enforcement authority against both data brokers and carriers to help address this problem. As a first step in its investigation and enforcement activities, the Commission issued subpoenas to several of the most prominent data brokers in late 2005, and again in 2006, seeking information about how companies obtained phone record information and then sold it. Some companies failed to respond adequately to our requests and almost all companies denied any knowledge of wrongdoing. As a consequence of the companies' failure to respond, the Commission issued letters of citation, and ultimately was forced to issue a Forfeiture Order against one company,

Locate Cell, for its continued failure to respond to the Commission's subpoenas. We also referred Locate Cell's inadequate response to the Department of Justice for enforcement of the subpoena.

Additionally, the Commission focused its attention on the telecommunications carriers' practices to fulfill section 222's duty to protect customer information. As a result of numerous meetings with various carriers, a review of the carriers' annual section 222 compliance certificates, and a review of the carriers' responses to formal Letters of Inquiry sent to nearly 20 carriers, the Commission issued three Notices of Apparent Liability for Forfeiture to carriers for failure to comply with the Commission's rules implementing section 222.

Throughout these investigations, the Commission closely coordinated with Federal Trade Commission staff. In addition, the Commission has offered assistance to state attorneys general in their efforts to combat pretexting.

Conclusion

The Commission takes very seriously any breach of consumers' privacy, as well as carriers' statutory duty to protect the customer information that they collect. The Commission also remains committed to strengthening its rules as warranted to help ensure that carriers implement adequate practices to protect their customers' privacy, as required by the Act. We likewise will continue to coordinate with the Federal Trade Commission, state and federal attorneys general, and other law enforcement authorities about our findings, and work with them in any way we can to take legal action against data brokers and pretexters. We look forward to working collaboratively with the

members of this Committee and other Members of Congress to ensure that consumers' personal phone data remains confidential. Thank you for the opportunity to testify, and I would be pleased to respond to your questions.

Ms. DEGETTE. Thank you, Mr. Navin.

Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Madame Chairman, Ranking Member Barton, members of the committee, thank you so much for the opportunity to testify before you on the very serious problem of pretexting.

As you may know, in the summer of 2005, EPIC undertook an extensive investigation of the problem of pretexting in the United States. We found that personal information, call detail information, was available for sale at more than 40 businesses on the Internet. We filed a petition with the Federal Trade Commission in which we asked the FTC to begin an investigation, and because it was so clearly the case that the information at issue concerned personal calling records, we petitioned the FCC to open an investigation and to establish stronger security standards to safeguard the privacy of the call detail information of American telephone consumers.

We provided very specific recommendations for the FCC: the use of passwords, the use of encryptions, and the use of audit trails that would ensure that when personal information in the possession of the telephone carriers was disclosed, it was disclosed for an appropriate purpose and not to a pretexter for a nefarious purpose.

I recall a year ago at this time having the honor to appear before this committee with the chairman and to discuss our petition, and at that time, he expressed support for our recommendations. He said that he was going forward and issued the petition in February, more than a year ago, recommending that stronger security standards be established for telephone record information.

We filed our comments. The telephone industry filed their comments. We filed our reply comments, and then nothing happened. No final rule was ever issued by the FCC, though, remarkably, as recently as January 2007 the Commission continued to warn consumers about the ongoing problem of pretexting of personal telephone record information.

I am here before you today to urge you to ensure that the FCC act on this petition. And because they have failed to act on this petition, we think it is absolutely vital for the legislation that you are considering now, which would establish these security standards by law, to go forward. The safeguarding of this personal information is absolutely crucial, as we have described in our testimony.

Some will raise the question regarding the legislation that was passed by the Congress during the last session, which criminalized the act of pretexting, but it did not deal with the source of the problem, and that concerns the information that is collected and maintains CPNI data that is used in the telecommunication sector, and that is the information that is being made available to pretexters to commit fraud, identity theft, and other types of crime. That is the information that we believe needs to be protected.

I thank you, again, for the opportunity to be here, and I would be pleased to answer your questions.

[The prepared statement of Mr. Rotenberg follows:]

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Prepared Testimony and Statement for the Record of

Marc Rotenberg,
President, EPIC

Hearing on

"Combating Pretexting: H.R. 936, Prevention of Fraudulent Access to Phone Records Act"

Before the

House Commerce Committee
United States House of Representatives

March 7, 2009
2123 Rayburn House Office Building
Washington, DC

Chairman Dingell, Ranking Member Barton, and Members of the Committee, thank you for the opportunity to testify on the privacy of telephone records and the problem of pretexting. My name is Marc Rotenberg and I am Executive Director and President of the Electronic Privacy Information Center in Washington, DC. EPIC is non-partisan research organization in Washington, DC that was established to focus public attention on emerging privacy and civil liberties issues. With me this morning is Caitriona Fitzgerald, a student at Northeastern Law School, who has assisted with our testimony.

We thank the Members of the Committee for holding this hearing and for introducing legislation to address the serious problem of pretexting and the associated problem of identity theft. In this statement, I will summarize EPIC's efforts at the FCC to establish stronger security standards for customer information, and express our support for H.R. 936, the bill now before the Committee.

The EPIC Petition to the FCC on Security for Calling Record Information

In the summer of 2005, EPIC undertook an extensive investigation of pretexting. a practice where an individual impersonates another person, employs false pretenses, or otherwise uses trickery to obtain personal information. We found that many web sites were making available personal information that had been wrongfully obtained and that these services were threatening the privacy and security of American consumers. In July 2005, we filed a complaint with the Federal Trade Commission concerning a website that offered phone records and the identities of P.O. Box owners for a fee through pretexting.

We supplemented that filing in August 2005 with a list of 40 websites that offered to sell phone records to anyone online.

In light of the fact that so many companies were selling phone records, EPIC turned to the Federal Communications Commission (FCC) to try to establish better safeguards for phone companies' customer records that were being improperly disclosed. On August 30, 2005, EPIC formally petitioned the FCC to initiate rulemaking for enhance security safeguards for individual's calling records. In our petition, we noted that, through § 222 of the Telecommunications Act of 1996[1], Congress has "specifically placed the burden of protecting Consumer Proprietary Network Information (CPNI) in [telecommunications carriers] hands."[2] Accordingly, the EPIC petition called for the FCC to immediately initiate a rulemaking proceeding to address CPNI protection measures used by telecommunications carriers, and to invite comment to develop adequate safeguards for verifying the identity of parties trying to access CPNI.[3] We suggested five forms of security measures that could be used by telecommunications carriers to more adequately limit disclosure of CPNI.[4]

The telecommunications industry quickly responded to EPIC's petition, suggesting that the FCC take enforcement actions against companies that sell phone records, but opposing any regulatory intervention that would require telecommunications carriers to change their security practices.[5] We responded, pointing out that enforcement

---

[1] 47 U.S.C. § 222 et seq. (2006).
[2] *See* Petition of the Electronic Privacy Information Center for Rulemaking to Enhance Security and Authentication Standards for Access to Customer Proprietary Network Information, CC Docket No. 96-115 (filed Aug. 30, 2005) ("EPIC Petition").
[3] *Id.*
[4] *Id.*
[5] *See e.g.* Opposition of BellSouth Corporation to EPIC Petition, RM Docket No. 11277 (filed Oct. 31, 2005).

actions against online data brokers alone was unlikely to prevent the sale of phone records, and that "FCC intervention is necessary to enhance security standards and authentication standards for access to CPNI."[6] The CTIA again responded, asserting that no additional rules were necessary, and suggesting that the FCC deny EPIC's petition to safeguard consumer phone records.[7]

In January 2006, after numerous news reports regarding the vulnerability of phone records to online data brokers, Senator Harry Reid sent a letter to the FCC, urging the agency to "begin an investigation into how online data brokers are obtaining Americans' private phone records, and whether phone companies are doing enough to protect the personal and private information with which they are entrusted." A few days later, on January 17, 2006, FCC Commissioners Adelstein and Copps released statements calling for action to address the illegal sale of telephone records.[8] Commissioner Adelstein noted that EPIC's petition "could be an appropriate vehicle for tightening [the FCC's] rules."[9]

On February 10, 2006, the FCC approved EPIC's petition, seeking comment on the five measures EPIC suggested in order to improve security of CPNI, as well as other measures.[10] The comment deadline was April 14, 2006.

---

[6] Reply Comments of the Electronic Privacy Information Center, CC Docket No. 96-115, RM Docket No. 11277 (Nov. 9, 2005) ("EPIC Reply Comments.")
[7] *See* Reply Comments of CTIA – The Wireless Association to EPIC Reply Comments, CC Docket No. 96-115, RM Docket No. 11277 (Nov. 15, 2005).
[8] Statement by Commissioner Jonathan S. Adelstein on Brokering of Personal Telephone Records (Jan. 17, 2006) ("Adelstein Statement"); Commissioner Michael J. Copps Calls for Action to Address Theft of Phone Records (Jan. 17, 2006) ("Copps Statement").
[9] Adelstein Statement.
[10] *See* 21 F.C.C.R. 1782, 1789 (2006).

FCC Investigation Into Telecommunications Carrier's Security Measures

On September 29, 2006, in a hearing before the House Subcommittee on Oversight and Investigations (Committee on Energy and Commerce), Kris Anne Monteith, Chief of the FCC Enforcement Bureau, discussed the ongoing FCC investigation into phone record security.[11] Chief Monteith asserted in his statement that once the record in the rulemaking proceeding closed in June, FCC Chairman Kevin Martin "directed the staff to expeditiously prepare an order resolving the issues raised in the rulemaking proceeding and intends to bring an order before the full Commission for its consideration this Fall."[12] Despite the apparent urgency of the situation, no such order has yet been promulgated.

All measures the FCC has taken with regard to telecommunications carrier responsibility for CPNI security seem to have taken place prior to its Notice of Proposed Rulemaking. On January 30, 2006, the FCC issued a Public Notice requiring telecommunications carriers to submit CPNI Compliance Certificates.[13] The investigation that followed resulted in the issuance of three "Notices of Apparent Liability for Forfeiture" to telecommunications carriers for failure to comply with CPNI compliance requirements. The FCC has reached consent decrees with two of these three carriers.[14]

---

[11] *See* Written Statement of Kris Anne Monteith, Hearing on "Internet Data Brokers & Pretexting: Who Has Access to Your Private Records?" Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, U.S. House of Representatives (Sept. 29, 2006) ("Monteith Statement").
[12] *Id.*
[13] Public Notice re: Enforcement Bureau Directs All Telecommunications Carriers to Submit CPNI Compliance Certificates (January 30, 2006) (available at http://www.fcc.gov/eb/Public_Notices/DA-06-223A1.html.)
[14] Monteith Statement at 5.

According the Chief Monteith, the FCC has also issued formal "Letters of Inquiry" to nearly twenty wireline and wireless carriers.[15] These letters "require the carriers to document their customer data security procedures and practices, identify security and disclosure problems, and address any changes they have made in response to the data broker issue."[16] Analysis of carrier responses is ongoing.

Despite Repeated Statements that CPNI Should be Protected, the FCC has Failed to Issue the Security Guidelines that Would Safeguard Consumer Information

In its Notice of Proposed Rulemaking (Notice), the FCC recognized that its rules implementing § 222 of the Telecommunications Act "require carriers to take specific steps to ensure that CPNI is adequately protected from unauthorized disclosure."[17] It further recognized that Congress granted CPNI the greatest level of protection available under § 222.[18] Thus, the safeguards protecting such information should be such that unauthorized access to it is nearly impossible to accomplish.

However, both the FCC and Congress have recognized that third-party unauthorized access to phone records is a widespread practice. As recently as January 18, 2007, the FCC issued a Consumer Advisory entitled "Protecting the Privacy of Your Telephone Calling Records," explaining to consumers that, despite rules protecting such information, illegal third-party access to phone records is occurring.[19] Congress recently passed legislation making "pretexting" a crime.[20]

---

[15] *Id.*
[16] *Id.*
[17] *Id.* at 1782; *see* 47 U.S.C. § 222(a).
[18] *Id.*
[19] FCC Consumer Advisory, Protecting the Privacy of Your Telephone Calling Records (Jan. 18, 2007) (available at http://www.fcc.gov/cgb/consumerfacts/phoneaboutyou.html.)
[20] *See* 18 U.S.C §1039 (2006).

Despite the recognition that both CPNI deserves the greatest level of protection available under § 222 due to its highly sensitive nature, and that such information is nonetheless being compromised, the FCC has failed to promulgate regulations to force telecommunications carriers to update its security measures to keep up with the changing technology available to data brokers.

Need for Passage of H.R. 936, Prevention of Fraudulent Access to Phone Records Act

Members of the Committee, Congress passed a law at the end of the last session regarding pretexting, but it addressed only a small part of the problem and did not provide the type of protection that is necessary to safeguard the privacy of American consumers. The Telephone Records and Privacy Protection Act criminalized pretexting but it failed to address the lack of security for telephone records or to resolve the question as to whether the FTC may use its section 5 authority to give after those who traffic in information that is obtained by means of pretexting.[21] The Act amends the federal criminal code to prohibit obtaining, or attempting to obtain, confidential phone records information from a telecommunications carrier (or any covered entity, as defined in § 1039(h)(2)) by: (1) making false or fraudulent statements or representations to an employee of a covered entity; (2) making such false or fraudulent statements or representations to a customer of a covered entity; (3) providing a document to a covered entity knowing that such document is false or fraudulent; or (4)accessing customer accounts of a covered entity via the Internet, or by means of conduct that violates section

[21] 18 U.S.C. § 1039.

1030 of this title, without prior authorization from the customer to whom such confidential phone records information relates.[22]

Although Congress' recognition of the seriousness of pretexting, and its efforts to criminalize it, are important, nothing in the law that was passed puts a duty on the telephone companies that are the actual source of this data to increase their security measures. Rather than going after the criminals after the crime occurs, wouldn't it make more sense to reduce the risk that our personal information will be wrongfully disclosed? The proposed Prevention of Fraudulent Access to Phone Records Act addresses the source of the pretexting problem.

Title I of the Act grants enforcement powers over the use of false pretenses to obtain Consumer Proprietary Network Information (CPNI) (a.k.a. pretexting) to the Federal Trade Commission (FTC) by treating it as an unfair or deceptive act or practice prescribed under § 18(a)(1)(B) of the Federal Trade Commission Act.[23] This will resolve any doubt as to the FTC's authority to prosecute these cases.

Title II of the Act establishes the Federal Communications Commission (FCC) provisions. In Section 201, Congress makes clear that telecommunications carriers have a duty to safeguard the confidentiality of its customers personal information.[24] In Section 202, the Act essentially sets forth more detail regarding a telecommunication carrier's obligations to only disclose CPNI to its owner or to authorized users. It prescribes requirements for disclosure of detailed information, requirements for affiliate use of both

---

[22] 18 U.S.C. § 1039(a) (2007). The Act also criminalized the activities of data brokers, prohibiting the sale or transfer of confidential phone records information. § 1039(b). It also makes those who use data broker services criminally liable, prohibiting the act of receiving such information with knowledge that it was illegally obtained. § 1039(c).
[23] H.R. 936, 110th Cong. § 103 (2007).
[24] § 201(2), (10).

general and detailed information, and requirements for partner and contractor use of general information. [25] It further amends § 222(c) of the Communications Act by adding a prohibition of sale, renting, leasing, or otherwise making available of CPNI.[26] Section 203 requires the FCC to prescribe regulations adopting more stringent security standards for CPNI to detect and prevent violations of the Act.[27]

Provisions in the proposed security standards mirror the safeguards suggested by EPIC in our August 2005 petition to the FCC. These measures would greatly benefit CPNI security. However, it should be noted that the only reference to increasing security standards by telecommunications carriers in the required regulations says that a carrier's security policy to should include "appropriate" standards to ensure security. This language does not seem to be much of a shift from the language of the Communications Act, which states that telecommunications carriers have a "duty to protect" CPNI. If carriers have always had a duty to protect such information, it is logical that they have been using "appropriate" standards to ensure such protection all along.

---

[25] § 202(a).
[26] § 202(d).
[27] The regulations that the Act requires the FCC to prescribe are:
(i) to require timely notice to a customer if there is a breach of CPNI regulations relating to his or her information;
(ii) to require timely notice to the FCC if there is a breach of CPNI regulations with respect to any customer;
(iii) to require periodic compliance audits by the FCC of telecommunications carriers;
(iv) to require telecommunications carriers to keep records of each time CPNI is requested, and if access is granted, a note of how the person's identity or authority to access the information was verified;
(v) to require telecommunications carriers to establish a security policy that includes "appropriate" standards to ensure security of CPNI;
(vi) to prohibit the use of pretexting by telecommunications carriers.

§ 203(h)(1)(A).

However, the Act does detail increased more security measures that would improve security of CPNI.[28] The measures it sets forth to consider are: (i) to require telecommunications carriers to "institute customer-specific identifiers in order to access CPNI"; (ii) to require encryption of CPNI (or other safeguards to secure the data); (iii) to require deletion of CPNI after a reasonable period of time if storage is no longer necessary.

These provisions also mirror the security measures suggested by EPIC in its petition to the FCC. If implemented, CPNI security would be significantly stronger. While only requiring the FCC to consider such measures is likely just oft-afforded administrative deference by Congress, given the measures' relative ease of implementation and the risk to privacy that unauthorized access to CPNI entails, it is vital that the FCC act to enforce such protections.

The Prevention of Fraudulent Access to Phone Records Act would provide much needed improved security for CPNI. The information that telephone companies collect and generate about the private activities of their customers should be subject to strong security standards that minimize the risk that individuals will be subject to pretexting and identity theft. CPNI was granted the highest level of protection under the Communications Act – acknowledgment of its extremely sensitive nature. As Congress recognizes in the Act, such information conveys details about the most intimate aspects of an individual's life. Moreover, such information is often used in furtherance of acts of stalking, domestic violence, and other violent crimes. Telephonme

[28] § 203(h)(1)(B).

Conclusion

Mr. Chairman, a year ago I had the privilege to appear before this Committee and to discuss EPIC's efforts to bring attention to the problem of pretexting well before the Hewlett-Packard matter was uncovered. I described our efforts to inform the FTC about this new threat as well as our petition to the FCC to establish stronger security standards for telephone record information. I was heartened at that time by Chairman Martin who expressed concern about the problem of pretexting and indicated that his agency was prepared to act on our petition. In fact, he thanked EPIC for bringing the Commission's attention to the problem.

Here we are now a year later and there has still been no proposal from the FCC to improve the security of the calling information of American consumers. There has been no concerted effort to work with the telephone companies to establish clear guidelines. Moreover, the Chairman has failed to address the question of whether the telephone companies violated the federal Communications Act when they disclosed the records of American citizens to the government without judicial approval. He should open an investigation on this issue as soon as possible.

The privacy provision for telecommunications service in the United States goes back to the original Communications Act of 1934.[29] Privacy protection is critical for consumer trust and confidence in our nation's communications services as well as the success of future communications services. The legislation before the Committee will begin to address the challenges the Commission has been unwilling or unable to.

Thank you for your attention. I will be pleased to answer your questions.

---

[29] § 605.

Ms. DEGETTE. Thank you, Mr. Rotenberg.

Mr. Largent.

STATEMENT OF HON. STEVE LARGENT, PRESIDENT, CHIEF EXECUTIVE OFFICER, CTIA-THE WIRELESS ASSOCIATION

Mr. LARGENT. Thank you, Chairwoman and Ranking Member Barton and members of the committee.

On behalf of CTIA, I am pleased to testify on H.R. 936 and the steps the wireless industry is taking to ensure the safety and security of wireless customers and consumers.

At the outset, I want to be clear. CTIA's member companies take seriously their obligation to protect customers' CPNI. In that sense, your goal is our goal, too.

In addition to meeting their duties under section 222, every carrier has a market-based interest in seeing that customer records are not disclosed without proper permission. Carriers employ a broad range of security measures to prevent unauthorized access to these records. In general, the system works well, as there are literally hundreds of millions of positive customer service interactions every year.

Nonetheless, well-publicized instances of pretexting and the legislative and oversight activities that followed in this committee and elsewhere served as a wake-up call for all of us. I am pleased to say that the wireless industry did not wait idly by for someone else to solve the problem. In addition to offering our assistance to the committee, each of CTIA's national carriers filed and obtained injunctions to shut down data thieves. The carriers also teamed with law enforcement to identify individuals and companies involved in fraudulent activities to help put these criminals out of business.

CTIA also supported legislation approved by the 109th Congress to criminalize the act of pretexting. Since the President signed the bill, the market for pretexting services has evaporated under the threat of Federal prison time and sizable financial penalties. The positive effect of this legislation cannot be overstated.

CTIA's members have not relied exclusively on the legal process to address pretexting. In the past year, wireless carriers have adopted a variety of procedures and tools to stop unauthorized access to CPNI. As is true in every other facet of the business, flexibility and innovation make a difference in the effort to defeat pretexters. Some carriers have focused on process. Others have chosen to use technology to help solve the problem. This variation between carriers is a positive, as static practices can become outmoded or avoided by third parties with ill intent. CTIA and its member companies strongly support additional enhanced security measures that can help to better protect consumers.

I detail each of these points in my written testimony, but let me briefly explain what CTIA supports.

We support giving customers the option of using pass codes to protect account detail. We support restricting disclosure of customers' Social Security numbers, tax ID, entire credit card number, or billing name and address in response to inbound customer calls. We support policies that preclude the release of call detail records via fax or e-mail, and we support confirmation of the FTC's jurisdiction in this area.

While CTIA supports reasonable measures to enhance the security of CPNI, any legislation the committee proposes should be narrowly targeted and responsive only to actual problems. Carriers must continue to have the flexibility to innovate and compete.

With this in mind, I have several specific observations to offer.

First, CTIA members are concerned about any provisions in H.R. 936 that would require carriers to obtain specific customer consent before they can share CPNI with affiliates and joint venture partners that provide marketing and other services to carriers that are otherwise permissible under the law. In instances where CTIA member companies share CPNI with third parties to aid in marketing, billing, and customer service efforts, they impose strict contractual obligations to protect customer information. There are also existing FCC requirements that cover such arrangements. Limiting the ability of carriers to share CPNI with third parties is burdensome and has no connection with the goal of preventing fraudulent access to phone records. We believe that an approach focused on enhanced security rather than introducing additional customer consent mechanisms is the best way to protect CPNI from unauthorized use.

Second, if Congress opts to act in this area, it should do so in the way that promotes uniformity and efficiency. We are seeing increased attention being paid to these issues at the State level, where, at last count, 34 different pieces of legislation related to call records have been introduced this year. Even when these bills are similar, they often contain variances that can make them difficult and costly to implement. What is needed is a uniform, national policy that properly balances consumer protection and carrier flexibility.

Let me conclude by underscoring the wireless industry's commitment to protecting CPNI. I can assure you that we will continue to enhance and improve our safeguards for sensitive customer information. It is already the law, it is common sense, and it is good business.

Thank you.

[The prepared statement of Mr. Largent follows:]

TESTIMONY OF
THE HONORABLE STEVE LARGENT
PRESIDENT AND CHIEF EXECUTIVE OFFICER
CTIA – THE WIRELESS ASSOCIATION®

BEFORE THE

U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON ENERGY AND COMMERCE

MARCH 9, 2007

Good morning, Chairman Dingell, Ranking Member Barton, and members of the Committee. On behalf of CTIA, I am pleased to have this opportunity to testify on H.R. 936 and the steps that the wireless industry is taking to ensure the safety and security of wireless consumers.

At the outset, I want to be clear: CTIA's member companies take seriously their obligation to protect their customers' CPNI. In that sense, your goal is our goal too.

* * * * *

The Wireless Industry Is Committed to Protecting CPNI

Carriers have a duty to protect CPNI under the Commission's existing rules and Section 222 of the Communications Act. Beyond that, every carrier has a market-based interest in seeing that customer records are not disclosed without the proper permission. Any carrier which fails to adequately safeguard the privacy of its customers will -- and should -- suffer in the marketplace. For this reason, wireless carriers employ a broad range of security measures to prevent unauthorized access to and disclosure of these records. In general, the system works

well, as there are literally hundreds of millions of positive customer service interactions every year.

While it is the exceptions that generate headlines, I am pleased to tell you that since I last appeared before the Committee on this subject, much progress has been made to ensure that CPNI is protected, and that those who attempt to procure it illicitly are thwarted and punished.

Incidents like the unauthorized release of General Wesley Clark's call records and the Hewlett-Packard pretexting scandal served as a wake-up call for all of us. The wireless industry did not wait idly by for someone else to solve the problem. Each of CTIA's national carriers filed and obtained injunctions that shut down data thieves and the carriers teamed with law enforcement to identify individuals and companies involved in fraudulent activities to help put these criminals out of business.

CTIA supported legislation approved by the 109th Congress to criminalize the act of pretexting. President Bush signed the *Telephone Records and Privacy Protection Act of 2006* (H.R. 4709, P.L. 109-476) in January. Since enactment of that legislation, the market for pretexting services has evaporated under the threat of Federal prison time and sizeable financial penalties. The positive effect of the legislation cannot be overstated. Although the law is less than two months old, a Google search performed prior to this hearing did not find the kind of advertisements offering to procure customers' call records that were prevalent just a short time ago.

CTIA's members have not relied exclusively on the legal process to address pretexting.

In the past year, wireless carriers have adopted, and continue to adopt, a variety of procedures and tools to stop unauthorized access to CPNI. As is true in every other facet of the business, flexibility and innovation make a difference in the effort to thwart pretexting. This variation between carriers is a positive, as static practices can become outmoded or avoided by third parties with ill intent.

Some carriers have focused on process. Alltel, Cingular (now AT&T), and T-Mobile have implemented policies prohibiting their customer service representatives from providing call-detail information over the phone to anyone. Verizon Wireless has made a major commitment to enhanced training of customer service representatives. Others have chosen to use technology to help solve the problem. SprintNextel has embarked on an effort to utilize interactive voice response (IVR) technology to authenticate customers before the customer is routed to a customer service representative. IVR authentication can improve the security of customer accounts by further distancing authenticating information from customer service representatives, and by masking certain account information, such as call-detail records from the customer service representative, pending successful IVR authentication.

CTIA and its member companies strongly support additional enhanced security measures that can help to better protect consumers.

Specifically, CTIA supports giving customers the option of using passcodes. Many carriers already offer password protection, especially for online account access, for those customers who seek extra protection beyond the typical verification procedures. Across the wireless industry, passcodes have become standard operating procedure. Nonetheless, a blanket obligation that all accounts be password protected is undesirable, as passwords may not be wanted by every customer. Surveys and carrier experience have shown that some customers are burdened by having to remember numerous passwords for various accounts that may easily be forgotten or lost, and thus resist password protection for access to their account. In addition, there are customers who freely share their passwords with significant others and family members, therefore compromising the security of their own accounts. As an alternative to forcing password usage for all account access, CTIA supports a requirement that carriers make passwords available to all customers for account access. Customers should then be informed of the benefits of such passwords and the ways to effectively safeguard account access.

CTIA believes a rule that prohibits disclosure of a customer's entire Social Security Number, Tax ID, entire credit card number, or billing name and address in response to inbound customer calls may provide a useful deterrent to pretexting. There is no good reason why a carrier should provide customers with their personal-identifying account information. Many carriers already have implemented this procedure.

CTIA supports, and its carriers have adopted, policies that preclude the release of call detail records via fax or e-mail. Consumers seeking call detail information can only be provided

with that information if it is mailed to the address of record for billing purposes, or after the customer is called back on his or her registered mobile number. While some customers may find this practice inconvenient, this inconvenience is outweighed by the corresponding security benefits of these policies.

Finally, the Chair of the Federal Trade Commission, Deborah Majoras, has declared that the FTC has sufficient authority to act against parties that engage in the theft and illegal sale of call records. Nonetheless, if the Congress seeks to confirm the FTC's jurisdiction in this area, as is proposed in Title I of H.R. 936, CTIA would support such action, as we did last year. We would hope, however, that providing the FTC with civil enforcement authority will not in any way diminish the criminal prosecution of data thieves.

Wireless Carrier Concerns with H.R. 936

While CTIA supports reasonable measures to enhance the security of CPNI, CTIA's members have strong concerns about "one size fits all" legislative proposals that do not provide carriers with the flexibility that has served them so well in the marketplace. Any legislative obligations the Committee proposes should be narrowly targeted and responsive only to actual problems rather than theoretical possibilities and provide the flexibility that carriers need to innovate and compete. With this in mind, I have several specific observations to offer.

First, CTIA's members are concerned about any provisions in H.R. 936 that would require carriers to obtain specific customer consent – whether "opt-in" or "opt-out" – before they can

share CPNI with affiliates and joint venture partners that provide marketing and other services to carriers that are otherwise permissible under the law.

In instances where CTIA member companies share CPNI with third parties to aid in marketing, billing, and customer service efforts, they impose strict contractual obligations to protect customer information. There are also existing FCC requirements that cover such arrangements.

Additionally, the imposition of new restrictions on the ability of carriers to share CPNI with joint venture partners or independent contractors is unduly burdensome and has no connection with the goal of preventing fraudulent access to phone records. Many CTIA members employ third-parties to assist with billing and customer care functions. The parties that engaged in these activities for our carriers are bound by strict safeguarding agreements that govern both confidentiality and security obligations.

In general, industry practice obligates subcontractors to (1) use administrative, technical, and physical safeguards to protect customer information, (2) access and use customer information only on a need-to-know basis, (3) maintain strict confidentiality of customer information, (4) return or destroy customer information when it is no longer needed, and (5) submit to security and privacy audits. Contractors generally work in highly controlled environments and handle information that, while technically considered CPNI, is not the call-detail CPNI that pretexters seek.

CTIA is not aware of any credible suggestion that third-party contractors or joint venture partners have misused any CPNI that has been shared with them by a wireless carrier. The national carriers and Tier II carriers such as U.S. Cellular Corp., Dobson Communications, and MetroPCS Communications have each noted in their FCC filings that restricting or imposing burdensome requirements on the use of independent contractors and joint venture partners to help deliver, bill for, and market products and services to consumers will raise costs without any corresponding benefit. This problem might be particularly acute for smaller carriers which lack the ability to spread potential compliance costs over a national customer base.

While the bill appears to permit some sharing of information with third parties to initiate, render, bill, and collect for services and to provide customer service, this exemption is potentially compromised by the sweeping restrictions on disclosures elsewhere in the bill. We believe that an approach focused on enhanced security rather than introducing additional customer consent mechanisms is the most effective, cost-beneficial, and constitutionally permissible means by which to protect CPNI.

As a general matter, wireless companies should have the flexibility to use CPNI to market services other than telecommunications and Internet access to customers whose prior purchasing habits suggest they may be interested in additional services. Amazon.com and L.L. Bean have that flexibility; wireless carriers should too. Wireless carriers do not safeguard CPNI any less when such information is used to market other services as compared to when it is used to market their core services, and, as the record in the FCC's proceeding on

the EPIC petition demonstrates, there is no causal connection between Section 222's existing "opt-out" regime and the fraud perpetrated by pretexters. Depriving wireless carriers of the ability to use CPNI to market additional services to existing customers is not a necessary part of the effort to eliminate pretexting.

Unfortunately, as drafted, the bill appears to preclude a wireless carrier from informing only that subset of customers who have handsets that can receive a new service such as mobile TV (e.g., Verizon Wireless' V-Cast or Qualcomm's Media Flo) that such services are available. Instead, a carrier wishing to offer these services would have to market them to its entire customer base – in some cases as many as 50 million people – just to reach early adopters. This is a terribly inefficient restriction on a competitive business, and it does not make CPNI any safer.

CTIA also opposes the provisions of H.R. 936 that direct the Commission to consider whether it should require carriers to encrypt all stored CPNI data. The Commission is already considering such a requirement in its current proceeding, and thus far the record shows no evidence of unauthorized access of stored CPNI within carriers' databases. Mandatory encryption of stored call records would not have the effect of preventing pretexting. Conversely, it would increase costs, potentially delay response to legitimate customer service inquiries, and needlessly complicate carrier storage and access methods. Accordingly, CTIA urges that this provision be dropped from the bill.

In addition, the bill's provisions on "Access to Wireless Telephone Numbers" are overly broad. I appreciate what the drafters of this language were attempting to achieve when it was added to the bill last year, and I can assure you that CTIA's member companies have no plans to create a wireless directory without a customer's express opt-in consent. However, wireless numbers are employed for other important and legitimate uses -- such as the sale and delivery of third-party content, including things like news alerts, games, and ring tones -- that should not be frustrated by efforts to limit the creation of a directory.

Finally, if Congress opts to act in this area, it should do so in a way that promotes uniformity and efficiency. We are seeing increased attention being paid to these issues at the state level, where at last count, 34 different pieces of legislation (in 17 states) related to call records have been introduced this year. In the last legislative session, there were 75 bills in 28 states. Even when these bills are generally alike, they often contain variances that can make them difficult and costly to implement. The wireless industry does not welcome having to deal with a multitude of varying state-by-state obligations in this area. How well a consumer is protected, or what obligations a carrier faces, should not vary widely by location, and what is needed is a uniform national policy that properly balances the need to protect consumers while allowing carriers the flexibility to operate in the most efficient and cost-effective manner possible.

* * * * *

I believe that the wireless industry is in a better place today than the last time I appeared before you on this subject. The carriers have invested significant time and resources to make CPNI more secure. The much-publicized criminal activity that prompted congressional attention led to enactment of important legislation that dried up the market for pretexting. Equally importantly, these actions have focused the industry on efforts to improve its practices. Real progress is being made, both in terms of employee training and investment in new and improved systems, and that commitment will continue.

I commend the Committee and the authors of this legislation for the attention you have focused on this issue. The wireless industry looks forward to continuing to work with you to ensure that our customers' phone records are protected. I do hope, however, that as the Committee considers H.R. 936, you will preserve the wireless industry's flexibility to continue to provide consumers with innovative new services at affordable prices.

Thank you for the opportunity to share the wireless industry's views on this matter.

Ms. DEGETTE. Thank you, Mr. Largent.

Mr. McCormick.

STATEMENT OF WALTER MCCORMICK, PRESIDENT AND CHIEF EXECUTIVE OFFICER, UNITED STATES TELECOM ASSOCIATION

Mr. MCCORMICK. Madame Chair, Mr. Barton, members of the committee, on behalf of the member companies of the United States Telecom Association, I want to thank you for this opportunity to testify on the important issue of safeguarding consumers' phone records from fraudulent use by pretexters.

This committee has a long history of working to protect consumers. Our industry shares your concern for protecting customer information. Protecting privacy is a critical component of our customer care.

In today's highly-competitive marketplace, no industry should take the privacy of its customers lightly. As our member companies begin offering a variety of new, advanced broadband services, we see our reputation for delivering quality service and protecting the privacy of our customers as a competitive advantage.

There is a strong business incentive to protect customer privacy. There is an existing legal obligation as well. Section 222 of the Communications Act provides that telecommunications carriers have a duty to protect the confidentiality of customer proprietary network information.

This legal obligation is taken very seriously by our member companies. We educate and train our customer service employees. We observe strict security protocols, and we tightly define our agreements with marketing firms.

We believe the best way to address the problem of fraudulent access to phone records is through the enforcement of existing laws and the strengthening of penalties on bad actors. In this regard, we applaud title I of this legislation, which would explicitly ban the practice of pretexting and give the Federal Trade Commission authority to enforce this prohibition. This provision complements and strengthens the action taken by Congress last year in establishing criminal penalties for pretexting.

We are concerned, however, that the broad approach taken in title II of the bill will have a number of negative consequences, consequences that appear to be unintended ones, ones that would impact legitimate marketing practices that are, in many ways, proconsumer. Consumers benefit when their communications carriers offer them new discount packages and innovative services. The information we typically rely upon in pursuing marketing opportunities focuses on purchasing patterns and the types of services that a customer is receiving, information that is of little or no use to pretexters, the kind of pretexters that this bill seeks to target.

For example, if a customer has caller ID in order to avoid unwanted calls at dinnertime, CPNI enables our marketers to identify a customer that might have an interest in receiving a bundle discount that could include call management or call-blocking features. If a customer has subscribed for both voice service and high-speed Internet access, this is a customer that might have an interest in

learning about savings that could be obtained by broadening this bundle to include video.

The provisions proposed in title II could significantly impede this pro-consumer outreach, all without addressing any identifiable problem of fraudulent access to phone records. We are aware of no evidence to suggest that marketing of services, either directly or through joint venture partners, has resulted in any abuse of customer proprietary information. Indeed, FCC regulations require that confidentiality agreements be in place before CPNI is shared with joint venture partners or contractors. Businesses succeed by being responsive to their customers.

As currently drafted, however, title II would severely impede the ability of our industry to bring to the attention of its customers the opportunity to take advantage of improved services or increased savings. We have been informed that this is not the committee's intent, that instead the committee intended to only impose new restrictions on the sharing and disclosure of detailed customer telephone records. There is currently an FCC proceeding underway that is considering the same thing.

if it is, in fact, the committee's intention to only address this limited, call-detailed information, information related to matters such as individual locations, duration, time, and date of specific customer communications, then we would suggest that the bill language be clarified so that our industry can continue offering to its customers new services and bundled savings, as it does under current rules, while affording new protection to detailed customer telephone records.

Our industry also has significant concerns with section 203, which would prescribe burdensome audit trail requirements. The last time the FCC looked at this issue, the cost of complying was enormous. It could range anywhere from $12 to $64 per line, which would clearly be a hardship for many consumers.

Madame Chair, again, thank you for the opportunity to testify today, and we look forward to working constructively with you to prevent pretexting and identity theft.

[The prepared statement of Mr. McCormick follows:]

Testimony of Walter B. McCormick
President and CEO
United States Telecom Association
Before the House Committee on Energy and Commerce

March 9, 2007

Mr. Chairman, Ranking Member Barton, and members of the Committee, on behalf of the member companies of the United States Telecom Association, I want to thank you for this opportunity to testify on the important issue of safeguarding consumer's phone records from fraudulent use by pretexters.

This Committee has a long history of working to protect consumers. Our industry shares your concern for protecting customer information. Protecting privacy is a critical component of our customer care.

In today's highly competitive marketplace, no industry should take the privacy of its customers lightly. As our member companies begin offering a variety of new advanced broadband services, we see our reputation for delivering quality service and protecting the privacy of our customers as a competitive advantage.

There is a strong business incentive to protect customer privacy. There is an existing legal obligation, as well. Section 222 of the Communications Act provides that telecommunications carriers have "a duty" to protect the confidentiality of customer proprietary network information.

This legal obligation is taken very seriously by our member companies. We educate and train our customer service employees, we observe strict security protocols, and we tightly define our agreements with marketing firms.

We believe the best way to address the problem of fraudulent access to phone records is through the enforcement of existing laws and the strengthening of penalties on bad actors. In this regard, we applaud Title I of this legislation, which would explicitly ban the practice of pretexting and give the Federal Trade Commission authority to enforce this prohibition. This provision complements and strengthens the action taken by Congress last year in establishing criminal penalties for pretexting.

We are deeply concerned, however, by the broad approach taken in Title II of the bill. We believe that it will neither increase customer security nor reduce the amount of marketing materials customers receive. In fact, customers would likely see an increase in such materials, as carriers would be forced to take a generic approach to their marketing – a direct result of provisions that would impede the kind of targeted marketing that consumers value most.

Consumers benefit when their communications carriers offer them new discount packages and innovative services. The information we typically rely upon in pursuing marketing opportunities focuses on purchasing patterns and the types of services a customer is receiving, information that is of little or no use to the pretexters this bill seeks to target.

For example, if a customer has caller ID to avoid unwanted calls at dinnertime, CPNI enables our marketers to identify a consumer that might have an interest in receiving a bundled discount that might include call management, a service that forces the caller to give their name before the call rings through, or call blocking features. If a customer has subscribed for both voice service and high-speed internet access, he might have an interest in learning about savings that could be obtained by broadening his bundle to include video. For consumers, this kind of targeted marketing can be highly informative, helpful, and result in real savings.

The provisions proposed in Section 202 could significantly impede this pro-consumer outreach — all without addressing any identifiable problem of fraudulent access to phone records. We are aware of no evidence to suggest that marketing of services, either directly, or through joint venture partners, contractors, or other third parties has resulted in any abuse of customer proprietary information. Indeed, FCC regulation §64.2007 requires that in order to share CPNI with joint venture partners or contractors, telecommunications carriers must first enter into confidentiality agreements with these third parties. The agreement must require that the third party only use the information for marketing or providing communications-related services for which the information was provided; that the third party be prohibited from sharing the data with any other party; and that the third party have appropriate protections in place to ensure the confidentiality of consumers' information.

Businesses succeed by being responsive to their customers. As currently drafted, however, Title II would severely impede the ability of our industry to bring to the attention of its customers the opportunity to take advantage of improved services or increased savings. We have been informed that this is not the Committee's intent – that, instead, the Committee intended to only impose new restrictions on the sharing and disclosure of "Detailed Customer Telephone Records." There is, currently, an FCC proceeding underway that is considering the same thing. If it is, in fact, the Committee's intention to only address this limited call detail information – information related to matters such as the individual locations, duration, time, and date of specific customer communications – then we would suggest that the bill language be clarified so that our industry can continue offering its customers new services and bundled savings, as it does under current rules, while affording new protection to detailed customer telephone records.

Our industry also has significant concerns with Sec. 203, which would prescribe burdensome audit trail requirements. The last time the FCC looked at this issue in the late 1990s, the cost of complying with similar requirements was estimated at up to $270 million per carrier. These mandates get factored into the cost of doing business and eventually affect the prices consumers pay … in this case with very little, if any, benefit. In fact, small, rural carriers estimated that the additional cost of compliance could range from $12-$64 per line — clearly a hardship for many consumers.

Mr. Chairman, again, we thank you for the opportunity to be here today. We look forward to working constructively with you and the members of the committee to develop sound policies that focus on preventing pretexting and illegal invasions of privacy.

I look forward to responding to any questions you may have.

###

Ms. DEGETTE. Thank you, Mr. McCormick.

Mr. Einhorn.

STATEMENT OF DAVID EINHORN, PRESIDENT, GREENLIGHT CAPITAL, INC.

Mr. EINHORN. Good morning, Madame Chairman and members of the committee, and thank you for holding this hearing. And I appreciate your sympathy.

Although I did not ask to participate in this hearing, I appreciate the invitation to describe my experience as a victim of pretexting.

My testimony is about a corporation and management team that, in attempting to ensure their survival, placed no limits on the exercise of their power.

Pretexting is a brazen invasion of privacy when a large corporation has its agents spy on private citizens in order to intimidate then and silence criticism that threatens more than just the sanctity of the individual's privacy. It threatens the freedom of the securities markets for which we take for granted.

I am the president of Greenlight Capital, a long-term, value-oriented investment company. One of our long-term investments is Allied Capital. Our research showed Allied suffered from significant accounting and operational deficiencies, and Greenlight took a short investment position based upon that belief.

Our research indicated that, among other things, Allied misled the public about the value of its investments, valuing them at original cost, even after the investments go bankrupt. We later found that small business lending unit defrauded the SBA and the USDA Government lending programs, costing taxpayers hundreds of millions of dollars.

In 2002, I voiced my concerns about Allied at an investment research conference, which was part of a charity fundraiser for a pediatric cancer hospital. I told the audience why I had sold Allied short and pledged to give half of my personal profits on this investment to the children's hospital sponsoring the event.

In response to my speech, instead of examining and cleaning up these problems, Allied attacked me. The company conducted a campaign to discredit me, attacking my reputation and my motivations. But ultimately, regulators and prosecutors have begun to see through Allied's tactics. The FCC began an investigation in 2004, and later that same year, the U.S. Attorney from the District of Columbia began a criminal investigation.

Some time that year, Herb Greenberg, a respected financial journalist for Dow Jones, who had written critically about Allied, told me that his phone records had been stolen. I subsequently learned a woman, unknown to me, had called my long distance provider, identified herself as my wife, provided her Social Security number, and opened an online account to obtain our home telephone records.

Somebody also stole the phone records of other known critics of Allied, including hedge fund managers, a journalist, a research analyst, an individual investor, and a former media relations advisor to Greenlight.

In March 2005, I wrote a private letter to Allied's Board of Directors, asking the Board to fully investigate what had happened. A

week later, I received a brush-off response. Last fall, after the Hewlett-Packard's chairman admitted to pretexting and later resigned, I again asked Allied's Board to investigate. Allied responded, saying they had found no evidence to support my claim.

Then Allied's management went on the offensive, yet again. On the company's November 8, 2006 quarterly earnings conference call, chief executive officer William Walton spent several minutes attacking my motivations and stating that my concerns about my stolen phone records were "yet just another example of Mr. Einhorn's tactics". And he issued his own denial that anyone at Allied had accessed my records, saying, "There is simply no evidence to support a claim that Allied tried to access Einhorn's phone records. We never received his records."

In December 2006, Allied was served with a grand jury subpoena, and then their story changed. In a press release dated February 6, 2007, Allied admitted that its agent had stolen not only my home phone records but also Greenlight's records. The press release, itself, was a model of evasion, however, and not at all consistent with the disclosure expected of a public company. It left unanswered a number of questions: who had obtained the records, who else's records did they steal, who had authorized the theft, and for what purpose, what did they do with this information, and what else did these agents do to gather information about their critics?

After the Hewlett-Packard pretexting scandal, HP immediately apologized to the victims and promised to give the victims a full account. But I have not heard from Allied. Nobody has contacted me to apologize or explain who invaded my privacy or for what purpose.

In conclusion, Allied's behavior strikes at the ethical heart of the securities markets, which are based on the free and fair flow of ideas, critical and otherwise. It is a cold reality that companies left to their own devices will rarely divulge the full truth about their problems. It is left to others, regulators, analysts, the media, and investors like myself to hold companies accountable. The free exchange of ideas in our market system depends on the very people who were pretexted in this case. There are many valuable voices in the marketplace who will choose not to criticize companies for fear of being retaliated against. Nobody wants their privacy invaded.

As the committee has noted this very legislation, action, such as pretexting, can lead to harassment and intimidation. It can also lead to less information in the marketplace. A line must be drawn. I support this legislation.

Thank you, Madame Chairman, and I am available to answer any questions you might have.

[The prepared statement of Mr. Einhorn follows:]

Statement of

David Einhorn, President
Greenlight Capital, Inc.

Before the

House Committee on Energy and Commerce
U.S. House of Representatives

Hearing on

H.R. 936 – the Prevention of Fraudulent Access to Phone Records Act

March 9, 2007

Chairman Dingell and Members of the Committee, thank you for holding this hearing on the "Prevention of Fraudulent Access to Phone Records Act." Although I did not ask to participate in this hearing, I appreciate the invitation to describe my experience as a victim of pretexting. Having said that, please understand that it is impossible to explain what happened to me without placing it in context.

My testimony is a cautionary tale. It is about a corporation and management team that, in attempting to ensure their survival, placed no limits on the exercise of their power. Pretexting is a brazen invasion of privacy. The thought of an individual engaging in pretexting is unnerving enough. But when a corporation, with millions of dollars at its disposal, has its agents spy on private citizens in order to silence criticism, that threatens more than just the sanctity of the individual's privacy; it threatens the freedom of the securities markets that we take for granted. I believe that the "Prevention of Fraudulent Access to Phone Records Act," which explicitly addresses pretexting, will send a strong message and act as a deterrent to those who feel that they can invade the privacy of citizens simply because they are suspicious of them or disagree with them. That is why I am testifying in support of this legislation.

My name is David Einhorn. I am the President of Greenlight Capital, a long-term oriented value investment company. One of our long-term investments is Allied Capital, a company headquartered a few blocks from here on Pennsylvania Avenue. Some time ago, our research led us to believe that Allied suffered from significant accounting and operational deficiencies, and Greenlight took a short investment position in Allied based upon that belief.

In 2002, I voiced my criticism of Allied publicly at an investment research conference, which was part of a charity fundraiser for a pediatric cancer hospital. I told the audience that I

had sold Allied short based on my research, and pledged to give half my personal profits based on this investment to the children's hospital sponsoring the event.

Our research indicated that Allied hides its problem investments by misleading the public about their value – valuing them at their original cost even as the investments go bankrupt – while stating publicly that the SEC valuation rules do not apply to them. Our research also indicated that Allied inflates its earnings by charging excessive interest rates and fees to companies it controls but does not consolidate in its financial results, while disclosing little about the performance of these companies. And its small business lending unit has defrauded the SBA and the USDA government lending programs out of hundreds of millions of dollars. All the while, we had seen Allied attempt to outgrow its problem investments by raising new capital from unknowing investors.

I discussed Allied's problems at the research conference in 2002. In response to my speech, instead of examining and cleaning up these problems, Allied decided to attack me. The company began a systematic campaign to discredit me, publicly attacking my reputation and my motivations. But ultimately the public – and the regulators – began to see through Allied's tactics. The SEC began an investigation into Allied in 2004 about the very practices I had accused Allied of from the beginning. Later that same year, the U.S. Attorney for the District of Columbia began a criminal investigation.

In its zeal to silence its critics, Allied used extreme measures. But even I did not believe Allied would go so far as to invade the privacy of my home and family. I was wrong. In an apparent attempt to find some piece of information to embarrass and discredit its critics, Allied retained private investigators to obtain its critics' personal and business phone records, including mine.

In 2004, Herb Greenberg, a respected financial journalist for Dow Jones who had publicly criticized Allied, told me that his phone records had been illegally accessed. I subsequently learned that a woman unknown to me had called my long distance provider; identified herself as my wife; provided my wife's social security number; and opened an online account to access our home telephone records. We then learned that the phone records of other known critics of Allied – including other hedge fund managers, a journalist, a research analyst, an individual investor and a former media relations advisor to Greenlight – had been similarly illegally accessed.

The FBI ultimately discovered the identity of the individual who had accessed my phone records, though they could not share that information with me. The phone records investigation was subsequently moved to the U.S. Attorney's Office in Washington D.C., where the criminal probe of Allied was already underway.

In March 2005, I wrote a private letter to Allied's Board of Directors and told them that someone had stolen my wife's social security number and used it to steal my phone records, along with the records of several other prominent Allied critics. I asked the Board to fully investigate what happened. A week later, I received a brush-off response that I had not provided sufficiently specific information for them to conduct an inquiry. A copy of my letter to Allied's Board of Directors and Allied's response is attached.

In September 2006, after Hewlett-Packard's CEO publicly admitted to involvement in very similar conduct and resigned, I wrote another private letter to the Chairman of the Audit Committee of Allied's Board, reminding them of the seriousness of pretexting and once again asking them to investigate. Two weeks later the Board responded that it had looked into my allegations and found no evidence to support my claim. Copies of these letters are also attached

At the same time, Allied's management went on the offensive yet again. On the November 8, 2006 earnings conference call, Allied's CEO, William Walton, spent several minutes attacking my motivations and stating that my concerns about my stolen phone records were "yet just another example of Mr. Einhorn's tactics." He recounted my letters to Allied's Board and their prompt denials. He criticized me for not providing more evidence. And he issued his own denial that anyone at Allied had accessed my records, saying:

> There is simply no evidence to support a claim that Allied tried to access Einhorn's phone records. We never received his records and all that the article points to in support of this claim is the word of Einhorn, an individual with a motive to depress Allied Capital's stock.

Only three months later, Allied completely changed its story. On February 6, 2007, Allied issued a press release innocuously titled "Allied Capital Comments on Recent Events." Allied admitted that its "agent" had stolen not only my home phone records, but also Greenlight's records. The release read:

> Allied Capital Corporation announced today that, in late December 2006, it received a subpoena from the United States Attorney's Office for the District of Columbia requesting, among other things, the production of records regarding the use of private investigators by Allied Capital or its agents. The Board established a committee, which was advised by its own counsel, to review the following matter.
>
> In the course of gathering documents responsive to the subpoena, Allied Capital has become aware that an agent of the Company obtained what were represented to be telephone records of David Einhorn and which purport to be records of calls from Greenlight Capital during a period of time in 2005.
>
> Also, while Allied Capital was gathering documents responsive to the subpoena, allegations were made that Allied Capital management had authorized the acquisition of these records and that management was subsequently advised that these records had been obtained. The management of Allied Capital states that these allegations are not true.

Until Allied issued this press release, I had not known that Greenlight's phone records had also been stolen. For them to admit this, the evidence must have been extremely clear. After denials since 2005, only a grand jury subpoena from the U.S. Attorney's Office finally pried the truth out of Allied.

The press release was a model of evasion, however, and not at all consistent with the disclosure expected of a public company. Who had made the allegations? Who had obtained the records? Who had authorized the theft, and for what purpose? What did they do with this information? And what else did these agents do to gather information about their critics? The release did not even deny that Allied had authorized the theft of my phone records. It only stated that "management of Allied Capital states" that this was not true. The release said there would be no further comment, effectively refusing to answer these questions or clarify this muddled statement.

For me, the theft of my personal phone records and my wife's personal information has done more than just confirmed my views about Allied. It has struck at my sense of security and the protection I have put around my family and my home. After the Hewlett Packard pretexting scandal, HP immediately apologized to the victims and promised to give the victims a full account. But to date, I have heard nothing from Allied. No one has contacted me to apologize or explain who invaded my privacy and my family's privacy. Allied has not yet admitted to taking anyone else's records. Of course, they don't deny it, either. It is simply not credible that Allied management did not know about this.

This pretexting strikes at the ethical heart of the securities markets, which are based on the free and fair flow of ideas, critical and otherwise. It is a cold reality that companies, left to their own devices, will rarely divulge the full truth about their problems. It is left to others –

regulators, analysts, the media, and investors like myself – to hold these companies accountable. The free exchange of ideas in our market system depends on the very people who were pretexted in this case.

But that system is under attack; more and more, the instinct of a company under attack from critics is to hit back harder, not to address the underlying problem. Unless companies like Allied are told in no uncertain terms to *stop*, this trend will escalate. There are many valuable voices in the marketplace who will choose not to criticize companies for fear of being retaliated against. Nobody wants their privacy violated. As the Committee has noted in this very legislation, actions such as pretexting can lead to harassment and intimidation. It can also lead to less information in the marketplace. A line must be drawn.

I support this legislation. There is no question that pretexting is a criminal activity under any number of federal and state laws. But there is no law specifically designed to address pretexting and the harm that it causes. That a company like Allied believes it can have agents pose as me or my wife in order to steal our personal records is proof that the seriousness of pretexting has not truly been communicated to the public. I believe that the Prevention of Fraudulent Access to Phone Records Act is an important step in raising the public's awareness of this issue and will enhance the protections available to the ordinary citizen against unauthorized invasions of their privacy.

March 11, 2005

Dear Allied Capital Corporation Director:

I write to inform you directly of the continuing misconduct of Allied Capital's management, conduct that I believe warrants an independent investigation by the Board.

As you know, I have been a critic of your company for almost three years and have documented many of my criticisms publicly. These criticisms have largely proven to be true over time and have been bolstered by the ongoing investigations by the U.S. Attorney for the District of Columbia and the SEC into Allied and its small business lending unit, Business Loan Express ("BLX").

Yet, instead of addressing the underlying problems with the company, Allied's management has attempted to deflect attention from such criticism by misrepresenting facts to the public, levying personal attacks against me and using other tactics which are troubling, to say the least. Such actions signal that Allied's management has more interest in concealing the company's problems than in addressing them. This is hardly surprising since it was Allied's management that engineered these problems in the first place. As this has all unfolded, however, it appears that Allied's Board of Directors has remained strangely silent.

As you are no doubt aware, the SEC and the U.S. Attorney's Office in the District of Columbia are investigating Allied and BLX. Management has told the public that these investigations relate to "issues similar to those raised by short sellers over the past two and one-half years,"[1] apparently referring to, among other things, the assignment of several defaulted loans by BLX to Allied in early 2003. That assignment, however, is only one example of the widespread fraud that has occurred at BLX under the stewardship of the current management.

Specifically, Allied has falsely maintained and increased its valuation of BLX through a scheme dependent on the commission of systematic fraud against the Small Business Administration and, as a result, against the taxpaying citizens of the United States. I have learned that BLX has maintained its loan origination volume only by knowingly approving loan applications that fail to comply with SBA regulations. These applications, among other things, have fraudulently inflated property and collateral values, failed to verify equity injections, contained impermissible property splits and property flips, and other violations of SBA rules that were concealed from the agency. Additionally, many of these loans were the subject of improper loan brokering arrangements.

[1] See Allied Press Release dated December 27, 2004, attached to its Form 8-K dated December 27, 2004 as Exhibit 99.1.

2 Grand Central Tower • 140 East 45th Street, 24th Floor • New York, NY 10017
Phone: 212-973-1900 • Fax 212-973-9219 • www.greenlightcapital.com

By approving such loans, BLX is able to immediately recognize income around the time of loan origination, because it uses gain-on-sale accounting. BLX needs to continually increase its origination volume to support its revenue growth. This pressure to increase origination volume leads to the approval of additional fraudulent loan applications. This pyramid scheme has allowed Allied to recognize enormous fees, interest and dividends from BLX, while it values BLX far above its actual worth. And it is Allied's and BLX's execution of this scheme, I believe, that has led the SEC and the U.S. Attorney's Office to initiate their investigations.

Eventually, when the loans default, BLX receives a guarantee payment from the SBA by concealing the fact that the loans should not qualify for a guarantee because of the fraudulent origination. It would not surprise me if BLX or Allied is ultimately required to repay the government millions of dollars upon completion of the government investigations.

Allied's management, however, has entirely failed to respond to these problems. Instead, management has issued false and misleading public statements dealing with such clearly material facts as the status of government investigations. For example, during Allied's fourth quarter 2002 conference call on February 13, 2003, I asked Ms. Joan Sweeney the following question:

> EINHORN: Could you comment at all relating to the office of Inspector General in the SBA that I understand has been calling around people close to Business [Loan] Express, what do you think they're looking into and is there an investigation and if so what do you believe the status to be?
>
> SWEENEY: You know, David, I don't know. I mean, clearly, BLX is a regulated entity by the SBA. They're routinely audited by the SBA. I know that the office of Inspector General typically works with the SBA looking at SBA lenders. It's usually a routine – they are usually routine inquiries, if there is an inquiry. So that's about all I can say. **We don't know the nature of any sort of inquiry.** So, you know, again this happens routinely in the SBA lending market. (Emphasis added.)

Ms. Sweeney made the above statement only weeks after she personally executed the questionable Assignment Agreement and the SBA required Allied/BLX to reimburse it for $5.3 million in guarantee payments relating to loans that the SBA had investigated and disqualified.

In light of these facts, Ms. Sweeney's claim that "we don't know the nature of any sort of inquiry" was materially false and misleading. Moreover, Allied management chose not to disclose either the SBA investigation, the disqualification of the loans, or the Assignment Agreement until more than a year afterward. This raises serious issues about the honesty of management with its shareholders and perhaps with the Board. As the Board of

Directors could not have sanctioned such public misrepresentations, the question you need to ask is, are they lying to you as well?

Finally, you may already have read a MarketWatch article published on February 1 of this year, which noted that an unknown individual had illegally accessed phone records of several prominent Allied critics. The article further noted that the FBI was conducting an investigation of this incident. Although I have refrained from commenting publicly on this matter, my home phone records were among the records that were illegally accessed. Specifically, according to my long distance provider, someone opened an online account in my wife's name, and directed the phone company to send copies of our bills to an AOL account. Like me, at least four additional individuals have been the victims of this identity theft and access device fraud. The only link that connects the victims is that they have all been critics of Allied.

I am quite familiar with Allied's aggressive tactics against its critics, including attacking them with untrue disparaging statements by management and its agents like Lanny Davis. It would not be surprising to me if the FBI discovered that Allied management was somehow involved in these identity thefts.

In short, there is considerable evidence that Allied's management has conducted business in a dishonest and inappropriate manner. Indeed, I have refrained from including in this letter the bulk of my research, numerous false and misleading statements issued by management and my financial criticism of the company.

I believe you have an obligation to examine the possibly unethical or even criminal behavior of Allied's management and take action to prevent further misconduct. I believe that the Board has a responsibility to ensure that individuals who act in this manner do not serve in a management capacity in a publicly traded company.

Respectfully,

David Einhorn

1919 Pennsylvania Avenue, NW
Washington, DC 20006-3434
202-331-1112
202-659-2053 Fax

March 18, 2005

Mr. David Einhorn
President
Greenlight Capital, LLC
140 East 45th Street
24th floor
New York, NY 10017

Dear Mr. Einhorn:

I write in response to your letter of March 11, 2005, on behalf of the Board of Directors of Allied Capital Corporation.

We are familiar with the allegations you have made in the past with respect to Allied Capital and its management, and have on a number of occasions requested and received information from management and from outside counsel with respect to the facts. That information has not supported your accusations of misconduct. This is combined with what we understand to be your financial stake in depressing Allied Capital's stock price and your efforts to persuade other parties not to do business with Allied Capital.

Pursuant to its charter, the Audit Committee is authorized by the Board to receive and evaluate any evidence of wrongdoing by Allied Capital, its officers or employees. If you provide us with specific information upon which you base your allegations, we can determine whether further action is warranted. Please address any correspondence, marked "confidential", to the Audit Committee Chairman, c/o Corporate Secretary, Allied Capital Corporation, 1919 Pennsylvania Avenue, NW, Washington, DC 20006.

Respectfully,

Brooks H. Browne
Chairman of the Audit Committee

September 15, 2006

Brooks H. Browne
Chairman of the Audit Committee
Allied Capital
1919 Pennsylvania Avenue, NW
Washington, DC 20006-3434:

Dear Mr. Browne:

On March 11, 2005, I wrote to you concerning the continuing misconduct of Allied Capital's management. I provided detailed specifics concerning several aspects of the fraud being perpetrated by management against both the public and the government, including: (1) management's scheme to maintain an artificially high valuation of its small-business lending unit, Business Loan Express ("BLX") by defrauding the Small Business Administration; (2) management's misrepresentations to public concerning the performance of Allied and BLX; and (3) illegal attempts to access my confidential, personal information (a technique called "pretexting") by individuals who likely acted at the direction of, or had some connection to, Allied management. As you are well aware, all of these aspects of management conduct are currently under investigation by the Department of Justice and the SEC.

Your response to my March 11 letter contained no specific information and simply said that the information received from management and outside counsel did not support any of the accusations of misconduct. You did not specifically address the "pretexting" issue.

However, recent public events have made clear the degree to which the Board has underestimated the seriousness – and criminal nature – of the conduct described in my earlier letter, including the "pretexting" issue. I therefore write again in the hopes that the Board will now take these issues more seriously.

Regarding pretexting: as the news media has recently reported, Hewlett-Packard's former chairwoman, Patricia Dunn, in an apparent effort to discover the source of boardroom leaks to the media, employed investigators who in turn illegally accessed the phone records of both members of HP's board and reporters for various news organizations who had published articles critical of HP. The methods employed by the investigators hired by Ms. Dunn were essentially identical to the methods used to access my own telephone records. As several news organizations have reported, the contractor falsely used individuals' names, telephone numbers and social security numbers to illegally access their phone records online. This is precisely the manner in which my own records – and the records of several notable Allied critics – were accessed.

As the investigations into HP's conduct plainly demonstrate, illegally accessing an individual's confidential records constitutes criminal conduct. The repercussions to HP

2 Grand Central Tower, 140 East 45th Street, 24th Floor, New York, NY 10017
Phone: 212-973-1900 • Fax: 212-973-9219 • www.greenlightcapital.com

for use of this technique have gone far beyond mere embarrassment to the company. Ms. Dunn has already resigned. Congress, federal and state prosecutorial and investigatory agencies have all initiated investigations into HP's use of pretexting. The Attorney General of California, Bill Lockyer, has indicated that he has sufficient information to indict several individuals, both within and outside HP.

The only group of individuals with any motive to access my phone records and the records of four other prominent Allied critics is Allied management. In light of the public outcry and potential criminal indictments resulting from HP's conduct, the Board cannot pretend that such use of pretexting is not a serious matter. Indeed, the pretexting in this case does not merely concern leaks, but is far more serious. If Allied management was involved in illegally accessing the phone records of its critics, such pretexting constitutes an attempt by a company to interfere with and chill its critics and therefore skew the flow of information which is critical to the securities markets. The Board clearly has an obligation to investigate such potential criminal conduct by Allied's management.

In short, the Board owes a fiduciary duty to Allied and its shareholders to conduct a thorough investigation to determine whether in fact Allied management was involved in any way in the pretexting scheme. If criminal conduct was committed, appropriate steps must be taken including but not limited to reporting that conduct. I will be happy to provide the Board with any additional information that will be of assistance in such an investigation, subject to any restrictions placed on such information by governmental agencies currently investigating the same matter. If you deny that Allied management or its agents were involved in any way in pretexting or accessing my telephone records then please confirm that fact for me; otherwise, I will assume that the clear inference that Allied management engaged in this illegal conduct is in fact true.

Yours,

David Einhorn

1919 Pennsylvania Avenue, NW
3rd Floor
Washington, DC 20006
voice 202-721-6100
fax 202-721-6101
www.alliedcapital.com

September 29, 2006

Mr. David Einhorn
President
Greenlight Capital, LLC
140 East 45th Street
24th Floor
New York, NY 10017

Dear Mr. Einhorn:

On behalf of the Board of Directors of Allied Capital Corporation, I write in response to your letter dated September 15, 2006, which was addressed to Brooks Browne, former Chairman of Allied's Audit Committee.

We have looked into your allegations that Allied's management played a role in an attempt to access your phone records and have found no evidence to support your claim. As noted in Mr. Browne's March 16, 2005, letter to you, the Allied Board remains skeptical of the motive behind your allegations, given your history of making broad accusations of misconduct against Allied management while simultaneously having an apparent financial motive to depress Allied's stock price. The Board is therefore not disposed to credit your claims without corroborating evidence. Notwithstanding our March 16, 2005 invitation for you to provide us with any supporting evidence of your own, you have supplied none.

As Mr. Browne explained in his March 16, 2005 letter, Allied's Board has authorized the Audit Committee to receive and evaluate any evidence of wrongdoing by Allied management that you are prepared to provide. In the event that we receive any such material, we will consider what, if any, further action is warranted. Please address any correspondence, marked "confidential", to the Audit Committee Chairman, c/o Corporate Secretary, Allied Capital Corporation, 1919 Pennsylvania Avenue, NW, Washington, DC 20006.

Respectfully,

Ann Torre Bates
Chairman of the Audit Committee

Ms. DEGETTE. Thank you very much, Mr. Einhorn.

The Chair recognizes herself for 5 minutes.

I am wondering, Ms. Parnes, if you can tell us what the position of the Department of Justice is on this legislation, because I know your agency works closely with the DOJ.

Ms. PARNES. We do work very closely with the Department of Justice, but unfortunately, I don't have their position on this legislation, on this bill.

Ms. DEGETTE. And are you aware of any objection by any law enforcement agency to this legislation?

Ms. PARNES. I am not, but honestly, we have not, at the FTC, done a kind of review of other Federal agencies and whether they have any concerns on this. We have worked with the committee's staff on technical issues, and as you know, we generally support this.

Ms. DEGETTE. Yes. And there is an exemption in the bill for law enforcement, I believe.

Ms. PARNES. Yes, there is.

Ms. DEGETTE. Ms. Parnes, I am wondering. Can you give me an update? And I am going to ask you, Mr. Rotenberg, also this question. What is the status of pretexting in America today? Have we seen the problem worsening since last year or improving?

Ms. PARNES. It is hard to know exactly what is going on in the industry generally. I can tell you what some of our experiences have been in investigations.

The targets that we have sued, we identified them, as I indicated, by going online and then by making some undercover purchases of phone records. And I should note, we bought the records of FTC employees.

Ms. DEGETTE. With their consent?

Ms. PARNES. Yes, absolutely with their consent. But we have done that. We have attempted some undercover buys more recently, and we have been told, "Oh, we don't do that anymore." Or, "We simply can't get that for you." So we have some sense that certainly the criminal law that was passed may be having a real impact here.

Ms. DEGETTE. Right.

Mr. Rotenberg.

Mr. ROTENBERG. Our understanding, Madame Chairman, is that the type of very brazen pretexting where the services were provided over the Internet in a 24-hour turnaround, for example, was guaranteed, there is much less of that today than there was in the past, in part because of the FTC investigation. The private investigators continue to use pretexting, as do others, as a way to obtain personal information about others.

Ms. DEGETTE. And have you seen any change in the type of information these private investigators are seeking?

Mr. ROTENBERG. That would be a difficult question to answer, but I will say, because people sometimes don't understand exactly what the significance of the call detail information is, those monthly billing statements that consumers receive from the wireless phone companies in particular, that listing is the type of information that is still very easy to get from the telephone companies by going, for example, to an online Web site that is set up to provide

that type of information. So we are still seeing the availability of the monthly call detail information being made available.

Ms. DEGETTE. Mr. Einhorn, you would have never known anything about the pretexting of your family and business records unless a market watch journalist told you what Allied Capital was doing, is that correct?

Mr. EINHORN. That is correct. I would not have had any way to know.

Ms. DEGETTE. And this is, by the way, what we also found last year in our investigation that people found out inadvertently that they had been pretexted. Do you know how many other people had their phone records pretexted by an agent of Allied Capital besides you and the journalist?

Mr. EINHORN. I believe, at least that we have been able to identify, at least six individuals.

Ms. DEGETTE. And can you identify, for the record, who the phone carrier who surrendered your records to the imposter pretending to be your wife?

Mr. EINHORN. It was AT&T.

Ms. DEGETTE. Have you talked to AT&T?

Mr. EINHORN. My wife talked to AT&T.

Ms. DEGETTE. And what was their response?

Mr. EINHORN. They were able to identify when the pretexting had occurred, how it was done, that her Social Security number had been provided, what date that happened at, where the records were sent in terms of an Internet e-mail account where they were e-mailed to, and when the account was most recently accessed. Beyond that, they had no other information for us.

Ms. DEGETTE. Do you agree with the bill's provisions that enhance the FTC's enforcement tools against pretexting, soliciting pretexting, or selling stolen phone records?

Mr. EINHORN. Absolutely. I think that there is really no place for this, and I would support all of the efforts that are being contemplated to cut down and eliminate this practice.

Ms. DEGETTE. Thank you very much.

The Chair now recognizes the distinguished ranking member, Mr. Barton, for 5 minutes.

Mr. BARTON. Thank you, Madame Chairman.

Mr. Rotenberg, is there any reason an individual would tend to want his or her phone records shared without them knowing about it?

Mr. ROTENBERG. Well, generally speaking, I don't think so, sir. A person who wants to disclose personal information to someone else would typically do that affirmatively. To get a bank loan, for example, you provide a lot of information to the bank so that they can make a determination, but that is a process you would initiate.

Mr. BARTON. But just as a matter of course, most normal human beings would rather they know if somebody wants that information so that they can make a decision whether to give it to them or not, would you agree?

Mr. ROTENBERG. Yes, I think that is correct.

Mr. BARTON. Now, I think we have general support for this bill, but Mr. Largent and Mr. McCormick, their trade groups seem to not like section 202, which changes current law from saying the

phone company can share that information without letting the individual know, unless the individual tells them ahead of time not to share it. That is the current law. section 202 changes it that Mr. Largent's company's trade groups and Mr. McCormick's would have to go to the individual and say, "May we share your information?" That seems to be the most controversial element in this new bill. It would seem, if we are trying to protect privacy, that changing this from opt-out to opt-in makes a lot of sense. Do you agree with this section 202?

Mr. ROTENBERG. Yes, I do, Mr. Barton, and if I may also say, while we are critical of the FCC's delay on our petition, we were nonetheless heartened, you may recall that Chairman Martin, when he spoke to this issue at the hearing last year, said that he thought the opt-in was important for consumer privacy. And I think there would be, certainly among consumers, recognition right away that the right way to do this is opt-in, based on permission.

Mr. BARTON. Now I want to give Mr. Largent and Mr. McCormick, who are both good friends of mine, an opportunity to expand if I understood incorrectly in their prepared testimony why they have a problem with section 202.

Mr. MCCORMICK. Thank you, Mr. Barton. I think that our concerns are fairly narrow and focused.

Let me give you an example.

We, today, look at purchasing patterns. For example, if a customer is taking telephone service and Internet access, as we move into new broadband applications, like video, we would like to be able to go to that customer and offer to that customer a promotional offering where we would add in video as part of a bundled package. In that regard, we would be competing against the cable industry, who is going to its video customers and saying, "We will add on voice service. Since you are already a cable customer, we will offer you a promotional offering to add on voice service." In that regard, no call-detail information is shared with anyone. There is nothing other than the knowledge of what kind of package that customer currently has and whether or not that customer would benefit from a broader package. And we believe that it would lead to a competitive imbalance if we were unable to approach our customers in that way.

Mr. BARTON. I don't understand. I have got a little bit of a cold, so maybe I am just not clued in, but there is nothing in the bill, if it becomes law, that prevents anybody from soliciting for new services to people that they have the addresses of, whether it is a hard-line address, a regular mail address, or a phone number, or an e-mail. All this says is if you want to share that individual's information, you have got to get their permission before you share it. I don't see how this bill would prevent what you just said you wanted to do.

Mr. MCCORMICK. Mr. Barton, if that is the intent, I think that it would be easy to come up with clarifying language that would clarify that we are permitted to engage in that kind of broader market.

Mr. BARTON. OK. Steve?

Mr. LARGENT. Yes, Mr. Barton. I just would say that there is some ambiguity about what the language actually does and what

it does not do. And the fact is that many of our companies utilize third parties to offer services just because it is less expensive. We can offer that type of discount to our customers. So if the legislation would get in the way of our use of third parties to offer services from our company, not anybody else's company but from our company's perspective, then that would be a problem, but if you are saying it is not going to get in the way of that, then perhaps we could work with you on the bill's language.

Mr. BARTON. My staff says there is some ambiguity, so maybe we can work on this.

My time is expired. Thank you.

Ms. DEGETTE. The Chair now recognizes the distinguished chairman of the Telecommunications Subcommittee, Mr. Markey, for 5 minutes.

Mr. MARKEY. OK. first let me say that the five FCC Commissioners will be appearing before the Telecommunications and Internet Subcommittee on Wednesday of next week, so we certainly hope that the CPNI order will be completed by then and that it will have been done well by them, because that will be a central part of that hearing on Wednesday.

Mr. Einhorn, is it important that victims be notified immediately that their carrier has learned that the privacy of the phone calls of an individual have been compromised?

Mr. EINHORN. I would support the notion of the immediate notification of anybody whose information was compromised in that fashion, yes.

Mr. MARKEY.Mr. Navin, do you think that is a good idea that immediate notice be given to people like Mr. Einhorn that their information has been compromised and that that becomes the rule for the telephone carriers?

Mr. NAVIN. I do agree that it is important that consumers get prompt notification.

Mr. MARKEY. I am saying immediate.

Mr. NAVIN. As I understand it, States that have addressed this issue typically have an exception for notification of law enforcement, and it calls for prompt notification, but there is some provision, specifically for law enforcement.

Mr. MARKEY. But what should be the deadline for calling law enforcement?

Mr. NAVIN. What should be the precise deadline?

Mr. MARKEY. See, what I want you to say is we call law enforcement and the customer immediately and let them know that they have been compromised and that law enforcement might be calling. But why should there be a delay?

Mr. NAVIN. In the record in front of the Commission right now, the Deputy Attorney General sent a letter to the Commissioners, indicating the Department of Justice's preference for law enforcement to be notified first, before the——

Mr. MARKEY. I have no problem with that, but what I am saying is Mr. Einhorn should get the next call, don't you think?

Mr. NAVIN. After law enforcement, yes, I think consumers should be notified.

Mr. MARKEY. Yes. How long do you think a gap should be? Seven days, 1 day, or 1 hour?

Mr. NAVIN. I believe the Department of Justice has advocated for allowing them 7 days.

Mr. MARKEY. I don't think the Department of Justice should be listened to on that issue, and I think Mr. Einhorn should be listened to and the millions of Americans whose information is compromised. I think that the FCC should listen to the consumer, listen to this committee. The CPNI laws are ours. We created them. We want the customer protected. Justice should not be given 7 days to wait to notify people who have an ongoing crime being committed against them. They should be notified immediately, as anyone whose house was burgled that it occurred. And if you don't want to do that, then I think we are going to have a real problem next Wednesday.

Mr. Largent, Mr. McCormick, a general question. Do you agree that customers have an ownership interest in their own personal information? Mr. McCormick?

Mr. MCCORMICK. I would say they have a strong privacy interest.

Mr. MARKEY. Do they have an ownership interest?

Mr. MCCORMICK. Yes.

Mr. MCCORMICK. I would agree that customers have a strong privacy——

Mr. MARKEY. No, do they have an ownership interest in their own personal information? It is called the customer proprietary network information law. Do they own that information?

Mr. MCCORMICK. We have always regarded that information as the customers' information, that is correct.

Mr. MARKEY. OK. Mr. Largent, do you agree that it is the ownership interest of the consumer, his or her own information?

Mr. LARGENT. I think Mr. Markey asked me that question last year at this hearing, and I said the same thing: yes, it is.

Mr. MARKEY. OK. Thank you. I appreciate it.

Mr. McCormick, what percentage of your member companies outsource customer support or billing or marketing functions to foreign countries?

Mr. MCCORMICK. I do not know, Mr. Markey, but I would be happy to provide that information for the record.

Mr. MARKEY. I would appreciate that.

Mr. Largent, do you know what percentage of your companies outsource this information to other countries?

Mr. LARGENT. No, I am not aware of what the exactly number would be, but we would be glad to get back to you on that.

Mr. MARKEY. Obviously, that is a good question. We will shut down a lot of regional FCC offices, but we don't have any FCC offices in India or Pakistan, so what happens with the information of the people in this room and watching this hearing is a good question when it is put overseas, so we would like to know what happens to that.

Mr. Navin, does the FCC intend to impose a minimum system security requirement on the transfer of customer information?

Mr. NAVIN. The proposed rule that the chairman has put before the Commission are prescriptive relating to access to the CPNI records, which deals directly with the pretexting issue. For example, they require a mandatory password to get access to call detail records. Relating to the security or safeguards, the proposed rules

ban the sharing of the CPNI with a joint venture partner or independent contractor without the express consent of the consumer.

On the issue of transferring the security among affiliated companies, the record is sparse on that issue. And right now, I am not sure if the Commission will determine to address that issue in this order or not.

Mr. MARKEY. OK. I would like to get back to you, and thank you, Madame Chairman.

Ms. DEGETTE. Thank you, Mr. Markey.

The Chair now recognizes the distinguished gentle lady from Wyoming, Mrs. Cubin, for 5 minutes.

Mrs. CUBIN. Thank you, Madame Chairman.

I would like to ask Mr. Navin and Ms. Parnes, under the scope of your Commissions' investigations into this issue, I wonder if you could tell the committee if any specifically-rural companies have been investigated, or does this seem to be a problem that is most prevalent in large companies with large lists of personal data?

Ms. PARNES. I am told that one of the cases that we brought actually is located in Wyoming.

Ms. CUBIN. Could you comment, just for a moment, on the state of rural carriers' privacy protection measures, if you are able to right now? I know you have a full plate.

Ms. PARNES. I would actually have to defer to my colleague at the FCC about security practices by carriers.

Ms. CUBIN. Mr. Navin, can you offer the committee an update, if it is available, on how much you believe sections 202 and 203 of the bill will cost small and rural carriers?

Mr. NAVIN. Unfortunately, we do not have an estimate on what it will cost carriers.

In answer to your first question, I know that the agency has issued 20 letters of inquiry to various carriers. I imagine some of those carriers are smaller carriers, given the number of large carriers, both on the wireless and wireline side. I don't know specifically what size of rural carrier the Commission has made those inquiries of. I know that the Commission is always sensitive as it relates to implementation of its rules in rural areas and tends to give special consideration. In the rulemaking that is pending before the Commission, the rural carriers have pointed out that they have more limited resources, and my sense is that the Commissioners will be sensitive to that.

Ms. CUBIN. That is my main concern, that possibly they be included before any final rules are initiated, because it is a whole different country out there.

So I have no more questions, Madame Chairman.

Ms. DEGETTE. The gentle lady yields back.

The Chair now recognizes the distinguished gentleman from Illinois, Mr. Rush, for 5 minutes.

Mr. RUSH. Thank you, Madame Chairman.

Ms. Parnes, I have three questions, and I am going to ask all three so that you can answer these questions, as you will.

First of all, it is good to see you again.

And the first question is, do I understand correctly that the FTC supports the thrust of this legislation, that you support this legislation?

The second question, in September, the FTC testified before the O&I Subcommittee that you needed more specific prohibitions against pretexting for consumer phone records and soliciting or selling consumer phone records obtained through actual or reasonably-known pretexting activities. Does this legislation adequately address that request? And if it doesn't, then what specific changes do you recommend.

And lastly, my question is you also recommended in that testimony that Congress give the FTC authority to seek civil penalties against violators, a remedy that the FTC does not currently have in cases involving matters such as pretexting. And for the record, I just want to know why the civil fine authority over at FTC does not apply in this situation and then whether or not our proposed legislation adequately addresses this need that you have voiced.

Those are the three questions. Would you respond to them, please?

Ms. PARNES. Absolutely. And thank you.

The FTC does support this legislation. And in terms of the specific prohibitions and the earlier testimony of the Commission, the legislation does address those issues.

What the Commission's concern has been is that, as I indicated, we have used our section 5 authority to go after both actual pretexters and those who solicit pretexting, the middlemen, so to speak. But we will want to make sure that any legislation that was adopted addressed both parts of this transaction, both the pretexters who call up the phone companies, engaging misrepresentations and get phone records and the middlemen, the data brokers who make claims and promise that they can get this information. The data brokers and the pretexters may sometimes be the same entity, but sometimes they may be separate entities, and we were just concerned, but this bill does address both sides of that. And we think that is a very good thing.

In connection with the Commission's civil penalty authority, the Commission has civil penalty authority in two circumstances. One is if conduct violates an order that the Commission has already obtained against a company. And the second is if conduct violates a role that the Commission has issued. We are able to get civil penalties only when we have engaged in rulemaking authority. And while we do have general rulemaking authority under the Federal Trade Commission Act, as you know, the FTC Act is very broad. It gives us authority over unfair or deceptive acts or practices in or affecting commerce. And in exchange for the ability to get civil penalties once we had adopted a rule, Congress set very specific procedures that the Commission has to go through in rulemaking. And they are very comprehensive. It takes a fairly long time for us to engage in. And so actually, what has happened since the 1990's is that Congress, when they have wanted the FTC to obtain civil penalties and to engage in rulemaking, they have used a model very similar to the model used here. They have either said that the law shall be enforced by the FTC as if it is a rule or they have given the Commission very specific authority to engage in rulemaking a particular area. Congress did that with the Telemarketing Act, with the Can Spam Act, and it has actually been a very successful approach.

Ms. DEGETTE. The gentleman's time has expired.

Mr. RUSH. Thank you, Madame Chairman.

Ms. DEGETTE. Thank you.

The Chair now recognizes the gentleman from Mississippi, Mr. Pickering, for 6 minutes.

Mr. PICKERING. Thank you, Madame Chairman.

Earlier, Mr. Largent and Mr. McCormick, you all mentioned the issue of whether you would be able to joint market a bundle of services. Is there language that you would have that could clarify that issue so that those types of services, which I think the Committee would want to see continued with the other protections as it relates to information, regardless of legitimate use of information, and is that something that you could supply the committee with?

Mr. LARGENT. Yes, it is. We can get you that kind of information, and that is our concern with the legislation.

Mr. PICKERING. You often raise in your testimony, Mr. Largent, that as we go across the country, there is a patchwork of different initiatives on different things. Recently, the Commission has indicated a possible proposal that would move all wireless services into title I, which would give a Federal framework. And if that happens, would you support consumer protections like this as part of a Federal framework?

Mr. LARGENT. Well, what we are talking about specifically that Chairman Martin has mentioned this year is just moving the broadband portion of the wireless industry into title I from title II that would put us on the same ground with DSL and cable offerings and broadband over power line. They are already in title I. Our services that are being rolled out over wireless are not in title I, so we are kind of competing on unleveled ground, and we are just trying to get to that level ground.

Does that answer your question?

Mr. PICKERING. And broadband services under title I, if that were to occur, you would support a national consumer protection standard on these types of issues?

Mr. LARGENT. Absolutely. Yes.

Mr. PICKERING. I thank you, Mr. Largent.

Mr. LARGENT. Mr. Navin, let me follow-up on a question that Mr. Markey asked.

If there are third parties that are being used to joint market and they are based overseas, whether it is Pakistan or India, are the U.S. laws still applicable and enforceable in those situations?

Mr. NAVIN. That is an issue that the Commission is considering as part of a reconsideration of the order that it had put out in 2002. I believe that the Department of Justice in its reply comments raised that exact issue. The Commission hasn't yet resolved it. I think it gets into issues of treaty law and international law and not to be the primary subject certainly of my bureau, but I know that the Commission is studying that issue. And I can also tell you that it is not an issue that we address in the order that Chairman Martin has proposed for the Commission.

Mr. PICKERING. Ms. Parnes, do you have any comment on that issue of whether you would be able to enforce the law that we pass here if a third party is based in a country like India or Pakistan?

Ms. PARNES. The Commission does not have any jurisdiction over common carriers, but if we are talking about other entities, I think that if a business was located in the United States and they moved data outside of the country, we would take the position that the entity in the United States is responsible for their own data. In terms of looking at data brokers, as I mentioned, smaller businesses that may be located here or entities that may be outside of the United States, we would use the new authority that Congress gave us in the 109th session, the U.S. Safe Web Act, to go after those individuals.

Mr. PICKERING. All right. Thank you very much.

Madame Chairman, I yield back the rest of my time.

Ms. DEGETTE. The gentleman yields back.

The Chair now recognizes the distinguished gentleman from Texas, Mr. Green, for 5 minutes.

Mr. GREEN. Thank you, Madame Chairman.

Mr. Largent and Mr. McCormick, are any of your companies now selling the information to third parties that you have on your customers?

Mr. LARGENT. No.

Mr. GREEN. OK.

Mr. MCCORMICK. No.

Mr. GREEN. OK. That is one of the concerns. I think years ago when we had jurisdiction, and I mentioned it to you before the committee hearing over what became Oxley-Bliley. In fact, Steve, you might have been on the committee when we had that battle over the privacy issue. And I was told, at that time, by some of our financial institutions that it was such a profit center for them to market that information that they would have killed the bill, which is something they had been working on for 10 years before that. And so that takes care of part of the concern. And I guess I have the same concern that both the chairman on our Telecom Committee and Mr. Pickering mentioned is enforcement of these privacy restrictions outside the United States. And I am glad the FTC said that you would hold responsible the person or the entity here, although you don't have jurisdiction over common carriers. But again, I guess we can provide that jurisdiction that would go with that contracting to somewhere else, because I know now it is a laugh line on late night television that whether it is your computer you bought or your Internet service provider, you very well may be talking to someone in Pakistan or India or no telling where, and they probably have as much private information on your use as the telephone companies or wireless companies would have.

I know numerous industries share information for marketing purposes, and that is part of our concern is Mr. Markey said that the consumers think it is their information, and they ought to be able to give permission to share it. This legislation, I know, puts restrictions on telephone companies as compared to cable because of where we are at today in our technology. And I know you have been asked for information on how we can address that issue, because obviously our committee wants that competition between cable and hard-line, both for video and over the air and computer, high-speed, and also telephone service. Is there a standard that could be set across the multiple industries? What information could

be shared? Is there a standard anyone? And again, not just for the two representatives in wireless and the hard-line, but anybody on the panel, is there a standard that could be dealt with where I, as the consumer, could say, "Yes, I am your customer. You can contact me, but I don't want you to share it with anyone else."

Mr. MCCORMICK. Well, Congressman, I think that that kind of a standard would be a very, very broad standard. I mean, in effect, it would be a do-not-call standard, because virtually every business in the United States contacts its customers to talk to its customers about ability to take advantage of new offerings or discounts that it might have available. And so the real focus of the bill that we heard in the opening statements is really to protect that information that is call-detailed information.

Mr. GREEN. OK. I am not talking about AT&T contacting me, but for AT&T providing my information to someone else or having access to it. so I don't have any trouble with, if I have a contract with a cell phone company, we get contacts all of the time for other every 6 months to come in and renew your contract. I don't mind that, because I am a customer, but for my information to be shared, and I think that is the concern of the committee and ultimately why we have this legislation.

Mr. LARGENT. I would just say, Mr. Green, that I think where you are going is right, that we don't have any problem saying, you know, that you can't sell customer information to the automobile industry or an automobile dealer, because that is not the way we are using the information anyway. We are using it to market more services from our carriers, and that is it. And that is what we worry that the legislation may go a step too far in impeding our ability to market our services to our customers. And that is what we want to try to protect is the ability to market our services to our customers only. We are not talking about we want the ability to market balloons or baseballs or cars.

Mr. GREEN. OK.

Mr. Einhorn, I know your situation is not that, but as the consumer sitting at the table along with, what is your feeling? And well, I have run out of time, but Madame Chairman, if he could just be allowed to answer.

Ms. DEGETTE. Yes, without objection, the gentleman will be allowed to answer.

Mr. EINHORN. I am not actually clear what the question I am being asked is.

Mr. GREEN. The question was your situation was different. I know you are here on, really, part one of the bill, and I don't think there is any question at all about support for that, but to also try to expand it to where consumers shouldn't have their information shared with someone else, do you think there is a standard that you, as a consumer, would feel comfortable with that they could share your information across industries, which——

Mr. EINHORN. I think my general view is that, who I am calling for how long at what time and what those people's phone numbers are, is information that really doesn't belong to anybody and really shouldn't be used for any purpose, in my mind, other than sending me a bill to tell me how much to pay the phone company.

Mr. GREEN. Well, I think we agree on that that who I call and whatever ought to be my own information, and I need to share that.

Ms. DEGETTE. Thank you, Mr. Einhorn.

The Chair now recognizes the distinguished gentleman from California, Mr. Radanovich, for 5 minutes.

Mr. RADANOVICH. Thank you, Madame Chairman.

I do have one question regarding the opt-in/opt-out impact of this kind of legislation, and if something like that were required in this bill, would it set this industry apart from other industries. In, for example, health medical records, it is an opt-out thing. Does anybody have any comment on that?

Mr. LARGENT. Well, Congressman Radanovich, I would just say that previous attempts to require opt-in consent have been held to be unconstitutional. And but to be fair, those instances did not involve cases where Congress had spoken on this issue, so we are talking about two different cases where Congress's, obviously, intent to speak on this issue, it may not be unconstitutional or found unconstitutional, but it could be, and I think that is an open question.

Mr. RADANOVICH. Well, and if it did become part of the language of the bill and come into law, it would be different than other industries, it does sound like, though, right?

Mr. LARGENT. Yes.

Mr. ROTENBERG. Congressman, could I respond?

Mr. RADANOVICH. Sure.

Mr. ROTENBERG. Two points. Just to clarify what Mr. Largent said, the U.S. West case from 1999 concerning an earlier opt-in rule was narrowly struck down, as Mr. Largent described, because it was based on the regulation and not statute, and so of course, if you have a statute, I think that problem goes away. And in subsequent cases, I should point out, other Federal appellate courts have upheld similar rules.

Now as to your original question, is there a reason for having opt-in here where there might not be opt-in in other privacy statutes, I think the answer to that question is the sensitivity of this information, that this is the real-time data associated with who you are calling, when, and for how long, and that is information that is specifically protected in section 222 of the Communications Act. That actually has a long, long history of privacy protection, and I think that is the reason you would want opt-in.

Mr. RADANOVICH. All right. Thank you.

If no other response, then I yield back.

Ms. DEGETTE. The gentleman yields back.

The Chair recognizes the distinguished gentleman from Texas, Mr. Gonzalez, for 8 minutes.

Mr. GONZALEZ. Thank you very much, Madame Chairman.

And quickly, just a kind of general observation so you know basically where I am coming from, and then I will get into specific questions.

But the way I view what we do here, and I know that we are visiting the same territory, is what Mr. Markey established from the beginning. No witness here and no witness in previous hearings, and those were representatives and CEOs from the tele-

communications industries themselves, that acknowledged that the property belongs to the customers. So let us start off with that basic premise. The information belongs to the citizen and to the customer.

As to disparate treatment of that information and the requirements, the Government may impose as to safeguards and security measures, that, I believe, is basically, established by what I think is the hierarchy of information depending on the type of information.

First and foremost, I think, it is always going to be medical records. And how we arrive at that is just, basically, human nature.

Second, I think you are going to run into telephone records.

And then third, financial records.

And the fact that we may treat the type of information, how we safeguard it and disseminate it differently is because there is that hierarchy. And I think we have to acknowledge that.

Now does it place any particular business that operates in those different areas at a disadvantage from those other businesses? The answer is going to be yes, because there are higher standards for healthcare providers and so on.

What I am getting at, and I am going to address Mr. Largent and Mr. McCormick's concern that it would place certain members of a specific industry at a disadvantage. That I think we can address within this hierarchy: telephone records, telecommunications, everything that is going out there in the telecom industry. And surely, we don't want to do something that does place you at a disadvantage regarding the marketing of your services and such and to expand and to be successful. So I am familiar with that.

Now the reason that the legislation we address to all of you is because you are the gatekeepers, and that is the most obvious starting point, and we are going to deal with the criminals and the scammers and everybody else. And we can do that criminally. But I think it still goes back to what Mr. Rotenberg pointed out is that if we really start with the safeguarding measures, we probably could avoid quite a bit, which leads me to the first question of the entire panel, not Mr. Einhorn, I am sorry, because you are actually the citizen victim, but I will reserve a question for you, and this involves you.

A yes or no answer, because I think you can answer this yes or no. To the extent that you understand this piece of legislation that we are attempting to pass, had it been in place at the time of the Einhorn family, what borders on a tragedy, actually, but their experience, would it have prevented that experience by the Einhorn family? Ms. Parnes, had it been in place, would it have made any difference?

Ms. PARNES. Well, to the extent that you are asking about the operation of title II, it is not an area for us.

Mr. GONZALEZ. If you can't answer, that is fine.

Mr. Navin?

Mr. NAVIN. Yes, I am afraid I have to tread carefully here, too. There is typically a protocol and procedure for the Commission to give technical assistance to the committee, which, of course, we are

always happy to do. I don't believe we were asked for it on this particular bill, but I would prefer to use that process.

Mr. GONZALEZ. OK. The Federal Government at work.

Mr. Rotenberg?

Mr. ROTENBERG. Well, Mr. Gonzalez, since we initiated the petition of security standards, while I can't say with certainty it would have prevented what happened to Mr. Einhorn, I think it is clear that if stronger security standards were in place, it would have been much more difficult for someone to improperly get access to Mr. Einhorn's family's calling records.

Mr. GONZALEZ. And this bill would have accomplished that?

Mr. ROTENBERG. Yes, I believe it would have.

Mr. GONZALEZ. Mr. Largent?

Mr. LARGENT. I would say that the security measures that the companies have enacted since this came to light, and it was about the same time that he had his problems, are going a long way to prevent it from happening again. I would tell you that the threat of prosecution of pretexters has essentially evaporated the Internet solicitation for people to get numbers through pretexting. So we have already come a long way, but whether it would have actually addressed his concern, I think that is an open question, and I am not sure.

Mr. GONZALEZ. Mr. McCormick?

Mr. MCCORMICK. Yes, Congressman. I would agree with Mr. Largent. I received a briefing the other day on the security protocols that had been implemented by the companies during the course of the last year, and the protocols would directly address the way in which an inbound call under pretexter-obtained information. Our concern, under this legislation, though, is that it also addresses outbound calls. There has never been a situation where one of our companies has called a pretexter to give them information. This marketing on the outbound, those provisions of the bill, would do nothing to address the situation that Mr. Einhorn had.

Mr. GONZALEZ. All right.

Ms. DEGETTE. The gentleman's time has expired.

Mr. GONZALEZ. I think my time is up, and I just thank you, Mr. Einhorn, for your participation.

Ms. DEGETTE. The Chair now recognizes the distinguished gentleman from Florida, Mr. Stearns, for 5 minutes.

Mr. STEARNS. I thank my colleague.

I think we have touched on this issue before, but there is some confusion. At least some of the staffs indicate there is confusion, so I would like to ask this question. Mr. Navin, you first. And then I will ask all of you, if you would, to comment on it. And I guess it is dealing with the bill's affect on the ability to use phone records to market other products. In your mind, does this bill prohibit the usage of just detailed information or all information from phone records?

Mr. NAVIN. Yes, I am the one that deferred on the last question involving an interpretation of your legislation.

Mr. STEARNS. Right. Yes.

Mr. NAVIN. What I can tell you is that the proposed rules that the Commission is considering would get at the situation that concerns disclosure of Mr. Einhorn's records in two ways. Number 1,

by virtue of the use of mandatory passwords, the person who set up the account would not have been able to do. And No. 2, because the proposed rules in front of the Commission provide for notification to the customer any time their information is changed or their call detail records are mailed. As it relates to the legislation, I would prefer to allow the other panelists to address that issue.

Mr. STEARNS. OK. Mr. Largent, go ahead.

Mr. LARGENT. Would you restate your question?

Mr. STEARNS. Yes. In your opinion, does the bill prohibit the use of detailed information or other information from phone records from the ability to market other products?

Mr. LARGENT. I think that is the open question that we are really concerned about this legislation, that it could possibly be read that way.

Mr. STEARNS. And that is what my staff is trying to understand. Do we need to change this bill so that you have this flexibility? And it is not clear. I guess, the confusion is whether we can do this, and do you feel it is strong enough that, in your mind, there is this confusion and you can't market information without breaking the law? And so we don't want to do that. We don't want to hurt the ability to market, so I think that is what we are trying to understand.

Mr. LARGENT. I think clarity is the key word that we would like to see in this bill.

Mr. STEARNS. And so you would like to see a change?

Mr. LARGENT. Yes.

Mr. STEARNS. OK.

Mr. McCormick?

Mr. MCCORMICK. Absolutely, Congressman. We see this ambiguity as creating a situation where we are potentially engaged in an illegal activity if we use our knowledge about the fact that an individual is a telephone customer and use that knowledge in order to go to that customer and offer them a bundled package of Internet access or video or even to add on a wireless service. We don't think that that was the intent of the committee. We understand that the intent of the committee was to protect the kind of information that was taken from Mr. Einhorn, but we believe that the bill goes much farther than that and does prevent these kinds of marketing activities.

Mr. STEARNS. Well, and we are in the early stages here, and so we are all listening, so this is the time to say, specifically, yes or no. Now the two of you are saying that this bill does make it a little bit dubious whether you can continue your marketing practices.

Anyone else?

Mr. ROTENBERG. Mr. Stearns, if I could speak to that issue.

Mr. STEARNS. Yes.

Mr. ROTENBERG. I think there really are two distinct questions here that need to be clarified. The first is whether or not a telephone company can communicate with their customers about their service offerings. There is nothing in this bill that prevents that, and every phone company is free to make available information about related services. The second question is whether the companies can take advantage of the call detail information, who people are calling, what they are doing, how they are communicating, and use that private information to determine what type of marketing

to direct to the customer. Now in my view, and I think the view of most American consumers, they would have no problem learning about new service opportunities from their current provider or from a competitor. That is obviously a good thing for the consumer and for the marketplace. I think the specific concern here, which the bill appropriately addresses, is that the companies take advantage of access to this detailed information and use that as part of the marketing determination, and that is where I think we need a stronger safeguard.

Mr. STEARNS. So would you, in your mind, then, based upon what you said, change the bill?

Mr. ROTENBERG. No, I would leave the bill as it is. I would leave it with the opt-in requirement, because if there is going to be use of CPNI information for that purpose, then I think the customer has the right to say, "Well, that is——

Mr. STEARNS. So the opt-in requirement would nullify the need to change the bill, because the customer is still in control?

Mr. ROTENBERG. Yes, that is correct.

Mr. STEARNS. Now I guess, Mr. Largent and Mr. McCormick, what do you say to that?

Mr. LARGENT. Well, I just think that it violates the basic marketing principle that exists in our world today. If we have got a company that, say, has 60 million customers and we want to target the 12 million that we think would be most inclined to want Internet service or download music or do whatever, and I mean, our companies do so many things today from music, video, television, as well as your basic phone service, but if we have got a group of 12 million customers out of 60 million that we think are kind of the heart of the market for accessing whatever service it might be, why would we have to market to 60 million customers when we know that 12 million are our real—that is the heart of our marketing strategy. Why should we have to market to 60 million when we know that these 12 million are the ones that are going to be most interested in the service?

Ms. DEGETTE. The gentleman's time has expired.

Mr. STEARNS. Yes, I just ask 30 seconds to let Mr. McCormick finish.

Ms. DEGETTE. Without objection.

Mr. MCCORMICK. Yes, thank you very much.

Congressman, several years ago, Congress provided for a do-not-call list. If you do not want to be solicited, it was an opt-out. The way we read this legislation is that for our industry alone, it would be a do not call unless the customer opts in. And so all we want to do is to make sure that our industry is not treated in an entirely unique and discriminatory way.

Mr. STEARNS. I thank you and the gentle lady.

Ms. DEGETTE. The Chair now recognizes the distinguished gentleman from Michigan, Mr. Stupak, for 5 minutes.

Mr. STUPAK. Thank you, Madame Chairman. I apologize for not being here. I have been on the floor with an amendment and argument down there.

So Mr. McCormick, the FCC rules require telecommunication carriers to have an officer of the company certify annually personal knowledge that the company has established operating procedures

that are adequate to ensure compliance with privacy regulations. And each of the companies certified that they have had adequate procedures, yet this appears to be a pervasive problem. Doesn't that indicate that something is slipping through the cracks of the current system? It would seem we cannot rely on either the certification requirement or the current FCC rules to adequately protect consumers.

Do you care to comment on that?

Mr. MCCORMICK. Yes, Congressman.

What we have in the pretexting community is that we have very sophisticated lawbreakers. Security protocols in the past, many of the companies were using Social Security numbers as identifiers. Since individuals like Mr. Einhorn had their records taken through pretexting, through the use of Social Security numbers, our companies have established protocols that no longer use that. In fact, the authentication procedures used by our companies are constantly being changed and upgraded in ways to protect against the increasing sophistication of pretexters. So it is a continuing battle. It is an ongoing battle, but we believe that it is important to our relationship with our customer to be able to protect our customers' privacy, and we take that very seriously.

Mr. STUPAK. But in response to Mr. Stearns, when I came in here, you were talking about opting in and opting out. And in our proposal, you have to opt in, which gives the consumer greater protection—or opt out, whatever it is there. But the consumer is going to hold the key here. Wouldn't that help to defeat this, what you call, sophisticated pretexters?

Mr. MCCORMICK. No, it would have nothing to do with that, because pretexting are calls that come in and the opt-in requirement today says that we cannot share the information with anybody beyond selling communication services unless the customer opts in. This opt-in requirement doesn't have to do with calls that are coming in, pretexting calls that are coming in asking us for information. This opt-in requirement has to do with forcing a customer to first say to us, "You may contact me about offering new services, and if I don't give you express authorization beforehand, do not call. Hands off."

Mr. STUPAK. That isn't related to a third party and not to your company? The opt in? Isn't that related to the third party that wants to use it?

Mr. MCCORMICK. The way we read this bill, no, the law already requires opt in with regard to sharing information with third parties. With regard to this bill, the way we read it is that our own companies would not be allowed to market services beyond the bucket that they have, the telecom service, without opt in.

Mr. STUPAK. In the investigation here, the way I remember, the summary of it, if I will, was the record reflected that it was in which where administration sloppiness by the carriers. And in our investigation, we saw this as sort of like the key part of the program. So I mean, if the carriers are going to be sloppy, no matter how sophisticated you are going to be, but if you are going to be sloppy in the way you administer it, you are still going to have this pretexting problem, correct?

Mr. MCCORMICK. Again, I think that we are in full agreement with the committee with regard to the need for inbound calls requesting customer proprietary network information, particularly call data information, be authenticated so that you do not have people who should not be getting that information are getting that information. What we don't want to do, though, is to go on the other side where we are making calls out to our customer to offer them services that may be offering them greater discounts or savings, for those to get swept up. There has never been an instance where there has been a problem with pretexting or identify theft on the part of marketing calls from our companies out.

Mr. STUPAK. Well, having sat through that pretexting investigation, I would say you are right. There is none that we know of, because we still get back to this administration sloppiness.

Mr. Navin, if I may, the FCC order, which prohibits the carriers, I am sorry, prohibits providers from releasing call detail information. And that order has been circulated to other commissioners, when do you anticipate the order being issued, when it will be completed, and what is sort of the hold-up here?

Mr. NAVIN. I can tell you that, first of all, it is not a complete ban on the release of the call details. It just put in place some security measures, like the use of mandatory passwords.

Mr. STUPAK. OK.

Mr. NAVIN. I don't want to totally frustrate consumers in their endeavor to get access to the information. The chairman circulated the order at the end of last year. I know that he has been working actively with his Commissioner colleagues to try to build consensus on the item. He tends to take a consensus approach, because he believes that these two stronger opinions by the FCC. That said, I am sure that there are many at the Commission who are anxious and interested in the Commissioners all being——

Mr. STUPAK. Can you give me a timeframe or a guess of when this order may be—a consensus on it? It has been a while.

Mr. NAVIN. I know that one of the tools that the chairman has to bring an item to a vote is by an agenda meeting.

Mr. STUPAK. Right.

Mr. NAVIN. So I know that is available to the chairman. I don't know if he has made that decision with regard to this item.

Ms. DEGETTE. The gentleman's time is expired.

Mr. STUPAK. Thank you, Madame Chairman.

Ms. DEGETTE. The Chair now recognizes the distinguished gentleman from Pennsylvania, Mr. Pitts, for 5 minutes.

Mr. PITTS. Thank you, Madame Chairman.

First, a question for Ms. Parnes.

Section 202(a)(1)(E) on page 10 of the bill is similar to the legislation that the gentleman, Mr. Markey, and I introduced last session, the Wireless 411 Privacy Act, which seeks to keep wireless services from disclosing wireless numbers without the affirmative consent of the consumer. And we have heard of the unintended consequences from Mr. Largent and Mr. McCormick that we may need to tweak this language to keep it from having these unintended consequences regarding marketing of services. But phone numbers can be used to help prevent fraud and identity theft, because they can be cross checked with information on credit and

loan applications. And we certainly don't want to make it harder to prevent fraud. Your bureau has a mandate to protect consumers, so I would appreciate your thoughts on that.

Ms. PARNES. Thank you. We do have a mandate to protect consumers from identity theft. And we actually are very focused on how consumers can authenticate themselves in ways to prevent the misuse of their own personal information.

But because this is in title II and it is a part of the bill that falls outside the scope of the FTC's jurisdiction, we would have to really go back and look at this and consult with our colleagues at the FCC to understand how this would operate. And we would be happy to get back to you on that.

Mr. PITTS. All right.

Steve, it is great to see you. You are a good friend and former colleague, and it is always good to work with you. And I understand that you are willing to work with us on clarification regarding marketing of services, but the phone number is not CPNI. That refers to data about the phone records and the behavior. Phone numbers can be cross checked on applications for credit, and other critical services. And do you see the unintended consequences regarding that that we need to tweak this language about?

Mr. LARGENT. We would be glad to work with you on that, Congressman. And I would just tell you that on the other issue, on the wireless directory assistance, that there is no evidence——

Mr. PITTS. I was just going to ask you, is there still any interest in creating a directory?

Mr. LARGENT. None that I am aware of.

Mr. PITTS. Good. I am happy to hear that. And thank you for agreeing to work with us and providing language to work out any unintended consequences.

Thank you, Madame Chairman.

Ms. DEGETTE. The gentleman yields back.

The Chair now recognizes the distinguished gentleman from Washington State, Mr. Inslee, for 5 minutes.

Mr. INSLEE. Thank you. I would like to ask about this third party sharing of information for marketing and other purposes to make sure I understand it.

Just give a hypothetical. XYZ Phone Company wants to enter into a joint venture with Acme Travel Company, and they want to share databases so that the travel company can focus their marketing efforts to see who is traveling and who is calling Paris, and maybe they want to market these people. I want to ask, Mr. Navin, Mr. Largent, and Mr. McCormick, under want circumstances should the phone company be able to share that information with Acme Travel Company? What would happen to happen first or second in that regard? And in particular, Mr. Navin, if you could tell me about the relationship between your proposed rule and this legislation and how they contrast or compare or are similar? If I could ask you three gentlemen that question.

Mr. NAVIN. Well, currently, as has been discussed, the rule that the Commission has as it relates to joint venture partners is an opt-out rule. In other words, the carriers do not need the express consent by consumers to use this CPNI to market communications-related services. So that is the current state of the Commission's

law. What the chairman has proposed to do is to change that from an opt-out approach to an opt-in approach, in other words, you would need express consent from the consumer to use this CPNI to market communications-related services. So that is specifically what the chairman has proposed in the order in front of us.

Mr. INSLEE. And I am sorry. I would think these would be non-communication-related services.

Mr. NAVIN. I believe under our existing rules, they would not be allowed to market or be allowed to disclose the information to joint venture partners for non-communication-related services on an opt-out approach. They would not be allowed to do that.

Mr. INSLEE. So what your proposed rule under consideration now would be to treat non-communication services and communication services the same, which is you would have to opt in before it was allowed? Is that the current play?

Mr. NAVIN. That is correct. I would like to get back to you on whether or not the carriers could actually disclose the information to a joint venture partner for non-communications-related services.

Mr. MCCORMICK. I think I can answer that, Mr. Inslee. Our reading of the law is that the law would not allow us to share any information with an allied travel without the express consent of the customer, and that, as a matter of practice, none of our companies do it anyway. The legislation under consideration would, instead, say that with regard to any communications-related services, for example, if a local company, one of our local companies, wanted to offer to its customer a bundle package that included local and long distance, we would not be able to contact that customer unless the customer first opted in and allowed us to use the fact that it was a local customer for us to then say, "You are paying $25 for local service. We will offer you a bundle package with long distance for $35." Or to add that customer in for DSL service. And if that is not the intent of the committee, then what we would hope is that the bill would be clarified so that that ambiguity would not be there.

Mr. LARGENT. Yes, I would just ditto everything Walter said. We feel the same way. Our companies are not taking customers' names or numbers and marketing them or selling them to third parties that don't have anything to do with telecommunications. We use those to market our services to our own customers only.

Mr. INSLEE. Mr. McCormick, you discussed this, you would be discriminated against if this was an opt-in. I am thinking about this, so I don't show you any position that I have right now, but I do want to say that, at least I have taken a position that if other industries should be an opt-in, for instance, I believe you should have to opt in to get my checking account records. I lost that battle in the past couple of Congresses. If I come down and it sounds differently, it is not to discriminate against you but to remain consistent, of course, according to what I think most of my constituents want at the moment.

Mr. MCCORMICK. Well, I understand the desire to opt in in order to get checking account records, call detail information. What we are really talking about here is kind of like a do-not-call list. And as I said before, Congress passed the do-not-call law that was an opt-out. If you don't want to be called, you can opt out. This would

say, with regard to our industry alone, customers would have to opt in before we were allowed to call our own customer. And I don't think that is the committee's intent, and that is what we would like to clarify.

Mr. INSLEE. OK. Is there any middle ground here where you would not disclose specific identity of the callers or callee but certain general characteristics if you reach some joint venture marketing situation? Is that possible?

Mr. MCCORMICK. Yes, there is a lot of middle ground here. I think that all of the concerns that the committee has about identity theft and pretexting and privacy of customer records are concerns that we share. And what we want to be able to do is to simply be able to work in an effective way to market new services, particularly bundled services, in a way that competes with all of the other businesses out there that are looking for new and innovative ways of offering consumers a package that the consumers will find more efficient, higher savings, and more convenient.

Mr. INSLEE. Thank you.

Ms. DEGETTE. The Chair now recognizes Mr. Burgess, distinguished gentleman from Texas, for 6 minutes.

Mr. BURGESS. Thank you, Madame Chairman.

Let me just follow-up on Mr. Inslee's comments. Mr. McCormick, why do you need the CPNI information to market to your customers? Can't you just do this from other data that you would have?

Mr. MCCORMICK. There is a difference between CPNI, customer proprietary network information, and call-detail information. Customer proprietary network information is, arguably, everything about that customer: his service package, does he take a local service, does he take call answering, does he take call forwarding, does he also take Internet access, does he take long distance? That is different than the call-detail information. Call-detail information, we don't even keep call-detail information for local calls. On long distance calls, call-detail information is kept only for billing purposes. It is the call-detail information that is sought by pretexters. It was sought in the case of Mr. Einhorn. We understand the desire of the committee to afford additional safeguards to third parties being able to come in and access that call-detail information, people who should not have access to it. but for purposes of our being able to use joint venture partners to go out and to market for us add-on services like Internet access, video, or even new pricing packages for long distance, family plans, favorite five plans, that information for being able to market outward has never been used for pretexting. There is not any case whatsoever where there has ever been an inappropriate use of that information that has violated the privacy of an individual for outward marketing purposes.

Mr. LARGENT. And I would just add to that, not even when third parties were located not in the United States. Those third-party agreements that they had with the carriers are sacrosanct to those third parties, because if they violate them, then they are out the door, their business is out the door.

Mr. BURGESS. I guess it was in the O&I Subcommittee, I think we had 17 people take the fifth one morning. And I can't even do the math to figure out what number that would be, 17 times 5. But

I am very glad that you don't call those individuals and provide them information. Mr. Stupak was here that morning. That was an unbelievable arrangement of individuals. I still have nightmares about Ma Bell from Arizona.

Well, then, so I understand we are obviously trying to craft a piece of legislation that will endure, and your industry moves and changes very fast, and our legislation will be there in perpetuity for the rest of my natural lifetime, so we want it to be done correctly. And I guess I get the impression from the way the questions have been going back and forth, that you have some concerns about the overly-broad drafting of the language in title II of this bill, is that correct?

And I assume you have made those concerns available to the appropriate committee staff?

And Mr. Navin, you are not allowed to help in that or at some point will you be able to help us in that?

Mr. NAVIN. No, the Commission would be happy to help and happy to provide technical assistance on the bill, but I just reviewed the bill for purposes of preparing for this hearing, and I don't want to simply give my impressions. I would rather coordinate with the folks at the Commission.

Mr. BURGESS. OK. But that information or that technical assistance is going to be available to the committee staff and committee members as we go through the process of marking up and delivering this bill?

Mr. NAVIN. Absolutely.

Mr. BURGESS. OK. Mr. Einhorn, you have been so kind to sit with us all morning, and I appreciate your involvement in this. It won't do any good for me to apologize to you, but I will do it anyway, that you suffered the problems that you did.

Now just so that I understand clearly when Mr. Markey was asking you the question, and he is gone, but I will try to paraphrase it, and I hope I am accurate, where he said shouldn't the company have notified you immediately about a breach of security or the pretexting that occurred. How did they know that the pretexting had occurred? When these guys have sat in front of us and gave us examples of pretexting, they were so cleaver about how they did stuff, how did they know that your information had been delivered to the wrong hands?

Mr. EINHORN. Well, I am glad you came back to that, because I wanted to elaborate on the question that was asked before. I am actually a victim of pretexting in two separate circumstances. The first relates to my home telephone records where the company did not, in any way, notify us that we were pretexted. What actually happens is——

Mr. BURGESS. Well, let me just interrupt you there. How did they know?

Mr. EINHORN. Who is "they"?

Mr. BURGESS. The company, AT&T, I guess.

Mr. EINHORN. AT&T did not notify us or even necessarily know that we had been pretexted.

What happened was we tried to sign up for an online account to pay our bills, and they said, "You can't do that, because the account has actually already been opened." And then you say, "Well, who

opened the account?" And then AT&T was able to tell us the details of how the account was opened.

Mr. BURGESS. So they did not verify that with mailing that information back to you after the new account was opened?

Mr. EINHORN. That is correct. I was not contacted.

And then second, our business records were involved with pretexting. And in that particular case, we only learned about that when Allied Capital put out a press release saying they had things that were purported to be our business records in response to an investigation they were conducting in response to a grand jury subpoena. So if they hadn't been asked that by the Justice Department or by the grand jury to find out whether or not they had actually taken our records, we never would have known until this day that these records were taken.

Mr. BURGESS. And the same situation, that company that was pretexted did not call back for verification after? Did they open a new account as well?

Mr. EINHORN. Well, even now we don't know how they did it. We don't know whether they did this somehow online. We don't know if they bribed an official at the phone company. We have no idea what records they have or how they obtained those records or for what use they made. And that is still true to this moment, because we have gotten no explanation from Allied Capital as to what they have done.

Mr. BURGESS. So if Allied Capital hadn't issued a press release, you wouldn't even, in fact, know about it until this day?

Mr. EINHORN. Relating to the business records, that is correct.

Ms. DEGETTE. The gentleman's time is expired.

Mr. BURGESS. Thank you, Madame Chairman.

Ms. DEGETTE. Yes. The Chair would inquire of the Federal Trade Commission. Are you investigating these business practices by Allied Capital?

Ms. PARNES. Madame Chairman, the Commission investigations are non-public, so we would be happy to talk to you in a non-public briefing.

Ms. DEGETTE. Thank you. The Chair wants to thank all of the witnesses today. And following up on some questioning by Mr. Burgess, I would say, we are not in the initial stages of developing this legislation. We are in the final throws, and so if witnesses today or other members of the audience wish to give specific suggestions on development of this legislation, the committee would much appreciate those efforts.

And again, I want to thank everybody for coming, and the hearing is adjourned.

[Whereupon, at 1:30 p.m., the committee was adjourned.]

○