PHONE RECORDS FOR SALE: WHY AREN'T PHONE RECORDS SAFE FROM PRETEXTING?

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

FEBRUARY 1, 2006

Serial No. 109-53

Printed for the use of the Committee on Energy and Commerce

Available via the World Wide Web: http://www.access.gpo.gov/congress/house

U.S. GOVERNMENT PRINTING OFFICE

26-442PDF WASHINGTON : 2006

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) 512-2250 Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON ENERGY AND COMMERCE

JOE BARTON, Texas, *Chairman*

RALPH M. HALL, Texas
MICHAEL BILIRAKIS, Florida
Vice Chairman
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
Vice Chairman
VITO FOSSELLA, New York
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey
MIKE ROGERS, Michigan
C.L. "BUTCH" OTTER, Idaho
SUE MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
GRESHAM BARRETT, South Carolina

JOHN D. DINGELL, Michigan
Ranking Member
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, JR., New Jersey
SHERROD BROWN, Ohio
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
TED STRICKLAND, Ohio
DIANA DEGETTE, Colorado
LOIS CAPPS, California
MIKE DOYLE, Pennsylvania
TOM ALLEN, Maine
JIM DAVIS, Florida
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas

BUD ALBRIGHT, *Staff Director*
DAVID CAVICKE, *General Counsel*
REID P. F. STUNTZ, *Minority Staff Director and Chief Counsel*

CONTENTS

	Page
Testimony of:	
Martin, Hon. Kevin J., Chairman, Federal Communications Commission	37
Leibowitz, Hon. Jon, Commissioner, Federal Trade Commission	43
Madigan, Lisa, Attorney General, State of Illinois	67
Largent, Hon. Steve, President and Chief Executive Officer, Cellular Telecommunications and Internet Association	72
Merlis, Edward, Senior Vice President, Law & Policy, United States Telecom Association	77
Rotenberg, Marc, Executive Director, Electronic Privacy Information Center	80
Douglas, Robert, Chief Executive Officer, PrivacyToday.com	87

PHONE RECORDS FOR SALE: WHY AREN'T PHONE RECORDS SAFE FROM PRETEXTING?

WEDNESDAY, FEBRUARY 1, 2006

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

The committee met, pursuant to notice, at 2:04 p.m., in Room 2123 of the Rayburn House Office Building, Hon. Joe Barton [chairman] presiding.

Members present: Representatives Barton, Hall, Upton, Stearns, Gillmor, Deal, Whitfield, Cubin, Shimkus, Radanovich, Pitts, Walden, Terry, Ferguson, Otter, Murphy, Burgess, Blackburn, Barrett, Markey, Rush, Stupak, Wynn, Green, DeGette, Schakowsky, Gonzalez, Inslee, Baldwin, and Ross.

Staff present: Howard Waltzman, Chief Counsel for Telecommunications and the Internet; Kelly Cole, Counsel; Shannon Jacquot, Counsel; Will Carty, Professional Staff Member; Chris Leahy, Policy Coordinator; Tom Feddo, Counsel; David Cavicke, General Counsel; Brian McCullough, Professional Staff Member; Peter Filon, Minority Counsel; Johanna Shelton, Minority Counsel; Consuela Washington, Minority Counsel; Billy Harvard, Legislative Clerk; and Anh Nguyen, Legislative Clerk.

CHAIRMAN BARTON. The committee will come to order. Before I give my opening statement, I want to take upon a personal privilege just to thank everyone for their phone calls, e-mails, and good wishes during my recent medical problem. I have been 100 percent cleared by the doctors to resume a full schedule and the doctors tell me if they didn't know my problem, they couldn't tell that I had a problem now. And I want to thank Mr. Martin. He sent me a very nice note, I appreciate that, and so I just wanted to thank everybody for your warm wishes. I now recognize myself for an opening statement.

I want to thank our distinguished panelists for coming this afternoon to talk about pretexting and the sale of phone records. Our e-mail is clogged with spam; our computers are covertly monitored with spyware; our personal information is bought and sold by information brokers; and now we learn that a phone number and $100 can buy you a month's worth of call information for just about anybody from our cell phones. These are very personal and private records of who we call, when we

call, and how long we spend on the telephone call. This is an invasion of personal privacy and if I have anything to do about it, it will not be allowed to continue very much longer.

Typically, these phone records are being obtained through the phone carriers by data brokers who are "pretexting," or impersonating either a customer or an executive within a telecommunications company to fraudulently obtain a customer's records. This fraud is already illegal for financial information and, although the Federal Trade Commission currently has some enforcement powers under its Section 5 authority, pretexting for phone records is not explicitly regulated at the Federal level. Does it make sense? These are sensitive, personal records that deserve the same protection as financial information has right now.

The ease with which data brokers can obtain these telephone records is disturbing on many levels. Not only does the leaking of these records assist a scam artist in perpetuating identity theft, but even more shadowy figures, such as organized crime, stalkers, and abusive spouses, have co-opted this confidential information to locate and target their victims. Even the police are worried that their undercover officers could be outed by drug dealers for the cost of a few dollars and a few minutes on the Internet.

In the next few days this committee is going to ask the tough questions to these data brokers; what on Earth they think they are doing? I can only guess at the excuses that will be offered by the people who profit by engaging in an obvious fraud by invading our personal privacy and assisting criminal behavior.

For all of these reasons, I have been working during the past several weeks with Ranking Member Dingell and other members to introduce legislation that makes pretexting for telephone records illegal, period. I plan to introduce this legislation very shortly and my goal is to quickly move it through the committee and to the House floor so we can provide meaningful protection to these sensitive records. I am also aware that Congressman Inslee and Congresswoman Blackburn of Tennessee, I think today, have introduced a companion bill on this issue.

I am very pleased to welcome Chairman Martin of the FCC and Commissioner Leibowitz of the FTC to the committee today. There is an important role to be played by each of the agencies that these gentlemen head. Certainly, the Federal Trade Commission is the government's consumer fraud watchdog. The FTC is the appropriate agency to target the criminals who attempt to make money trading in our most personal information. The FCC additionally has a role to play to ensure that telecommunication carriers are compliant with their current legal obligations to protect confidential customer information.

I look forward to working with members on both sides of the aisle to stop this predatory practice. I want to thank the witnesses on our first panel for being here, and before I turn it over to Ms. Schakowsky to make an opening statement, we have a former member of the committee who is going to testify on the second panel, Steve Largent. We want to welcome him and I am really surprised that he is here today since his former football team, the Seahawks, is actually in the Super Bowl. So I hope that he can focus on the issue today and not on what the Pittsburgh Steelers might do to his team this coming Sunday.

If Congressman Doyle shows up, be careful, since he is a big fan of the Pittsburgh Steelers. With that, I yield back the balance of my time and welcome the gentlelady from Illinois, Ms. Schakowsky, for an opening statement.

[The prepared statement of Hon. Joe Barton follows:]

PREPARED STATEMENT OF THE HON. JOE BARTON, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Good afternoon. I'd like to thank our distinguished panel for coming in this afternoon to talk about pretexting and the sale of phone records.

Our e-mail is clogged with spam. Our computers are covertly monitored with spyware. Our personal information is bought and sold by information brokers. And now we learn that a phone number and one hundred dollars can buy you a month's worth of call information for just about anyone. These are very personal and private records of who we call, when we call, and how long we spend on the line. This is an invasion into our personal privacy and it cannot be allowed to continue.

Typically, these phone records are being obtained through the phone carriers by data brokers who are "pretexting", or impersonating either a customer or an executive within the telecommunications company to fraudulently obtain a customer's records. This fraud is already illegal for financial information, and although the FTC currently has some enforcement powers in this area under its Section 5 authority, pretexting for phone records is not explicitly regulated on the federal level. This doesn't make sense. These are sensitive, personal records that deserve the same protection as financial information.

The ease with which data brokers can obtain these phone records is disturbing on many levels. Not only does the leaking of these records assist scam artists in perpetrating identity theft, but even more shadowy figures, such as criminals, stalkers and abusive spouses, have co-opted this confidential information to locate and target their victims. Even the police are worried that their undercover officers could be outed by drug dealers for the cost of a few dollars and a few minutes on the Internet.

In the next few days, we're going to begin asking some of these data brokers what on earth they think they are doing. I can only guess at the excuses that will be offered by people who profit by engaging in an obvious fraud, by invading personal privacy and by assisting criminal behavior.

For all of these reasons, I have been working during the last week with Ranking Member Dingell and others to introduce legislation that makes pretexting for telephone records illegal. I plan to introduce this legislation shortly and my goal is to quickly move it through the Committee and to the House floor so we can provide meaningful protections to these sensitive records.

In addition to our expert witnesses, I'm very pleased to welcome Chairman Martin of the FCC and Commissioner Leibowitz of the FTC to the Committee. There is an important role to be played by each of these agencies. Certainly, the Federal Trade Commission (FTC) is the government's consumer fraud watchdog. The FTC is the appropriate agency to target the criminals who attempt to make money trading in our most personal of information. The Federal Communications Commission additionally has a role to play to ensure that telecommunications carriers are compliant with their current legal obligations to protect confidential customer information.

I look forward to working with members on both sides of the aisle to stop this predatory practice. I thank the witnesses for being here today and I look forward to hearing their testimony.

And I especially want to offer a warm welcome to a former member of the Energy & Commerce Committee, and Hall of Fame football player, Steve Largent. As important as our hearing is today, I'm guessing that his mind may wander to this weekend's upcoming Super Bowl, where his former team of 14 years, the Seattle Seahawks, take on the Pittsburgh Steelers. You may want to steer clear of Congressman Doyle's questions today, since he is from Pittsburgh, but don't worry, you've got Congressman Inslee of Washington to defend you.

MS. SCHAKOWSKY. Thank you, Chairman Barton, and I think I speak for everyone to say how very glad we are to see you here looking so well and gladly to hear that you are feeling so well and I thank you for holding today's hearing on one of the latest examples of consumer scams, a new version of Dialing for Dollars. For about $100, scam artists can earn cash by getting access to and selling someone else's phone records. Now Congress needs to act to plug this legal loophole. I am proud to say that my State of Illinois has been the leader in the Nation on cracking down on pretexting or posing as others in order to obtain and sell their phone records.

Frank Main of the Chicago Sun Times first broke this story. Senator Durbin introduced the first bill in his chamber, the Phone Records Protection Act. Illinois Attorney General Lisa Madigan, one of our witnesses here today, who has quickly become recognized as one of the most effective consumer advocates in the country, has brought the first case against a phone call broker, and I have introduced the SAFECALL Act, which is a somewhat tortured acronym for the Stop Attempted Fraud Against Everyone's Cell and Landline Act, which would end all ambiguity in the law and make pretexting for phone records illegal, no question about it. I am glad we are looking into this invasion of privacy on a national level and I hope that the SAFECALL Act becomes the base for a strong bipartisan Energy and Commerce bill.

Privacy is a scarce resource these days. Personal and business phone records can be assessed with just the click of the mouse by anyone who wants them. There are around 100 web sites offering phone logs with proclamations such as bargain prices, smart deals, accurate, dependable, results within hours. Data Trace USA's web site brags about what it can

deliver. Listen to this. "You provide us with a working cell phone, name and possible address. We will provide you all incoming and outgoing calls from the most recent billing cycle available. If you have target dates you want, please provide them to us, as well." Of course, Data Trace's site also has the disclaimer that "All performed searches are intended for research purposes only. This information will only be obtained legally by a private investigator's research." But who is checking for compliance?

Say it is a competitor trying to steal contacts. Is that such a smart deal for the small business that is ruined? What if it is a stalker who has made that request? Think the victim of domestic violence is comforted knowing that her records are so easily accessed? The Chicago police department has already put out a warning that drug dealers could use pretexting to identify undercover cops, identifying--putting law enforcement officers at deadly risk. There is a lot more than privacy that is at stake. It is time to put any question of legality about pretexting to rest. It is time to tell phone call brokers that getting into our private business is not going to be the bread and butter of their business, and it is time that phone companies stop being freewheeling with their customers' calls.

Chairman Barton, Ranking Member Dingell, I thank you for today's hearing. I am glad that we are deciding to ring in this new legislative year by acting to better secure the privacy of phone records. I look forward to hearing from our witnesses. Once again, I want to thank Attorney General Lisa Madigan for joining us today and I look forward to hearing what you are doing for consumers in Illinois. Thank you.

CHAIRMAN BARTON. We thank the gentlelady. Mr. Upton, Chairman of the Subcommittee on Telecommunications.

MR. UPTON. Thank you, Mr. Chairman. I welcome our witnesses and our friend, Mr. Largent. I just want to know, as a Michiganer, did you have to get a four-day minimum stay in Detroit?

We have made a lot of advances in technology since the days of the old black rotary phone. There are now 190 million of us that have cell phones and we garner the privacy that comes with those phones. But the unfortunate reality is that along with the great advances in technology, there have been great advances in fraud, too, and over the last couple of weeks, pretexting has garnered the national spotlight. Someone with as little as $100 might be able to purchase just about anybody's cell phone records. Those are ours and they feel like they are our documents that we have made, as well, and I think that it is wrong. I would guess that every American with a cell phone would probably say that it would be wrong for those records to fall into just about anybody else's hands.

It doesn't matter what the motive might be, no matter how barbaric or innocent the intentions, pretexting is wrong and it is a violation of an individual's right to basic privacy. I look forward to working with you, Mr. Chairman, to work on bipartisan legislation that we can move through this committee very quickly to close those loopholes and to make sure that every cell phone user and payer of those bills knows that those records are going to remain private. I yield back my time.

CHAIRMAN BARTON. The gentleman yields back his time. We have a vote on the floor that just started. I think it is just one vote. Two votes, one vote? We are going to try to continue as long as possible and go vote. Mr. Markey, the Ranking Member of the Telecommunications subcommittee is recognized for three minutes.

MR. MARKEY. Thank you, Mr. Chairman. You are looking good, Mr. Chairman.

CHAIRMAN BARTON. Thank you.

MR. MARKEY. We are all glad for that. And we thank you, on the first day back, for getting right back into action on a very important issue, the sale of telephone records and we look forward to working with you and Mr. Dingell and Mr. Upton, Mr. Stearns, Ms. Schakowsky, to develop legislation on this issue.

Mr. Chairman, personal privacy is the cornerstone of individual freedom. It is no surprise, therefore, that this is an issue that has captured nationwide attention. Millions of consumers today are rightly outraged to discover that their telephone records are for sale on the Internet and alarmed by the apparent ease with which they are obtained and disclosed. Undoubtedly, many such records are obtained illegally by individuals who place pretexting calls to the phone companies; in other words, a fraudster will pretend to be someone they are not and trick a telephone company employee into giving out personal information.

Last November 7th, I wrote to the chairman of the Federal Communications Commission and the chairman of the Federal Trade Commission on this issue and urged those agencies to ensure that consumer phone records are not for sale in some cyberspace bazaar and to take action to shut down these practices. The Federal Trade Commission response to my letter confirmed that although pretexting for telephone records is not explicitly mentioned in the law, the agency has the power today to go after pretexters of phone records, using the prohibition against unfair or deceptive business practices.

I believe that the sale of a commodity which is obtained by impersonating another person is, per se, unfair and deceptive. In my opinion, legal action against those fraudsters is long overdue. The Federal Trade--the Federal Communications Commission response to my letter noted that pending before the agency is a petition from the

Electronic Privacy Information Center requesting FCC action to tighten consumer privacy rules. I hope the Commission will act favorably upon this petition soon. The FCC letter also noted that telephone companies are required to certify their compliance with the rules annually and explain the measure they are taking to safeguard consumer information. Chairman Barton, Mr. Dingell, Chairman Upton and myself sent a follow-up letter to the FCC asking for copies of these annual certifications, and I would observe that two days ago the FCC levied fines on two companies for failure to comply adequately with those rules.

As this committee proceeds in our own investigation and in developing legislation, I believe we need to question why a person's telephone record should ever be for sale commercially, at all. In addition, it may be useful to stiffen the fines and penalties for those violating the law. I think we also need to analyze the measures taken by phone companies to secure consumer data, the rules under which they are permitted to disclose and share consumer information, not only with their own affiliates, but also with joint venture partners and private contractors.

And finally, I think that Congress and the FCC should examine the adequacy of the privacy notice consumers are currently given advising them of what the phone company does with their personal information and their right to exercise choice and how their personal information is used, shared or disclosed. I look forward to hearing from both agencies this afternoon on the status of these investigations of this issue, as well as the additional efforts they are taking to better enforce the law and tighten existing rules and I look forward to the experts on privacy on the second panel. I thank you, Mr. Chairman, for this timely hearing and I look forward to hearing from our witnesses.

CHAIRMAN BARTON. We will have Mr. Whitfield, and then Mr. Rush, and then we will probably break briefly for a vote. I don't think we can get any other members in before we go vote, after Mr. Whitfield and Mr. Rush.

MR. WHITFIELD. Mr. Chairman, thank you very much and we are all quite excited about your having this hearing entitled Phone Records For Sale: What Aren't Phone Records Safe From Pretexting? All of us are troubled that private cell phone records and call logs of Americans are available to anyone for a price, and it is particularly troubling that data broker businesses acquire and sell these records without consumers' informed consent. It is unacceptable that the privacy and personal records of so many Americans are so easily obtainable, and as chairman of the Oversight and Investigations Subcommittee, I look forward, Mr. Chairman, with you of sending out letters to these data brokers to learn more explicitly how they are obtaining this confidential information. I

am delighted that you will soon be introducing legislation to correct this inequity. I look forward to thoroughly investigating this issue and you holding this hearing, and I yield back my time.

CHAIRMAN BARTON. Mr. Rush will be our final opening statement before we go vote. Mr. Rush.

MR. RUSH. Thank you, Mr. Chairman. Mr. Chairman, the recent reports about the sale of consumer cell phone records is of great concern to me and to other members of this committee and also to the witnesses, I believe. Apparently, unscrupulous data brokers are advertising on a dozen of web sites for prices as low as $110 the calling patterns and histories of phone customers without their consent or without their knowledge. This practice, Mr. Chairman, was so--in a recent series by the Chicago Sun Times, issued a warning to its officers--it said that the Chicago police department issued a warning to its officers and undercover agents that their cell phone records can easily be obtained by these brokers which can place them and their families in harm's way.

Our committee has the jurisdiction, Mr. Chairman, to stop these illegal activities. As you know, Federal law expressly prohibits pretexting for financial data. The Federal Trade Commission has jurisdiction to enforce this illegal activity through its deceptive practice, which is under Section 5 of the FTC Act which prohibits unfair or deceptive practices, and also within the Financial Modernization Act of 1999, the Gramm-Leach-Bliley Act. The Federal Communications Committee--Commission, rather, under Section 222 has the jurisdiction to protect the confidentiality of a customer's phone records. As such, Mr. Chairman, I am interested in knowing what the FCC and the FTC are doing to stop these bad actors from employing pretexting tactics to get one's information.

Moreover, I would like to know whether the Gramm-Leach-Bliley Act should be amended to include telephone records or whether the FTC can actively pursue these perpetrators under Section 5 of the Unfair or Deceptive Practices Act. In addition, Mr. Chairman, I am interested in any enforcement measures that the FTC and the FCC are taking in this particular area. Mr. Chairman, the privacy of the American people is of paramount importance and cannot allow to be breached. I look forward to hearing from our distinguished panelists today and Mr. Chairman, with the time that I have remaining, I want to also welcome to this committee, to this hearing, the Illinois State Attorney General, Lisa Madigan. Attorney General Madigan has been a leader in this particular area and in many other areas. She is one of the rising stars of the Democratic party, both locally, statewide, and nationally and she is probably one of the most energetic State's Attorney General, rather that

we have ever had in our State and I again welcome her and I look forward to her insightful testimony to this committee this morning.

CHAIRMAN BARTON. We are going to recess. We have one vote on the floor. We should try to be back here about ten until 3:00 p.m.

MR. MARKEY. Mr. Chairman?

CHAIRMAN BARTON. Mr. Markey.

MR. MARKEY. Could I just ask unanimous consent to insert into the record my November 7th letter to the FCC and the FTC on this issue, the FTC and FCC responses and the January 23rd letters from yourself, Mr. Dingell, myself and Chairman Upton to the Federal--

CHAIRMAN BARTON. Without objection, so ordered.

MR. MARKEY. Thank you.

[The information follows:]

EDWARD J. MARKEY
7TH DISTRICT, MASSACHUSETTS

ENERGY AND COMMERCE COMMITTEE
RANKING MEMBER
SUBCOMMITTEE ON
TELECOMMUNICATIONS AND
THE INTERNET

SELECT COMMITTEE ON
HOMELAND SECURITY

RESOURCES COMMITTEE

Congress of the United States
House of Representatives
Washington, DC 20515–2107

2108 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–2107
(202) 225–2836

DISTRICT OFFICES:

5 HIGH STREET, SUITE 101
MEDFORD, MA 02155
(781) 396–2900

188 CONCORD STREET, SUITE 102
FRAMINGHAM, MA 01702
(508) 875–2900
www.house.gov/markey

November 7, 2005

The Honorable Kevin J. Martin
Chairman, Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

The Honorable Deborah P. Majoras
Chairman, Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Dear Chairmen Martin and Majoras:

I am writing with respect to recent reports in the media about the commercial availability of consumer telephone records. I am concerned about the proliferation of sources through which wireless and wireline records of consumer calling and billing information is available for sale without consumer approval. The privacy of American citizens is priceless and the phone records of consumers should not be commodities for sale in any cyberspace bazaar.

As you may know, Congress enacted consumer privacy provisions as part of the Telecommunications Act for "customer proprietary network information" to assure consumers that the privacy of their calling and billing information would be safeguarded. It is illegal to disclose this information without the approval of telephone subscribers. Nevertheless, several Internet websites (e.g., locatecell.com, celltolls.com) are now offering services in which they sell information about the telephone calls placed from a wireless phone, including the date, time and duration of calls place by a consumer. In addition, several websites also offer similar information for landline phones and even sell unlisted phone numbers and related consumer information.

I am interested in knowing what your respective agencies are doing to shut down these activities. Moreover, I am interested in knowing how and whether specific "customer proprietary network information" rules contained in Section 222 of the Communications Act may be being circumvented or violated. In addition, it is apparent that many of these websites may be obtaining this private consumer information illicitly from unscrupulous employees of telecommunications carriers through "pre-texting" or

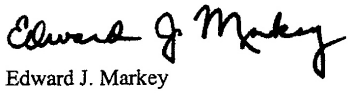
PRINTED ON RECYCLED PAPER

other unethical methods. I would like information on how such information is being disclosed, whether you are aware of any carriers currently disclosing such information (either in a manner consistent, or in violation of, current FCC rules or Section 222.) Please provide me with information regarding steps carriers are currently obligated take under FCC rules to secure and protect consumer information, if any, as well as any measures you are aware they may be taking to better safeguard consumer calling information in their possession.

Finally, given the growing nature of this problem, I am interested in any stepped-up enforcement measures your respective agencies are taking in this area. We must send a signal to the public and these website companies that the abuse of private information will not be tolerated.

Thank you in advance for your time and attention in responding to this request.

Sincerely,



Edward J. Markey
Ranking Democrat
House Subcommittee on
Telecommunications and the Internet

THE CHAIRMAN

FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

December 13, 2005

The Honorable Edward J. Markey
United States House of Representatives
Washington, DC 20515-2107

Dear Representative Markey:

Thank you for your letter of November 7, 2005, regarding websites offering consumer telephone information for sale. Maintaining the privacy and security of consumers' personal information is one of the Commission's highest priorities. Although I cannot discuss publicly any specific investigations that Commission staff currently may be undertaking, the Commission has investigated and brought cases against companies that offer to procure and sell sensitive consumer information to third parties and will continue to do so in the future.

Through our investigations, we have learned that some individuals and firms use the practice of "pretexting" to obtain sensitive consumer information for sale to third parties. Typically, the pretexter impersonates the consumer in communicating with the business holding the consumer's information, to convince the business to turn over that information. As you may know, Section 521 of the Gramm-Leach-Bliley Act ("GLB"), 15 U.S.C. § 6821, prohibits any person from obtaining customer information of a financial institution by making fictitious or fraudulent statements. As part of "Operation Detect Pretext," an enforcement sweep of pretexters of financial information, the Commission reviewed over 1,000 websites and 500 print advertisements of firms that offered to sell or obtain consumers' financial account information. The Commission sent approximately 200 warning letters to these companies and in several instances brought federal district court actions to permanently enjoin the illegal conduct.[1] Because Section 521 also has criminal penalties, the Commission also may refer pretexters to the Department of Justice for criminal prosecution as appropriate; one such individual recently pled guilty to one count of pretexting under GLB.[2]

---

[1] For more information about the cases the Commission has brought under GLB Section 521, please see the Commission's web page at: http://www.ftc.gov/privacy/privacyinitiatives/pretexting_enf.html. Since GLB's passage in 1999, the FTC has brought over a dozen cases alleging violations of Section 521 in various contexts.

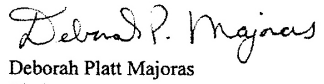
[2] United States v. Easton, No. 05 CR 0797 (S.D.N.Y).

Although consumer telephone records are not generally covered by GLB, the Commission may still bring a law enforcement action against a pretexter of telephone records if it has reason to believe that the pretexter's activities constitute unfair or deceptive practices under Section 5 of the FTC Act.

Because this area involves information principally held by telephone companies under the jurisdiction of the Federal Communications Commission, FTC staff are working with their counterparts at the FCC to share information and coordinate strategies, as we have done successfully with the enforcement of the "Do Not Call" legislation.[3]

Should you have questions or require additional information, Commission staff would be happy to meet with you or representatives from your office to discuss this further. Please contact Anna Davis, Director of Congressional Relations, at (202) 326-3680, for assistance.

Sincerely,



Deborah Platt Majoras
Chairman

---

[3] As you note in your letter, consumer telephone records are considered "customer proprietary network information" under the Telecommunications Act of 1996 and accordingly are afforded privacy protections by the regulations under that Act. The Act imposes obligations on common carriers, but does not prohibit pretexters from obtaining phone records. Common carriers are regulated by the Federal Communications Commission.

FEDERAL COMMUNICATIONS COMMISSION
WASHINGTON

OFFICE OF
THE CHAIRMAN

January 13, 2006

The Honorable Edward J. Markey
Ranking Member
Subcommittee on Telecommunications
and the Internet
Committee on Energy and Commerce
U.S. House of Representatives
2108 Rayburn House Office Building
Washington, D.C. 20515

Dear Congressman Markey:

Thank you for your letter regarding recent reports in the media about the commercial availability of consumer telephone records. The Commission also is very concerned about the availability and sale of such records, and is looking into the troublesome practices described in recent media reports.

The Commission's Enforcement Bureau is currently investigating this practice. Specifically, we are looking into how companies who are selling these records have obtained customer proprietary information. To the extent that they have acquired this information from telecommunications carriers, we will take strong enforcement action to address any noncompliance by carriers with their obligations to protect customer proprietary information under the Communications Act and the Commission's existing rules. To the extent that those involved in obtaining and selling such records have obtained this information fraudulently and without implicating any noncompliance by telecommunications carriers with the Communications Act or Commission rules, the conduct may be more appropriately handled by the Federal Trade Commission. Commission staff have been coordinating with FTC staff on activities underway in both agencies to address this disturbing conduct. We will continue to work closely and cooperatively with FTC staff in this area.

In addition, the Commission recently received a petition filed by the Electronic Privacy Information Center (EPIC) expressing concerns about this issue and requesting that the Commission conduct a rulemaking to enhance security and authentication standards for access to consumer records. According to EPIC, telecommunications carriers' current security standards and measures are not sufficient to prevent private investigators and on-line data brokers from acquiring and selling private customer records. EPIC reports that data brokers use several methods to penetrate security screens, one of which is pretending to have legitimate authority to access protected records, or "pretexting."

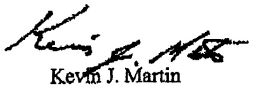
Section 222 of the Communications Act obligates carriers to protect the confidentiality of customer proprietary network information (CPNI), but permits carriers to release such records in certain narrow situations. The Commission's rules implementing Section 222 require carriers to establish a system for obtaining customer approval before release of CPNI records, and to train their personnel as to when they are and are not authorized to release such information. In addition, the rules require carriers to record all instances where customer records were disclosed or provided to third parties, or where third parties were allowed access to the records. Each carrier must certify annually that it has established operating procedures that are adequate to ensure compliance with these rules, and must provide a statement explaining how its operating procedures ensure such compliance.

EPIC's petition asks the Commission to examine what additional steps should be taken to strengthen safeguards for customer records. Suggested measures include the adoption of rules requiring carriers: (1) to adopt consumer-set passwords (which may be changed and are not searchable, in contrast to biographical identifiers); (2) to maintain "audit trails" (recording all instances of disclosure of customer records); (3) to store records in encrypted form, (4) to notify the customer and the Commission when security is breached; and (5) to delete customer records that are no longer needed for billing or resolution of disputes.

The Commission placed EPIC's petition on public notice on September 29, 2005, and the record is now closed. Ensuring consumers' privacy is of fundamental concern to the Commission. The record now being reviewed will help the Commission establish whether carriers are meeting consumers' privacy expectations as contemplated by Section 222 and, if the carriers' security measures are falling short, how best to implement appropriate safeguards to protect consumer privacy.

I appreciate your interest in this very important area. Please do not hesitate to contact me if I can be of further assistance.

Sincerely,



Kevin J. Martin
Chairman

RALPH M. HALL, TEXAS
MICHAEL BILIRAKIS, FLORIDA
VICE CHAIRMAN
FRED UPTON, MICHIGAN
CLIFF STEARNS, FLORIDA
PAUL E. GILLMOR, OHIO
NATHAN DEAL, GEORGIA
ED WHITFIELD, KENTUCKY
CHARLIE NORWOOD, GEORGIA
BARBARA CUBIN, WYOMING
JOHN SHIMKUS, ILLINOIS
HEATHER WILSON, NEW MEXICO
JOHN B. SHADEGG, ARIZONA
CHARLES W. "CHIP" PICKERING, MISSISSIPPI
VICE CHAIRMAN
VITO FOSSELLA, NEW YORK
STEVE BUYER, INDIANA
GEORGE RADANOVICH, CALIFORNIA
CHARLES F. BASS, NEW HAMPSHIRE
JOSEPH R. PITTS, PENNSYLVANIA
MARY BONO, CALIFORNIA
GREG WALDEN, OREGON
LEE TERRY, NEBRASKA
MIKE FERGUSON, NEW JERSEY
MIKE ROGERS, MICHIGAN
C.L. "BUTCH" OTTER, IDAHO
SUE MYRICK, NORTH CAROLINA
JOHN SULLIVAN, OKLAHOMA
TIM MURPHY, PENNSYLVANIA
MICHAEL C. BURGESS, TEXAS
MARSHA BLACKBURN, TENNESSEE
J. GRESHAM BARRETT, SOUTH CAROLINA

BUD ALBRIGHT, STAFF DIRECTOR

ONE HUNDRED NINTH CONGRESS

U.S. House of Representatives
Committee on Energy and Commerce
Washington, DC 20515–6115

JOE BARTON, TEXAS
CHAIRMAN

January 23, 2006

JOHN D. DINGELL, MICHIGAN
RANKING MEMBER
HENRY A. WAXMAN, CALIFORNIA
EDWARD J. MARKEY, MASSACHUSETTS
RICK BOUCHER, VIRGINIA
EDOLPHUS TOWNS, NEW YORK
FRANK PALLONE, JR., NEW JERSEY
SHERROD BROWN, OHIO
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
TED STRICKLAND, OHIO
DIANA DEGETTE, COLORADO
LOIS CAPPS, CALIFORNIA
MIKE DOYLE, PENNSYLVANIA
TOM ALLEN, MAINE
JIM DAVIS, FLORIDA
JAN SCHAKOWSKY, ILLINOIS
HILDA L. SOLIS, CALIFORNIA
CHARLES A. GONZALEZ, TEXAS
JAY INSLEE, WASHINGTON
TAMMY BALDWIN, WISCONSIN
MIKE ROSS, ARKANSAS

The Honorable Kevin J. Martin
Chairman, Federal Communications Commission
445 12th Street, S.W.
Washington, D.C. 20554

Dear Chairman Martin:

We write with respect to the disclosure of consumer telephone records. The protection of consumer privacy in an age where an increasing amount of personal information and transactions are contained in electronic form is more vital than ever. Consumers are rightly concerned when they learn that their personal information has been compromised. In the recent cases involving the online sale of telephone records the apparent ease with which such personal information has been compromised, obtained, and then sold, is shocking and unacceptable.

In your January 13th response to Representative Markey's November 7th letter, you note that the Federal Communications Commission (the Commission) has before it a petition from the Electronic Privacy Information Center, which was filed last year and for which the public record is now closed. We are eager to know when the Commission will complete its review of the record and determine what actions should be taken in response to the petition.

In addition, in your response, you also note that each telecommunications carrier, under existing customer proprietary network information rules, "*must certify annually that it has established operating procedures that are adequate to ensure compliance with these rules, and must provide a statement explaining how its operating procedures ensure such compliance.*" As part of our ongoing investigation of this issue, as well as the Commission's response to consumer privacy concerns, we request that you forward to us the last annual certifications the Commission has received from the 5 largest wireline telecommunications carriers and the 5 largest wireless telecommunications carriers, along with the accompanying statements from each company explaining how their internal procedures protect the confidentiality of consumer information.

January 23, 2006
Page 2

Please provide our office the requested documents by January 30, 2006. Thank you in advance for your time and attention in responding to this request.

Sincerely,

Joe Barton
Chairman
Committee on Energy and Commerce

John D. Dingell
Ranking Member
Committee on Energy and Commerce

Fred Upton
Chairman
Subcommittee on Telecommunications and the Internet

Edward Markey
Ranking Member
Subcommittee on Telecommunications and the Internet

CHAIRMAN BARTON. So we are in recess until approximately ten until 3:00 p.m.

[Recess]

MR. STEARNS. [Presiding] The committee will come to order. Chairman Barton is going to be with us shortly, and he requested that we continue with the opening statements so we keep moving and I will start with my opening statement, take the prerequisite here.

My colleagues, I want to thank Chairman Barton for holding this important hearing on the sale of phone records and the nefarious practices used to obtain them. Once again, the entrepreneurship con artists, identity thieves and illicit enterprise are making the lives of all Americans less secure and less private. The growing world market for personal information which benefits all of us with faster, cheaper products and services is also spawning more sophisticated and brazen criminal activity that challenges traditional regulation and enforcement.

Many illicit phone records data brokers that pretext are not lurking underground, rather they are openly advertising their exploitation of the law and the Internet to broadcast our private records to any taker, anywhere in the world for a price. Let me be clear. I believe pretexting should be illegal in any context, financial or otherwise. But the stark reality is that there will always be fraudsters and cyber thieves to keep the enforcement community busy. The other half of this battle, however, is about things we cannot control, like protecting personal data from criminals, regardless of their methods.

Vigilance, both in the public and private sector is critical to combating the fastest growing criminal enterprise in America, identity theft. As Mr. Barton knows, the Subcommittee on Commerce, Trade, and Consumer Protection, which I chair, has held extensive hearings on data security and we have already marked up a bill, H.R. 4127, the Data Accountability and Trust Act. Now, this bill is intended in part to ensure that personal information is secured and protected. And while the telecommunications companies are currently exempt from FTC regulation as common carriers, I believe the committee would be well-served to carefully examine the approach in the data bill to understand how the telecommunication companies can better protect their customers' telephone records and data.

In addition, I would like to hear why the telephone companies don't institute better security measures like advance authentication techniques to prevent unauthorized account access. Likewise, the FCC and the Federal Trade Commission need to explain what they are doing to drive better security practices in this sector and how aggressively they are prosecuting these sleazy pretexting outfits. The subcommittee I chair had a hearing on the data bill and made it clear that all of us are facing an unprecedented assault on our personal data and more specifically, this goes to our private lives.

Personal data in electronic form can be extremely destructive when misused. Just ask anyone who has suffered identity theft. In fact, someone on this committee has. So Mr. Barton realizes that the best we can do now is to put some control back in the hands of the consumer and require just simple, reasonable, workable security policies for entities maintaining personal data about individuals' lives. Congress needs to act on the data security issue before personal privacy becomes just another sentimental notion, rather than the right that all Americans deserve.

[The prepared statement of Hon. Cliff Stearns follows:]

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

I want to thank Chairman Barton for holding this important hearing on the sale of phone records and the nefarious practices used to obtain them. Once again, the entrepreneurship of con-artists, identity thieves, and illicit enterprises is making the lives of all Americans less secure and private. The growing world market for personal information, which benefits all of us with faster, cheaper products and services, is also spawning more sophisticated and brazen criminal activity that challenges traditional regulation and enforcement. Many illicit phone records data brokers that pretext are not lurking underground, rather they openly advertise their exploitation of the law and the Internet to broadcast our private records to any taker, anywhere in the world, for a price.

Let me be clear, I believe pretexting should be illegal in any context, financial or otherwise, but the stark reality is that there will always be fraudsters and cyber-thieves to keep the enforcement community busy. The other half of this battle, however, is about

things we can control like protecting personal data from criminals, regardless of their methods. Vigilance, both in the public and private sector, is critical to combating the fastest growing criminal enterprise in America - identity theft.

Mr. Chairman, as you know, the Subcommittee on Commerce, Trade, and Consumer Protection, which I chair, has held extensive hearings on data security and has already marked up a bill, HR 4127, the "Data Accountability and Trust Act." HR 4127 is intended, in part, to ensure that personal information is secured and protected. And while the telecommunication companies are currently exempt from FTC regulation as common carriers, I believe the Committee would be well-served to carefully examine the approach in the DATA bill to understand how the telecommunications companies can better protect their customers' telephone records data. In addition, I'd like to hear why the telephone companies don't institute better security measures like advanced authentication techniques to prevent unauthorized account access. Likewise, the FCC and FTC need to explain what they are doing to drive better security practices in this sector and how aggressively they are prosecuting these sleazy pretexting outfits.

The CTCP Subcommittee hearings on the DATA bill made it clear that all of us are facing an unprecedented assault on our personal data, and more specifically, our private lives. Personal data in electronic form can be extremely destructive when misused. Just ask anyone who has suffered identity theft. Mr. Chairman, the best we can do now is to put some control back in hands of the consumer and require reasonable, workable security policies for entities maintaining personal data about our private lives. The Congress needs to act on the data security issue before personal privacy becomes just another sentimental notion rather than the right all Americans deserve.

Thank you Mr. Chairman.

MR. STEARNS. With that, on the Democrat side, Ms. DeGette for an opening statement. She waives her opening statement. Mr. Inslee.

MR. INSLEE. Mr. Chairman, I was--just before Christmas I was surfing the Net. It was raining in Seattle for 34 days in a row and so I was surfing the Net. When I read about this, to see that actually in the open, people were selling private cell phone records, it was, to me, like stumbling across a web site for Hit Men Are Us and it just flabbergasted me that this was happening. I couldn't believe that in a sense they would be brazen about it because of this loophole and it showed a couple things. First, I think it showed that as electronic data becomes absolutely woven into every single fabric of our lives, the price of privacy really is eternal vigilance and I think this particular disaster that we have of this loophole existing shows how Congress needs to be continuing adept and alert about privacy issues on a daily or weekly basis. And I hope that we will get this job done to solve this problem.

I think there is going to be bipartisan belief that no woman who has a restraining order out should have to worry about web sites selling her private personal cell phone information so that someone could find out who she was calling and where she was going to be at a particular location. I think there will be bipartisan agreement that no detective sheriff ought to worry about his cell phone records to his informants getting into the hands of those he seeks to apprehend.

I think there is going to be bipartisan agreement that no individual should worry about folks finding out and being put on the Internet at some point, the doctors they have called, the psychiatrists they have called, friends and relatives they have called. This is going to be broad bipartisan consensus in this regard. To that end, Representative Blackburn and myself have introduced a bill, first one out of the chute, and we don't claim to have the only ideas about this, that will, in fact, drop a dime on these folks who are using pretext calling and not only that, our bill basically would stop four prohibited behaviors, which includes pretext calling, would also criminally penalize those accessing customer accounts via the Internet, which is also done. This can be done. People can ferret out your information over the Internet, as well; would criminally penalize soliciting someone to obtain records under false pretext and would criminally penalize selling phone records obtained under false pretext, penalties up to five years in prison, a $500,000 fine.

And also, something I think is important, I think the committee should consider is that when this occurs, there would be an obligation of the phone entity to, in fact, share information with the consumer when they have been victimized in this regard. It is important that that information to a consumer when this happens, that the victim know about it. Victims can be silent victims, but they shouldn't have to suffer in the darkness in this regard, particularly to stop identity theft. We have talked about various issues of law enforcement. This is a principal way of enhancing the ability to do identity theft, as well.

So I am looking forward to agreed bipartisan success here. I want to credit Jan Schakowsky for her early leadership on this. She was ahead of the curve, I think, months ago in this regard and Mr. Chair, I look forward to Working with you all. Thank you.

MR. STEARNS. I thank the gentleman. Mr. Ferguson.

MR. FERGUSON. Thank you, Mr. Chairman. I appreciate you holding this hearing. I am pleased that we have such distinguished witnesses and panelists and we certainly welcome back Mr. Largent to this committee. I am pleased, Mr. Chairman, that the committee is taking steps to ensure that personal phone records remain private. Maintaining the security of our personal phone records is of great importance and in data security, as well as in health, the adage an ounce of prevention is worth a pound of cure rings particularly true. With the expanding possibilities and conveniences of the Internet, we also face the expanding possibilities of identity theft and identity pretexting. While the ease of online banking and online mobile phone records makes managing our accounts easier, it also may grant easier access for unethical data brokers who would auction our personal information for their own gain.

But the price of convenience does not have to be insecurity. Working together with the telecommunications companies, the FTC and the FCC, Congress can develop effective measures to curtail pretexting and the unscrupulous dissemination of phone records. I urge this committee to consider legislation that will penalize those who sell illegally obtained phone records, as well as those who, from within telecommunications companies break company rules and give out sensitive information to anyone other than the account holder. It is amazing to me that anybody can get private telephone information, mobile phone information.

Over the recess, my wife asked me if I could call our cellular telephone company to make some changes to her account. So of course, we have four young kids at home. She has got a lot on her plate. I was happy to make the phone call on her behalf, so I am on the phone with the company, going through the various plans. She wanted to increase her monthly minutes, which I wasn't necessarily in favor of, but figured give her the benefit of the doubt. So I am speaking with the representative of our company on the phone and as we talked through her various options, we decided what we thought would be best, called to her in the other room, she said sounds good, I said okay, let us make the change and this person said well, I am sorry, you are not authorized to make changes on this account. So a person's spouse is not authorized to make changes on an account, yet someone who has no connection to an account holder, whatsoever, is able to obtain their information. It seems a little bit silly and in fact, dangerous.

My sense is that by empowering the FTC to enforce against phone record sales and pretexting, we can send a clear message to data brokers that if you compromise personal telephone records and information, you will be prosecuted. I look forward to hearing the testimony today from our witnesses and I hope that based on the information that they can provide that we can devise a substantive response to mobile phone record pretexting. Thank you, Mr. Chairman. I yield back.

MR. STEARNS. I thank the gentleman. Ms. Baldwin.

MS. BALDWIN. Thank you, Mr. Chairman. I want to thank the chairman and ranking member for holding this timely hearing on the practice of pretexting to obtain personal private cell phone records, and I want to echo my colleagues' concerns that pretexting not only violates a person's right to privacy, it also poses serious risks to victims of domestic violence and stalking, and to police officers who are engaged in undercover work. People are really aghast at the practice and use of pretexting in the wireless phone industry, and it is really up to this committee to end such practice once and for all.

In reviewing the written testimony provided to our committee, it is clear that various stakeholders agree that pretexting should be

punishable, but disagreements emerge over the method best to achieve the most comprehensive and effective protection of consumer privacy. Imposing penalties on the action of pretexters is certainly a necessary component of stemming the problem, but it is not the only one. This committee ought to also explore the possibility of updating existing laws, in particular, Section 222 of the Telecommunications Act of 1934 and Section 5 of the Federal Trade Commission Act to ensure that a market for pretexted cell phone records no longer exists.

Still, shutting down pretexting in one market is not going to prevent such a practice in another. It may even encourage it. I believe that pretexting in the wireless industry is only the tip of the iceberg and a comprehensive legislative approach is necessary to cover all sectors where the breach of personal data security is a possibility. At the very least, the punishment of pretexting should encompass the full spectrum of telecommunications and communication services, including records obtainable through calling cards, Internet web sites, and Internet telephony. The protection of consumers' fundamental right to privacy simply cannot rely on a patchwork of policy making.

In considering the proper legislative response to pretexting, I am cognizant of the efforts by wireless phone companies to police this situation and I applaud those efforts. To an extent, these cell phone companies are also victims of the deceptive and unethical behavior. However, I am convinced that relying on the free market forces alone to create the business incentives necessary to safeguard consumer privacy will amount to too little, too late. I also applaud the efforts by states, state governments, to protect their own citizens from this fraudulent behavior and I sincerely hope that this committee will not preempt the authority of State governments to enforce their own laws.

I applaud the bipartisan spirit in which this committee is working to address this problem. It is my understanding that the committee will examine and possibly mark up legislation in the coming weeks and I look forward to working to address this serious problem. Thank you, Mr. Chairman.

[The prepared statement of Hon. Tammy Baldwin follows:]

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

I want to thank the Chairman and Ranking Member for holding this timely hearing to examine the practice of "pretexting" to obtain personal, private cell phone records. I echo my colleagues' concerns that "pretexting" not only violates a person's right to privacy, it also poses serious risks to victims of domestic violence and stalking, and to police officers doing undercover work. People are aghast that the use of pretexting is actually legal in the wireless phone industry, and it is up to this Committee to end such practice once and for all.

In reviewing the witness testimonies provided to the Committee today, it is clear that various stakeholders agree on the criminalization of pretexting. But disagreements emerge over the methods to best achieve the most comprehensive and effective protection of consumer privacy. Imposing penalties on the action of "pretexters" is certainly a necessary component of stemming the problem, but it is not the only one. The Committee must be open and willing to look at updating existing laws, in particular Section 222 of the Telecommunications Act and Section 5 of the Federal Trade Commission Act, to ensure that a market for pretexted cell phone records no longer exists.

Still, shutting down pretexting in one market sector is not going to prevent such practice in another. It may even encourage it. I believe pretexting in the wireless industry is only the tip of an iceberg, and a comprehensive legislative approach is necessary to cover all sectors where the breach of personal data security is a possibility. At the very least the criminalization of pretexting should encompass the full spectrum of telecommunications and communication services, including records obtainable from calling cards, internet web sites, internet telephony. The protection of consumers' fundamental right to privacy simply cannot rely on patchwork policymaking.

In considering the proper legislative response to pretexting, I am cognizant of the efforts by wireless phone companies to police the situation, and I applaud their efforts. To an extent, the cell phone companies are also victims of a deceptive, unethical behavior. However, I am concerned that relying on the market forces alone to create the business incentives necessary to safeguard consumer privacy will amount to too little, too late. I also applaud the efforts by state governments to protect their own citizens from this fraudulent behavior, and I sincerely hope the Committee will not pre-empt the authority of state governments to enforce their own laws.

I applaud the bi-partisan spirit in which the Committee is working to address this serious problem. It is my understanding that the Committee will mark up legislation in the coming weeks, and I look forward to reviewing a draft text of the legislation and working with the Chair and Ranking Members of the Full and Subcommittees to address this serious problem.

Thank you Mr. Chairman for the time. I look forward to the testimonies.

MR. STEARNS. Thank the gentle lady. The gentle lady from Tennessee, Ms. Blackburn.

MRS. BLACKBURN. Thank you, Mr. Chairman. I want to thank the committee, also, for moving forward on this issue. I know that many of my colleagues have received numerous phone calls; we certainly have, on this issue. I also want to thank our witnesses for bearing with us this afternoon as we do have a busy day and being here to help us as we begin to work through the issue. As Mr. Inslee has said, we have presented one possible approach to solving this problem yesterday. We did introduce the Consumer Telephone Records Privacy Act of 2006. Currently, we have 21 cosponsors, both Democrat and Republican. As Ms. Baldwin very correctly said, this is something where you are going to see some bipartisan work, and I want to thank Mr. Inslee and his very capable staff for the leadership that they have put into this issue. I appreciate that they have moved forward so quickly with us on this.

The legislation is really relatively straightforward. Several provisions are modeled after the Gramm-Leach-Bliley provisions for obtaining

financial records and specifically, as Mr. Inslee said, the legislation prohibits someone from either obtaining or selling another person's telephone records under false pretext. Violations would be consider criminal offenses. They would carry prison time, heavy fines for individuals and companies. The FTC would enforce the Act, the FCC would issue regulations to ensure consumers are notified when their data has been disclosed.

I want to thank our chairman, also, for the work that he has done on the other data security issues. I think there is a lot of water to go under the bridge and a lot of work that needs to go into how we designate and identify electronic commerce, electronic records and how we make certain that consumers are protected in this new era. I look forward to continuing to work with the chairman, with my cosponsor, with Ranking Member Dingell on the issue and with that, I yield back.

MR. STEARNS. Mr. Wynn. Yield back. Mr. Terry. Waive. Mrs. Cubin.

MRS. CUBIN. I will submit mine.

[The prepared statement of Hon. Barbara Cubin follows:]

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

Thank you, Mr. Chairman.

I want to thank you for holding this timely hearing. Frankly, I've been taken aback about media reports of the illicit acquisition and sale of telephone records to third parties. The Internet has served as a magnfiying glass on all of our human traits – good and bad. While it provides nearly limitless information and educational opportunities, it also fills our homes and computers with smut, viruses, worms and spyware. Now we are learning how web-based companies are offering up our most private information for a hundred bucks.

Part of this Committee's job is to make certain the laws we pass are properly crafted to meet the needs of our constituents and society as a whole. And while Congress has acted in the past to strengthen the protections on a consumer's personally identifiable information, we are called to action again on this matter.

It seems to me that our expert agencies have been swift and diligent in their actions on the sale of phone records to those with questionable motives. I appreciate their work so far. But this problem involves more than agency action. We need to make pretexting, or the act of lying and cheating to get someone's information, illegal. Another step should be to empower consumers to bring them into this fight through some sort of notification process. Self-interest in the protection of ones privacy is an excellent check against the overly-broad availability of these records. How this will all look will be based on the input from our witnesses here today.

I look forward to hearing from both of our distinguished panels today and want to continue our dialog as we tackle legislation protecting American phone records.

MR. STEARNS. Okay. Mr. Radanovich, all right. Mr. Shimkus.

MR. SHIMKUS. Mr. Chairman, sorry. But I will be brief. I just want to welcome my Attorney General; she is on the second panel. It is good

to have you here and unfortunately, you have to listen to us as we wait to listen to you. She is also a new mother, a relatively new mother who has a ketchup bottle onezie from Collinsville, Illinois that we sent to her office and I hope her baby is wearing it proudly. And also on the second panel, I am sure he has been introduced already, Steve Largent, our former colleague, well respected on the Hill. We are glad to have you here, Steve. And I yield back my time.

MR. STEARNS. The gentleman yields back his time. Mr. Green.

MR. GREEN. Thank you, Mr. Chairman, and I will be as brief and again, like my colleagues, I want to welcome our former member of the committee, Steve Largent, back to us. I am glad our committee has moved swiftly on this and certainly, over the January break I heard from a lot of constituents at home when the publicity about people were being able to get their cell phone numbers and I want to thank our witnesses today, particularly our Chairman Martin and the FTC Chairman, Commissioner Leibowitz.

The amount of personal information floating around the Internet about all of us is staggering and this is just an example. Our committee has dealt with financial records, medical records, and our Data Privacy Bill, addressing credit records. Now we are faced with the unscrupulous Internet business of selling phone records to anyone, stalkers, identity thieves, abusive ex-spouses and any type of shady character--particularly get personal information on the Internet. I support regulatory action, private sector legal action, and the legislative efforts by this committee to stop pretexting for phone records. I am concerned, however, that every time we use our finger to plug a hole in the levy for one type of personal information, soon we find there is another leak and I am afraid we are running out of fingers.

Going after phone records may not be enough since these people are also selling the private personal information behind e-mail addresses and instant messenger paging. I think we need to look at a more comprehensive approach on privacy of personal information as opposed to reacting every new breach of privacy that makes the headlines. Relying on Section 5, covering unfair deceptive business practices at the Federal Trade Commission is probably not enough. As we have seen with credit information and now phone information, scattered privacy law specifically only to one type of information made the legal or semi-legal loopholes.

In any comprehensive privacy protection approach, we need the strong cooperation of the legitimate businesses that are on the front lines in protecting our information from bad actors.

Companies need to have the state-of-the-art privacy standards, but it is difficult for Congress to specify what these standards are for the state-

of-the-art protection has changed and criminal methods can change constantly. We must rely on the independent agencies like the FCC and the FTC to monitor what companies could do and what they are doing, but reliance only works when combined with oversight. For a comprehensive privacy framework, I think we need three things: empowering as many people as possible to do the enforcement with flexible tools to achieve that enforcement; educating and informing the public so they are not in the dark; and encouraging businesses that hold this personal information to continuously evolve better privacy protections. And with that, Mr. Chairman, I yield back my time and look forward to the hearing.

MR. STEARNS. Mr. Walden.

MR. WALDEN. Thank you very much, Mr. Chairman. I want to thank the full committee chairman for holding this hearing. I, like many Americans, became aware of this issue the last few months due to news reports and was greatly disturbed by what I heard and so I am delighted the committee is moving forward to plug this loophole, to close this process that allows people to snoop in my phone records and yours and every American's, find out who we are calling, when we are calling, why we are calling. This has to stop and so I look forward to the committee's action and leadership of the commission and the Congress to give Americans the security they want, the privacy that they deserve, and so I look forward to the hearing and I look forward to us acting expeditiously. Thank you, Mr. Chairman.

MR. STEARNS. Thank the gentleman. Mr. Ross.

MR. ROSS. Thank you, Mr. Chairman. The idea of individuals fraudulently representing themselves in order to obtain personal phone records that are then sold by numerous data brokers is quite frankly unacceptable. I received numerous calls from constituents who are outraged that their personal information is vulnerable and that they want to know what we, as elected officials, are going to do about it. I was shocked to learn that my fellow Arkansan, General Wesley Clark, a man who has served as a Supreme Allied Commander for NATO and a former presidential candidate, was a victim of this crime, or what should be a crime. I am deeply disturbed by this and believe it is imperative this committee addressed the issue of pretexting aggressively and effectively.

Companies that engage in pretexting, the practice of obtaining personal information under false pretenses, must be stopped. Their actions are not only an invasion of privacy, but have the potential to result in illegal activity or harm to others by those who obtain such records. As a former member of the House Financial Services Committee, the Gramm-Leach-Bliley Act explicitly prohibits pretexting of customer data from financial institutions. However, no such law

exists for phone records, and it should. Therefore, we must provide those who are responsible for protecting the information of consumers with the tools and resources needed to do their job.

I commend the efforts of the FFC and the FTC, using their respective authority to combat this illegal practice and I encourage their continued coordination. In Chairman Martin's earlier testimony, one of the actions he stated Congress could take to prevent data broker companies from selling consumers' phone records is to "specifically make illegal the commercial availability of consumers' phone records." I am a co-sponsor of legislation sponsored by our colleagues of this committee, Mrs. Blackburn and Mr. Inslee, to take several measures to stop phone record privacy invasions. This proposal is similar to legislation introduced in the Senate.

I also understand that the chairman, ranking member and others are working on legislation to address this problem. I welcome the opportunity to work with them, as well. I look forward to reviewing their product and working with them to end this practice and strengthen the security requirements for those who maintain this information.

Closing, I want to reiterate the importance of consumer confidence in our marketplace and the need to maintain it. Unless we do something to protect those we serve from unscrupulous acts, we risk jeopardizing their trust, which will lead to unfortunate consequences. Again, I thank the witnesses for their participation here today and I look forward to the testimony.

[The prepared statement of Hon. Mike Ross follows:]

PREPARED STATEMENT OF HON. MIKE ROSS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ARKANSAS

- Thank you Chairman Barton and Ranking Member Dingell for holding this important hearing today regarding the sale of personal phone records.
- The idea of individuals fraudulently representing themselves in order to obtain personal phone records that are then sold by numerous data brokers is unacceptable.
- I have received numerous calls from constituents who are outraged that their personal information is vulnerable and they want to know what we, as elected officials, are going to do about it.
- I was shocked to learn that my fellow Arkansan General Wesley Clark, a man who has served as the Supreme Allied Commander for NATO and a former Presidential candidate was a victim of this crime.
- I am deeply disturbed by this and believe it is imperative this Committee address the issue of pretexting aggressively and effectively.
- Companies that engage in pretexting—the practice of obtaining personal information under false pretenses, must be stopped.
- Their actions are not only an invasion of privacy but have the potential to result in illegal activity or harm to others by those who obtain these records.

- As a former member of the Financial Services Committee, the Gramm-Leach- Bliley Act explicitly prohibits pretexting of customer data from financial institutions. However, no such law exists for phone records.
- Therefore we must provide those who are responsible for protecting the information of consumers with the tools and resources needed to do their job.
- I commend the efforts of the FCC and the FTC using their respective authority to combat this illegal practice and I encourage their continued coordination.
- In Chairman Martin's testimony, one of the actions he stated Congress could take to prevent data broker companies from selling consumers' phone records is to "specifically make illegal the commercial availability of consumers' phone records."
- I am a cosponsor of legislation sponsored by our colleagues on this committee, Ms. Blackburn and Mr. Inslee that takes several measures to stop phone record privacy invasions. This proposal is similar to legislation introduced in the Senate.
- I also understand that the Chairman, Ranking Member, and others are working on legislation to address this problem. I look forward to reviewing their product and working with them to end this practice and strengthen the security requirements for those who maintain this information.
- In closing, I want to reiterate the importance of consumer confidence in our marketplace and the need to maintain it. Unless we do something to protect those we serve from unscrupulous acts, we risk jeopardizing their trust which will lead to unfortunate consequences.
- Again, I thank the witnesses for their participation and I look forward to the testimony.

MR. STEARNS. Thank you, Gentleman. Mr. Burgess, just on record, do you want to do an opening statement?

MR. BURGESS. Mr. Chairman, I will submit for the record, in the interest of hearing the witnesses.

MR. STEARNS. Okay, that is good. Mr. Gillmor.

MR. GILLMOR. Thank you, Mr. Chairman. I am going to enter my statement in the record, but I just want to say that shocking as this is, this is just one example of the large number of instances of misuse of individuals' personal data and I think it is vital that we protect our citizens against those who unconscionably traffic in other people's personal data. My personal view is that an individual's personal data is theirs and that nobody should be able to use it, particularly for profit, without the consent of the individual whose information is being conveyed and if that individual wants it, even compensation, so I hope we can elicit some indications of how we can deal with this problem and I thank you, Mr. Chairman.

[The prepared statement of Hon. Paul Gillmor follows:]

PREPARED STATEMENT OF HON. PAUL GILLMOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Thank you for holding this important hearing today. I applaud your efforts to tackle this, and other, important data security matters that lie before this committee in such a decisive manner.

As Americans' access to technology grows it is necessary that we ensure the safety and security of these new experiences. The advent of the digital age has brought new public policy concerns before this committee—such as the matter before us today—and in order to persuade consumers that these technologies are worthwhile they must be convinced that we have left no stone unturned when examining methods to ensure the privacy of their data. A failure on our part as stewards of the public and a failure by industry participants to provide adequate "safety nets" for their customers' information will result in our country falling further behind the global technological curve—resulting in potential devastating economic consequences.

Mr. Chairman, I also am concerned that the practice of "pretexting," if ignored, will become a resource for violent criminals. Recent media reports of victimization have made the American public more aware of the dangers that sexual predators pose to our country's families and all too often it is the details of a situation that are overlooked that lead to a very preventable disaster. As an advocate for more stringent sexual violence laws, I look forward to working with all of my colleagues on this committee to ensure that those seeking to locate a potential victim will have another avenue closed off to them. The implications of crafting a sound policy are real. Our efforts must compliment industry efforts to secure personally identifiable information by setting forth concrete penalties for those who attempt to unlawfully attain this private data—doing so might just help save a life.

Mr. Chairman, thank you again for holding this hearing today. I am confident that the testimony given by our witnesses will provide us with invaluable insight as we work to gain a better understanding of how much of a threat "pretexting" actually poses to American consumers and how best to address it in the forthcoming bipartisan legislation.

CHAIRMAN BARTON. Staff indicates the next member that seeks recognition is Mr. Gonzalez of Texas, is that correct? What about Ms. Baldwin, have you already done it? Okay, Mr. Stupak.

MR. STUPAK. Thank you, Mr. Chairman, and thanks for holding this hearing. I just came back from a hearing at Charity Hospital, which provides services down in New Orleans. As you know, this committee did an Oversight and Investigations hearing last week down in New Orleans, and we found there that since the hurricane of August 29th, Charity Hospital still has not been reimbursed by the Federal government to the tune of over $50 million, where they have failed to provide one penny for care for the people in New Orleans. Even though Charity Hospital is required to provide care, they are not being paid.

Mr. Chairman, I bring that up because maybe it is like Americans who have been under the misconception that their phone records are private. You provide medical services, you expect to get paid. You talk on your telephone, you believe your phone records are private. Many Americans have been shocked to learn recently that their phone records are, in fact, not private and may be bought for a mere $100. For a price, at least 40 websites today will help criminals, abusive spouses, employers and others obtain your personal cell phone records. It is called pretexting. Congress passed a law to make pretexting illegal in 1999. According to the Federal Trade Commission, this law covers phone records.

So why are people's private phone records being sold today? It seems to me that the FTC isn't enforcing the law and now Congress is going to have to act again to make sure it does. I want these rogue sites to understand with no uncertainty that what they are doing is probably illegal and will probably put them in great legal and financial jeopardy. But I would like to hear today from the Federal Communications Commission and the Federal Trade Commission about how long they have known about this problem and what exactly have they been doing to stop it. My question to us in the Federal government is why have these Internet sites been allowed to flourish?

I wish to hear from the phone companies about what safeguards they have in place to prevent these rogue actors from gaining the personal records of their clients. My question is, are the phone companies doing enough to protect the consumers? As a former law enforcement official, I understand investigators need tools to get their job done and there should be laws that should protect consumers and they should be enforced. The privacy of phone records is crucial for victims of domestic violence, police officers, judges, and public officials. Their personal safety may be placed at risk with the information obtained from their personal cell phone records. I urge this committee to act quickly and responsibly to pass comprehensive legislation to safeguard the privacy of consumers.

In addition, this committee must exercise its oversight authority to ensure that the Federal agencies are doing their jobs. We will hear lengthy testimony from the second panel about numerous instances where the FTC, in fact, knew there was a problem but did nothing. Passing another law will not help consumers if it is not enforced.

Finally, Mr. Chairman, I would be remiss without saying that the committee must address another consumer issue immediately and that is 41 million Americans who have been hung out to dry under the new Medicare Part D law. I have been contacted by far too many seniors whose costs have increased, whose medicines have been denied, whose coverage has lapsed, whose appeals have been denied and whose low-income applications have not been approved. Another crisis that is hitting seniors in my district this winter is the dramatic increase in home heating costs, which has overwhelmed their pocketbooks.

Mr. Chairman, we cannot deny that consumers of this great Nation face cell phone records being readily available to anyone, Part D Medicare prescription drugs not being available and home heating costs being unaffordable. Mr. Chairman, the American people expect the Energy and Commerce Committee, especially the Oversight and Investigations Subcommittee, to do its job. It is our responsibility to address these issues, and I stand ready to assist the American people, and

I hope the majority party will join me in trying to get to the bottom of these issues. Thank you, Mr. Chairman.

CHAIRMAN BARTON. Thank you, Congressman Stupak. Is there any member that has not had a chance to make an opening statement? Seeing no hands raised, the Chair would ask unanimous consent that all members not present be given the requisite number of days to include their opening statements in the record. Is there objection? Seeing none, so ordered.

[Additional statements submitted for the record follow:]

PREPARED STATEMENT OF HON. MARY BONO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Chairman Barton and Ranking Member Dingell, thank you and good afternoon. I would also like to extend a warm welcome to FCC Chairman Martin, FTC Commissioner Leibowitz, and other testifying panelists.

As members of this Committee know, the power of our nation's communications infrastructure and equipment are vital to our economic strength. The Internet based and telecommunications carrier industries are two integral components of this economic sector. Let there be no question, the health and integrity of these two industries are vital to continued economic growth and technological innovation.

That is why we must act swiftly and deliberately when individuals or entities threaten the integrity of these industries and the valuable services they provide. Imagine the consequences to our societies if a witness to a crime was afraid to make an anonymous call to law enforcement authorities to report a crime out of fear the criminals would track that caller down.

At the present moment, Section 5 of the FTC Act prohibits unfair or deceptive trade practices. Additionally, section 222 of the Communications Act of 1934 requires compliance by telecommunications carriers with customer proprietary network information (CPNI) obligations. It is the responsibility of the FCC and the FTC to help maintain the integrity of these two industries by bringing swift legal action to those who violate the law. Moreover, it is our responsibility as the legislative body to pass laws that provide such authority when it is not provided.

However, this responsibility is not the government's alone. The telecommunications carriers must do their part to protect the phone records of its customers from those who attempt to obtain those numbers fraudulently and illegally. With that said, it is important to remember that the focus needs to be kept on bringing those individuals and entities that commit fraud and break the law to justice.

I thank the Chairman for yielding and I yield back the balance of my time.

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

Chairman Barton, thank you for holding this hearing today. We all agree that pretexting is bad. Illegally obtaining or selling telephone records -- or any other sensitive personal information, for that matter -- poses a serious threat to American citizens. And we are talking about more than just embarrassment here. Pretexting poses serious risks, including possible injury or death to victims of domestic violence and stalking, and to law enforcement and homeland security personnel, especially those operating under cover. What is happening is a crime and we need to put a stop to it.

In that regard, I am pleased that we have both the Chairman of the Federal Communications Commission (FCC) and a Commissioner from the Federal Trade Commission (FTC) before us today. We need to get to the bottom of whether the laws that they administer are up to the task at hand. If not, we need to strengthen their statutes and require better coordination and cooperation between the two agencies in order to halt the outrageous and dangerous conduct that has been allowed to run rampant. If their respective statutes are deemed sufficient, then the question arises why have the FCC and the FTC not been more vigorous and timely in shutting down this threat?

Specifically, is Section 5 of the FTC Act sufficient to protect consumers against this deceptive activity? Likewise, does Section 222 of the Communications Act give the FCC enough authority to ensure that the carriers are properly protecting consumer telephone records? Every telecommunications carrier under the statute has "a duty to protect" their customers' information. That begs the question -- how effective are the FCC's rules? For example, FCC regulations require annual certifications regarding protection of telephone records by carriers. Yet, the FCC did not ask for a copy of the certifications until after this Committee's request. Perhaps that explains why 20 percent of the carriers were apparently not in compliance.

The use of pretexting to obtain consumer telephone records is not new. A Washington Post article dated July 8, 2005, was headlined "Cell Phone Records for Sale." But the FCC appears to have been in a blissful slumber until just recently. I would appreciate knowing whether the FCC audited a single carrier prior to Rep. Markey's November 7th letter.

The fact remains, if carriers collect information about consumers, it is the responsibility of carriers to protect that information, the FCC's job to ensure that the carriers are doing just that, and the FTC's role to enforce against those who fraudulently obtain such information. And it is this Committee's responsibility to conduct the oversight necessary to ensure that the agencies are doing their jobs.

Web sites offering phone records for sale are proliferating like cockroaches and are equally as unwelcome. I therefore look forward to receiving the testimony of all of our witnesses today on the nature and scope of the problem and on what we as the Committee of jurisdiction over both telecommunications and consumer protection should do about it.

Chairman Barton has called for bipartisan cooperation in crafting a legislative solution. I am happy to participate in that endeavor and I look forward to working with all of my colleagues on this issue.

PREPARED STATEMENT OF HON. RALPH HALL, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF TEXAS

Mr. Chairman, thank you for having this hearing today. I think it's important that we stay on top of ways to protect our constituents from unwanted intrusions into their lives. People will always be looking for new ways to make money, but doing so by acquiring personal information under false pretenses should not be one of them.

I was encouraged to read in our witness' testimony that the wireless and wireline companies take the issue of customer privacy very seriously and have as much reason to see pretexting end as we all do. I was also pleased to read that the FCC is making this a priority and that the FTC is investigating companies that engage in the practice. All of our witnesses' knowledge, expertise and desire to end pretexting is extremely beneficial as we go forward with this matter. I would like to thank our witnesses for being here and look forward to their oral testimony and the ensuing discussion.

PREPARED STATEMENT OF HON. C.L. "BUTCH" OTTER, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF IDAHO

Thank you, Mr. Chairman, for holding this hearing today to address this important issue and its alarming repercussions on privacy and personal security. I am looking forward to hearing from each of the witnesses to learn more about "pretexting" and how loopholes in the law are exploited by those with no regard for the privacy of personal information or the protection of due process.

As I have begun looking into this issue over the past few weeks, I have become increasingly concerned about the implications that this form of identity theft has on law enforcement, as private and public investigators purchase most of the private telephone records available for sale. It is no secret that I been a strong advocate for preserving the civil liberties protected by the Constitution and the due process outlined by our Founding Fathers. That law enforcement can, for a price, skirt around these protections and acquire this information without obtaining the warrant required by law causes me great consternation. In the same way, the practice of "pretexting" provides information to criminals and thugs that they can then use to undermine our system of justice or cause death and destruction.

Beyond these basic Constitutional concerns, I worry about the long-reaching consequences of this type of identity theft. I look forward to the testimony of these witnesses and the opportunity to have a frank and honest discussion regarding the best ways to protect personal information and privacy.

PREPARED STATEMENT OF HON. HILDA L. SOLIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

- Chairman Barton, Ranking Member Dingell, thank you for holding this hearing today to look into the practice of "pretexting."
- The right to privacy has long been held as one of the tenets of American democracy yet the practice of fraudulently purchasing personal phone records violates just that.
- As the Democratic Chair of the Bipartisan Congressional Caucus for Women's Issues and a long time advocate for the protection of victims of domestic violence, I am especially concerned about the ability of abusive spouses and stalkers to use phone records to track and harass their victims.
- Through this recent comprehensive reauthorization of the Violence Against Women Act, Congress has shown it is committed to addressing crimes such as violence against women and stalking as serious offenses.
- Pretexting is just another tool for these abusers.
- As this Committee considers legislation to make pretexting illegal, I hope it keeps in mind the need to protect these vulnerable communities.
- I want to thank our witnesses for testifying today and look forward to future action to protect our privacy and the rights of victims.

CHAIRMAN BARTON. We now want to welcome our first panel. We have the Honorable Kevin Martin, who is Chairman of the Federal Communications Commission, and the Honorable Jon Leibowitz, who is Commissioner of the Federal Trade Commission. Gentlemen, we welcome you, again, to the committee. We are going to start with you, Chairman Martin, and then Commissioner Leibowitz. We will recognize each of you for such time as you may consume, but hopefully, that will be less than seven or eight minutes. Mr. Martin.

STATEMENTS OF THE HONORABLE KEVIN J. MARTIN, CHAIRMAN, FEDERAL COMMUNICATIONS COMMISSION; AND JON LEIBOWITZ, COMMISSIONER, FEDERAL TRADE COMMISSION

MR. MARTIN. Thank you and good afternoon and thank you, Chairman Barton, and all the members of the committee. I appreciate the opportunity to speak to you all today about what appears to be an alarming breach of privacy of consumers' telephone records. The entire Commission is deeply concerned about the disclosure and sale of these personal telephone records. We will take strong enforcement action to address any noncompliance by telecommunications carriers with the customer proprietary network information, or CPNI, obligations contained in Section 222 of the Communications Act and the Commission's rules.

As the committee is aware, the issue of third parties, known as data brokers, obtaining and selling consumers' telephone call records is a tremendous concern for consumers, lawmakers and regulators alike. Determining how this violation of consumers' privacy is happening and addressing it is a priority for the Commission. We are taking several steps to combat the problem.

First, we are investigating the data brokers to determine how they are obtaining this information. Second, we are investigating the telecommunications carriers to determine whether they have implemented safeguards that are appropriate to secure the privacy of the personal and confidential data entrusted to them by American consumers. And third, we are initiating a proceeding to determine what additional roles the Commission should adopt to further protect consumers' sensitive telephone record data from unauthorized disclosure.

The issue of the disclosure and sale of consumer phone records was brought to the Commission's attention late last summer. On August 30th, the Electronic Privacy Information Center, EPIC, filed a petition expressing concern about the sufficiency of carrier privacy practices and the fact that online data brokers were selling consumers' private telephone data. The Commission's Enforcement Bureau began researching and investigating the practice of data brokers. This research culminated in the Commission issuing subpoenas to several of the most prominent data broker companies. These subpoenas sought details regarding how the companies obtained this telephone record information and contained further questions about the companies' sale of consumer call records.

Unfortunately, the companies failed to adequately respond. We issued letters of citation to these entities for failing to fully respond to a Commission order and referred the inadequate responses to the Department of Justice for enforcement. In addition, we subsequently served another approximately 30 data broker companies with subpoenas and are still awaiting their responses. In support of these investigations we have also made some undercover purchases of phone records from various data brokers. The purpose of this information is to assist us in targeting additional subpoenas and in determining, or trying to determine, the exact method by which consumer phone record data is being disclosed.

In conjunction with our investigation of data brokers, the Commission also focuses attention on the practices of telecommunications carriers. Specifically, in December, Commission staff began meeting with the major wireless and wireline providers to discuss the efforts they have undertaken to protect their confidential customer data and to prevent data brokers from obtaining and using such information.

In order to have carriers' responses in written form, we have also sent formal letters of inquiry to these carriers, and 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.

In addition, under the Commission's rules, a telecommunications carrier must have an officer of the company sign a compliance certificate on an annual basis stating that the officer has personal knowledge that the company has established adequate operating procedures. Earlier this week, the Enforcement Bureau issued Notices of Apparent Liability in the amount of $100,000 against AT&T and Alltel for their failure to adequately file or have on file such certifications. We also issued a notice requiring all telecommunications carriers to submit their most recent certification to us. To the extent that other carriers do not respond adequately, we are prepared to take appropriate enforcement action against them, as well.

Because this problem implicates the jurisdiction of both the FCC and the FTC, we have coordinated with FTC throughout this investigation. Beginning last summer, Commission staff and the FTC have been in regular contact regarding the sale of phone records by data brokers, and I met with Chairman Majoras late last year to address this issue, among others. Commission staff will continue to coordinate closely with FTC staff and share with them any evidence of fraudulent behavior that we detect in the course of our investigation. We have also responded to

several inquiries and provided guidance to individual State attorneys general and the National Association of Attorneys General.

And, as I mentioned previously, EPIC has filed a petition with the Commission raising concerns about the sale of calls. Several weeks ago I circulated an item to my fellow commissioners granting EPIC's petition and inviting comment on whether additional Commission rules are necessary to strengthen the safeguards of customer records. Specifically, we seek comment of EPIC's five proposals to address the unlawful and fraudulent release of CPNI, including consumer-set passwords, additional audit trails, encryption, limiting data retention and notice procedures to the customer on release of CPNI data.

In addition to these proposals, we also seek comment on whether carriers should be required to report further on the release of CPNI. Further, the item tentatively concludes that the Commission should require all telecommunications carriers to certify on a date certain each year that they have established adequate operating procedures. They would then need to file these certifications with the Commission. This item has been distributed to the Commission for their consideration and will be acted on by no later than February 10 of this year.

In addition to the Commission actions, several members have asked for the Commission's views on any potential changes to the law that could help combat this troubling trend. There are three primary actions that I believe Congress could take to help prevent data broker companies from selling consumer phone records. First, I believe Congress could specifically make illegal the commercial availability of consumers' phone records. Thus, if any entity is found to be selling this information for a fee, regardless of how it obtained such information, it would face liability.

Second, Congress could overturn the ruling of a Federal court that limited the Commission's ability to implement more stringent protection of consumer phone records. Specifically, when the Commission first implemented Section 222, it required carriers to obtain express consent from their customers, an opt-in requirement, before a carrier could use any customer phone records to market services outside the customer's existing service relationship with that carrier. The Commission held that this opt-in requirement provided consumers with the most meaningful privacy protection. In August of 1999 the 10th Circuit struck down these rules, finding that they violated the First and Fifth Amendments to the Constitution.

Required by the 10th Circuit to reverse its opt-in rule, the Commission adopted an opt-out approach. A customer's phone records may be used by carriers, their affiliates, agents and other partners that provide communications related services unless a customer expressly

withholds consent for such use. This ruling has resulted in a broader dissemination of consumer phone records and thereby may have contributed to the proliferation of the unlawful practices of data brokers that we are seeing today.

Third, I recommend that the Commission's enforcement tools be strengthened. For example, eliminating the citation requirement in Section 503(b) of the Act, which would enable us to more streamlined and effective enforcement. I also believe that we could raise the statutory maximum for forfeiture penalties that would assist the Commission in taking effective enforcement action. And additionally, the one year statute of limitations in Section 503 of the Communications Act for bringing action has been a source of difficulty at times.

The disclosure of consumers' private calling records is a significant privacy invasion. The Commission is taking numerous steps to try to address this practice as soon as possible. I look forward to working collaboratively with the members of this committee, other members of Congress, as well as my colleagues at the Commission and at the Federal Trade Commission, to ensure that consumers' personal phone data remains confidential. Thank you for the opportunity to testify and I look forward to answering your questions.

[The prepared statement of Kevin J. Martin follows:]

PREPARED STATEMENT OF HON. KEVIN J. MARTIN, CHAIRMAN, FEDERAL COMMUNICATIONS COMMISSION

Introduction

Good afternoon, Chairman Barton, Ranking Member Dingell, and members of the Committee. I appreciate the opportunity to speak with you today about what appears to be an alarming breach of the privacy of consumers' telephone records. The entire Commission is deeply concerned about the disclosure and sale of these personal telephone records and will take strong enforcement action to address any noncompliance by telecommunications carriers with the customer proprietary network information ("CPNI") obligations under section 222 of the Communications Act of 1934, as amended, (the Act) and the Commission's rules.

In my testimony, I will describe the Commission's current investigation into the procurement and sale of consumers' private phone records and the steps the FCC is taking to make sure that telecommunications carriers are fully meeting their obligations under the law to protect those records.

As the Committee is aware, the issue of third parties known as "data brokers" obtaining and selling consumers' telephone call records, which has been widely reported, is a tremendous concern for consumers, lawmakers, and regulators alike. Determining how this violation of consumers' privacy is happening and addressing it is a priority for the Commission. As outlined below, we are taking numerous steps to combat the problem. First, we are investigating the data brokers to determine how they are obtaining this information. Second, we are investigating the telecommunications carriers to determine whether they have implemented safeguards that are appropriate to secure the privacy of the personal and confidential data entrusted to them by American consumers. Third, we are initiating a proceeding to determine what additional rules the Commission

should adopt to further protect consumers' sensitive telephone record data from unauthorized disclosure.

Background

Numerous websites advertise the sale of personal telephone records for a price. Specifically, data brokers advertise the availability of cell phone records, which include calls to and/or from a particular cell phone number, the duration of such calls, and may even include the physical location of the cell phone. In addition to selling cell phone call records, many data brokers also claim to provide calling records for landline and voice over Internet protocol, as well as non-published phone numbers. In many cases, the data brokers claim to be able to provide this information within fairly quick time frames, ranging from a few hours to a few days.

The data brokers provide no explanation on their websites of how they are able to obtain such personal data.[1] There are several possible theories for how these data brokers are obtaining this information. These data brokers may be engaged in "pretexting," that is, obtaining the information under false pretenses – often by impersonating the account holder. In addition, they may be obtaining access to consumers' accounts online by overcoming carriers' data security protocols. To the extent this is the cause of the privacy breaches, we must determine whether this is in part due to the lack of adequate carrier safeguards. Finally, various telecommunications carriers could have "rogue" employees who are engaged in the practice of sharing this information with data brokers in exchange for a fee.

The mandate requiring telecommunications carriers to implement adequate safeguards to protect consumers' call records is found in section 222 of the Act. Congress enacted section 222 to protect consumers' privacy. Specifically, section 222 of the Act provides that telecommunications carriers must protect the confidentiality of customer proprietary network information. CPNI includes, among other things, customers' calling activities and history, and billing records. The Act limits carriers' abilities to use customer phone records even for their own marketing purposes without appropriate consumer approval and safeguards. Furthermore, the Act prohibits carriers from using, disclosing, or permitting access to this information without approval of the customer, or as otherwise required by law, if the use or disclosure is not in connection with the provided service.

When it originally implemented section 222, the Commission required telecommunications carriers to obtain express written, oral, or electronic consent from their customers, i.e., an "opt-in" requirement, before a carrier could use any customer phone records to market services outside the customer's existing service relationship with that carrier. The United States Court of Appeals for the Tenth Circuit (10th Circuit) struck down these rules finding that they violated the First and Fifth Amendments of the Constitution. Required by the 10th Circuit to reverse its "opt-in" rule, the Commission ultimately adopted an "opt-out" approach whereby a customer's phone records may be used by carriers, their affiliates, agents, and joint venture partners that provide communications-related services provided that a customer does not expressly withhold consent to such use.

The Commission must determine whether carriers are complying with their obligations under section 222. In order to make this determination, we are examining the

---

[1] The websites often contain statements that the information obtained is confidential and not admissible in court, and may specify that the purchaser must employ a legal avenue, such as a subpoena, for obtaining the data if t he purchaser intends to use the information in a legal proceeding.

methods that data brokers use to gain access to consumers' call records, and the methods employed by carriers to guard against such breaches.

Commission Investigation

The issue of the disclosure and sale of consumer phone records was brought to the Commission's attention late last summer. On August 30th, the Electronic Privacy Information Center (EPIC) filed a petition for rulemaking expressing concern about the sufficiency of carrier privacy practices and the fact that online data brokers were selling consumers' private telephone data. At this same time, the Commission's Enforcement Bureau began researching and investigating the practices of data brokers. This research culminated in the Commission issuing subpoenas to several of the most prominent data broker companies. These subpoenas, served in November 2005, sought details regarding how the companies obtained this phone record information and contained further questions about the companies' sale of consumer call records. Unfortunately, the companies failed to adequately respond to our request. As a consequence, we issued letters of citation to these entities for failing to fully respond to a Commission order and referred the inadequate responses to the Department of Justice for enforcement of the subpoenas. In addition, we subsequently served another approximately 30 data broker companies with subpoenas and are currently waiting for their response. Finally, in support of these investigations, we have made undercover purchases of phone records from various data brokers. The purpose of this information is to assist us in targeting additional subpoenas and in determining the exact method by which consumer phone record data is being disclosed.

In conjunction with our investigation of data brokers, the Commission also focused its attention on the practices of the telecommunications carriers subject to section 222. Specifically, in December and January, Commission staff met with the major wireless and wireline providers to discuss efforts they have undertaken to protect their confidential customer data and to prevent data brokers from obtaining and using such information. Discussions focused on the specific procedures employed to protect consumer call records from being accessed by anyone other than the consumers themselves. Staff also probed who within the companies has access to call record information and the procedures the carriers use to ensure that employees and other third parties with access to such information do not improperly disclose it to others. The carriers generally expressed their belief that the problems they have experienced in this area are largely, if not exclusively, related to attempts by individuals outside the company to obtain information through pretexting, rather than by "rogue" employees selling information to data brokers.

In order to have the carriers' responses in written form, last month, we sent formal Letters of Inquiry to these carriers. Inquiry letters are formal requests for information from carriers that may trigger penalties if not answered fully. 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.

In addition, under the Commission's rules, 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. In response to this Committee's letter, we asked the five largest wireline and wireless carriers to send us their CPNI certifications. Earlier this week, the Enforcement Bureau issued Notices of Apparent Liability in the amount of $100,000 against both AT&T and Alltel for failure to adequately respond to this request. We also issued a public notice requiring all telecommunications carriers to submit their most recent certification with us. To the extent that carriers are unable to do so, or do not respond adequately, we are prepared to take appropriate enforcement action against them as well.

Coordination with the FTC and State Attorneys General. Because this problem implicates the jurisdiction of both the FCC and FTC, we have coordinated with the FTC throughout our investigation. Beginning last summer, Commission staff and FTC staff have been in regular contact regarding the sale of phone records by data brokers. In addition, I met with Chairman Majoras late last year and discussed this issue, among others. Commission staff will continue to coordinate closely with the FTC staff and share with them any evidence of fraudulent behavior that we detect in the course of our investigation.

The FCC has also responded to several inquiries and provided guidance to individual state Attorneys General, and the National Association of Attorneys General (NAAG). As you are aware, a number of states, including Florida, Illinois, and Missouri have taken recent legal action against data brokers.

Commission's Efforts to Strengthen Existing CPNI Rules

As I mentioned previously, EPIC filed a petition with the Commission raising concerns about the sale of call records. Specifically, EPIC petitioned the Commission to open a proceeding to consider adopting stricter security standards to prevent carriers from releasing private consumer data. Several weeks ago, I circulated an item to my fellow Commissioners granting EPIC's petition and inviting comment on whether additional Commission rules are necessary to strengthen the safeguards for customer records. Specifically, we seek comment on EPIC's five proposals to address the unlawful and fraudulent release of CPNI: (1) consumer-set passwords; (2) audit trails; (3) encryption; (4) limiting data retention; and (5) notice procedures to the customer on release of CPNI data. In addition to these proposals, we also seek comment on whether carriers should be required to report further on the release of CPNI. Further, the item tentatively concludes that the Commission should require all telecommunications carriers to certify on a date certain each year that they have established operating procedures adequate to ensure compliance with the Commission's rules and file these certifications with the Commission.

This item has been distributed to the Commissioners for their consideration and will be acted on by February 10, 2006.

Legislative Assistance

In addition to the Commission's actions, several members have asked for the Commission's views on any potential changes to the law that could help combat this troubling trend. There are three primary actions that I believe Congress could take to prevent data broker companies from selling consumers' phone records. First, I believe that Congress could specifically make illegal the commercial availability of consumers' phone records. Thus, if any entity is found to be selling this information for a fee, regardless of how it obtained such information, it would face liability.

Second, Congress could overturn the ruling of a federal court that limited the Commission's ability to implement more stringent protection of consumer phone record information. Specifically, when the Commission first implemented section 222, it required carriers to obtain express written, oral, or electronic consent from their customers, i.e., an "opt-in" requirement before a carrier could use any customer phone records to market services outside the customer's existing service relationship with that carrier. The Commission held that this "opt-in" requirement provided consumers with the most meaningful privacy protection. In August of 1999, the 10th Circuit struck down these rules finding that they violated the First and Fifth Amendments of the Constitution. Required by the 10th Circuit to reverse its "opt-in" rule, the Commission adopted an "opt-out" approach whereby a customer's phone records may be used by carriers, their affiliates, agents, and joint venture partners that provide communications-related services provided that a customer does not expressly withhold consent to such use. This ruling

shifted the burden to consumers, requiring them to specifically request that their personal phone record information not be shared. This ruling has resulted in a much broader dissemination of consumer phone records and thereby may have contributed to the proliferation of the unlawful practices of data brokers that we are seeing today.

Third, I recommend that the Commission's enforcement tools be strengthened. For example, the need to issue citations to non-licensees before taking any other type of action sometimes hinders us in our investigations, and allows targets to disappear before we are in a position to take action against them. Eliminating the citation requirement in section 503(b) of the Act would enable more streamlined enforcement. In addition, I believe that raising maximum forfeiture penalties, currently prescribed by statute, would assist the Commission in taking effective enforcement action, as well as act as a deterrent to companies who otherwise view our current forfeiture amounts simply as costs of doing business. Further, the one-year statute of limitations in section 503 of the Communications Act for bringing action has been a source of difficulty at times. In particular, when the violation is not immediately apparent, or when the Commission undertakes a complicated investigation, we often run up against the statute of limitations and must compromise our investigation, or begin losing violations for which we can take action.

Conclusion

The disclosure of consumers' private calling records is a significant privacy invasion. The Commission is taking numerous steps to try to address practice as soon as possible. I look forward to working collaboratively with the members of this Committee, other Members of Congress, as well as my colleagues at the Commission and at the Federal Trade Commission 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.

CHAIRMAN BARTON. Thank you, Chairman. Now Commissioner Leibowitz.

MR. LEIBOWITZ. Thank you, Mr. Chairman, Ms. Schakowsky, Mr. Markey, members of the committee. I appreciate the committee's invitation to appear today with Chairman Martin to discuss the important topic of the privacy and the security of telephone records. I ask that the Commission's written statement be made part of the record and of course, my oral testimony and responses to questions reflect my own views and not necessarily the views of the Commission or of any other individual commissioner.

Let me start by making this absolutely clear. For the past several months, the FTC has been vigorously investigating companies that engage in the disturbing practice of selling consumers' telephone records. Indeed, maintaining the privacy and security of consumers' sensitive personal information is one of the Commission's highest priorities. It has been a mainstay of our consumer protection work in recent years as we have wrestled with issues ranging from spam to spyware to identity theft.

I would like to spend a minute or two describing the FTC's past efforts to protect consumers from pretexters, generally, and then I will

address the Commission's efforts to investigate the pretexting of telephone records, specifically.

The Commission filed its first pretexting case in 1999 against Touch Tone Information, which offered to provide consumers' bank or brokerage account numbers and balances to anybody for a fee. The FTC alleged that Touch Tone obtained these records from financial institutions by posing as the consumers whose records they were seeking. Under Section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices, the Commission charged that using such false pretenses was deceptive and that the sale of such information was unfair.

Later that year Congress enacted the Gramm-Leach-Bliley Act, which this committee was instrumental in authoring. As you know, the Act expressly prohibits pretexting for financial records. Shortly thereafter, the Commission launched Operation Detect Pretext. FTC staff sent warning letters to 200 firms that sold asset information to third parties. We also released a consumer alert. And we filed a trio of actions against information brokers who, posing as customers, called banks to obtain private account information. Since Gramm-Leach-Bliley's passage, the FTC has brought more than a dozen financial pretexting cases in various contexts.

The Commission has also challenged business practices that unreasonably expose consumer data to theft and to misuse. In fact, just last week, as you know, we announced a record breaking $15 million settlement against ChoicePoint, a data broker, which requires the company to implement much tougher security standards and procedures. The ChoicePoint settlement sends a strong signal to industry that it has to do a better job of safeguarding sensitive consumer information.

Now let me turn to telephone records. Disturbingly, a cottage industry of companies is peddling cell phone and landline records. Recent news stories report the easy purchase of phone logs of prominent figures, such as General Wesley Clark, as one of the members mentioned earlier, Mr. Ross. Although the acquisition of telephone records doesn't threaten immediate economic harm, the consequences could, nevertheless, be dire. Consider, for example, an abusive ex-husband trying to track down his estranged ex-wife or an ex-con trying to track down the law enforcement officer who put him in jail. But for most people, that is the 200 or so million cell phone users in the United States, the basic issue is this, as you pointed out, Mr. Chairman, and as Mr. Stearns did, too, in his opening statement: it is an intrusion into their personal privacy. They just don't want their private call records available to the public.

Moreover, it is far too easy to obtain this type of information. Here is what one web site offers and as Ms. Schakowsky pointed out, it's just

one of the dozens. I will just tell you about another one. If you provide them with a cell phone number, they will provide you with a list of outgoing calls, and they will do it in less than an hour. They will also provide the owner's name, billing address and home phone number.

The Commission has been actively investigating companies that obtain such information through pretexting. Commission investigators started by surfing Internet web sites for data brokers who sell consumers' phone records. Next, we identified appropriate targets for investigation and made undercover purchases. Commission attorneys are currently evaluating the evidence. Stay tuned, we hope to have an announcement for you very soon.

As you know, Gramm-Leach-Bliley does not prohibit pretexting for telephone records, but the Commission may bring an action against a telephone pretexter for unfair or deceptive practices, as we did in the Touch Tone case, as Mr. Markey noted earlier in his statement. What we can't do generally under the FTC Act, though, is seek civil penalties. Nor do we have jurisdiction over phone companies if they have inadequate safeguards. Having said that, we are working very closely with the FCC, which has jurisdiction over telecommunications carriers. Our two agencies are committed to coordinating our work here, as we have done successfully with enforcement of the Do Not Call program and the Do Not Call List.

Again, thank you for letting me testify. We look forward to working with the committee and its staff on this very important issue. Thank you.

[The prepared statement of Jon Leibowitz follows:]

PREPARED STATEMENT OF HON. JON LEIBOWITZ, COMMISSIONER, FEDERAL TRADE COMMISSION

I. Introduction

Mr. Chairman, Mr. Dingell, and members of the Committee, I am Jon Leibowitz, Commissioner of the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate the opportunity to discuss telephone records pretexting and the Commission's significant work to protect the privacy and security of telephone records and other types of sensitive consumer information. The Commission is currently investigating companies that offer consumer telephone records for sale, and we plan to pursue these investigations vigorously.

Maintaining the privacy and security of consumers' personal information is one of the Commission's highest priorities. Companies that engage in pretexting – the practice of obtaining personal information, such as telephone records, under false pretenses – not only violate the law, but they undermine consumers' confidence in the marketplace and in the security of their sensitive data. While pretexting to acquire telephone records has recently become more prevalent, the practice of pretexting is not new. The Commission

[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.

has used its full arsenal of tools to attack scammers who use fraud to gain access to consumers' personal information.

Aggressive law enforcement is at the center of the FTC's efforts to protect consumers' sensitive information. The Commission has taken law enforcement action against companies allegedly offering surreptitious access to consumers' financial records, and will continue to challenge business practices that unnecessarily expose consumers' sensitive information. The Commission also continues to provide consumer education and outreach to industry to ensure that the marketplace is safe for consumers and commerce.[2]

Today I will discuss the FTC's efforts to protect consumers from firms engaged in pretexting and the practice of pretexting for telephone records.[3]

II. FTC Efforts to Protect Consumers From Firms That Engage in Pretexting

The Commission has a history of combating pretexting. Using Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce,"[4] the Commission has brought actions against businesses that use false pretenses to gather financial information on consumers. In these cases, we have alleged that it is a deceptive and unfair practice to obtain a consumer's financial information by posing as the consumer.

The Commission's first pretexting case was filed against a company that offered to provide consumers' financial records to anybody for a fee.[5] According to our complaint, the company's employees obtained these records from financial institutions by posing as the consumer whose records it was seeking. The complaint charged that this practice was both deceptive and unfair under Section 5 of the FTC Act.[6]

In 1999, Congress passed the Gramm-Leach-Bliley Act ("GLBA"), in large part through the efforts of this Committee. The GLBA provided another tool to attack the unauthorized acquisition of consumers' financial information.[7] Section 521 of the Act directly prohibits pretexting of customer data from financial institutions. Specifically, this provision prohibits "false, fictitious, or fraudulent statement[s] or representation[s] to an officer, employee, or agent of a financial institution" to obtain customer information of a financial institution.[8]

---

[2] For example, the Commission recently launched OnGuard Online, a campaign to educate consumers about the importance of safe computing. *See* www.onguardonline.gov. One module offers advice on avoiding spyware and removing it from computers. Another module focuses on how to guard against "phishing," a scam where fraudsters send spam or pop-up messages to extract personal and financial information from unsuspecting victims. Yet another module provides practical tips on how to avoid becoming a victim of identity theft. These materials are additions to our comprehensive library on consumer privacy and security. *See* www.ftc.gov/privacy/index.html.

[3] Pretexting is not the only way to obtain consumers' telephone records, however. Such records also reportedly have been obtained by bribing telephone company employees and hacking into telephone companies' computer systems. *See, e.g.,* Jonathan Krim, *Online Data Gets Personal: Cell Phone Records for Sale*, Wash. Post, July 13, 2005, *available at* 2005 WLNR 10979279; *Simple Mobile Security for Paris Hilton*, PC Magazine, Mar. 1, 2005, *available at* 2005 WLNR 3834800.

[4] 15 U.S.C. § 45(a).

[5] *FTC v. James J. Rapp and Regana L. Rapp, d/b/a Touch Tone Information, Inc.*, No. 99-WM-783 (D. Colo.) (final judgment entered June 22, 2000). *See* http://www.ftc.gov/os/2000/06/touchtoneorder.

[6] 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. 15 U.S.C. § 45(n).

[7] *Id.* §§ 6801-09.

[8] *Id.* _ 6821.

To ensure awareness of and compliance with the new anti-pretexting provisions of the GLBA, the Commission launched Operation Detect Pretext in 2001.[9] 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 spot 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 provided information about how to comply with the law.[10]

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.[11] The alert warns consumers not to provide personal information in response to telephone calls, email, or postal mail, and advises them to review their financial statements carefully, to make certain that their statements arrive on schedule, and to add passwords to financial accounts.

While consumer education is important, it is only part of the FTC's efforts to combat pretexting. Aggressive law enforcement is critical. The FTC therefore followed up the first phase of *Operation Detect Pretext* in 2001 with a trio of law enforcement actions against information brokers.[12] 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. The FTC alleged that the defendants or persons they hired called banks, posing as customers, to obtain balances on checking accounts.[13]

The FTC's complaints alleged that the defendants' conduct violated the anti-pretexting prohibitions of the GLBA, and further was unfair and deceptive in violation of Section 5 of the FTC Act. 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.[14]

Because the anti-pretexting provisions of the GLBA provide for criminal penalties, the Commission also may refer pretexters to the U.S. Department of Justice for criminal

---

[9] *See* 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. For more information about the cases the Commission has brought under Section 521 of the GLBA, see http://www.ftc.gov/privacy/privacyinitiatives/pretexting_enf. Since GLBA's passage, the FTC has brought over a dozen cases alleging violations of Section 521 in various contexts.

[10] *See* FTC press release "FTC Kicks Off Operation Detect Pretext" (Jan. 31, 2001), *available at* http://www.ftc.gov/opa/2001/01/pretexting.htm.

[11] *See* http://www.ftc.gov/bcp/conline/pubs/credit/pretext.htm.

[12] *FTC v. Victor L. Guzzetta, d/b/a Smart Data Systems*, No. CV-01-2335 (E.D.N.Y.) (final judgment entered Feb. 25, 2002); *FTC v. Information Search, Inc., and David Kacala*, No. AMD-01-1121 (D. Md.) (final judgment entered Mar. 15, 2002); *FTC v. Paula L. Garrett, d/b/a Discreet Data Systems*, No. H 01-1255 (S.D. Tex.) (final judgment entered Mar. 25, 2002).

[13] In sting operations set up by the FTC in cooperation with banks, investigators established dummy bank account numbers in the names of cooperating witnesses and then called defendants, posing as purchasers of their pretexting services. In the three cases, an FTC investigator posed as a consumer seeking account balance information on her fiancé's checking account. The defendants or persons they hired proceeded to call the banks, posing as the purported fiancé, to obtain the balance on his checking account. The defendants later provided the account balances to the FTC investigator.

[14] *See* http://www.ftc.gov/opa/2002/03/pretextingsettlements.htm.

prosecution, as appropriate. One such individual recently pled guilty to one count of pretexting under the GLBA.[15]

Finally, the Commission is aware that it is not enough to focus on the purveyors of illegally obtained consumer data. It is equally critical to ensure that entities that handle and maintain sensitive consumer information have in place reasonable and adequate processes to protect that data. Accordingly, the Commission has challenged data security practices as unreasonably exposing consumer data to theft and misuse.[16] Companies that have failed to implement reasonable security and safeguard processes for consumer data face liability under various statutes enforced by the FTC, including the Fair Credit Reporting Act, the Safeguards provisions of the GLBA, and Section 5 of the FTC Act.[17]

In fact, last week the Commission announced a record-breaking proposed settlement with data broker ChoicePoint, Inc. This proposed settlement requires ChoicePoint to pay $10 million in civil penalties and $5 million in consumer redress to settle charges that its security and record-handling procedures violated the Fair Credit Reporting Act and the FTC Act. In addition, the proposed settlement requires ChoicePoint to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive information security program, and to obtain audits by an independent third-party security professional every other year until 2026. Further, the proposed settlement sends a strong signal to industry that it must maintain reasonable procedures for safeguarding sensitive consumer information and protecting it from data thieves.

III. Pretexting for Consumers' Telephone Records

An entire industry of companies offering to provide purchasers with the cellular and land line phone records of third parties recently has developed. Recent press stories report on the successful purchase of the phone records of prominent figures.[18] Although the acquisition of telephone records does not present the opportunity for immediate financial harm as the acquisition of financial records does, it nonetheless is a serious intrusion into consumers' privacy and could result in stalking, harassment, and embarrassment.[19] Although pretexting for consumer telephone records is not prohibited

---

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

[16] In addition to law enforcement in the data security area, the Commission has provided business education about the requirements of existing laws and the importance of good security. *See, e.g.,* Safeguarding Customers' Personal Information: A Requirement for Financial Institutions, *available at* http://www.ftc.gov/bcp/conline/pubs/alerts/safealrt.htm.

[17] *United States v. ChoicePoint, Inc.* (N.D. Ga.) (complaint and proposed settlement filed on Jan. 30, 2006 and pending court approval); *In the Matter of BJ's Wholesale Club, Inc.,* FTC Docket No. 042-3160 (Sept. 20, 2005); *In the Matter of DSW, Inc.,* FTC Docket No. 052-3096 (proposed settlement posted for public comment on Dec. 1, 2005); *Superior Mortgage Corp.*, FTC Docket No. C-4153 (Dec. 14, 2005). As the Commission has stated, an actual breach of security is not a prerequisite for enforcement under Section 5; however, evidence of such a breach may indicate that the company's existing policies and procedures were not adequate. It is important to note, however, that there is no such thing as perfect security, and breaches can happen even when a company has taken every reasonable precaution. *See* Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft (June 16, 2005) at 6, *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

[18] News stories state that reporters obtained cell phone records of General Wesley Clark and cell phone and land line records of Canada's Privacy Commissioner Jennifer Stoddart. *See, e.g.,* Aamer Madhani and Liam Ford, *Brokers of Phone Records Targeted*, Chicago Trib., Jan. 21, 2006, *available at* 2006 WLNR 1167949.

[19] Albeit anecdotal, news articles illustrate some harmful uses of telephone records. For example, data broker Touch Tone Information Inc. 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 police officers and their families. *See, e.g.,* Peter Svensson,

by the GLBA, the Commission may bring a law enforcement action against a pretexter of telephone records for deceptive or unfair practices under Section 5 of the FTC Act.[20]

The Commission is currently investigating companies that appear to be engaging in telephone pretexting. Using the approach that proved successful in *Operation Detect Pretext*, Commission staff surfed the Internet for companies that offer to sell consumers' phone records. FTC staff then identified appropriate targets for investigation and completed undercover purchases of phone records. Commission attorneys currently are evaluating the evidence to determine if law enforcement action is warranted.

In addition, the FTC is working closely with the Federal Communications Commission, which has jurisdiction over telecommunications carriers subject to the Communications Act.[21] Our two agencies are committed to coordinating our work on this issue, as we have done successfully with the enforcement of the "National Do Not Call" legislation.[22]

IV. Conclusion

Protecting the privacy of consumers' data requires a multi-faceted approach: coordinated law enforcement by government agencies as well as action by the telephone carriers, outreach to educate consumers and industry, and improved security by record holders are essential for any meaningful response to this assault on consumers' privacy. Better security measures for sensitive data will prevent unauthorized access; aggressive and well-targeted law enforcement against the pretexters will deter others from further invasion of privacy; and outreach to consumers and industry will provide meaningful ways to avoid the harm to the public.

Calling Records Sales Face New Scrutiny, Wash. Post, Jan. 18, 2006, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2006/01/18/AR2006011801659.html.

[20] Under Section 13(b) of the FTC Act, the Commission has the authority to file actions in federal district court against those engaged in deceptive or unfair practices and obtain injunctive relief and other equitable relief, including monetary relief in the form of consumer redress or disgorgement of ill-gotten profits. However, the FTC Act does not authorize the imposition of civil penalties for an initial violation, unless there is a basis for such penalties, i.e., an applicable statute, rule or litigated decree.

[21] 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. Moreover, the FTC's governing statute specifically states that the Commission lacks jurisdiction over common carrier activities that are subject to the Communications Act. 15 U.S.C. § 46(a). The Commission opposed this jurisdictional gap during the two most recent reauthorization hearings. *See* http://www.ftc.gov/os/2003/06/030611reauthhr.htm; *see also* http://www.ftc.gov/os/203/06/030611learysenate.htm; http://www.ftc.gov/os/2002/07/sfareauthtest.htm.

[22] In addition, the Attorneys General of Florida, Illinois, and Missouri recently sued companies allegedly engaged in pretexting. *See* http://myfloridalegal.com/__852562220065EE67.nsf/0/D510D79C5EDFB4B98525710000Open&Highlight=0,telephone,records; http://www.ag.state.il.us/pressroom/2006_01/20060120.html; http://www.ago.mo.gov/newsreleases/2006/012006b.html. Several telecommunications carriers also have sued companies that reportedly sell consumers' phone records. According to press reports, Cingular Wireless, Sprint Nextel, T-Mobile, and Verizon Wireless have sued such companies. *See, e.g.,* http://www.upi.com/Hi-Tech/view.php?StoryID=20060124-011904-6403r; http://www.wired.com/news/technology/1,70027-0.html; http://news.zdnet.com/2100-1035_22-6031204.html.

The Commission has been at the forefront of efforts to safeguard consumer information and is committed to continuing our work in this area. We also are committed to working with this Committee to provide greater security and privacy for American consumers.

CHAIRMAN BARTON. Thank you, Commissioner, and the chair recognizes himself for the first five minute question round. Neither of you indicated in your opening statements the scope of this problem. Do either of you have information about the number or the volume of instances in the aggregate, or the volume of calls that have been sold without the real phone holder's permission? Either one.

MR. MARTIN. No. No, we don't at the FCC.

MR. LEIBOWITZ. I know from, I believe, the EPIC petition that there are at least 40 telephone pretexters out there. We think there are probably considerably more companies that are doing it. A lot of them are small, they are bottom feeders, but we don't have information about how many people's numbers.

CHAIRMAN BARTON. We don't know the number or the volume of the financial impact or anything like that, we just know that it is a problem?

MR. LEIBOWITZ. We know it is a big problem.

CHAIRMAN BARTON. Okay.

MR. LEIBOWITZ. And we have investigations open.

CHAIRMAN BARTON. Do you both agree that it is a growing problem?

MR. MARTIN. Yes. I think that it is a growing problem and it has become more and more of a problem for consumers.

MR. LEIBOWITZ. I agree with Chairman Martin.

CHAIRMAN BARTON. Okay. You alluded, Chairman Martin, to some things that needed to be done or could be done. Could you again reiterate any additional, also Commissioner Leibowitz, statutory authority that your agencies would like to have to address this problem, that we can make changes in the Federal law?

MR. MARTIN. Well, as I mentioned in my opening statement, I think that the most direct way to address this problem would be a change that would prohibit the commercial sale of peoples' phone records so that the question wouldn't be whether or not they had been obtained through a pretext or through a fraudulent means, but rather that the law would just outright prohibit the sale of consumers' individual personal phone records. So I think that would be the easiest change to address that. As far as additional tools, I think that the Commission could have some additional enforcement tools, as I mentioned, both increasing some of its fining authority -- particularly for those who are not common carriers, and increasing, for example, its subpoena power for people that aren't

common carriers -- or licensees of the Commission. We are only allowed to ask for documents; we are not allowed to ask for oral testimony from any individual. So those are some of the examples that I think that we could use within the FCC.

CHAIRMAN BARTON. Okay. Mr. Leibowitz?

MR. LEIBOWITZ. Well, I agree generally with Chairman Martin. Under Section 5 of the FTC Act we can go after pretexters and even beyond telephone pretexters, but if you had a statutory prohibition, I think that would send a very, very strong signal. That is sort of what you did with Gramm-Leach-Bliley for financial pretexting. Beyond that, if you give us civil penalty authority, we will use it effectively, as you did with the Can Spam Act and as you would do with your spyware legislation. And then finally, although we are working very closely with the FCC on these investigations, if we go after a telephone pretexter, obviously, the information came from somewhere – that's how the pretexter had it. It didn't fall into his lap like manna from heaven. And because of the common carrier exemption, our investigation has to stop at the door of the telephone company, at least with respect to whether they have adequate safeguards.

CHAIRMAN BARTON. Okay. My last question, Commissioner Martin, you alluded to the court case that overturned the Commission regulation, or the Commission ruling about opt-in, and in order to release these records, you had to go and actually get permission from the phone user to release it. You mentioned that the court ruled that your rule, the Commission rule, was in violation of, I think you said the First Amendment and the Fifth Amendment to the Constitution. Would the same charge be leveled if we put it in the statutory authority as opposed to a Commission rule, that we required an opt-in?

MR. MARTIN. The court actually said that there hadn't been specific Congressional findings, that there had been a sufficient harm to overcome the presumption so that in our interpretation of the Congressional statute, it would raise a significant First Amendment issue. Therefore, we weren't entitled to deference, as we normally would be in an agency action. I think if Congress were taking some more specific action based upon a finding that there was specific harm, I think it would have the potential to overcome the First Amendment concerns. But the Commission's ruling wasn't afforded any deference on that issue, at least as the 10th Circuit had interpreted.

CHAIRMAN BARTON. Well, it is a moot point if we just outlaw it. If we just say you can't do it, then you don't have to opt into anything because there is nothing to opt in to. But if we don't want to go that far, I would think an opt-in requirement would be very necessary, so I was

concerned about that. My time is expired. We would now yield to the gentlelady from Chicago, Ms. Schakowsky, for five minutes.

MS. SCHAKOWSKY. Thank you. Mr. Martin, how currently does the consumer know anything about opt-in, opt-out? I mean, until this story broke, I never knew that there were options. How is that communicated and how would someone exercise that option right now with what we have?

MR. MARTIN. Well, there are two different issues that I was hearing involved in your question. One is whether or not the telephone companies are able to use any information about you in their marketing of their commercial services or the commercial services of their affiliated companies. And, in that sense, they are not allowed to do that unless they have gotten your permission. And they can, but they can send you a notice. Currently under the law, they can send you a notice and say that if you don't want that information to be used by one of their affiliated companies, then you can opt out of that, but--

MS. SCHAKOWSKY. Are they doing that? I mean, I--you know, we get all kinds of privacy--unintelligible mail about privacy policies and am I getting a mailing about what you just said? Is it possible that I got one?

MR. MARTIN. Yes, you probably--

MS. SCHAKOWSKY. I probably did.

MR. MARTIN. You probably did get one. There have been a very few instances in which companies have potentially not provided that opt-out. In those instances, sometimes they have been actually self-disclosed by a few of the companies and we have investigated those and have consent decrees when companies haven't provided that. But in the vast majority of circumstances, they have provided those opt-outs. But the pretexting problem is significantly different. This is where someone is pretending that they are you and getting that information, so there is no opt-in or opt-out at issue in that sense. So the pretexting problem raises a fundamentally different issue of whether or not people are actually posing as you in a fraudulent manner and then getting that information, so whether there was an opt-in or an opt-out in that sense, it wouldn't end up addressing just the pretexting problem. It does address how far and wide the information is disseminated, including to other companies.

MS. SCHAKOWSKY. And I am, of course, interested and have a bill in to deal with the pretexting issue, but I just want to make the point that while we try diligently to provide all these protections for consumers, that often they are so lost in, you know, as junk mail, or if you get it, it is really hard to understand exactly the consequences of what they are saying or what they are saying, at all. And I think that, you know, while we may think we are doing a good thing and a consumer service, it is

very hard to understand, so let me ask Commissioner Leibowitz a question. How is having the explicit authority to pursue pretexting for phone records? Is that--how would that help you to do your work?

MR. LEIBOWITZ. Well, I think it would send an unambiguous signal to the marketplace that this is absolutely illegal. We don't have to use our general statute, which is the FTC Act Section 5. And then if you gave us civil penalty authority--and I haven't looked at your bill, yet--but if you gave us civil penalty authority, we will enforce that vigorously. We don't have civil penalty authority in most circumstances under Section 5.

MS. SCHAKOWSKY. You said the pretexting for financial issues, that there were 12 cases. It didn't sound like a lot to me since 1999. Is it because this was so effective that they just stopped doing it or that--

MR. LEIBOWITZ. I would like to say that is true.

MS. SCHAKOWSKY. Uh-huh.

MR. LEIBOWITZ. But, you know, we are a small agency with a big mission and we think 12 cases is pretty significant and we think it has had an effect on the marketplace. We have also brought, during that time or in recent years, 80 spam cases, which is also about consumer security and privacy. We have brought a half dozen spyware cases in the last year alone and those are very difficult to bring. We have brought ten data security cases, as well. And so we are trying our best and we are concentrating on it and we do believe that the specificity has helped.

MS. SCHAKOWSKY. In other words, though, the passage of even this legislation--I was hoping you would say that, you know, the law was so effective that that problem doesn't exist anymore. We are still going to be facing, then, the capacity issue of protecting consumers?

MR. LEIBOWITZ. We will face a capacity issue and you know, malefactors are very, very innovative. They find ways to go around the law and they find ways to violate the law. But having said that, specificity helps. And, speaking for myself, and of course, I will go back and talk to the other commissioners. We are a consensus driven body, but speaking for myself, I think a specific law would be very helpful.

MS. SCHAKOWSKY. And would it not also, then, be helpful to hear the next panel for State attorneys general to get involved in this issue and help us out?

MR. LEIBOWITZ. State attorneys general are very helpful in many of the law enforcement actions we bring. The Attorney of Illinois, who is here, has brought a case. So too, I think, has the attorney general from Missouri. We work with the attorneys general all the time and they are terrific law enforcement partners.

MS. SCHAKOWSKY. Great, thank you.

CHAIRMAN BARTON. Mr. Deal.

MR. DEAL. Thank you, Mr. Chairman. Mr. Leibowitz, with regard to the pretexting violators, are many of these offshore, in other countries? And if so, does that present any particular problems to you and how do you deal with those that may be offshore?

MR. LEIBOWITZ. Well, I can't speak to where--publicly, to where these pretexters are, but we do know that many of the malefactors engage in spyware offshore -- it is over a third. In spam it is over half that are offshore. And we have a problem because of an anomaly in the law; we have no cross-border fraud authority to share information with our law enforcement partners overseas, so it makes it very difficult to do investigations. The Senate Commerce Committee passed a bill to close that loophole in the law and I know that this committee is looking at it, too.

MR. DEAL. Okay. With regard to the information that is being shared, is it something that you can definitively show has had economic effects, adverse economic effects on the individuals whose numbers are being sold and given to people, or is it simply a privacy issue alone? And is it essential to prove the former as a prerequisite to making whatever we do meet Constitutional muster?

MR. LEIBOWITZ. Well, from my perspective, I think it is a combination of both. It is about protecting privacy, it is about the economic harm and consequences that might result from this information being given to someone inappropriate. It is really about the danger that could happen or that someone could be put in through pretexting telephone information, which leads to addresses. And from our perspective, as long as there is harm to consumers, we believe that we can go with existing law after the malefactors. Having said that, if you give us a more specific law, we will use it and try to use it effectively.

MR. DEAL. It would seem to me that the more direct approach would be, as has been talked about here, just simply making it unlawful to sell these numbers. With regard to the 10th Circuit case, the chairman has already asked what would be required and whether or not certain proof would be required to be shown there. What would be a prerequisite to make that statute stronger other than a Congressional finding of certain facts? Is that the primary thing that would bolster just an outright prohibition?

MR. MARTIN. Yes, I think it would be finding of certain facts, obviously in talking about both the difficulty and the prevalence of it and the harm that it would be having, whether it was economic harm or other issues that have been raised by individuals about the disclosure of that private information. But it would be just the potential harm that the consumers would face by it.

MR. DEAL. Is there any proprietary interest in these numbers that can legitimately be advanced as an argument against an outright prohibition? A proprietary interest by any of the ones who might possess these numbers in a legitimate fashion, so that would prohibit them from--if it is a proprietary interest in their behalf to prohibit them to do something with it, is there a problem there?

MR. MARTIN. I will let the carriers on the second panel speak to it directly. They certainly have advocated in the past before the Commission concerns about being able to continue to use that information, at least themselves. I don't know if they would advocate that their proprietary interest would extend to being able to sell it to others if they so wanted. They have said that they would want to be able to use it, for example, for cross-marketing purposes, which is the original purpose some of these restrictions were put in place. I don't know if they would advocate that and I don't believe they have in front of the Commission. You would have to ask them.

MR. LEIBOWITZ. And if I could add to Chairman Martin's comments. You could take the same approach you did with Gramm-Leach-Bliley, which is you prohibit certain activities, financial pretexting, and then you make exceptions where appropriate.

MR. DEAL. Okay. I yield back, Mr. Chairman.

CHAIRMAN BARTON. The gentleman from Massachusetts, Mr. Markey.

MR. MARKEY. Thank you, Mr. Chairman, and we thank both of you today and your agencies' work on this issue. Do either of you know what percent of Americans have exercised their right to opt out of the sale of their information?

MR. MARTIN. I don't know. I know that in 1999 in the court case, we actually referenced a study that had been done in which only, I believe, 28 percent of the people had actually allowed for their records to be shared. The court said that, despite the study that we submitted, that was insufficient evidence that people didn't want their information being shared.

MR. MARKEY. Mr. Leibowitz, do you know any--

MR. LEIBOWITZ. I will defer to Chairman Martin, who is the expert on common carriers.

MR. MARKEY. I have got a telephone company's notice here that we all received at each of our homes, all 300 million of us in America are in it, and this notice comes to us as customer proprietary network information special notice and then it explains to each of us, in our little phone bill, what our rights are and if you don't respond in 30 days, you have lost your rights. So how many people threw this away? What percentage of all Americans? Can we do a survey of that, you know, in

the first instance? So this isn't really clear. There is no real attempt to communicate that you will lose your privacy, we will be able to sell this to anyone we want to and we should just, you know, deal with the fundamental problem here, that people don't want their information sold. So let me just clarify, so we get each agency's view on this. Should we just ban the commercial availability of phone records, period? Mr. Martin.

MR. MARTIN. Yes, I have said I think that would be the easiest way to end up addressing this problem.

MR. MARKEY. Thank you. Mr. Leibowitz.

MR. LEIBOWITZ. And I have to go back to the Commission, obviously, to discuss that with them, but from my own perspective, I think that would be very useful. Again, looking at whether there are some exceptions for law enforcement purposes that might be permissible.

MR. MARKEY. Okay, that is the bottom line on your testimony and I think our committee will take that to heart. Chairman Martin, in 1999 the 10th Circuit issued a decision that forced the FCC to adjust the standard for consumer approval of a telephone company's disclosure of their customer proprietary network information, which includes consumer phone records and doing so, the Commission adopted rules allowing telephone companies to disclose CPNI to their own affiliates under a so-called opt-out standard. An opt-out standard means the phone company gives consumers notice of their intent to disclose the information and consumers have 30 days in which to contact the company to object, otherwise the company can proceed.

Our problem, however, is that the FCC permits disclosure under an opt-out standard, not only to telephone company affiliates, but also to joint venture partners and private contractors. Now, I believe this is a problem because joint venture partners and private contractors not only extend the consumer data out further from the phone company, possibly exposing it to greater compromise, but also from a consumer perspective, it goes to entities with whom they may have no knowledge or business relationship.

And finally, under an opt-out standard, these private contractors may be overseas, where the FCC or the Federal Trade Commission have no presence and no enforcement is existent. Now, in April of 2004 I received a response to an inquiry on this issue from then Chairman Michael Powell of the Federal Communications Commission, which highlights why this standard is problematic. Let me quote from the letter that I wrote to him and then the answer I received. I asked him, "Do the Commission's rules allow the disclosure of customer proprietary network information to entities or persons operating in territories outside the United States?" Chairman Powell's response was, "Nothing in our rules

prohibits the otherwise lawful disclosure of CPNI to persons operating outside the United States."

So Mr. Chairman, do you think that this is the right standard for such disclosure to joint ventures and private contractors and is the FCC prepared to revisit this issue soon?

MR. MARTIN. The standard as it applies to joint ventures/private contractors is opt-out, as you said. There are certain limitations in our rules. The only thing I would say is that the telephone company is required to have a certain knowledge of and a certain business relationship with those joint ventures, and there are certain restrictions that were put in our rules. However, I don't disagree with you that it has become an increasing problem. It is one of the reasons why I did highlight the fact that I think the 10th Circuit case had pushed the Commission, in a certain sense, to adopt an opt-out regime for everything that wasn't explicitly included as an opt-in under the statute, under 222. But the Commission would be prepared, then, to revisit that in the upcoming EPIC petition that we are going to be doing next week. So that would be one of the issues that we would actually say could be potentially reconsidered. It is about whether or not there would be certain other limitations we could put on that opt-out regime so that there could be more of an opt-in for certain other private contractors.

MR. MARKEY. Can you switch it to an opt-in?

MR. MARTIN. You know, I think that is one of the things the Commission is considering, whether it would be able to. That is what we will be seeking comment on next week and I think there will be people who will say that we will be unable to after the 10th Circuit decision. And that is one of the things that I think we are asking for comment on from other parties about whether we can switch that part to an opt-in.

CHAIRMAN BARTON. The gentleman's time is up.

MR. MARKEY. I thank the Chairman, I thank the commissioners for their great work.

CHAIRMAN BARTON. Mr. Terry.

MR. TERRY. One quick question. Do either of you know if we would even need to write in a law enforcement exemption? They have the tools to go in and get a warrant and usually that is the way around when there is an absolute ban on obtaining general information.

MR. MARTIN. I mean, there are already certain law enforcement exceptions to be able to go acquiring this information and what we are talking about in the legislation we were discussing earlier would be the commercial sales. I don't think there would be a need for an explicit law enforcement exemption when you are talking about prohibiting the commercial sale of that information.

MR. LEIBOWITZ. And let me say this, generally we are very happy to help the committee as it drafts legislation, which it seems very intent to do and we will get back to you with a specific answer on that, but I think Chairman Martin is probably correct.

MR. TERRY. I appreciate that. I just--and I want to thank both of you for coming up here today and helping us.

MR. MARTIN. Thank you.

CHAIRMAN BARTON. The gentleman yields back. Mr. Rush. No questions? Who was here--I know Mr. Stupak--Mr. Inslee, would you be next in order of appearance? Or do you want to just go by order of where they sit? Geez, if we go by order of strength, that would be like the Bowl index. I mean, there would be one argument after another over that. Mr. Inslee.

MR. INSLEE. Thank you, thank you. I want to again thank Mr. Chairman for holding this hearing. It is of tremendous--I just got handed to me a fax letter from the King County, Washington sheriff about the great law enforcement concern about this involving so many undercover agents and I think it notes the importance of us acting with dispatch to get this job done and so I appreciate you gentlemen being here. I have several questions.

First, when we started this, the immediate concern was about the source of this information now being on the Internet is through pretexting, that that would be the modus operandi of getting this information. But listening to you talk about the commercial distribution of this information through joint ventures, through private contractors, perhaps outright sales, I guess it causes me some concern that are we really going after the right target? Is pretexting really the majority of the method of acquisition of this information? What do we know about that, as to whether pretexting is the majority or a significant part of the source of this, or are there other commercial distribution that is winding their way into some of these nefarious websites?

MR. MARTIN. Well, we don't know for sure how they are obtaining all of that information. That is what we have actually been trying to investigate and that is why it is so important to be able to try to get responses from the data brokers, themselves, so that we can try to understand how they have been able to obtain this information. Most of the reports have thus far been about pretexting as being the primary means of how they are getting access to this information. But I can't tell you that that is the only way that they are doing it. I do think that you raised, though, a good point about trying to address the problem more fundamentally, not by trying to get at the action about how they are obtaining the information, but rather the prohibition on the general disbursement of the information, regardless of how it was obtained.

MR. LEIBOWITZ. Yes, and I agree with everything Chairman Martin said. I mean, we think most of it is coming through pretexting, but it is conceivable that some may be through bribery or through hacking, and that also goes to how you respond to it. I mean, we are doing investigations together. We are working together on investigations, but you really need a multifaceted approach. You need State attorneys general and you really need telephone companies to make sure that they have tough safeguards on consumers' information.

MR. INSLEE. Is there some concern that, given the non-universal opting out, that if we don't change that situation, even though we close the pretexting door, that we end up with the same situation that this information is available on the Internet?

MR. MARTIN. I think that if you close the pretexting door, obviously that is how the majority of it is getting obtained, that would be a significant step. I don't know whether it would close the door completely or not. If you took broader legislative action of just prohibiting the commercial sale of it, then not only would we be able to take action against anybody selling it, but then it would also be easier, for example, to shut down websites if they were selling information illegally. So it depends upon the level of Congressional activity of whether it would actually address all the issues.

MR. INSLEE. The bill Representative Blackburn and I have introduced would require notification of a consumer when there is a known breach by the phone company. Is there any reason that we would not require that? Do you have any comment on that? Have you considered that in your rulemaking?

MR. MARTIN. We are considering that in the rulemaking as being one of the other things, but I don't have any particular comment as to why that wouldn't be something else that would be an additional safeguard that could be put in place.

MR. INSLEE. Okay. Are you giving--is there any law enforcement assistance you need or do you need any investigatory help in determining the source of this information?

MR. LEIBOWITZ. Yes, we have investigators and they are working very, very hard on our investigations and we hope to be able to announce something soon and we are working with the FCC. I mean, we never turn down more resources, if you want to give them to us, but--

MR. INSLEE. Is there any--one of the things that is flabbergasting to me is if you look at these websites, it sounds like it is a guarantee. You send us $100, we will send it to you in an hour without--it is not like 10 percent of the time we will or 50 percent of the time we will, we are going to do it. That, to me, leads me to conclude that perhaps there is a source of this information well beyond pretexting. For instance,

penetration, perhaps, of cell phone companies, themselves. I mean, I get this sense almost that there is some broad based structural loss of this information. What do you have to indicate whether that might be the case?

MR. MARTIN. When we have had our investigation and meetings with all of the telephone companies and carriers, they haven't given us any indication that any evidence of that is how this information is getting out. I certainly agree with you that it seems like it could be getting out in multiple ways, which again, I think only furthers my concern with just saying that we should be trying to address whether or not this information should be allowed to be sold in a commercial way at all. Because if we do that, then that would take away anybody's incentive to get it, no matter how they are doing it.

MR. INSLEE. One quick question. As far as jurisdiction across borders, you indicated there is a lack of ability to share information. To me, that seems to be something we should cure in this legislation, or someone else. I hope they will do that. But what could we do about folks offshore in this regard? I know I have been asked a lot of my constituents. What is the most effective means to prevent offshore pretext calling where we have this essentially taking place from Timbuktu?

MR. LEIBOWITZ. Well, it is difficult--I mean, it is a very, very difficult question in terms of all types of pretexting. If you look at the FTC website where we provide advice about how to avoid pretexting when someone is trying to pfish you, and most of that phishing comes from out of the country.

MR. INSLEE. But as far as enforcement, I am just thinking from the angle of what we can do from a multinational standpoint, to have enforcement cross-border in this regard.

MR. LEIBOWITZ. Well, one thing you could do is close what we call our cross-border fraud loophole. We have a bill, it is the U.S. Safe Web Act, and it has some interest in this committee and on the Senate Commerce Committee, they have passed it unanimously--and I am happy to make a copy of that available to you. And we have to make this a priority to try to go after these malefactors and fraudsters wherever we see them. It is just hard to do it when we are talking about international borders.

MR. INSLEE. Thank you, and that is the first time I have heard the term fraudsters, so I certainly learned something today. Thank you very much. Thanks for your work.

CHAIRMAN BARTON. Mr. Otter. Mr. Shimkus. Mr. Green.

MR. GREEN. Thank you, Mr. Chairman. Chairman Martin, Section 222 of the Communication Act said that carriers have a duty to protect

all consumer proprietary network information. Can you tell us what the standard in Section 222 of the Communication Act means in more detail? Has the FCC or the courts fleshed out what exactly that duty entails?

MR. MARTIN. The Commission has adopted several requirements on telephone companies to make sure that they are meeting the standard of protecting that information. As I said, our initial implementation of some of that did go to court and was challenged. But the telephone companies currently are required to, for example, flag all customer service records with the status of whether or not the customer has provided them the ability to share that information or not, so that would be on their computer systems. They must have all of their employees that have access to that information go through training about how they are appropriately allowed to-or not allowed to-share that information. There has to be a disciplinary program in place for any violations by any employees who use that information either for commercial purposes at the company or distribute it to anybody else, and they have to have that done ahead of time.

There is an electronic audit mechanism that is required so that the companies can tell with a specific record, they should be able to tell us who it was opened by and for what purpose, within the company and they have to maintain that auditing mechanism for at least one year. And then there has to be a supervisory process before any of that information can be used for any kind of outbound marketing, so that it can't just be a regular employee, but has to go up through a supervisor's process. And then there has to be a corporate certification once a year by an officer of the company that he has personal knowledge that the company is complying with all of these rules; and that certification must be made publicly available to anyone who would want it.

MR. GREEN. Okay. I would hope the FCC would respond, hopefully without waiting on Congressional action to the concern. I am concerned, however, that the new FCC rules may not stop the abuses or even slow them temporarily unless standards evolve along with tactics being used against our constituents. If the FCC produces new rules setting standards for privacy protection by carriers, how will the FCC keep these standards up to date and respond proactively to new techniques by people who steal personal information so that we can prevent abuses like we have seen in the last few months from making the headlines? Is there an ongoing process to see new techniques from folks who are trying to get that information at the FCC?

MR. MARTIN. Well, one of the changes that we have proposed, and there is a series of them in response, as I said, to the EPIC petition. For example, we have asked whether or not the consumer information should only be available if there is a certain password that consumers put in

place and are able to use, or whether or not the consumer should only be able to access it from the telephone number of which the information that they are trying to obtain. So those would be the kinds of protections that we could end up putting in place to try to further protect it. As far as additional investigations, I think EPIC has proposed some additional auditing trails that would be put in place, similar to the audit mechanisms that I talked about, opened by whom and for what purpose, but for additional mechanisms.

I think that we discussed whether or not some additional encryption should be placed on the information in case it was being accessed electronically in an illegal fashion. But again, we don't have any evidence of that occurring, but there have been at least some allegations of that. One of the--

MR. GREEN. I need--I have got one question--I only have a minute--I need to ask of the FTC, but I appreciate what you are doing and hopefully, you will--it is an ongoing process. Before I run out of time, Commissioner Leibowitz, the hearing is focused on phone records and pretexting, but the testimony we are going to hear shortly from Electronic Information Privacy Center reveals that some websites also are selling private information, personal information behind e-mail addresses and instant messenger names, along with the Internet dating websites. I don't want our legislative and regulatory response to focus only on merely on phone records and the Internet. A lot of people, including children, use e-mail and instant pager with the belief that someone can't find out where they live or their e-mail address. Apparently, that belief is mistaken. Is the FTC focused on that problem of privacy violations regarding Internet personal information, as well?

MR. LEIBOWITZ. Yes, we are, Congressman. We have brought more than a dozen cases under Gramm-Leach-Bliley, close to a dozen data security cases and we can use Section 5 to go after all these practices, as you pointed out, you know, someone who is selling phone records may also be selling other things. The one thing we don't have under Section 5 is, for the most part, is the ability to give penalties and penalties, we think, are usually a pretty effective deterrent.

MR. GREEN. Okay, thank you. Thank you, Mr. Chairman. I actually didn't take any more time.

CHAIRMAN BARTON. Mr. Stupak.

MR. STUPAK. Thank you, Mr. Chairman. I thank both witnesses for being here today. Commissioner Martin, Mr. Inslee had asked about disclosure when there is a known breach of confidential information, but what about notifying consumers each time their confidential information is given out to anyone? That way, the consumers would be empowered to determine whether or not that was appropriate, if they gave that

permission, to allow this information to given out. Would you be supportive of that?

MR. MARTIN. I guess I would say potentially, but I think it is important to remember that that might not address the very problem we are talking about today because you are saying that you would want to know when the information was provided to someone else. But in many instances here, the companies are saying that the information, as they understand, was provided to you already and it was you that was asking for it, so because of the nature of the problem, the pretexting is what we are talking about at the hearing--

MR. STUPAK. But if they give out my cell phone number, shouldn't I have a right to know that?

MR. MARTIN. No, I am saying that that might be a requirement that might not fully address alone the problem that we are having in the sense that the company thought that it was you that asked for that information already, so they wouldn't re-contact you, so that requirement alone wouldn't be enough. That might be an additional requirement. It is one of things, actually, we are considering doing so yes, that might be something we should do. All I meant is in isolation, that might not be enough.

MR. STUPAK. Well, it should be disclosed to me if they gave me the information because you don't know if I am really the person on the other end of the line, correct?

MR. MARTIN. That is right. I guess I wasn't sure exactly how they would--if they thought that it was you already, I wasn't sure exactly what you meant.

MR. STUPAK. This investigation you have looked at and you said you went to some websites and you tried to do a sting operation to obtain the information. When, in your investigation, when these people ask for the information, they just ask for a cell phone number, a couple of cell phone numbers? How does it usually go? I mean, they don't ask for a whole laundry list, do they.

MR. MARTIN. Go ahead.

MR. LEIBOWITZ. Well, I think it--I mean, you are a former law enforcement officer, so you know I don't want to talk too much about our investigations, but I think it depends and I think there is a range in what they are asking for.

MR. STUPAK. Okay. How do they pay for the information, through credit cards?

MR. LEIBOWITZ. Yes, very often through credit cards. Yes, absolutely.

MR. STUPAK. Okay. Have you spoke to credit card companies, advising them that this information is being obtained through a credit card and may be illegal?

MR. LEIBOWITZ. I have not personally spoken to credit card companies.

MR. STUPAK. Have your investigators?

MR. LEIBOWITZ. You know, I think we are getting into a place where we can provide this committee with a confidential briefing about what we are doing, but I don't want to go too far down this road.

MR. STUPAK. Okay, maybe that is right, because as we have found on oversight investigation, Mr. Chairman, through Internet pharmacies, people can buy anything using credit cards or when they come to mask the drugs that they are taking, there are drug masking things out there. They use it to cover up the drugs they make be taking that is required for a commercial driver's license and when we find the credit card companies are ready, willing to provide anything, provided you have a credit card or consumer companies will sell you anything as long as you have a valid credit card and one of the ways that we should do it is look at the credit card company and make sure the purchase is proper and not illegal or being used for illegal means. With that, Mr. Chairman, I will yield back.

CHAIRMAN BARTON. Seeing no other member present who--oh, Mr. Gonzalez, did you want to ask questions?

MR. GONZALEZ. Yes, sir.

CHAIRMAN BARTON. Okay. Mr. Gonzalez is recognized.

MR. GONZALEZ. No other Republican member present.

CHAIRMAN BARTON. No, I actually thought you had passed. I apologize.

MR. GONZALEZ. A couple of things that I will be asking the witnesses quickly and there is a two-pronged approach to this and one, of course, is prevention and that is what we have been talking about, safeguarding standards and such and there is a lot to be done with that that may not require a real big legislative fix and only your imagination, creativity and then maybe judicial review. The only is the deterrent part and we are talking about Jay's bill and Congresswoman Blackburn's on criminalization, and that is a thought. You all had talked about enhancing the regulatory scheme of things, opt-in and such, and also significant civil penalties.

I would like for you all to consider something else and--but before we do any of that, I think there has to be a presumption and I want to make sure that I am right. Do we all agree that this information that is being kept and stored by the company belongs to the customer, that they have a proprietary right that is just not superior to, but it is solely owned

by them absent any permission by them to share it, provide it to someone else, give it up or whatever. Is this information Charlie Gonzalez's information? It is not AT&T's?

MR. MARTIN. I agree with you that it is ultimately the consumers' information and they are able to control how it ends up being used or certainly how it ends up being distributed to others. In light of the way that Congress's statute works in Section 222, I am not sure that we could prohibit the company that has it from using it themselves, currently. It is different when you talk about how they would share it with others or how others would have access to it. But I am not sure that the company, that they don't have some inherent right to it, at least currently in the way that the law is structured. So I am not positive we could actually prohibit the person who has it.

Now, one of the proposals to try to address that has actually been to try to limit how long they can keep it. I think that has been one of the ways that they try to address it more like what you are talking about.

MR. GONZALEZ. Commissioner, do you agree that it belongs to the customer?

MR. LEIBOWITZ. I mean, as a legal or technical matter it may, to some extent, belong to the telephone company, but as a practical matter, of course it belongs to the customer. It is the customer's proprietary personal information.

MR. GONZALEZ. There is going to be a big problem if we don't all agree that it belongs to the customer, I guarantee you. Legally, I mean, privacy, whatever the legal principles involved, you still have to have a proprietary interest and I understand that we are looking here as government and our role as a regulator and such, so what I want to go to, assuming that this is information that is protect-able because there is a proprietary interest, obviously, solely in the hands of the customer, if we start saying the person that is collecting it is free to do things outside of their own company--and I don't want to get way out on the affiliates and all that good stuff and what is related to the service that they are providing, but if we start talking about that, well then we are empowering the individual that collects it to do pretty much what they want to do with this information, forget about pretext and such, but I was going to ask you.

What would really enhance this and so when we are addressing it we also provide a private cause of action? Federal, with punitive damages being emphasized, because I think Congressman Deal hit on a real important point and that is how do you prove how you have been damaged? Privacy claims are always very difficult to show actual damages. If we criminalize it, we will have intentional tort and so on, but let us just talk about a private cause of action. Would you all agree

that it would assist you, indirectly, but nevertheless be a very effective tool, to have a private cause of action against the individual that acquires it illegally, right, or under pretext or otherwise, or the misuse by the individual company that is maintaining the information?

MR. LEIBOWITZ. I guess I would say this: that is a very interesting idea and I will take it back to the Commission. I would say that whatever you do, don't preempt the State attorney general's role because I think that is vitally important. And then can I just come back to your previous--

MR. GONZALEZ. But you won't find too many Democrats that are going to preempt State attorneys general.

MR. LEIBOWITZ. If I could come back to your previous point. I didn't mean to misstate it. I think this is a fundamental privacy matter and you know, there is a precedent for banning this type of information from dissemination and that is DVD rentals and video rentals, which the judiciary committee which I used to work on in the Senate did after the Bork hearings, so I pass that along.

MR. MARTIN. I don't think the Commission has considered whether or not a private right of action would be a good thing or not from a policy perspective. I am not sure exactly how it might help us uncover what was going on unless it just helped us uncover just additional facts, in general, but I would have to go back and I don't know even if--

MR. GONZALEZ. Thank you all very much for your testimony.

CHAIRMAN BARTON. Seeing no other member present on either side, we are now ready to go to our second panel. I would like to thank our first panel, Chairman Martin and Commissioner Leibowitz, and we will be in touch very quickly with you and your staffs to work on this legislation. We do intend to legislate very quickly. Let us have the second panel come forward. We have Attorney General Lisa Madigan of the great State of Illinois; Steve Largent, the president and chief executive officer of Cellular Telecommunications and Internet Association; Mr. Edward Merlis, who is the Senior Vice President for Law and Policy for the United States Telecom Association; Mr. Marc Rotenberg, who is the Executive Director of the Electronic Privacy Information Center; and Mr. Robert Douglas, who is the Chief Executive Officer of PrivacyToday.com. As soon as we get everybody seated, we will do the introductions. I think we have got everybody seated and we have your nameplates. I am going to yield to Congresswoman Schakowsky to more formally introduce Attorney General Madigan.

MS. SCHAKOWSKY. Thank you so much, Mr. Chairman. I am proud to introduce the first woman attorney general of Illinois, Lisa Madigan, elected in 2002, where she has been a great advocate for the consumers, seniors, women, children, crime victims, the environment, for the Illinois

community. As Illinois' chief legal officer, Attorney General Madigan has not shied away from the good fight. In the month of January alone she has taken on a contractor who was scamming down payments out of consumers for work that was never completed, settled with 18 gas stations across Illinois who were allegedly gas gouging in the wake of Katrina, unveiled legislation to combat two types of mortgage fraud, announced that after investigations by her and other attorneys general across the country--the nation's largest sub-prime lender has agreed to pay $295 million in restitution to consumers and to make sweeping reforms of its sales practices and filed the first lawsuit in the country against those who fraudulently obtain and sell phone call records. This is just a sampling of one month's work.

She has been a great resource to me for my work on spyware, data broker breaches, and now pretexting. And I think we can all learn a lot from her about what she is doing in Illinois on this issue and I thank her for joining us here today and Mr. Chairman, she needs to leave by 5:30, so I will end this introduction. Thank you.

CHAIRMAN BARTON. Welcome. And I had asked if you are any kin to the former Congressman Ed Madigan, but I am told your family is a different family than Mr. Madigan's family. Okay. He was a member of this committee and then later, Secretary of Agriculture. Lady and gentlemen, you are welcome. Your statements are in the record in their entirety. We are going to start with you, Madam Attorney General. I ask each of you to summarize in five minutes your testimony and then we will have some questions. Attorney General.

STATEMENTS OF LISA MADIGAN, ATTORNEY GENERAL, STATE OF ILLINOIS; STEVE LARGENT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CELLULAR TELECOMMUNICATIONS AND INTERNET ASSOCIATION; EDWARD MERLIS, SENIOR VICE PRESIDENT, LAW & POLICY, UNITED STATES TELECOM ASSOCIATION; MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER; AND ROBERT DOUGLAS, CHIEF EXECUTIVE OFFICER, PRIVACYTODAY.COM

MS. MADIGAN. Thank you, Mr. Chairman.

CHAIRMAN BARTON. You have to push the little--

MS. MADIGAN. It is on now.

CHAIRMAN BARTON. There you go.

MS. MADIGAN. Thank you, Mr. Chairman, members of the committee and thank you, Ms. Schakowsky, for that kind introduction. I

appreciate being given the opportunity to testify before the committee today on this very important issue. As a State attorney general, it seems that every day when I open the newspaper or go to work, I am bombarded with articles and complaints about identity theft, but with the recent revelation that people's cell and landline records are for sale, I am now reading and hearing about a new problem that we are all confronting, the problem of privacy theft. Privacy theft is an outrageous violation of people's personal lives and has the potential to put them at great physical risk.

Let me take my time this afternoon to briefly tell you about how I learned about privacy theft and what we in Illinois are doing about it. In early January, as Ms. Schakowsky and Mr. Rush indicated, the Chicago Sun Times ran an article that disclosed that the Chicago Police Department, as well as the FBI, had issued a warning to their officers and agents. They issued that warning because companies were able to obtain call record information that would compromise their undercover status and investigations, thus putting those officers and agents at great risk. An officer that we spoke to was able to purchase the records for an undercover narcotics unit's cell phone from locatecell.com within four hours for $175. He merely gave the company the cell phone number he wanted the records for, his name, a mailing address and a way to contact him. At no time did he ever identify himself as the account holder, nor did he identify himself as a police officer.

The ability of strangers to obtain phone records also, as has been noted by others here today, jeopardizes survivors of domestic violence. All an abuser or a stalker has to do is contact a data broker to find out who you are talking to or potentially, where you are. We have heard testimony about how data brokers access this information and we have also heard some indication of how many brokers there are. But if you are curious yourself, I would encourage you to get on the Internet and do a simple search by putting in "cell phone records" and you can see well over 40 to 50 companies show up.

What I would like to do today is to focus on the legal action that my office is taking to prevent these services from continuing to operate and devastate people's personal, as well as professional, lives. On January 20th, I filed a lawsuit against 1st Source Information Specialists, Incorporated under our State consumer fraud act for engaging in unfair and deceptive practices by offering and obtaining phone records. There are other lawsuits that have been filed by my colleagues in Missouri and Florida and there may be other lawsuits that State attorneys general have filed that I am unaware of.

I can tell you that as a group, the Attorneys General are committed to bringing additional lawsuits to stop these data brokers from committing

privacy theft, but we are well aware that enforcement alone is not enough to stop privacy theft. We also need to know what security measures the phone companies have in place to protect customers' information. Earlier we heard that the FCC has launched an investigation into these practices and is reviewing the CPNI rule. And while that is heartening, attorneys general are directly responsible for consumer fraud matters affecting citizens in our State, as well as often being directly responsible for criminal prosecution, so we have sent out a letter to all the major cell phone companies requesting that they review with the attorneys general their past and any updated policies and procedures they have put in place for protecting their customers' phone record information.

We have also, in conversations with phone companies, and we have heard a little bit about it today, heard of some of the potential protections. Password protection, unfortunately, has repeatedly not worked in protecting customers' phone record information and we think that further investigation of how to notify customers that their information has been accessed would be well worth looking into.

Finally, as numerous members here today have indicated, there is significant momentum in Washington, as well as in State capitals across the country, to affirmatively protect customers' phone record information. I appreciate that Representative Schakowsky has introduced the SAFECall Act and I also appreciate numerous other suggestions that we have heard today. I can tell you that in Illinois there are at least five bills that are currently pending in our general assembly.

Let me also say that as a State attorney general, I would say to the committee that when drafting or proposing any legislation, please do consider dual enforcement by both State, as well as Federal agencies, in order to bring more resources to our efforts to eliminate the sale of phone records. In that regard, I certainly hope that Congress will not choose to preempt any State legislation that is passed regarding this issue. Again, thank you for allowing me the opportunity to address the committee on this important issue. I urge you to act quickly to stop the crime of privacy theft and I would be happy to answer any questions you may have.

[The prepared statement of Lisa Madigan follows:]

PREPARED STATEMENT OF LISA MADIGAN, ATTORNEY GENERAL, STATE OF ILLINOIS

Good morning Chairman Barton, Ranking Member Dingell, and distinguished members of the Committee. I am Lisa Madigan, the Attorney General of Illinois. Thank you for inviting me to testify before the Committee on the topic of the sale of phone call records.

It seems that every day we are bombarded with headlines about identity theft. But the sale of peoples' cell and land line phone records is in a new category of its own. It is

privacy theft – the theft of details of peoples' lives – who they called, when they talked and for how long.

And the potential harm to our citizens cannot be underestimated.

I would like to tell a story of a disturbing undercover purchase of cell phone call records in Chicago. On January 6, 2006, after reading a law enforcement warning, a Chicago police officer went online to www.locatecell.com to test whether he could obtain the cell phone records for an undercover narcotics unit cell phone number. The Web site operators did not require that the officer verify that he was the account holder for the cell phone number. They merely required the cell phone number, his name, mailing address, and day and night time phone numbers.

The police officer requested the records and received accurate call records within four hours of the request for a total of $175. For $175, lives were placed in jeopardy. The call records listed a long string of phone numbers with the dates of calls placed by undercover narcotics agents. The results also included a confirmation of the name and address of the account holder.

These records were obtained in a very short amount of time without any verification that the officer was the proper account holder.

And let me run another scenario by the members of the Committee. Imagine that you are a victim of domestic violence. You have found the courage and the means to flee a cycle of violence. You have not established a land line because you do not want any utility records that might alert your abuser to your whereabouts.

Now all the abuser has to do is call a data broker. Your abuser will know who you are talking to and when. He will know when you pick the kids up at school and when you get home. Now he can find you.

Both of these instances – the undercover cop and the victim of domestic abuse – illustrate this enterprise for what it is: an outrageous invasion of privacy that could put lives in danger. The possibility of harm from this "service" to law enforcement and domestic abuse victims is truly enormous.

As we know, the Federal Communications Commission's Customer Proprietary Network Information, or CPNI, rules prohibit telecommunications carriers from disclosing or selling phone call records to third parties without the permission of the account holder. So how could call records be obtained so quickly and with no verification?

Various methods of obtaining phone call information have been suggested in the press: (1) a data broker calls the carrier and pretends to be the account holder or an employee of the carrier to obtain call record information; (2) a data broker accesses the online billing features of a carrier's Web site and pretends to be the account holder; or (3) a data broker pays an employee of a carrier to steal the call record information.

Regardless of how this information is obtained, it is illegal to give out this information without the permission of the account holder.

On January 20, 2006, my office filed a lawsuit against 1st Source Information Specialists, Inc., located in Florida, doing business as locatecell.com, celltolls.com, datafind.org, and peoplesearchamerica.com, and two individuals, alleging that 1st Source engaged in unfair and deceptive practices under Illinois' Consumer Fraud and Deceptive Business Practices Act by:

*calling the telecommunications provider and representing that the caller is the account holder or an employee;

*attempting to access online telephone billing records by posing as the account holder; and

*representing online to Illinois consumers that the services the defendants offer are legal through such representations as "...Get calls made from any cell phone number. All Carriers. No Results, No Charge. ..."

(www.peoplesearchamerica.com); "...Cell Phone Call Records $110 Give us the cell phone number and we will send you the calls made from the cell phone number. ..."

My office has performed online searches only to find that there are approximately 100 such Web sites, selling everything from phone call records to credit histories. While we are committed to bringing lawsuits to stop these data brokers, we also need to look at how the carriers are protecting their customers' call record information.

I understand that the FCC's Enforcement Bureau has launched an investigation into these practices, and that the FCC is reviewing its CPNI rules. However, some Attorneys General also have concerns and have requested that the major carriers review with the Attorneys General their past, and any updated, policies and procedures for protecting their customers' call record information.

There is also significant momentum in Congress and in legislatures across the country to pass laws to protect consumers' information. At the federal level, U.S. Sen. Dick Durbin and U.S. Rep. Jan Schakowsky – both from Illinois – have introduced legislation to address this issue. At least five bills have been introduced in the Illinois General Assembly thus far, the majority of which prohibit the disclosure or sale of CPNI unless permitted by law, including disclosure with the account holder's permission. The bills provide that a violation of the provisions are a violation of the Illinois Consumer Fraud and Deceptive Business Practices Act, and also have criminal penalties. One bill amends the state ID theft criminal law to cover the data broker's practices of using deception to obtain phone call records.

As a state Attorney General, I would ask that this committee consider, when proposing legislation, that the states many times bring new perspective to the legislative process and can be innovative in the approaches they devise to address problems confronting their citizens. I hope Congress will choose not to preempt any state legislation that is passed regarding this issue.

Furthermore, as the Committee looks at this issue, I ask that you prohibit the obtaining and sale of phone call records and other account information, and that you consider tightening up the requirements that the carriers must follow in ensuring that data brokers do not obtain this information illegally.

It is truly frightening to think that someone with a grudge and $100 can find out how you live your life. I urge Congress, and the General Assembly in my State of Illinois, to act immediately to stop the crime of privacy theft.

Thank you for allowing me this opportunity to address the Committee on this important subject. I'd be happy to answer any questions.

MR. SHIMKUS. [Presiding] I want to thank you for coming to Washington for your testimony and I would like to recognize our former colleague, Steve Largent, for five minutes.

MR. LARGENT. Thank you, Mr. Chairman. I want to thank you and the other members of the committee for the opportunity here this afternoon to appear before you and to testify on the theft and illegal sale of phone records by data brokers. With your consent, I would like to have my full statement, written statement, made a part of the record.

MR. SHIMKUS. Without objection, so ordered.

MR. LARGENT. At the outset of my testimony, I want to make it unequivocally clear that the wireless industry, and more specifically, the wireless carriers that I represent take this matter seriously. The theft of this data is unacceptable and CTIA and the wireless carriers believe that

the current practice of pretexting is illegal. Chairwoman Majoras has declared that the Federal Trade Commission currently has the authority it needs to prosecute these thieves, and carriers have successfully filed injunctions to take these sites down. Additionally, CTIA and the wireless industry are on record as supporting Congress's efforts to enact Federal legislation that criminalizes the fraudulent behavior by third parties to obtain, sell or distribute call records.

I believe that it is important to note that the four national carriers, Verizon Wireless, Cingular, Sprint Nextel, and T-Mobile, have all filed complaints and obtained injunctions across the country to shut these data thieves down. The fact that data brokers apparently have been able to break and enter carrier customer service operations to obtain call records has given our industry a black eye. To quote from one of CTIA's member companies, their code of conduct, it says, "Great companies are defined by their reputation for ethics and integrity in every aspect of their business. By their actions, these companies demonstrate the values that serve as the foundation of their culture and attract the best customers, employees and stakeholders in their industry."

The wireless industry is dedicated to being responsive to its customers' requests for assistance with their service. To the extent that the theft of customer call records has jeopardized the industry's reputation is most unfortunate. Trust is a currency that is difficult to refund. As we all know, the way that these thieves are obtaining call records is through the use of pretexting, otherwise known as lying. I will let Rob Douglas, who is an expert on pretexting, give you greater insight into this.

I would note that no two carriers can or should employ the exact same security procedures. I would caution committee members that as you proceed forward in drafting legislation, that you consider that the threat environment is constantly changing and static rules can quickly become outmoded or easily avoided by fraudsters. Additionally, CTIA, in its comments on the EPIC petition for rulemaking at the FCC, noted that requiring wireless carriers to identify security procedures on the record and to further identify any inadequacies in these procedures would provide a road map to criminals to avoid fraud detection measures. Public disclosure potentially could lead to serious harm to consumers and carriers, alike.

One security practice that we know works is litigation. I cannot emphasize enough how seriously wireless carriers are taking these illegal and unauthorized attempts to obtain and traffic our customers' private information. These internal investigations have led to the carriers filing these cases, which began months before the current media glare. As I mentioned at the beginning of my testimony, the four national carriers

have all filed complaints and obtained injunctions across the country to shut these data thieves down.

Carriers have taken additional security steps that require personal identification numbers and passwords when obtaining call record information. Many carriers have instituted a ban on faxing or e-mailing call records. It is important to remember carriers are under tremendous pressure to quickly respond to customer calls. What was largely perceived as good customer service yesterday is now a practice seen as a potential security flaw. Because of the highly competitive nature of the wireless phone industry, customer service is extremely important to wireless carriers.

Wireless carriers collectively received hundreds of millions, if not billions, of customer inquiries in 2005. Inside our member companies, customer service reps are striving to address the requests of customers as best they can with the very best interest of the customer at heart. Bearing this statistic in mind, it would prove counter-productive to enact legislation that would impede wireless customers' access to their own account information. Rules that may require in-person customer service would be a step backwards from the convenient and responsive customer service wireless carriers strive to achieve.

Clearly, the privacy of a small percentage of our customers and your constituents has been compromised. As far as I am concerned, the breach of even one wireless customer calling record is one customer too many. But to the best of my knowledge, no system is foolproof, especially one that handles hundreds of millions of customer calls each year without the customer being present. The wireless industry wholeheartedly supports making it explicitly clear that the marketing, possession, and sale of call records is against the law.

CTIA and its carriers are on the record as supporting Congress's efforts to enact Federal legislation that criminalizes the fraudulent behavior by third parties to obtain cell industry call records. If we have learned anything from this experience, it is that combating pretexting is a war where the unscrupulous continuously seek our vulnerabilities and weaknesses in the carriers' defenses. Unfortunately, no defense will be perfect, which is why we need a good offense and strong enforcement measures against these criminals. Again, I want to thank you for this opportunity and I welcome any questions you may have. Mr. Chairman.

[The prepared statement of Steve Largent follows:]

PREPARED STATEMENT OF THE HON. STEVE LARGENT, PRESIDENT AND CHIEF EXECUTIVE OFFICER, CELLULAR TELECOMMUNICATIONS AND INTERNET ASSOCIATION

SUMMARY

CTIA and wireless carriers believe that the current practice of "pretexting" is illegal. Chairwoman Majoras has declared that the Federal Trade Commission currently has the authority it needs to prosecute these thieves. Carriers have successfully filed injunctions to take these sites down. CTIA and the wireless industry support Congress's efforts to enact federal legislation that criminalizes the fraudulent behavior by third parties to obtain, sell or distribute call records.

Overwhelmingly, the vast majority of cell phone records are being fraudulently obtained through the use of "pretexting," which is nothing more than lying to get something you aren't entitled to obtain lawfully. No combination of identifiers is safe against pretexting. We have had cases where the data brokers have possessed the customer password. We have had cases where they knew the date of birth of the customer and the full Social Security number.

CTIA's members are committed to protecting customer privacy and security. This is no hollow pronouncement – we are talking about carriers protecting the privacy of their most valued assets – their customers – as well as the very infrastructure of their networks. No carrier has an interest in seeing customer records disclosed without authority and every carrier has security policies and technical defenses to guard against it. Wireless carriers employ a broad range of security measures beyond those put in place by the Federal Communications Commission's (FCC) customer proprietary network information (CPNI) rules to prevent unauthorized access to and disclosure of CPNI. CPNI is protected from unauthorized disclosure under Section 222 of Title 47, and the FCC's implementing rules.

The CPNI rules are well implemented by carriers. Customer Service Representatives (CSR) are trained extensively on the rules related to access, use and disclosure of CPNI. Technical restrictions are placed on access to CPNI to ensure that no one can walk off with a data base of customer information, and CSRs are monitored to ensure they follow the rules.

One security practice we know now works is litigation. The four national carriers: Verizon Wireless, Cingular, Sprint Nextel, and T-Mobile have all filed complaints and obtained injunctions across the country to shut these data thieves down. Moreover, smaller Tier II and Tier III wireless carriers are re-examining their security protocols to ensure their customers' privacy.

Because of the highly competitive nature of the wireless phone industry, customer service is extremely important to wireless carriers and their customers. In 2005, wireless carriers collectively received hundreds of millions, if not billions, of customer inquiries. Rules that may require in-person customer service may be counter-productive, considering the convenient and responsive service that carriers work hard to achieve.

Though the wireless industry believes that government agencies need not wait for an act of Congress to prosecute these thieves, CTIA and its carriers are on record as supporting Congress's efforts to enact federal legislation that criminalizes the fraudulent behavior by third parties to obtain, sell, or distribute call records.

Chairman Barton, Ranking Member Dingell and members of the Committee, thank you for the opportunity to appear before you this afternoon to testify on the theft and illegal sale of phone records by data brokers. At the outset of my testimony, I want to make it unequivocally clear that the wireless industry, and more specifically, the wireless carriers that I represent take this matter very seriously. The theft of this data is unacceptable, and CTIA and wireless carriers believe that the current practice of "pretexting" is illegal. Chairwoman Majoras has declared that the Federal Trade

Commission currently has the authority it needs to prosecute these thieves. Carriers have successfully filed injunctions to take these sites down. Additionally, CTIA and the wireless industry are on record as supporting Congress's efforts to enact federal legislation that criminalizes the fraudulent behavior by third parties to obtain, sell or distribute call records. I believe that it is important to note that the four national carriers: Verizon Wireless, Cingular, Sprint Nextel, and T-Mobile have all filed complaints and obtained injunctions across the country to shut these data thieves down.

The fact that data brokers apparently have been able to break and enter carrier customer service operations to obtain call records has given our industry a black eye. To quote from one of CTIA's member companies' Code of Conduct, "Great companies are defined by their reputation for ethics and integrity in every aspect of their business. By their actions, these companies demonstrate the values that serve as the foundation of their culture and attract the best customers, employees and stakeholders in their industry." The wireless industry is dedicated to being responsive to its customers' requests for assistance with their service because of its concern for wireless customers. To the extent that the theft of customer call records has jeopardized the industry's reputation, I believe this is most unfortunate because trust is a currency that is difficult to refund.

PRETEXTING

Overwhelmingly, the vast majority of cell phone records are being fraudulently obtained through the use of "pretexting," which is nothing more than lying to obtain something you aren't entitled to procure lawfully. Allow me to explain how these data thieves operate. For the sake of illustration, if someone -- and in most cases it appears to be a private investigator – wants to acquire my call records, the private investigator will go to a website that publicly offers to obtain such records such as locatecell.com. The person trying to obtain my call records will provide the website in most cases with nothing more than my name and phone number. At that point, the website or a subcontractor of the website will pose as *Steve Largent* and call a carrier's customer service department to get the records. Customer Service Representatives (CSR) are trained to require more than just a name and phone number, but the thieves are well trained too and often badger, threaten or plead with the CSR to acquire the records as if they are the actual customer. Our carrier investigations confirm that these calls are rebuffed, but these data brokers are quite determined. The data broker will scour other sources on the Internet or elsewhere to obtain my Social Security number or date of birth so that eventually the data broker will appear to be *Steve Largent* calling customer service, and thus, the CSR is duped into releasing the records. To be clear, from the carrier perspective, the CSR is dealing with the actual customer.

Make no mistake, these data thieves are extremely sophisticated. If they are unable to deceive one CSR on the first attempt, they will place multiple calls to customer service call centers until they are able to mislead a CSR into providing the call records.

No combination of identifiers is safe against pretexting. We have had cases where the data brokers have possessed the customer password. We have had cases where they knew the date of birth of the customer and the full Social Security number. Because many of these cases seem to arise in divorce or domestic cases, it is common for a spouse to have all of the necessary identifying information long after a divorce or separation to obtain call records.

WIRELESS CARRIER SECURITY PRACTICES

CTIA's members are committed to protecting customer privacy and security. This is no hollow pronouncement – we are talking about carriers protecting the privacy of their most valuable assets – their customers – as well as the very infrastructure of their networks. No carrier has an interest in seeing customer records disclosed without authority and every carrier has security policies and technical defenses to guard against it.

I am also confident that our carriers are utilizing the best industry practices for combating fraud and ensuring security; however, the thieves who want to commit these crimes are constantly changing their tactics and approaches – staying one step ahead of them requires flexibility.

Wireless carriers employ a broad range of security measures beyond those put in place to meet the Federal Communications Commission's (FCC) customer proprietary network information (CPNI) rules to prevent unauthorized access to and disclosure of CPNI. I would note that no two carriers can or should employ the exact same security procedures. I would caution Committee members that as you proceed forward in drafting legislation that you consider the threat environment is constantly changing and static rules can quickly become outmoded or easily avoided by the fraudster. Additionally, CTIA in its comments to the EPIC petition for rulemaking at the FCC, noted that requiring wireless carriers to identify security procedures on the record and to further identify any inadequacies in those procedures would provide a roadmap to criminals to avoid fraud detection measures. Public disclosure potentially could lead to serious harm to consumers and carriers alike.

CPNI is protected from unauthorized disclosure under Section 222 of Title 47 and the FCC's implementing rules. "Every telecommunications carrier has a duty to protect the confidentiality of proprietary information." Every wireless carrier takes that duty seriously; it is the law. The FCC, too, has followed up strongly on that mandate. In its very first order after the passage of the Telecommunications Act of 1996, the FCC directly addressed security concerns related to the protection of CPNI, and it has addressed the CPNI rules multiple times over.

Consistent with Congress's intent in Section 222, the wireless industry has worked continuously to maintain and improve the security of its customers' private information. CSRs are trained extensively on the rules related to access, use and disclosure of call records. Technical restrictions are placed on access to call records to ensure that no one can walk off with a data base of customer information, and CSRs are monitored to ensure they follow the necessary procedures. While we have heard stories about insiders selling call records on the side, we have not actually seen these cases. Instead, the vast majority of cases we have seen involve pretexting where the fraudster actually has all the necessary customer information to obtain the records.

Wireless carriers have taken additional measures to reiterate to their customers that it is important to continue to take steps to protect their accounts by utilizing passwords. For example, T-Mobile "urges all users of mobile services to take the following password protection steps:"

- create separate passwords for voicemail, online access, and for use when calling customer care about your billing account
- set complex passwords using both numbers and letters where appropriate
- avoid common passwords such as birthdates, family or pet names and street addresses
- change your passwords at least every 60 days
- memorize your passwords; and
- don't share passwords with anyone

But passwords get lost or forgotten and in many cases, customers call a CSR to refresh a password. The ability to change a password remotely presents another pretexting opportunity. In short, passwords are not a "silver bullet." Some carriers also report that some customers rebel against mandatory passwords, preferring instead to be empowered to make that choice individually, rather than by dictate.

The Committee should be aware that carriers are extremely cautious when allowing any third party vendor access to call records. Carrier contracts contain strict confidentiality and security provisions. It is common for carriers, for example, to require

that vendors represent and warrant that they have adequate security procedures to protect customer information and to provide immediate notice of any security breach to the carrier. This contractual framework flows down a carrier's own security standards to vendors who conduct customer billing responsibilities creating security in depth.

One security practice we know now works is litigation. I cannot emphasize enough how seriously wireless carriers are taking these illegal and unauthorized attempts to obtain and traffic our customers' private information. These internal investigations have led to the carriers filing these cases which began months before the current media glare. As I mentioned at the beginning of my testimony, the four national carriers: Verizon Wireless, Cingular, Sprint Nextel, and T-Mobile have all filed complaints and obtained injunctions across the country to shut these data thieves down. Moreover, smaller Tier II and Tier III wireless carriers are re-examining their security protocols to ensure their customers' privacy. The carriers' internal investigations against the data brokers made it possible to secure injunctions aimed at taking down the sites and preserving evidence so we can determine exactly who is buying the records through these brokers. We look forward to working with the Committee to utilize this information so Congress will be in a better position to draft legislation aimed not only at those who engage in pretexting, but also those that solicited the deed in the first place and later received the stolen property.

CUSTOMER SERVICE PROTECTIONS

As I mentioned previously, carriers have taken additional security steps to require personal identification numbers and passwords when obtaining call record information. For example, when call records are accessed, it is logged in the customer service database, so the carrier can see who looked at what records. Further, CSRs are trained to annotate the customer record whenever an account change or event occurs. A CSR will note when a customer called and asked for his or her records. To prevent the fraudster from adding a fax or email account identifier to another's account, many carriers have instituted a ban on faxing or e-mailing call records. It is important to remember, carriers are under tremendous pressure to quickly respond to customer calls. What was largely perceived as good customer service yesterday, is now a practice seen as a potential security flaw.

Because of the highly competitive nature of the wireless phone industry, customer service is extremely important to wireless carriers and their customers. Wireless carriers collectively received hundreds of millions, if not billions, of customer inquiries in 2005. Inside our member companies, CSRs are striving to address the requests of customers as best they can with the very best interest of the customer at heart. Bearing this statistic in mind, it could prove counter productive to enact legislation that would impede wireless customers' access to their own account information. Rules that may require in-person customer service would be a step backwards from the convenient and responsive customer service wireless carriers strive to achieve.

CONCLUSION

Clearly, the privacy of a small percentage of our customers and your constituents' has been compromised. As far as I am concerned, the breach of even one wireless customer's calling records, is one customer too many. But to the best of my knowledge no system is foolproof, especially one that handles hundreds of millions of customer calls each year without the customer being present.

The wireless industry wholeheartedly supports making it explicitly clear that the marketing, possession, and sale of call records is against the law. CTIA and its carriers are on record as supporting Congress's efforts to enact federal legislation that criminalizes the fraudulent behavior by third parties to obtain, sell, or distribute call records. Carriers have been successful in using existing state and federal law to obtain injunctions to shut down these Internet sites.

If we have learned anything from this experience, it is that combating pretexting is a war where the unscrupulous continuously seek out vulnerabilities and weaknesses in the carrier defenses. Unfortunately, no defense will be perfect, which is why we need a good offense and strong enforcement measures against these criminals.

In closing, I echo Chairman Barton's sentiment that "(w)hile businesses have legitimate reasons to compile and keep the data that define our lives, they have a responsibility to safeguard it as if it were their own."

Again, thank you for this opportunity and I welcome any questions you may have.

MR. SHIMKUS. Thank you. And now I would like to recognize Mr. Edward Merlis, Senior Vice President, Law and Policy of the United States Telecom Association. Welcome.

MR. MERLIS. Thank you, Mr. Chairman and members of the committee. On behalf of our more than 1,200 innovative member companies ranging from some of the smallest rural telecoms to some of the largest corporations in the U.S. economy, I want to thank you for this opportunity to testify on protecting consumers' phone records. Our member companies offer a wide range of services across the communications landscape, including voice, video and data over local exchange, long distance, Internet, and cable networks. We are united in our belief that it is time to update the Nation's communications laws to reflect the dramatic technological and marketplace changes all consumers have witnesses in recent years.

U.S. Telecom and all of its members share your concern for protecting customer information. Protecting the privacy of customer communications and records is an essential component of customer care by our companies, critical to the success of their businesses, and a responsibility we all take very seriously. More importantly, it is the right thing to do. In today's intensely and increasingly competitive environment, carriers must take care of their customers if they are to succeed. The growth and the use of cell phones, e-mail, and text messaging has already reduced the number of wire line phone customers. Our member companies cannot afford to take any customer and his or her confidential information lightly, or else they risk losing that customer's business.

As our companies attempt to offer video services, they stand little chance of successfully winning customers away from incumbent video providers, despite lower prices and enhanced services, if consumers cannot trust our member companies to safeguard their private information. In addition to this strong business incentive to protect customers from potential harm caused by fraudulent operators, Section 222 of the Communications Act imposes a legal obligation, "a duty to protect the confidentiality of proprietary information of and relating to their customers." We take this responsibility very seriously and our member companies have devoted significant efforts towards

implementing a wide range of practices and procedures to safeguard the privacy of customer information.

The practices include: the education and training of customer service employees, implementation of security protocols, and tightly defined agreements between our members and other businesses. Nevertheless, there are those who seek to breach these safeguards for nefarious purposes. Thus, we believe the best way to address the problem is through the enforcement of existing laws and the strengthening of those laws, in addition, of penalties on bad actors who obtain information through unauthorized or fraudulent means.

Pretexters, by their very nature, pretend to be the customer in order to gain access to protected records. Thus, the pretexters' activities would seemingly constitute an unfair and deceptive practice under Section 5 of the FTC Act. Since many of the so-called data brokers who use fraudulent methods or employ pretexters to obtain consumer information are readily identifiable, they should be subjected to swift FTC enforcement. New rules related to this issue should focus on prohibiting bad actors, rather than increasing the burdens on parties acting responsibly to protect consumer information.

While some have called for new specified security measures, consideration and adoption of new laws must not give wrongdoers a roadmap to obtain confidential customer information, for it is highly likely that as soon as the carriers implement specified mandated security measures, crooks will quickly adapt their methods to circumvent these new requirements identified in any law or regulation. So too, we would caution care in the implementation of new specific security mandates that might risk adversely affecting consumers. Our member companies serve a diverse demographic background in terms of age, language, disability, and education and they need the ability to develop specific solutions to meet their individual customers' needs.

Imposing a one size fits all requirement may unduly impede legitimate transactions between our member companies and their customers. Mr. Chairman, we want to 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 apprehending bad actors, while not impeding the needs of our customers. I look forward to responding to any questions you may have. Thank you.

[The prepared statement of Edward Merlis follows:]

PREPARED STATEMENT OF EDWARD MERLIS, SENIOR VICE PRESIDENT, LAW & POLICY, UNITED STATES TELECOM ASSOCIATION

Mr. Chairman, Ranking Member Dingell and members of the Committee, I am Edward Merlis, Senior Vice President, Government and Regulatory Affairs of the United

States Telecom Association (USTelecom). On behalf of our more than 1,200 innovative member companies ranging from the smallest rural telecoms to some of the largest corporations in the U.S. economy, I want to thank you for this opportunity to testify on protecting consumers' phone records.

Our member companies offer a wide range of services across the communications landscape, including voice, video and data over local exchange, long distance, Internet and cable networks. We are united in our belief that it is time to update the nation's communications laws to reflect the dramatic technological and marketplace changes all consumers have witnessed in recent years.

This Committee has a long history of engagement in consumer protection and given Chairman Barton and Representative Markey's Co-Chairmanship of the Congressional Privacy Caucus, I know that the issue of safeguarding customer proprietary network information (CPNI) is of acute concern. I also appreciate the interest of Representatives Blackburn and Inslee in this issue and look forward to working with them as they move forward with their legislation.

USTelecom and all of its member companies share your concern for protecting customer information. Protecting the privacy of customer communications and records is an essential component of customer care by our companies and critical to the success of their businesses.

In today's intensely and increasingly competitive environment, carriers must take care of their customers if they are to succeed. The growth in the use of cell phones, email and text messaging has already reduced the number of wireline phone customers. Millions of customers have also switched their phone service over to those using Internet technologies. Our member companies cannot afford to take <u>any</u> customer and his or her confidential information lightly – or else they risk losing that consumer's business. As our companies attempt to offer video services, they stand little chance of successfully winning customers away from incumbent video providers – despite lower prices and enhanced services – if consumers cannot trust our member companies to safeguard their private information.

In addition to this strong business incentive to protect customers from potential harm caused by fraudulent operators, Section 222 of the Communications Act imposes a legal obligation as well. Telecommunications carriers have "a duty to protect the confidentiality of proprietary information of, and relating to, … [their] customers." This existing legal obligation is one taken very seriously by our member companies that have, in turn, devoted significant resources towards implementing a wide range of practices and procedures to safeguard the privacy of customer information. These practices include the education and training of customer service employees, implementation of security protocols and tightly defined agreements between our members and other businesses.

As Chairman Martin recently noted in his response to Representative Markey's inquiry, FCC rules already require "carrier[s] to certify annually that it has established operating procedures that are adequate to ensure compliance" with their Section 222 obligation, and "provide a statement explaining how [their] operating procedures ensure such compliance."

We believe the best way to address this problem is through the enforcement of existing laws and the strengthening of penalties on the bad actors who obtain information through unauthorized or fraudulent means. "Pretexters" are those who *pretend*to be the customer in order to gain access to protected records. By definition, these pretexters' activities would seemingly constitute an unfair or deceptive practice under Section 5 of the FTC Act.

Additionally, many of the so-called "data brokers," who use fraudulent methods or employ pretexters to obtain consumer information, are readily identifiable and should be subject to swift FTC enforcement. In fact, these brokers boldly advertise their purported ability to obtain confidential calling data. Any new rules related to this issue should focus

on prohibiting bad actors rather than increasing the burdens on parties acting responsibly to protect consumer information.

While some have called for new mandated security measures, consideration and adoption of a new law must not give wrong-doers a roadmap to obtain confidential customer information. Moreover, it is highly likely that as soon as carriers implement specified, mandated security measures, crooks will quickly adapt their methods to circumvent new requirements identified in law or regulation.

As the Committee considers this issue, we would caution that new, specific security mandates also run the risk of adversely affecting consumers. Our member companies serve a diverse demographic background in terms of age, language, disability, and education, and they need the ability to develop specific solutions to meet their individual customers' needs. Imposing a one-size-fits-all requirement may unduly impede legitimate transactions between our member companies and their customers.

Mr. Chairman, 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 apprehending bad actors while not impeding the needs of our customers.

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

MR. SHIMKUS. Thank you, Mr. Merlis. Now I would like to recognize Mr. Marc Rotenberg, Executive Director of Electronic Privacy Information Center. Welcome, sir. Your full statement is in the record. You have five minutes.

MR. ROTENBERG. Thank you very much, Mr. Chairman, members of the committee. It is a real pleasure and an honor to be here today and I thank you for holding this hearing. EPIC contacted the Federal Trade Commission last summer when we first realized that there were companies on the Internet that were selling personal call detail information. Those monthly bills that we each receive listing the people that we have called were available for sale, and we supplemented our filing to the Federal Trade Commission in August when we had identified 40 such companies that were making this information for sale on the Internet. We filed a petition with the FCC because we believe that if this type of telephone record information was being made available for sale to the public, the FCC should take action, and I have to say I was very pleased to hear the Chairman of the FCC say on the last panel that the Commission plans to act on our petition.

We do think, though, it is very important that Congress send a clear signal that pretexting is a crime and we can't rely on the current ambiguous interpretations of Section 5 of the FTC Act to provide adequate protection. It has to be clear to the public and to anyone who would engage in this practice that it is unfair, it is deceptive, it is unethical, it is illegal, it is wrong, and it should stop. But we also believe it will be important to strengthen the security standards for the companies that collect personal information about their customers. This was the point that we raised in our petition to the FCC. There is an obligation on companies that have information on customers to ensure

that it is not used for improper purposes, and the problem of the illegal sale of this type of information arose in part because the telephone companies made this information available too readily.

Mr. Chairman, I would also like to point out in my statement that I emphasize the ongoing concern about the collection and use of call detail information. Even if you criminalize pretexting, and even if you raise the security standards for the companies that collect this type of information, there is still the risk that it can be improperly accessed by others for security breaches. And we would like you to consider the long-term, whether the best possible solution to this problem might not involve limiting the collection and use of this type of personal information.

Finally, Mr. Chairman, during the last panel there was quite a bit of discussion of an important case called U.S. West v. FCC, and I am very familiar with that case because we participated when it was before the 10th Circuit. It was during the discussion on the last panel that I had the opportunity to go on line and find EPIC's web page on that case. I would like to read for you, if I may, the sentence that the FCC included in their petition when they urged the 10th Circuit to reconsider their decision to eliminate the opt-in rule that the FCC had announced.

When the FCC filed the petition for rehearing, the FCC wrote, "This case involves questions of exceptional importance affecting governmental efforts to protect the privacy of telephone customers and to promote competition in the telephone industry." My organization, EPIC, gathered 22 consumer and privacy organizations and 15 legal scholars and technical experts in support of the FCC petition. We felt the Commission was absolutely correct to try to safeguard the opt-in rule and since the issue was raised on the last panel, I hope this is something that the committee will come back to. Consumers are at risk in the opt-out environment and we are seeing that today in the way that pretexters take advantage of the online sale of personal information.

Thank you again for the opportunity to testify. I would be pleased to answer your questions.

[The prepared statement of Marc Rotenberg follows:]

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

Introduction

Chairman Barton, Ranking Member Dingell, and Members of the Committee, thank you for the opportunity to testify on the privacy of telephone records. My name is Marc Rotenberg and I am Executive Director and President of the Electronic Privacy Information Center in Washington, DC. EPIC is a not-for-profit research center established to focus public attention on emerging civil liberties issues and to protect

privacy, the First Amendment, and constitutional values. We have played a leading role in emerging communications privacy issues since our founding in 1994.

We thank the Members of the Committee and others who are developing legislation to address pretexting and to increase security standards at companies that collect and maintain data. In this statement today, I will summarize EPIC's efforts to bring public attention to the problem of online data brokers and pretexting, suggest several approaches to the problem, and make specific recommendations concerning future legislation.

EPIC's Efforts to Address Pretexting

In July 2005, EPIC 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. Pretexting is a practice where an individual impersonates another person, employs false pretenses, or otherwise uses trickery to obtain records.

These sites offer unscrupulous people an illegal shortcut around legal methods of getting data. For instance, if an individual has a legitimate reason to obtain records, they can go to a court and obtain a subpoena. Online data brokers, on the other hand, try to sidestep these legal procedures even as they make personal information available to others. For instance, online data broker "Bestpeoplesearch.com" wrote: "This search is for RESEARCH purposes ONLY. If you find information contained in our reports and need them for legal purposes you must subpoena the records from the telephone carrier to use them in a court of law. This is a confidential report between Best People Search and you (our client)."[1]

EPIC supplemented that filing in August 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 online, EPIC also petitioned the Federal Communications Commission, urging the agency to require enhanced security precautions for phone companies' customer records.[2] Telephone carriers unanimously opposed enhanced security requirements, and proposed that lawsuits against pretexters would solve the problem. But enforcement alone will not solve this problem. It will simply drive these practices underground, where they will continue with less public scrutiny. Simple security enhancements, such as sending a wireless phone user a text message in advance of releasing records, could tip off a victim to this invasion of privacy and block the release.

Cell Phone Records Are the Tip of the Pretexting Problem

While the sale of cell phone records has gained significant media attention, pretexting is used to obtain many other types of records. Alongside many advertisements for cell phone records, wireline records and the records associated with calling cards are advertised. As individuals shift to VOIP telephones, it is safe to assume that those records will be targeted with pretexting as well.

Pretexting Presents Serious Risks to Victims of Domestic Violence and Stalking

Some websites, such as Abika.com, advertise their ability to obtain the real identities of people who participate in online dating websites. A page on Abika.com advertises the company's ability to perform "Reverse Search AOL ScreenName" services, a search that finds the "Name of person associated with the AOL ScreenName" and the "option for address and phone number associated with the AOL Screenname."[3] The same page

---

[1] Exhibit E to *In re Intelligent e-Commerce, Inc*., *available at* http://www.epic.org/privacy/iei/

[2] Petition of EPIC for Enhanced Security and Authentication Standards, *In re Implementation of the Telecommunications Act of 1996*, CC Docket No. 96-115, *available at* http://www.epic.org/privacy/iei/cpnipet.html.

[3] See http://www.abika.com/Reports/tracepeople.htm#Search%20Address/Phone%20Number%20associated%20with%20email%20Address%20or%20Instant%20Messenger%20Name.

offers name, address, and phone number information for individuals on Match.com, Kiss.com, Lavalife, and Friendfinder.com. These are all dating websites that offer individuals the opportunity to meet others without immediately revealing who they are.

The availability of these services presents serious risks to victims of domestic violence and stalking. There is no reason why one should be able to obtain these records through pretexting. If someone on one of these services harmed another, their identity could be determined through normal legal processes.

It is important to recall that a stalker employed online data broker Docusearch.com and a private investigator who used pretexting in order to locate and kill Amy Boyer in 1999. The killer hired Docusearch to request Boyer's social security number (SSN) and employment information. Docusearch located the SSN, but could not find her employment address in a database. Docusearch then obtained Boyer's work address by having a subcontractor, Michelle Gambino, to place a pretext call to Boyer. Gambino lied about who she was and the purpose of her call in order to convince Boyer to reveal her employment information--Gambino pretended to be affiliated with Boyer's insurance company, and requested "verification" of Boyer's work address in order to facilitate an overpayment refund. Docusearch charged Youens $109 for this information. Boyer's address was given to her stalker who later killer her and committed suicide.

Pretexting Should be a Crime

In light of the fact that pretexting is being used to sell a wide variety of private personal information, and that pretexting has been used to stalk individuals, we believe that there should be a broad prohibition on pretexting. We urge the Committee to examine the services that should be protected against pretexting, because this technique is used against many businesses. At a minimum, the federal legislation should cover all communications services, including web sites, Internet Service Providers, dating services, and emerging communications systems, such as GM's OnStar automobile navigation service.

Pretexting is a dangerous practice that should not be employed by investigators for hire. We urge the Committee to oppose any exemptions to a ban on pretexting. Investigators will claim that they have legitimate uses for pretexting, such as locating lost children. However, where investigators have a legitimate need for datathere are routine legal measures to obtain information. An exemption for investigators would be a green light to engage in this behavior. Private investigators, who are major buyers of personal information, are not licensed in all fifty states, and in some states that require licensure, it is a pro forma process.[4]

Reasonable exemptions should be in place. For instance, companies should be able to use pretexting to test their own systems' defenses against fraud.

New Laws Are Necessary

Despite the fact that online data brokers are committing fraud and breaking the law, these sites continue to advertise openly and claim that their methods are legal. Though some of the more infamous sites, in light of recent attention to their practices, have removed offers of cell record searches from their sites, dozens, if not hundreds, of other companies exist and advertise that they can obtain cell phone records.[5] Even more

---

[4] "Some States have few requirements [for private investigator licensure], and 6 States—Alabama, Alaska, Colorado, Idaho, Mississippi, and South Dakota—have no statewide licensing requirements while others have stringent regulations." U.S. DEPARTMENT OF LABOR, BUREAU OF JUSTICE STATISTICS, PRIVATE DETECTIVES AND INVESTIGATORS, Mar. 21, 2004, available at http://www.bls.gov/oco/ocos157.htm.

[5] As of January 28th, some of these sites include aaaskiptrace.com, completeskiptrace.com, datafind.org, datatraceusa.com, discountphonebust.com, gum-shoes.com, locatecell.com,

importantly, those sites that claim to have repented and removed phone record dossiers from their sites still advertise the ability to: (1) track down the home addresses of email account holders; (2) the home addresses and phone numbers of people who use online dating services, eBay, or AOL; the home addresses of P.O. box owners, and much more.[6]

Current fraud laws, even if more zealously enforced, will not be enough to stem the tide of companies that insist that their methods are legal. A pretexting company sued or prosecuted under fraud laws may still attempt to paint its practices as non-deceptive, and thus not covered by Section 5 of the Federal Trade Commission Act. For instance, companies may claim that, since the consumer whose records they have taken is not their customer, they have no business relationship, and thus no duty to act fairly and honestly with that consumer's information or with the phone company. In arguing that they are not regulated by the FTC Act, these companies may rely upon a statement made by Commissioner Orson Swindle in 2001, in which he questioned whether pretexting was in fact a deceptive or unfair practice.[7]

In that case, however, Congress had created another means for punishing the wrongdoers.[8] Section 521 of the Financial Services Modernization Act, otherwise known as the Gramm-Leach-Bliley Act,[9] specifically prohibits pretexting, by making it crime to obtain financial records "by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution." Coupled with FTC enforcement, this provision has killed the public market for pretexted financial information. However, in the twisted logic of online data brokers, the GLBA has become an argument that pretexting to phone companies is legal. They argue that if Congress wanted to ban pretexting more broadly, it could have expanded the GLBA prohibition beyond financial institutions. A new law is needed to provide the same protections for cell phone and other communications records that the GLBA has provided for financial information.

A law banning pretexting would make clear that this practice is unfair, deceptive, illegal, and wrong.

Carriers and Other Holders of Personal Information Should Have Legal Obligations to Shield Data from Fraudsters

Pretexting, however, is only half of the problem. Pretexting works because phone companies and others who store our communications records fail to adequately protect our personal information. Phone companies can be fooled into releasing information easily because releases of customer information are so routine, and because they use inadequate means to verify a requester's identity. If carriers only require a few pieces of easily-obtained information to verify a requester's identity (such as date of birth, mother's maiden name, or a Social Security number), then pretexters can impersonate account holders and obtain records with ease. All of this information is easily obtained in commercial databases or in public records. Furthermore, the online data brokers who do the pretexting often have easy access to these banks of private dossiers on individuals.

---

mrandmrsdetective.com, peoplesearchamerica.com, personsearch.us, publicpeoplefinder.com, records.com, and secret-info.com.

[6] See, e.g., abika.com, bestpeoplesearch.com, information-search.com, matecheckpi.com, phonebust.com, piedmontpi.com, and usaskiptrace.com.

[7] Dissenting Statement of Commissioner Orson Swindle, *In re Touch Tone Information*, File No. 982-3619. (Jun. 27, 2000), *available at* http://www.ftc.gov/os/2000/06/touchtoneswindle.htm. See also Dissenting Statement of Commissioner Orson Swindle, *In re Information Search, Inc.*, File No. 0123083 (Apr. 18, 2001).

[8] Commissioner Swindle expressly noted this in his *Touch Tone* dissent. See note 7 *supra*.

[9] Pub. L. No. 106-102, §521, 15 U.S.C. §6821 (2000).

Any legislation that is to fully address the problem of private information sales must therefore look not only at the tactics used by bad actors, but the loopholes and vulnerabilities they exploit.

Security standards for communications carriers must therefore be strengthened. EPIC's August 2005 petition to the FCC notes that telecommunications carriers are obligated under Section 222 of the Telecommunications Act to protect customer information. Though previous FCC actions have focused on the rules and guidelines for the disclosure of customer information for marketing purposes, this provision should also require the FCC to address the security standards necessary to protect records from pretexters. The FCC has recently acknowledged the seriousness of this problem, and Commissioners Adelstein and Copps have both cited EPIC's petition as a possible means for improving security.[10] Congress should encourage the FCC to act, by having the Commission create and enforce regulations that require commonsense security practices. Such practices include: requiring better customer identity verification (such as customer-defined passwords); limiting the addresses to which sensitive customer records may be sent; and keeping audit trails of when and by whom customer information is accessed and disclosed.

Carriers Should Limit Data Retention and Disclosure

An even more fundamental question in this discussion—more fundamental than how data brokers pretext information, or what vulnerabilities they exploit—is why this sensitive information is there to be stolen in the first place. The records that data brokers buy and sell online are often simply our past phone bills. The numbers we dial, the times of our calls, and the length of our conversations are known because of the way in which the cellular billing system is structured. Since our bills are based on when we talk, how long we talk, and what numbers we call, consumers want and need an accounting of these facts so that they can track the charges on their bills. But what happens then is that this collected information is then available to be misappropriated and abused.

One way to alleviate this problem would be to delete records after they are no longer needed for billing or dispute purposes. This, however, could leave consumers still vulnerable in the time between payment periods. Another alternative would be simply to not record and disclose all of this information. If telephone service were billed as a utiltity, as it was in the past for local service and may be in the future with VOIP service, many of the threats to privacy would simply disappear.

The vulnerabilities that our by-the-minute system of billing build into our phone records is a good example of how decisions made about a communication system's initial structure and function create built-in privacy issues. In a letter that EPIC sent to then-Chairman Powell of the FCC, we noted that the emergence of new communications systems, such as Internet telephony, requires that Congress and executive agencies look forward in creating privacy-protective regulatory frameworks into which the new technologies can grow.[11] We support the efforts that some members of Congress have made in extending proposed anti-pretexting provisions to Internet telephony and other communications services.

CHAIRMAN BARTON. Okay. We are going to hear from Mr. Douglas and then we have three votes on the floor, the first one is a 15 minute

---

[10] See Statement of Commissioner Adelstein on Brokering of Personal Telephone Records, Jan. 17, 2006, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263216A1.pdf; Commissioner Copps Calls for Action to Address Theft of Phone Records, Jan. 17, 2006, *available at* http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-263222A1.pdf.

[11] Letter of EPIC to FCC Chairman Powell, Dec. 15, 2003, *available at* http://www.epic.org/privacy/voip/fccltr12.15.03.html.

vote. I am hopeful that the next two are five minute votes, so once we hear from Mr. Douglas, we are going to recess and then we will reconvene as quickly as possible, which is probably going to be about ten minutes after 5:00 p.m. So we are going to hear from you, Mr. Douglas, and then we are going to go vote.

MR. DOUGLAS. Thank you very much, Mr. Chairman. For the last nine years I have studied the issue of pretext identity theft, the use of deceptive practices to steal personal information, of all types of consumer information, and I have been an expert witness three times that are relevant to this hearing; Operation Detect Pretext, which the FTC has mentioned; the murder of Amy Boyer in New Hampshire when her information was sold through one of these brokers after being obtained through and pretext sold to a stalker who gunned her down as she left work; and in the Florida statewide grand jury on identity theft, I testified as an expert on pretext.

What I would like to do is submit my written statement, which is quite extensive and it answers an awful lot of the questions that were asked of the first panel, but uses pictures instead of words. With the assistance of your staff, we have put some sites up. All of these I collected this morning, and I would like to paint a picture with these sites.

Cellulartrace.com is relevant because this is named in the EPIC complaint. Even though some suits have been brought against some providers, this company is still out there as of this morning and you can see they are selling cellular number traces, detailed cellular number traces, and most specifically, cellular call records and talks about in great detail for the price what you get. But I thought this was more interesting than all. The publicity in the last few weeks is driving their business higher. It says on here "Notice: As a result of the recent newscasts on cellular research, we have been completely inundated with orders. We are getting caught up as quickly as possible, but those placing new orders should expect delays."

The next is a page from hackershomepage.com, which I have been talking about for the last five years, at least, that sells all types of different hacking devices. This one is most relevant, a telephone voice changer, because I noticed in some of the published reports surrounding the Verizon suits that have been brought, Verizon has acknowledged that one of the means of deception has been to imitate a non-realistic division of Verizon called the Disabled Customer Division and they call in and pretend they are sitting with a disabled customer. Even if the Verizon customer service representative asks for an acknowledgement from the customer, they use one of these voice changing devices to sound as if they are disabled and that they are the customer.

The next is an issue that I think is also worthy of the attention of the committee and to expand upon that, this isn't just phone records, per se, or just pretext, which is the number one method. Bribery is the number two method. Using online access deceptively is the number three method being used in the country today. This is a website called SpoofTel or others like this. There are devices sold, there are chat rooms where this is discussed. SpoofTel allows you to make your phone look like anybody else's phone. Social hacker Kevin Mitnick once said or demonstrated for a reporter in a magazine article how he made a call look like it was coming from the White House.

Well, you can make these calls look like they are coming from law enforcement, as we have talked about. You can make these calls look like they are coming from your phone company or your bank in order to deceive, like phishing, p-h-i-s-h-i-n-g, to deceive the customer into turning over information, themselves believing they are speaking to their phone company or their bank. That is why when we attacked this from Gramm-Leach-Bliley, and I believe Mr. Markey was very involved in that and may recognize me from 1998, when we attacked that, we also outlawed the use of these tactics against the customer, not just the companies, because it works both ways.

Very quickly, this is Docusearch and there is a real convergence here back around 1998, 1999. As Gramm-Leach-Bliley was being passed and as Docusearch was advertising that they were the cover story of Forbes Magazine November 1999 documenting how they stole financial records, how they stole most particular for here, phone records. Mr. Markey may remember precisely what happened in November of 1999. President Clinton signed Gramm-Leach-Bliley into law. So here we had at the same time that that was happening, he was advertising what he was doing.

I know my time is short, Mr. Chairman. A few more slides. At that same time period, October 15th, 1999, this woman was murdered when that company, Docusearch, sold her information obtained through pretext imitating an insurance company, calling her mother saying there was a refund to be made. As her mother said, I was made an accomplice to my own daughter's murder. So all of this has been going on since that time and there is the killer, Liam Youens, who was documenting on a web site for more than a year his plans to kill Amy Boyer. The last sentence on this, he says "It is actually obscene what you can find out about a person on the Internet" and documented specifically how he was using these companies that we are talking about in order to steal that.

And you will forgive me, Mr. Chairman, if I am having a case of deja vu today because of the hearing in 1998 and I had forgotten about this until I pulled out my friend, Bob Sullivan's book, Your Evil Twin:

Behind the Identity Theft Epidemic. One paragraph, Mr. Chairman, talks about me sitting next, on CSPAN, to a convicted felon who documented exactly what was happening. The FTC was sitting precisely behind me in the chair and he said Schweitzer tells Douglas--that is the convicted felon that testified in the hearing—"in the hallway that he has become disgusted by the business, this information broker business, which now sells everything and anything." Police pager numbers are sold to Mafia figures--that is the Touch Tone case that the FTC has known about and not done anything when it came to those phone records, to Mafia figures. Pretty girls' home addresses are sold to stalkers.

Schweitzer agreed to testify to blow the lid off the business. Here is the paragraph. "Throughout my career I have been involved in the gathering of confidential information of all types; credit information, unlisted telephone numbers, telephone toll records, medical records, and on and on and on." So the issue has been out here since 1998. The FTC has known about it since 1998 and they have not brought a single case when it comes to phone records. Thank you, Mr. Chairman.

[The prepared statement of Robert Douglas follows:]

PREPARED STATEMENT OF ROBERT DOUGLAS, CHIEF EXECUTIVE OFFICER, PRIVACYTODAY.COM

Chairman Barton, Ranking Member Dingell, members of the Committee, my name is Robert Douglas and I thank you for the opportunity to appear before the Committee to address the Committee's concerns about the theft of Americans' phone records.

I. Background and Basis of Knowledge

I am the CEO of PrivacyToday.com and work as an information security consultant to the private and public sectors on issues involving all aspects of identity theft, identity fraud, and customer information security. During the past nine years I have assisted the financial services industry, the general business community, government, and law enforcement agencies to better understand the scope and methodology of identity crimes through educational materials, presentations, auditing, and consultation.

My specialty is monitoring and investigating the practices of identity thieves, illicit information brokers, and illicit private investigators that use identity theft, fraud, deception, bribery, social engineering, and "pretext" to steal customer and proprietary records from a wide range of businesses. Additionally, I teach businesses, government agencies, and law enforcement how to detect and defend against these forms of theft in order to better protect all Americans.

This is my sixth appearance before the United States Congress to discuss information security. Most relevant to today's hearing, I worked in 1998 with the House Financial Services Committee to expose the use of "pretext" and other forms of deceptive practices to steal and sell consumers private financial records maintained by financial institutions. That work resulted in the July 28, 1998 hearing titled "The Use of Deceptive Practices to Gain Access to Personal Financial Information". Testimony offered at that hearing resulted in the Gramm-Leach-Bliley Act provisions outlawing the use of deceptive practices to gain access to financial account information. In follow-up testimony I presented in a September 13, 2000 hearing before the same committee acting in its oversight capacity, I discussed the emerging and growing threat of deceptive practices

being used to gain access to phone records--the precise issue before you today. [The 1998 & 2000 testimonies, along with my other congressional testimonies are available at PrivacyToday.com/speeches.htm]

Following the 2000 testimony I served as a consultant and expert to the Federal Trade Commission in the design and execution of Operation Detect Pretext, a sting operation to catch and civilly prosecute companies participating in the illicit information market.

In 2002 I testified as an expert witness on illicit information brokers and the role they play in identity theft and fraud before the Florida Statewide Grand Jury on Identity Theft.

From 2001 to 2004 I was an expert witness and consultant for the plaintiffs in Remsburg v. Docusearch, a suit brought by the parents of Amy Boyer against a private investigator selling illicitly obtained personal information via a web site. Ms. Boyer was murdered by an infatuated young man who purchased Ms. Boyer's social security number, date of birth, and place of employment from Docusearch who employed a "pretexter" to impersonate an insurance company official to obtain the employment address of Ms. Boyer. Subsequently the killer gunned down Ms. Boyer as she left work.

I am currently serving as a consultant in a Pennsylvania murder case involving the sale by a private investigator of data-mining "research" about the victim to a deranged former employee who used the "research" to locate the victim and kill him.

I assisted Chris Hoofnagle of EPIC West, who deserves full credit for this issue reaching the attention of Congress, with the amended complaints submitted to the FCC & FTC by compiling the 40 companies named therein.

I have lectured before local, state, federal and international law enforcement, banking, and business associations on the topic of identity crimes.

I am the author of "Spotting and Avoiding Pretext Calls" which was distributed by the American Bankers Association to all member institutions. I am also the author of "Privacy and Customer Information Security – An Employee Awareness Guide", a training manual that has been used by numerous banks and businesses to train employees to defend against deceptive practices designed to steal customer information.

Prior to my work as an information security consultant I was a Washington DC private detective.

II. Identity Thieves Use the Same Methods

I'd ask the Committee to keep one important fact in mind while investigating the practices of illicit information brokers and illicit private investigators stealing phone and other consumer rerecords. The methods used by those industries are used by identity thieves and financial criminals every day in this country to defeat customer information security systems for a wide-range of businesses.

Additionally, in each case I've worked involving web-based illicit information providers, when we have been able to review the files of the company, there have been indications of identity thieves and other criminals – including stalkers – using those companies to buy information about Americans. Finally, as we are focusing on phone records today, I would hazard an educated opinion that one of the reasons that the FTC lists cell phone fraud as one of the most common forms of fraud resulting from identity theft is the ease with which cell phone records are stolen or purchased on the Internet.

For further background information, I recommend reading "Your Evil Twin", by Bob Sullivan. I'd also like to recommend Robert O'Harrow's "No Place To Hide" as an excellent work on the growing data-mining industry and a number of the public policy issues raised by this industry.

III. The Illicit Sale of Phone Records and Much More

News reports have served an important role in bringing the problem of web-based information brokers and private investigators selling detailed phone records to the

attention of this committee, Congress, and the American people. While reporting by Robert O'Harrow of the Washington Post and Bob Sullivan of MSNBC on the sale of phone records dates back to the late 1990's, the issue has only recently caught the full attention of the American consumer and law enforcement agencies across the country.

In part this was due to the work of Frank Main at the Chicago Sun-Times who discovered that the Chicago Police were concerned that the sale of detailed cell phone records could jeopardize the safety of police officers and criminal investigations. Subsequently, Frank Main reported that the FBI was alarmed to learn in a test purchase of a web-based information broker that anyone could obtain the cell phone records of a FBI agent within a matter of hours from placing the order.

As the committee will learn a bit later in my testimony, the Chicago Police and FBI were correct in their concerns as years ago the phone records of Los Angeles police officers had been sold by an information broker to organized crime.

But for the most part, the overwhelming number of news reports has inadvertently served to minimize the scope and extent of the problem. While the vast majority of reporting has focused on cell phone records and a small number of web-based brokers selling those records, the reality is that all entities that maintain consumer and proprietary information are under attack. The list includes, but is not limited to, telecommunication (including email and Internet service providers), cable and satellite television, utility (including electric, gas, water & sewer companies), and financial industries, plus all government agencies. In short, any business or government agency maintaining customer records or confidential proprietary information is at risk because identity thieves, illicit information brokers, illicit private investigators, corporate spies, and con artists know quite often the most effective tool for stealing highly valued information is the telephone.

In addition to minimizing the types of consumer information for sale, recent news reports have also inadvertently minimized the number of outlets and methodologies via which phone records can be purchased or stolen. Even the range of telecommunications records for sale has been inadvertently minimized with most media focusing on just the sale of cell phone records.

Specifically, there are far more web-based illicit information brokers and illicit private investigators than the 40 cited in the EPIC West complaint and there are a myriad of methods used to defeat phone company information security protocols far beyond the simple pretext of impersonating the customer. Additionally, when considering phone records, all types of telecommunications records are for sale—from home and business phone records to cell phone records to reverse-911 cell tower location information to pager records to GPS tracking devices to name just a few categories.

Finally, the reporting has inadvertently minimized the dangers posed by phone records and other forms of information stolen by means of pretext falling into the wrong hands when information brokers and private investigators sell either information obtained through pretext, or even database information, to individuals without any understanding of why the individual wants the information. Murders and assaults have occurred when information brokers and private investigators have not taken adequate steps to understand who they are providing information to.

With the caveat that <u>all</u> consumer records and government/business proprietary information are at risk; that there are far more than the 40 brokers and investigators selling phone and other records cited in the EPIC West complaint; and, that these records in the wrong hands have caused severe harm – including loss of life, I will confine the remainder of my testimony to the sale of phone records obtained most commonly through pretext and other forms of deception.

<u>IV. To Understand Why Records Are Sold, You Need To Know Who Buys Them</u>

To understand why the phone records of practically any American – from former presidential candidate General Wesley Clark to women hiding under threat of violence – are for sale on the Internet, you need to know who is buying the bulk of the phone records that are obtained through illicit means. The overwhelming majority of phone records are purchased by attorneys, private investigators, skip tracers, debt collectors, and the news media.

Attorneys purchase the records as a means of discovery in all forms of litigation from divorce, to criminal defense, to "business intelligence". Private investigators buy phone records as a means of locating witnesses, developing leads, and developing evidence. Skip tracers use phone records to locate hard to find individuals who may be using deceit themselves to cover their tracks. Debt collectors find phone records a valuable tool in locating "deadbeats" who may be hiding from the collector and/or hiding assets. The news media – especially the tabloid press – want phone records to track celebrities' lives and develop leads in cases like the Jon Benet Ramsey murder, the Columbine massacre, and the freeway slaying of Bill Cosby's son. Each of these categories of users and purchasers have at one time or another made impassioned pleas to me that they need access to phone records – outside of normal judicial review processes – to conduct what they argue are socially beneficial services.

These buyers and their thirst for the information contained in detailed phone billing records resulted in the market and the cash flow that fed and encouraged the online sale of phone records. Specifically, the methods for stealing phone records had been known and in use for decades in order to service attorneys, private investigators, skip tracers, debt collectors, and the news media. With the advent of the Internet and the World Wide Web it was only a matter of time before some illicit information broker or private investigator decided to advertise the availability of phone records on the web. And once the first ads appeared and other brokers and investigators learned how much money could be made selling phone records via the Internet – in some instances more than a million dollars per year for small operations – the feeding frenzy was on. So today there are hundreds of ads on the web (and in legal and investigative trade journals) for phone records and phone "research". And contrary to the language on those sites claiming to limit sales of personal information to attorneys; investigators; skip tracers; debt collectors; and, bail bondsmen, most of these companies will sell to anyone as long as they think you're not a reporter or law enforcement agency conducting a media expose or sting operation. Frankly, greed is the name of the game.

Those hundreds of ads on the web only represent the tip of the iceberg. Two other factors combine to push the total to thousands of outlets for purchasing phone records. First, many brokers and investigators don't advertise on the web or at all. These brokers and investigators work beneath the surface and develop clients by word of mouth while shunning publicity. Many of these hidden brokers and investigators are the actual sources – once removed – for the information sold via the web as many of the web-based operators are not skilled in the methods of stealing customer information and serve as mere front companies. Second, the brokers and investigators who shun a web presence but supply many of the web-based operations, also supply other brokers and investigators throughout the country who don't openly advertise on the web or anywhere else. And often those brokers and investigators service other brokers and investigators in a spider web or pebble-dropped-in-the-pond effect. Through this black market phone records may pass through several sources – at times including a bribed phone company insider – before reaching the eventual buyer. So in reality there are thousands of brokers and investigators, on the web and off, comprising the totality of suppliers of illicit phone records. And the records are now for sale to anyone who wants them – regardless of reason.

V. How Phone Records Are Obtained

Phone records are obtained through numerous methods and sources. Some of these methods and sources have been publicly discussed – some have not.

By far the most common method is the use of "pretext". Pretext, used in this fashion, is the method of convincing someone you are a person or entity entitled to obtain the records sought. The term "pretext" when used in the context of obtaining confidential, statutorily protected, or consumer and proprietary information is actually a misnomer used by illicit brokers and investigators to add an air of legitimacy to the fraud they commit. The reality is pretext is a combination of identity theft and fraud. Identity theft because the individual carrying out the pretext needs to assume the identity of the rightful owner of the information sought – usually including biographical information such as name, address, social security number, and date of birth – in order to impersonate that individual during the pretext. Fraud because once impersonating that individual, the pretexter defrauds the rightful custodian of the information sought into turning the information over to an improper recipient.

To further understand pretext you need to know the code of the identity thief, broker, or investigator seeking information they don't have legitimate access to.

1) Know what piece of information you want.
2) Know who the custodian of the information is.
3) Know who the custodian will release the information to.
4) Know under what circumstances the custodian will release the information.
5) Become that person with those circumstances.

Once you know the code and apply a little imagination and bravado, you can steal almost any piece of information in this country.

But again, contrary to most reporting on this subject, the number of pretext methods and variations of those methods are vast and far beyond just merely impersonating the consumer. By way of example, in a state action brought under an unfair and deceptive trade practice statute captioned Massachusetts v. Peter Easton, Easton was caught calling into banks impersonating a federal banking official in order to get the banks to surrender consumer financial account records. In one of the current Verizon cases involving phone records, there is report indicating the information brokers were impersonating Verizon employees assisting disabled account holders. These are just two of literally dozens of variations of methods I am aware of that succeed thousands of times each day in defeating phone and other companies customer authentication procedures.

An important aspect in the conduct of a pretext is the ability of the illicit information broker or private investigator to purchase data about the individual consumer they seek to impersonate. After all, to fraudulently convince a customer call center representative that the pretexter is the actual customer, the pretexter needs to know the full name; social security number; date of birth; address; and, other forms of personal identifying information of the actual account holder. In order to gain access to this information, the illicit information brokers and private investigators need to have subscriber accounts with legitimate data-mining companies—also commonly referred to as information brokers.

Beginning approximately a year ago, it became more difficult for illicit information brokers and private investigators to get or maintain subscriber accounts with the large legitimate data-mining information brokers. This is because in the wake of reports of data breaches by legitimate information brokers and a wide variety of other businesses maintaining consumer records – coupled with congressional hearings examining the data breach problems and the ease with which personal information like social security numbers could be purchased from many of the illicit brokers and investigators we are discussing today – the legitimate data-mining information brokers began to curtail and in some cases terminate all sales of information to private investigators and other business lines with a history of improper resale or use of database information.

But other small and mid-size companies have stepped in to fill the void and continue to provide social security numbers and other personal identifiers to illicit information

brokers and private investigators. I am aware of at least a dozen companies that illicit information brokers and illicit private investigators are using to obtain full social numbers and other biographical data in order to conduct pretexts against consumers and businesses. This is an issue crying out for attention by Congress.

The second most common method of gaining illicit access to phone records is bribery of a company employee or even the trade of information with inside employees working in skip-tracing and collection divisions within phone companies. There is a small but constantly present underground network of employees who trade information – sometimes lawfully, sometimes not – and those seeking information that have no lawful right to that information have learned how to tap those resources.

While I am not aware specifically of a case involving phone records where threats of violence were used to coerce phone company employees to supply information to criminals, that has happened in the financial services community resulting in federal banking regulatory agencies warning financial institutions of the trend a number of years ago. I would not be surprised if this was happening to phone company employees as well. Remember – information equals cash to all sorts of information thieves and they will do anything necessary to obtain the information they seek.

Finally, I have a substantial amount of evidence developed over nine years on methods, tactics, and sources used to obtain phone records that is inappropriate for revelation in an open hearing. I'd be happy to share this with the Committee, enforcement agencies, the phone associations, or companies in a closed setting.

VI. Phone Record Sales and "Spoofing" Services on the Web Are Most Alarming

While the totality of brokers and investigators selling phone records are troubling, the Internet-based operations are most alarming for the simple reason that by their very nature they allow a buyer to easily conceal their identity and intent in purchasing another citizen's records. This anonymity is a criminal's delight. From identity thieves to stalkers to child predators to corporate spies, the ability to conceal the identity and intent of the end user of the records is paramount.

Additionally, when consumers see the web sites advertising the sale of phone records and services like Caller-ID "spoofing" services designed to defeat Caller-ID, it increases mistrust between the consumer and businesses Americans provide information to, and increases the belief by many consumers that the government isn't protecting the American consumer.

Web based services like spooftel.com and the open sale of devices designed to show a different number on a Caller-ID system than the actual number the call is being placed from can be used as part of pretext and can even be used to defeat security systems for voicemail. In one well known demonstration of Caller-ID spoofing, convicted "hacker" Kevin Mitnick demonstrated for a reporter how he could make a call look like it was coming from the White House.

The use of spoofing services and devices as part of pretext is so well known within the investigative and information broker industries that advice on how to pick the best services is often bantered about. Here's an example:

If you are considering using one of the numerous Caller ID Spoofing services, you may want to know several things before you sign-up.

1. Can this service be employed as part of your PI business, or is it just to be used for entertainment purposes?
2. If it is to be use only for entertainment purposes, do they offer a commercial version, and if so what are the differences?
3. Do they record/log all transactions?
4. Can you call 800 numbers, or other toll free line?
5. Can you call financial institutions through their web site, even if the financial

institution is one you have an account with?
6. Can you use an anonymous Internet surfing software product (these change your IP number and make you appear as if you are accessing the internet from another state, country, etc.) to access their web site?
7. Will they inform you if they suspect fraudulent activity? What is their method for settling such a dispute?
8. Will they supply you with a list of all the activities that can lead to a cancellation of your account?

I raise the issue of Caller-ID spoofing fraud so this Committee will be aware that the extent of the problem is far more than just the sale of phone records. It is a myriad of techniques and use of technology designed to defeat information security systems. The use of these technologies – specifically Caller-ID spoofing devices and services should be outlawed immediately.

VII. Did The FTC Give Tacit Approval To The Sale Of Phone Records?

Given how prevalent and open the sale of phone records is, this Committee must be wondering how these companies and their devious practices have remained untouched by the Federal Trade Commission and other enforcement agencies. After all, the FTC is charged with stopping unfair and deceptive trade practices.

Congress and the American people have a right to ask a series of questions of the Federal Trade Commission when it comes to the sale of phone records. The questions include:

a) Was the FTC aware of the sale of phone records prior to recent news accounts?
b) If the FTC was aware, for how long has the FTC been aware?
c) Prior to recent media revelations and Congressional demands, did the FTC take aggressive steps to stop the sale of phone records?
d) Did the FTC signal tacit approval of the sale of phone records by private investigators?
e) Why has the FTC been AWOL when it comes to protecting phone records?

These questions are fair as, after all, the FTC is supposed to be the watch dog for the American consumer. Given my work with, study of, and access to information concerning the role of the FTC when it comes to illicit information brokers and private investigators I'd like to posit answers to the above questions as I believe the reality is that when it comes to phone records – and all other illicitly obtained consumer records – the watch-dog is nothing more than a lap-dog on a leash held by the illicit information brokers and private investigators.

a) Was the FTC Aware of the Sale of Phone Records Prior to Recent News Accounts?

Yes. The FTC has been aware of the sale of phone records due to the Touch Tone Information case; Operation Detect Pretext; the Boyer murder case; and direct interaction and communication with the private investigative profession – including direct inquiries from PI Magazine on the FTC's views regarding pretexting for phone records.

b) If the FTC Was Aware of the Sale of Phone Records, For How Long Has the FTC Been Aware?

The FTC has been aware of the problem since at least April of 1999 when the FTC filed an action against Touch Tone Information. While the FTC brought the action against Touch Tone for the sale of consumer financial information obtained by means of deception, the Touch Tone records available to FTC staffers were replete with thousands of instances of phone records being obtained and sold by means of deception.

In 2002 I interviewed the Colorado Bureau of Investigation detectives who broke the Touch Tone case and whose work the FTC piggy-backed in bringing the FTC complaint against Touch Tone. The detectives informed me the FTC showed little interest in following up on the voluminous records contained in the files of Touch Tone showing a vast network of hundreds of private investigators, attorneys, and media outlets around the country using Touch Tome to obtain phone and other records.

For example, as documented by the Washington Post, Touch Tone sold Kathleen Willey's phone records to a Montgomery County, Maryland private investigator during the investigation of President Clinton.

Additionally, the Touch Tone records contained the following letter listing phone and other records sold by James Rapp, co-owner of Touch Tone, about participants in the Jon Benet Ramsey murder investigation as reported by the Denver Post in a June 26, 1999 article titled, "Letter Details Information Rapp Dug Up". Each reference to "tolls" means detailed phone records.

Here is the text of an undated letter purportedly written by James Rapp to a private investigator in California named Larry Olmstead, owner of Press Pass Media. Olmstead used Rapp to get information for his clients, primarily tabloid media outlets, prosecutors say.

Dear Larry,

Here is a list of all Ramsey cases we have been involved with during the past lifetime (sic).

1. Cellular toll records, both for John & Patsy.
2. Land line tolls for the Michigan and Boulder homes.
3. Tolls on the investigative firm.
4. Tolls and home location on the housekeeper, Mr. & Mrs. Mervin Pugh.
5. Credit card tolls on the following:

a. Mr. John Ramsey, AMX & VISA
b. Mr. John Ramsey Jr., AMX.

6. Home location of ex-wife in Georgia, we have number, address & tolls.
7. Banking investigation on Access Graphics, Mr. Ramsey's company, as well as banking information on Mr. Ramsey personal.
8. We have the name, address & number of Mr. Sawyer & Mr. Smith, who sold the pictures to the Golbe (sic), we also have tolls on their phone.
9. The investigative firm of H. Ellis Armstead, we achieved all their land and cellular lines, as well as cellular tolls, they were the investigative firm assisting the Boulder DA's office, as well as assisting the Ramseys.
10. Detective Bill Palmer, Boulder P.D., we achieved personal address and numbers.
11. The public relations individual "Pat Kroton" (sic) for the Ramseys, we achieved the hotel and call detail where he was staying during his assistance to the Ramseys. We also have his direct cellular phone records.
12. We also achieved the son's John Jr.'s SSN and DOB.
13. During all our credit card cases, we acquired all ticket numbers, flight numbers, dates of flights, departing times and arriving times.
14. Friend of the Ramseys, working with the city of Boulder, Mr. Jay Elowskay, we have his personal info.

But that was not all, nor was it the most alarming aspect of the sale of phone records contained in the Touch Tone case the FTC had access to. Through a conduit Touch Tone had sold phone and pager records of Los Angeles Police Officers to organized crime.

Again, the Denver Post reported on this shocking set of facts in a June 29, 1999 article titled, "Accusations against Rapps Widen, Pair Allegedly Sold Phone Numbers of L.A. Cops to Mobster". Here is the text of the article:

James Rapp, the Denver private detective charged with trafficking in confidential information about the Ramsey murder case, also furnished the private phone numbers of police officers to a member of the so-called "Israeli mafia," authorities say.
Rapp allegedly got the unlisted home phone numbers and pager numbers for some Los Angeles police officers and funneled them through a middleman to Assaf Walknine, a reputed Israeli mafia member who'd been arrested on forgery charges, according to an affidavit unsealed Monday. Colorado Bureau of Investigation agent in charge Mark Wilson said the release of officers' numbers can be extremely dangerous.

"Not only is it dangerous, but it definitely could compromise any investigation that could be ongoing," he said.

Rapp and his wife, Regana, were indicted last week by the Jefferson County grand jury on two counts of racketeering, charges that carry maximum penalties of 24 years in prison and fines of $1 million on conviction.

Authorities claim the Rapps ran a detective agency, Touch Tone Information Inc., that used subterfuge to obtain confidential information about the Jon Benet Ramsey murder investigation and passed it to the world tabloid media.

The pair surrendered Monday. They were jailed, then released on bond of $25,000 for him and $10,000 for her.

The CBI started investigating the Rapps in January after getting a referral from the Los Angeles Police Department, the affidavit says.

The LAPD alleged that the Rapps helped get phone numbers of police officers for Walknine after Walknine's arrest in connection with an alleged scheme to forge credit cards and gold coins.

Authorities believe that Walknine also "cloned" the pagers worn by the officers. For instance, every time L.A. Detective Mike Gervais would be paged, the person paging him would get a call from Walknine, the affidavit says.

The middleman between Walknine and the Rapps was a former L.A. cop and convicted felon named Mike Edelstein, the affidavit says.

"LAPD is most interested in Edelstein," CBI agent Bob Brown said. "He was buying the information for Walknine from (the Rapps). As I understand it, when Walknine was arrested, he admitted he got this information from Edelstein - the pager numbers, the home telephone numbers and home addresses of LAPD officers.

"At one point, Edelstein actually showed up at the front door of one of the police officers while the officer was at work and his wife answered the door," Brown said. "He gives his name and walks away. The officer believes Edelstein was stalking him or in some way trying to intimidate him."

Brown said Edelstein was a cop who was fired from the Los Angeles Police Department. Edelstein served a prison sentence for possession of an automatic weapon and, after getting out of prison, became a private investigator, Brown said. He later began using the Rapps and their Touch Tone Information Inc.

Brown said that Los Angeles police discovered Edelstein's connection with the Rapps after a Los Angeles shoplifter claimed he was a LAPD officer and showed them identification. It was a forgery and traced to Edelstein.

During a search of Edelstein's home, officers found a cover letter from Touch Tone Information Inc. with a price sheet stating that the company could obtain the address and phone tolls for any telephone in the United States or internationally. Touch Tone also claimed it could provide banking information on an individual or corporation.

A former employee of the Rapps told investigators that they excelled at obtaining confidential phone numbers and bank records.

The former employee said he overheard phone discussions between James Rapp and his clients, which led him to believe that Touch Tone clients were a mix of private investigators, lawyers and news reporters. [end of article]

c) Prior to Recent Media Revelations and Congressional Demands, Did the FTC Take Aggressive Steps to Stop the Sale of Phone Records?

The simple answer is no. Given the wealth of knowledge and intelligence coupled with client lists for hundreds of private investigators, attorneys, media outlets, and other buyers of phone records contained within the Touch Tone files - not to mention what the FTC learned in the Boyer murder case and Operation Detect Pretext - what did the FTC do to root out this market and stop the sale of phone records? Not a thing.

d) Did the FTC Signal Tacit Approval of the Sale of Phone Records by Private Investigators?

Arguably yes. In direct and indirect ways the FTC has signaled to the illicit brokers and investigators that the sale of phone records will be tolerated—as long as it isn't too blatant.

This happened indirectly by brokers and investigators noting the FTC was aware of the sale of phone records for years and had taken no actions against any individuals or companies selling the records. In places where investigators and brokers meet to discuss sources, tactics, methods, enforcement actions, and legislation, there has been a continuing dialogue for years that argues the practice of selling phone records must be OK since the FTC has done nothing about it.

Another indirect signal was sent to brokers and investigators as an unintended consequence of the passage of the anti-pretexting for financial information statute contained with the Gramm-Leach-Bliley Act. Brokers and investigators, rather than looking at the spirit of the law, interpreted the letter of the law to allow the continued use of pretext and other forms of deception to obtain consumer records other than financial records. And the FTC, in bringing the paltry number of cases it has to date under Gramm-Leach-Bliley and the Unfair and Deceptive Trade Practices Act, has inexplicably ignored the evidence in those cases of phone record sales. This did not go unnoticed by the illicit information brokers and private investigators and was again read as a green light to sell phone records.

In addition to indirect signals, the FTC, whether intending to or not, has directly signaled the brokers and investigators that phone record sales would be tolerated.

In January of 2005, the cover story of PI Magazine was "The FTC on Pretexting: The PI Magazine Interview with Joel Winston". The interview was conducted by PI Magazine Editor-in Chief, Jimmie Mesis. In the set-up to the interview Mesis describes the reason he interviewed Joel Winston as the following:

"In an effort to get a definitive definition of pretexting and the potential risks and penalties for conducting pretexts, PI Magazine was granted an interview with Joel Winston, Associate Director of the FTC, Division of Financial Practices. His office has the responsibility to monitor and regulate the use of pretexting." [Emphasis added]

During the course of the interview which covered a number of aspects regarding the definition of pretexting; various pretexting tactics; Gramm-Leach-Bliley; Operation Detect Pretext; and, the Unfair & Deceptive Trade Practices Act, Mesis asked Winston about the use of pretext for phone records. The following Q & A resulted:

PI Magazine (PIM): Do you classify the acquisition of telephone toll records as a clear violation of deceptive business practices?
Winston: It's not what we traditionally look at as deception because you're deceiving party A, but party B is the actual party being harmed. But, we believe that, even though it has not been tested in the courts, that acquiring toll records through false statements constitutes deceptive business practices.
PIM: Is this an area the FTC is going to start looking into?
Winston: We are aware that there have been some concerns about that and were continuing to consider it.

Not exactly a clear and strong message from Mr. Winston, the FTC official charged with pretext regulation, that the sale of phone records will not be tolerated when Mr. Winston was afforded an ideal forum to send an unambiguous warning. And I would note that a year later when this issue exploded in the media, 6 months after the EPIC West complaint was filed with the FTC, the FTC still had not brought a single enforcement action against any company selling phone records.

The interview continued and in a later question Winston was asked:

PIM: Are there currently any FTC concerns about private investigators?
Winston: Not as a general matter. If I thought that there were major problems in the PI industry that concerned us, I would certainly tell you. As with any industry, there are occasional bad apples, but the PI industry as a whole is not an area about which we have any particular concerns… [Winston then discusses an area dealing with credit reports unrelated to pretext and phone records]

An objective reader—not to mention a subjective reader, like a broker or investigator, trying to read the tea leaves of Winston's answers—comes away with the distinct impression that the sale of phone records by brokers and investigators is not high on Joel Winston's or the FTC's priority list. Particularly when coupled with the fact that in the seven years that the FTC has been aware of the sale of these records, they hadn't brought a single enforcement action against a company selling phone records.

But don't take my word on how the investigators and brokers reading Mr. Winston's comments interpreted them. Instead, read how the interviewer, Jimmie Mesis, Editor-in-Chief of PI Magazine interpreted Mr. Winston's answers. In a statement to fellow investigators and brokers on July 11, 2005 titled EPIC FIGHTING PHONE RECORDS SALES, Mr. Mesis, responding to other investigators and brokers that were angered by the complaint EPIC West filed, stated:

([Bracketed comments and emphasis added by Douglas])

Greetings,
There is no doubt that that one complaint to the FTC does not constitute "a

problem" . However, when that complaint comes from EPIC, we have a problem. This organization continues to exist by its consistent efforts to blast alleged violations of consumer privacy. **My immediate concern is not the FTC**, rather EPIC for their aggressive negative media publicity campaigns against PI's and their strong lobbying efforts in Washington, DC.

I recommend that you read my interview with the FTC and the specific comments about telephone records at www.pimagazine.com/ftc_article.htm **The FTC wasn't too concerned about telephone information, but if PI's are going to blatantly advertise tolls directly to the public as a commodity, the FTC will get involved and we are going to lose that commodity and our ability to solve many cases because of it.**
[**Note that Mesis considers Americans' phone records a "commodity"!**]

PI's need to STOP promoting the selling toll records directly to the public as a commodity. Rather, use it as an investigative tool used in the course of your investigation to lead you to a missing person or to the lead you need to solve the case. **I also suggest that PI's promote such services as "telephone research" as compared to coming right out and mentioning tolls, non-pubs, etc.**
[**Note that Mesis recommends hiding what is actually being sold on web sites by using terminology designed to deceive—this is a common practice within the trade and its web advertising**]

Roe and I decided last January to voluntarily remove our magazines from the books shelves at Barnes & Noble and many other book stores. We did this at a financial loss to make it a bit more difficult for the public to readily learn and see the suppliers of information that shouldn't be directly accessible to the public. We as professional investigators need to know who these sources are, yet we all need to do something to stop this avalanche of perceived identity theft hysteria that the media has latched onto.

Remember, one day....soon, you will no longer be able to get non-pubs, addresses for telephone numbers, and tolls, all because some new law is going to be passed. Why? Because PI's shouldn't be promoting these investigative tools as a commodity. Then, just like with GLB, a new law will eventually prevent us from using an amazing investigative resource that will be lost, and it won't be anyone's fault other than our own.

Please do you part,
Jimmie Mesis, Editor-in-Chief, PI Magazine, Inc.

So in Mr. Mesis' own words – again, this is the man who sat in the room and interviewed the FTC's Joel Winston – "There is no doubt that that one complaint to the FTC does not constitute "a problem"…My immediate concern is not the FTC… The FTC wasn't too concerned about telephone information…"

One wonders what additional off the record discussion may have taken place between Mr. Mesis and Mr. Winston that may have bolstered Mr. Mesis' belief that the FTC "wasn't too concerned about telephone information."

But the interview was a year ago and before the EPIC West complaint. Perhaps in light of the EPIC West complaint and resultant media attention to the issue, Mr. Winston of the FTC has had a change of heart - perhaps not.

In an article by Peter Svensson of the Associated Press published less than two weeks ago on January 18, 2006, Joel Winston again stated why he doesn't see the sale of phone

records as an issue rising to the level of seriousness surrounding the sale of financial records.

In the context of the article, Winston stated:

So why didn't the Touch Tone case put such businesses out of business?

> For one, the FTC went after Touch Tone not for snooping on the private lives of police officers but for "pretexting" financial information from banks.
>
> "Our primary focus there was on financial, because that's really where the most direct harm is," Joel Winston, associate director of the FTC's division of privacy and identity protection, said in an interview. "If I'm pretexting a bank and getting your bank account records I can drain your account."
>
> "With phone records ... not to minimize the intrusion on one's privacy, but generally it doesn't lead to any specific economic harm. It's a different kind of harm," Winston said. Nevertheless, he added, the practice "raises significant privacy concerns."

Perhaps Mr. Winston should sit down with police officers and their families and explain those responses. Perhaps Mr. Winston should sit down with the parents of murder victim Amy Boyer and explain those responses. Perhaps Mr. Winston should stop focusing on "economic harm" and start worrying about the lives at stake—and already lost—because of pretext for "non-economic" information. Perhaps it is time the FTC finds a replacement for Mr. Winston who, unlike Mr. Winston, understands the dangers inherent in the sale of phone records. Given Mr. Winston's inability to even analyze the information contained in the FTC's own case files—notably the Touch Tone case and Operation Detect Pretext —American consumers and this Congress should not believe that the FTC, even if armed with a new law, will be aggressive in the protection of phone records area as long as Mr. Winston is in charge.

But as hard as it may be to believe, the problems at the FTC are more extensive than Mr. Winston. The problems are institutional. Even when the FTC has brought cases against individuals and firms using pretext to steal financial information, the result has been to signal the brokers and investigators selling such information that the odds of being caught are slim and that the FTC will not impose serious sanctions.

In the Touch Tone case the FTC trumpets that they fined Touch Tone $200,000. What the FTC is slower to point out is that they suspended the fine. So Touch Tone paid not one penny in fines. In Operation Detect Pretext 1,500 advertisements for the sale of personal financial information were located by the FTC. From that universe, only 3 firms were the subject of court action. And once again the FTC settled for minimal fines of $2,000 in two of the cases, and waived the fine in its entirety in the third case.

But perhaps the most brazen evidence of all that the FTC is viewed as a toothless, paper tiger is the case of FTC v. Information Search, Inc, and David Kacala. This is the third case of Operation Detect Pretext mentioned in the preceding paragraph where the FTC waived the fine entirely.

Not only is Information Search, Inc. still in business, until just a matter of days ago the web site, located at www.information-search.com was selling cell phone and other telecommunications records. And on a page named for the FTC, Information Search, Inc. has been publicly thumbing its nose at the FTC and Congress for what Information Search, Inc. views as the wrong-headed passage and enforcement of the Gramm-Leach-Bliley Act.

So for years, Information Search, Inc., having been once prosecuted by the FTC for selling financial records obtained through pretext, has continued to sell phone records with all the indicia that they too were obtained through deceptive means, and the FTC has

not done a thing. I seriously doubt the FTC ever went back and looked at the information-search.com web site.

Only when increased media attention was brought to bear on the problem of the sale of phone records and EPIC West named Information Search, Inc. in its complaint, did Information Search, Inc. take down the web ads for phone records—hoping that by the time the FTC looked they wouldn't find the ads. But EPIC West's Hoofnagle was savvy enough to capture the offending pages and various search engines continue to have cached pages showing Information Search, Inc. offered cell and other phone records for sale.

Bottom line. The message that is repeated loud and clear throughout the investigative and broker industries on a regular basis is: No need to fear the FTC. Fear EPIC West. But just lay low. The media storm will subside. And the FTC will look the other way as usual.

In fact, let me quote a North Carolina licensed private investigator who just days ago had this to say about the publicity surrounding the availability of cell phone records and his prediction for how this will play out in Congress once lobbyists for the illicit information brokers and investigators go to work:

Just my humble opinion, but the more we talk about this, and say things like what we are going to do, etc. the more we encourage people in general to use pay phones (if you can find one), office phone extensions, friends cell phones or friends home phones, etc. Lets stop this silly comments and discussions. The more "we stir it, the more it will stink." We keep shooting ourselves in the foot. Not to mention, the cost to obtain various "information" from various "brokers" will only rise, putting some items of investigative value out of reach! Let it die, the Media will soon lose interest, and our lobbyists will stay on top of it in our interests in Washington, DC.

e) <u>Why Has the FTC Been AWOL When it Comes to Protecting Phone Records?</u>

I wish I fully knew the answer to this question and it is one that this Committee and Congress should investigate. I do have definitive ideas about the problems at the FTC that I saw first hand when I served as a consultant to Operation Detect Pretext. I would be happy to share those observations and concerns with this Committee in a non-public setting if the FTC will release me from my non-disclosure agreement. All of my statements concerning Operation Detect Pretext in this testimony are based upon aspects of Operation Detect Pretext that the FTC has made public. But there is much more to the story that I am unable to discuss under threat of severe penalty given my signed agreement with the FTC which I will continue to honor.

<u>VIII. The FTC's Attitude Towards Pretexting is Inexcusable</u>

From an outsider's perspective it is very difficult to understand the lack of interest by the FTC when it comes to pursuing those who are using deception to obtain consumer records, including phone records. The FTC routinely goes after scams and fraud where there is a distinct element of buyer beware – in other words – the consumer using a little common sense could have avoided being scammed or defrauded. That's fine. Those types of con artists should be dealt with. Yet the FTC has shown great reluctance and reticence in stopping the theft of consumer records where the consumer has no way of knowing the records are being stolen and therefore cannot protect himself as the records are in the control of other corporate or government custodians. Given this fact – the theft of consumer records cries out for assistance and prosecution by appropriate government agencies in order to defend the American consumer.

How many murders of Americans will it take before the FTC gets serious? How many law enforcement officers, their families, and investigations have to be put at risk before the FTC gets serious? What will this Congress and future Congresses do to exercise oversight and force the FTC to get serious?

IX. The Need For A Comprehensive Statute Protecting All Consumer Records

While it is important that this Committee and Congress move quickly to outlaw the sale of phone records, it is also time for this Committee and Congress to pass a broad anti-pretexting statute designed to outlaw the use of deception to steal any consumer record.

In 1998 I first testified before Congress to expose the use of pretext to steal financial information and that practice was outlawed in 1999. In 2000 I again testified before Congress warning that phone records had become the new record of choice for information brokers and private investigators to steal. Here we are six years later dealing with the consequences. If Congress does not move to outlaw the tactics used to steal information – instead of merely protecting categories of information in a piecemeal approach – I fear we will be meeting again and again to address category by category.

Already other categories of information are under attack. I have tape of an information broker recorded surreptitiously describing how he defeats cable and satellite television providers and public utility providers information security systems. In fact, many of the web-sites under scrutiny today advertise the sale of utility information and Post Office Box underlying street address information. Post Office Box information is protected by regulation, but is commonly obtained by the filing of fraudulent forms stating that the requestor needs the underlying address information for service of process when that is not the case.

Bottom line. If Congress only moves to protect phone records, Congress will create a nightmare for another industry similar to what the phone companies are experiencing today.

Finally, Congress should consider making the use of deceptive practices to gain access to consumer information a criminal act with primary jurisdiction falling to the Department of Justice and F.B.I. while simultaneously empowering state attorney generals to act as well. As an aside, I would note that several state attorneys general have already begun prosecutions under their state unfair and deceptive trade practices acts within weeks of learning of the problem, while the FTC with knowledge of the phone records issue since 1999 has yet to bring an action. This is all the more reason that primary authority for enforcement should not be given to the FTC. To vest primary authority with the FTC acting in a civil capacity, given the agencies history of impotence, is to almost guarantee that the illicit practices will not stop.

X. Congress, Enforcement Agencies, and The Private Sector Must Work Together

Just passing legislation will not be enough. The enforcement and regulatory agencies must actively work to root out and prosecute those who are stealing information. Congress must exercise regular oversight of the enforcement agencies to keep the agencies focused on protecting the American consumer. And the phone companies, along with all consumer services companies, must use appropriate customer authentication protocols to protect their customers.

Following the 1998 hearings on the use of deceptive practices to steal financial information from financial institutions, the American Bankers Association moved aggressively to educate all member institutions about the theft of customer account information. Working together with the ABA, I authored several training documents that were provided free of charge by the ABA to member institutions. We conducted numerous telephone seminars and I appeared at dozens of ABA conferences all over the country to teach financial institutions about the threats posed by the practices of identity thieves, illicit information broker, and illicit private investigators. While it is still possible to find financial records for sale on the web, the number of offerings has been dramatically reduced through those efforts. I believe the phone companies – indeed all

consumer services companies – working together with Congress, enforcement and regulatory agencies, and their representative associations can have similar success.

One final item for consideration. I have reluctantly come to the conclusion that it may be time for federal regulation of the private investigative trade. By this means minimum standards may be set to assist in weeding out those who have no regard for the law and are destroying the hard earned reputation of thousands of professional private investigators who serve in a vital capacity in out nation's justice system.

XI. Conclusion

Mr. Chairman, thank you for your invitation to appear before this Committee. I will do anything I can to be of assistance to the Committee, Congress as a whole, the enforcement agencies, the trade associations, or individual companies affected by these issues.

CHAIRMAN BARTON. We thank you. We are going to change that record and we are going to start very quickly, hopefully as early as next week. Committee stands in recess until approximately 10 minutes after 5:00 p.m.

[Recess]

MR. FERGUSON. [Presiding] We will reconvene and we will go to Ms. Schakowsky for questions as soon as she is ready.

MS. SCHAKOWSKY. Thank you. Ms. Madigan, I appreciate your patience, all of you. Steve, you know what it is like. I just wanted to ask you, do--I guess the Section 222 says that phone companies do have a legal responsibility to protect our records. What, if anything, do you see happening in terms of legislation that would involve security protections by wireless or wire line phone companies?

MS. MADIGAN. Are you asking me?

MS. SCHAKOWSKY. Yes, I am asking you. Because you said there were a number of pieces of legislation that have been introduced in the State legislature. I wondered if you were contemplating anything or if you knew if other States were?

MS. MADIGAN. Well, in terms of the CPNI rule, we don't have jurisdiction. In order to make any changes there, they would have to reopen that rulemaking and they could, and we would certainly encourage them to do that. Particularly to determine if enhanced protections are needed, including notice to consumers if there has been any access to their phone records so that they would at least be alerted to the potential that there then was maybe a security breach of their phone record information similar to what we have been working on in the aftermath of ChoicePoint with our financial information.

In addition, there probably should be a look at enhanced verification methods so that prior to information being released there would have to be some form of verification that you are talking the customer and there are a number of ways of doing that. So we certainly think that that is one of the things that should be considered at the Federal level.

MS. SCHAKOWSKY. Mr. Rotenberg, in terms of the responsibility of the phone companies, what do you recommend?

MR. ROTENBERG. Well, our petition is similar to the FCC. Am I okay? Isn't that interesting? That was a cell phone. Our petition to the FCC this summer, in effect, asked the Commission to reopen the rulemaking on the CPNI standards because we don't think that they are adequate security safeguards. We were pleased that Chairman Martin indicated that he would move in that direction and that several of the proposals that we included, for example, the requirement of a password and better verification procedures, I think, will also be considered. That would be a step in the right direction, but as I suggested earlier, one of the large issues also in the original CPNI proceeding was whether to adopt an opt-in or opt-out approach to the disclosure of the data. The FCC had recommended opt-in; we thought that was the right approach. It was overturned by a 10th Circuit Court of Appeals opinion, and it may be an issue that could be corrected by statute.

MS. SCHAKOWSKY. Mr. Largent and Mr. Merlis, you were talking about the 190 million, I think it was one of you, the calls that you get in terms of inquiries or complaints, et cetera, and that clearly, you want to act quickly to respond to those, but I think a lot of consumers do feel that the companies, themselves, have some real responsibility and as I understand your testimony, the concern was that if more security measures need to be revealed, that actually that is going to advantage the fraudsters in some way. Maybe that is right, but isn't there--don't you accept some responsibility for this problem?

MR. LARGENT. I will go first. Well, first of all, I want you to know that this is a very serious issue and we are taking it very seriously. I spoke yesterday with the leaders of the industry about this issue and I can tell you that this issue is a top priority. It is something they are taking very, very seriously, and the most valuable asset that our companies have are our customers.

MS. SCHAKOWSKY. No, I understand the incentive that--from a business point of view and I believe you take it seriously, but the responses that you gave mainly were directed at fraudsters, those people who are doing it, and I agree and I have legislation that would do that. But I think most people do expect that the phone companies, themselves, are going to act, not just against the fraudsters, but to take some action, themselves.

MR. LARGENT. Well, our companies are acting, themselves. First and foremost, they are seeking the lawsuits against the fraudsters that are perpetrating this against our companies, but second of all, our carriers have stopped sending requests for call records through e-mail or faxes, which was one of the ways that the criminals were perpetrating these

sorts of crimes. Our carriers are also providing subscribers with the opportunity to submit personalized pass codes for their accounts and our carriers are strongly encouraging our customers to take these measures.

MS. SCHAKOWSKY. Thank you, Mr. Chairman. How are you encouraging customers? I sure do not recall--again, I was talking earlier. Maybe I have gotten something that says I could do something about a pass--I was completely unaware of that as an option until this story broke in the Sun Times and the Attorney General filed suit. Have I received something that said I can have a pass code?

MR. LARGENT. Well, it would be hard for me to stay--

MS. SCHAKOWSKY. No, I mean, have you said--what does it look like when you send something out that tells people that they can establish a pass code? In what way do you communicate that?

MR. LARGENT. These would be inserts in your bills and that sort of thing.

MS. SCHAKOWSKY. You know, as was stated before, very few people really pay attention to that or notice that. Mr. Douglas, you look like you wanted to say something.

MR. DOUGLAS. You are reading my eyebrows.

MS. SCHAKOWSKY. Yes.

MR. DOUGLAS. Mr. Largent is exactly right and I want to give him great credit in his oral testimony for acknowledging that one of the problems here for the companies, whether it is bank, phone companies, any utility company, cable television, or satellite television. They are caught between a little bit of a rock and a hard place, between customers who want information and they want it yesterday and the ability to safeguard that information. So there is a constant struggle there. The bad actors, if you will, the criminals that are doing this always stay on top of what are the latest methods.

So it is almost as if whatever you do, unless you are vigilant on a constant basis, unless the companies are constantly training and educating their customers, but importantly, their workforce, because after all, when you call these companies, who you normally get is the employee with the least amount of experience, who is paid the least, and the division of the company in the customer call center, sometimes domestic, sometimes overseas, that have the highest turnover rate of employees. Call centers have the highest turnover rate in the industry out there. So it is a constant struggle that needs to go on, but why I was really raising my eyebrows, Congresswoman, was when you talk about what did you get in passwords and PINs, and I think the Attorney General referenced this.

Passwords and PINs are being beaten. I have on this very little computer right here in the Docusearch murder case, a woman out of New

York City, Michelle Gambino, Queens, New York, who was their pretexter who stole Amy's information, her records of walking through Wall Street like there are no doors on the vaults, including PINs and passwords for accounts and balances and account numbers. So they are always out there.

But one of the problems is, and I experienced this on the way over, sitting in the Red Carpet Club in Denver, signing up for a Quick T-Mobile one day pass, what is the default password? Last four of your Social Security number. So unfortunately, when many companies even use PINs and passwords, they default to biographical information that identity thieves routinely get. And last point, and one thing I didn't cover in my testimony, this is about identity theft. This is precisely how identity thieves and organized identity theft rings are defeating our Nation's businesses, whether it is moving hundreds of thousands of dollars out of banks over the phone or whether it is using phone company information--and this is where I differ from the FTC, who say that there is not a financial element here.

If they would go back and look at their own files in Touch Tone, they will see that phone records are then used as part of accumulating the information to defeat banks and move money out. It is not about the separate categories that we are discussing eight years apart, it is about the tactics that are being used in the methodology. Thank you.

MR. FERGUSON. We may have time for another round, if you feel like sticking around. The chair recognizes himself for five minutes for questions. I want to pick up on that a little bit about the easy access of some of the biographical personal information and just back to Mr. Largent. With the proliferation of Social Security numbers and date of birth records and all sorts of identifying information that is on the Internet, it is available on the Internet now and we have heard a little bit today about how available it is. Does it still make sense for wireless carriers to still use these kinds of data points to verify someone's authenticity when they call and identify themselves or when they say who they are, even if they have some of this information? Does it still make sense to be using some of this information because it is widely available?

MR. LARGENT. Well, the thing is about the wireless industry, because it is so highly competitive, is that it would be hard to find two companies that are doing it the same way. They all are hypercompetitive, they require different types of information to receive, you know, validation into the account. And we view that as a good thing, particularly when we are talking in this arena. That is a good thing that nobody said that you have got to do one way and this is the way you have got to do it. So my perspective is that this a good thing and yes,

some companies are doing that and some companies aren't, and we view that as a good thing.

MR. FERGUSON. Does it make sense for the industry to talk or the association to talk to companies about perhaps discouraging using that type of information as verification for folks who are calling in, because it seems to not be working.

MR. LARGENT. Well, I can tell you that this is on the front of their minds and we are talking about, our association had a call yesterday. I spoke with the leaders of the industry yesterday about this and I can tell you, their comments suggested to me that this is at the highest level, so it is a great concern. It is something that they are making specific steps to address as quickly as possible, as well as prosecuting the criminals who are perpetrating this.

MR. FERGUSON. What happens when one of your companies realizes that someone's information may have been fraudulently obtained from anybody at one of the companies? Is--what notifications--what are the--something gets triggered and something happens. What happens? Is the customer notified?

MR. LARGENT. Well, the problem is that we don't know because people are telling us that they are the customer and giving all the proper documentation. We don't know that they are not the customer and we literally are receiving not millions, not hundreds of millions, but billions of phone calls about customer records every year. The problem is, is that, you know, 99.9 percent of our calls are legitimate calls and they are handled properly, and we get this fraction of one percent that is illegitimate calls that we are trying to address right here in this legislation.

MR. FERGUSON. But have any of the companies been able to determine at any point through either happenstance or some mechanism, some security mechanism that if someone's information is fraudulently obtained from someone from within the company? That must have happened at some point. I mean, one of the companies must have figured out at some point that information was given out when it shouldn't have been given out.

MR. LARGENT. I am not aware of that happening. I know that our companies have all done stringent testing of the people that are their customer service representatives, to see if they can't find a person that is, you know, working for them that is giving out information that they shouldn't be. And I know that none of our companies have been able to find anybody that has done that purposely and doing it for profit.

MR. FERGUSON. We have heard a little bit about how a pretexter will call a company multiple times until they get a service representative who they can dupe, who they can convince to give them information

when they shouldn't be and if they get rebuffed by someone, they will call again and try and get somebody else on the line and they will kind of do it until they get somebody. If someone calls and is rebuffed and it is said you may not, you know--I can't verify that you are this person or I can't give you this information, is any kind of notation made in the person's account that someone may have perhaps been fraudulently trying to obtain their information? It just seems like if that were to happen, then maybe the next person, it would be a little tougher to dupe the next person if a notation had been made in the person's file, in their record that someone had been fraudulently trying to get this person's information. Do you know that--

MR. LARGENT. Well, all I would say is that what typically takes place is the fraudster doesn't just go from one call to another call until he finds somebody that is weak enough to give him the answer that he wants with the information he has. He will find out, over the course of the conversation, what information he doesn't have and then go attempt to get it, so that when the next call he makes, he has got more information that he has found through, you know, some other sources and he gives the person the necessary information that he knows is going to work then.

MR. FERGUSON. But are you aware of any of your companies--is there any mechanism to make a notation in the file or in the record?

MR. LARGENT. I am sure companies are doing that. I can say that, unequivocally.

MR. FERGUSON. Did you want to add something to that?

MR. DOUGLAS. Well, typically, the CRT terminals that the call centers have, there are commercial products out there; some of them do have audit trails, two types of audit trails, both calls coming in, for notation of the calls coming in, and also internal audit trails for who internally in the company is accessing the information. Some of these guys even know specifically how individual companies' terminals work and what they can even bring up with what function key on their boards. They have learned the companies that, precisely through the methodology that Mr. Largent points out, is calling in. It is a blend of the two. Calling in and if rebuffed, moving on to another call, but also piecing together information and learning what they will need, then going out and buying it or stealing it somewhere else. But there are various products available to all industries, including the phone industries, to have those kinds of audit trails, absolutely.

MR. FERGUSON. My time is up. I recognize Mr. Markey for five minutes.

MR. MARKEY. Thank you very much. You know, Mr. Merlis, I understand that no defense against dedicated, nefarious fraudsters will be

100 percent failsafe. On the other hand, if there are, as Mr. Douglas says, 40 websites that he can identify that are doing business--

MR. DOUGLAS. Hundreds.

MR. MARKEY. Hundreds of websites doing business right now, overloaded with requests from people willing to pay to get the secret phone records, or the phone records of private citizens in our country, then one has to question the adequacy of existing defenses put up by the phone companies, Mr. Merlis. You say that you have strong protections, but to consumers, it looks like you are talking about the telecom equivalent of a marginal line as fraudsters are waving the phone records of people at the Arc d'Triomphe in Paris and it is just going on all over the country.

MR. MERLIS. But different--oh, excuse me, sir. Excuse me. Different companies use different mechanisms. For instance, one company with whom I discuss this issue said we will not provide phone records except by mail to the address on the bill and there is a five-day waiting period. Now, that is a pretty good method to prevent one of these characters from getting that information.

MR. MARKEY. Should that be the industry standard, Mr. Merlis?

MR. MERLIS. I don't know, sir.

MR. MARKEY. Do you think that should be the industry standard?

MR. MERLIS. I don't have enough breadth of experience to know what other methods--

MR. MARKEY. If that is a good standard--but if you are not ready to endorse it for the industry, then we shouldn't go to that place. Mr. Douglas, you said earlier--I thought you said that bribery is the number one?

MR. DOUGLAS. No, not number one. Pretext is number one.

MR. MARKEY. And who do they bribe, Mr. Douglas?

MR. DOUGLAS. When they do use bribery, it is insiders. There are--

MR. MARKEY. Insiders where?

MR. DOUGLAS. Inside of the phone companies, themselves.

MR. MARKEY. When you are talking about bribery as a second leading way that these hundreds of companies use, how many individuals are you talking about are engaging in this kind of illegal activity?

MR. DOUGLAS. Oh, there would easily be hundreds.

MR. MARKEY. Hundreds.

MR. DOUGLAS. In the Docusearch case, Docusearch was using--in any given month, they had three to five insiders within various phone companies.

MR. MARKEY. You are saying there could be hundreds of telephone company employees who are accepting bribes?

MR. DOUGLAS. Right. I have no doubt. And it is not always just bribery.

Sometimes--

MR. MARKEY. You are saying you have no doubt that there are hundreds of employees?

MR. DOUGLAS. I have no doubt.

MR. MARKEY. Really?

MR. DOUGLAS. Yes.

MR. MARKEY. Mr. Rotenberg, what do you think?

MR. ROTENBERG. I think there is a very serious problem, Congressman. I mean, it is clear from the materials that we provided to the FTC last summer that you can go on line. Mr. Douglas' demonstration during the hearing was that as this hearing is taking place, the companies that are making this information available are taking advantage of the publicity to promote the sale of our call detail information. So clearly, Congress needs to act.

MR. MARKEY. We thank you, by the way, Mr. Rotenberg, Mr. Douglas, Ms. Madigan for your heroic work in this area. Mr. Merlis or Mr. Largent, perhaps you could help us. What percentage of consumers opt out pursuant to notices sent to them advising them of their right to opt out? What percent is it, Mr. Merlis, do you know?

MR. MERLIS. I don't have any of the data on that, sir.

MR. MARKEY. You don't. Do you have any?

MR. LARGENT. I don't, either.

MR. MARKEY. Okay. Could you provide that information to us? I think it is going to be a very low number, given the CPNI information question that is, you know, came to my home obviously, and other homes. It is very low and I think that there really hasn't been an effort made by the phone companies to give that proper choice to the public. Mr. Merlis, when the phone company wants to disclose CPNI to an affiliate, a joint venture, a partner or a private contractor, is it typical to disclose a consumer's phone record or are such entities more interested in name, address, phone number of the consumer; how much a consumer generally spends monthly; what services they should subscribe to; what is more likely?

MR. MERLIS. My understanding is it is done for marketing purposes and so it would be name, address and fit some demographic, either a zip code where some new product is being offered, something of that sort.

MR. MARKEY. So other than for billing collection, billing or collection or marketing, would there be any other reason to disclose detailed phone records?

MR. MERLIS. No, sir. And the marketing is only internal product marketing. It is not marketing of television sets or of grocery store

online services; it is related to the fundamental business that these telecom companies are in.

MR. MARKEY. Mr. Rotenberg and Mr. Douglas, perhaps you could enlighten me on this. If someone sought to gain access to the phone records of another individual and said Joe Blow, I want my phone records. Here is the fax number, please send them to me. Is it the policy of the phone companies to then say well, we have your home phone number right here. You sit right there. We are going to call you at that number just to verify that it is you at that number. Is there a way for Spooftel to actually have you call--can they actually somehow or other not go to my home phone number and create, through this spoofing, the capacity to deceive the phone company?

MR. DOUGLAS. Well, let me take those in order. First of all, if the companies were even to do that, that is quite doubtful.

MR. MARKEY. Why wouldn't they do that?

MR. DOUGLAS. It is quite doubtful that they would ensure that the person was at their home phone to do it before releasing it. We are a very mobile society. Consumer organizations have to typically release records to wherever you are. When I test banks and I test companies and I audit them to see if I can get their customer service representatives to turn over information, I will do it while I am on the road. I live in Colorado. I will do a call from my hotel tonight and use the ruse of I am on travel and I need the records right away, but more directly to the point, is it possible to set it up so to have them call a number and have it forwarded to another number, yes, absolutely. Sure.

MR. MARKEY. Can I just say, Mr. Douglas, that you know that Mr. Barton and I are the principle reasons why there are privacy protections built into Gramm-Leach-Bliley?

MR. DOUGLAS. I have followed your career for quite some time.

MR. MARKEY. Okay, so we did that as part of that bill back there in 2000.

MR. DOUGLAS. And if I might, Congressman Jim Leach on the--

MR. MARKEY. But as you know, the bill, as it came out of the Banking Committee, had no privacy in it.

MR. DOUGLAS. Right.

MR. MARKEY. It only--and we added the privacy here and he kept it in, but--

MR. DOUGLAS. I am not going to disagree with you.

MR. MARKEY. No, I love the guy, I love the guy, but this was the last line of defense. Can I just--and I beg your indulgence, Mr. Chairman. Mr. Rotenberg, could you just--can you give the 30 second summary of what you want this committee to remember, Mr. Rotenberg?

MR. ROTENBERG. Pretexting has to be made illegal. Telephone companies have to be responsible for security, and over the long term, we have to minimize the collection of personal information in the communications network because that is going to be the ongoing risk.

MR. MARKEY. Okay, thank you. We thank all of you.

MR. FERGUSON. The gentleman's time is expired. The chair recognizes the distinguished chairman of the full committee, the gentleman from Texas, Mr. Barton, for five minutes.

CHAIRMAN BARTON. Well, thank you, Mr. Ferguson, and I appreciate you chairing the hearing while I could run to a couple of other meetings that I had to do. I want to start with the answer that Mr. Rotenberg just gave, and ask a basic question. In the old days, phone companies had to keep records of long distance calls because they charged them by the minute or by the second. So you had to have a record to bill the person. Today, more and more phone plans are unlimited and some of them that are not traditional phone companies, like Vonage, which the service is over the Internet; you can pick your area code. My first question would be, unless you are having to keep the record in order to charge for the service, is there any reason to allow that there be a record kept at all? Why wouldn't we just unless necessary for billing purposes no such record should be kept of your phone records?

MR. ROTENBERG. Mr. Chairman, I think it would be wonderful if there were broad based support for that position because, even though proposals that are being made today to deal with the problem of pretexting will not deal with some of these long-term issues; security breaches, for example, that is still a risk. So if there were no obligation to keep this information, I think a lot of these privacy problems would disappear, and as you know, even though the telephone companies billed for long distance, they did not bill for local service on an itemized basis. That was treated almost like utility, like it was heat or electricity.

CHAIRMAN BARTON. Right.

MR. ROTENBERG. And we may be moving in that direction.

CHAIRMAN BARTON. Mr. Largent or Mr. Merlis, do you have a comment on that question?

MR. MERLIS. I would just say, sir, you are right. Because of these bundles that people can buy, we don't keep records of that sort, then people don't pretext for them because there is no information to get.

CHAIRMAN BARTON. Well, I don't know. I have three cell phones. I have a campaign cell phone, a Congressional cell phone, and a foundation cell phone; I don't know what kind of plan I am on, you know. I don't know whether I am charged--I assume I am just kind of charged some huge number by the month, but all my phones record every phone call and I can go back and look at who I called six months

ago. I don't really need to know that, but unless there is a billing purpose, if you are still on a plan that charges you so much a minute, so be it. You have got to record that. But if you don't, could we just say if you don't have to do it for billing purposes, don't do it? The Attorney General, what do you say about that?

MS. MADIGAN. Well, I don't necessarily think that people need to receive a record of their calls, but I will say in terms of law enforcement purposes, we would like to make sure that there is still maintained a log of those calls because there are obviously--

CHAIRMAN BARTON. Why wouldn't you then require, you know, as a default no record unless law enforcement says that Barton guy is suspicious, let us track his calls for a while?

MS. MADIGAN. We would endorse that.

CHAIRMAN BARTON. Something like that.

MS. MADIGAN. And let me apologize. I need to leave, but thank you very much, Mr. Chairman.

CHAIRMAN BARTON. I know. Ms. Schakowsky said you were supposed to have left about 20 minutes ago.

MS. MADIGAN. Correct. Thank you.

CHAIRMAN BARTON. Okay. My next question, again, is a general question. What is the first thing most people get when they try to abuse this information, do they start with a person's Social Security number? And if so, as a part of this legislation, should we ban the use of Social Security numbers for anything except Social Security purposes?

MR. DOUGLAS. Well, first of all, yes. The most common pieces of information you need to conduct a pretext is the name, address, Social Security number, date of birth. And Social Security number, being primary, that is the key that unlocks the kingdom in the information theft world. As you know better than I, that is an issue that has banged around here for the better part of probably ten years, that I have been aware of, is what to do with Social Security numbers because there are so many different problems. You almost open more doors every time we go down that road, specifically because--the Attorney General left--but even for law enforcement issues, for fraud prevention, detection, and prosecution. Often that is needed, also, in the private sector. So I support, overall, the thought and the tenure of where you are going, but there would have to be some very specific issues addressed.

CHAIRMAN BARTON. But we are not. My latest cell phone is a foundation cell phone. I don't know if I have it with me or not. I may have it left it--

MR. DOUGLAS. If you can't find it, we can buy it on the Internet here real quick.

CHAIRMAN BARTON. But when I applied for that, I went to a national chain to apply for it. I had to give my Social Security number three or four times in the process of applying for the phone. I started not to do it, just say I am not going to give it, and then the attendant there, the salesperson, said well, basically, fine. You don't give us the Social Security number, you don't get the phone.

MR. DOUGLAS. And that is done, Mr. Chairman, for fraud prevention. If you go to the FTC's own website, one of the top categories of fraud or activity resulting from identity theft is cell phone fraud. It is one of the top, if not the top, fraud category at the FTC. So the carriers, in response to that, as with all consumer industries, want that Social Security number to run it both for credit, but also to see if it has been used in fraud before.

CHAIRMAN BARTON. Mr. Largent or Mr. Merlis, do either of you have any comment on the Social Security number?

MR. MERLIS. I would love to get rid of it. I have a credit union account and my account number is my Social Security number. Until six weeks ago, many States still issued driver's licenses with Social Security numbers as your ID. Under the Intelligence Reform and Terrorism Prevention Act, that was prohibited as of December 17th, 2005. So if you got a license three months ago, you might even still have your Social--I think it would be great to do away with it, but as Mr. Douglas said, if you seek information from a credit reporting agency, the first thing after your name is what is your Social Security number. Anything that could be done to do away with the Social Security number as being the ID driver in our society would be very desirable.

CHAIRMAN BARTON. Mr. Largent.

MR. LARGENT. I would just say that there are some cases where you don't have to have a Social Security number to get a phone. You can get a prepaid cell phone without a Social Security number today.

CHAIRMAN BARTON. Prepaid. So you recommend that? I would buy me a different phone every month, huh?

MR. LARGENT. Well, no, you don't do it every month, but--

CHAIRMAN BARTON. All right. I want some comment on--my time is expired--on Mr. Gonzalez's question to the first panel, whether the phone call record, itself, is owned by the individual and is the sole property of the individual or is somehow proprietary to the cell phone, or the telephone company. And I would like my two telephone representatives to comment on that.

MR. LARGENT. I will go first. I would say that the cell phone record is the proprietary property of the owner, not the company.

CHAIRMAN BARTON. Okay, that is a good answer.

MR. MERLIS. I would be inclined to agree. I mean, it may be used for company purposes such as billing, but it is the individual's information. He owns it, she owns it, it is theirs.

CHAIRMAN BARTON. Okay, and my final query--

MR. MARKEY. Mr. Chairman, if I may? Back in 1994 we had the hearing here on the Telecommunications Act.

CHAIRMAN BARTON. You just happen to have that handy? The hearing record from 1994?

MR. MARKEY. I do. And I asked the question you just asked of Mr. Phil Quigley, who was the CEO of PacBell at the time and he was testifying for all of the companies and I asked him that question of who owns the information and he answered, "You don't release it unless they authorize it. The customer owns the information. They own the profile."

CHAIRMAN BARTON. They agree. We have got concurrence here. My final question is do each of you gentlemen support Federal legislation on this issue?

MR. DOUGLAS. Absolutely.

MR. ROTENBERG. Yes.

MR. MERLIS. Absolutely.

MR. LARGENT. I would say we support legislation to go after the criminals, absolutely.

CHAIRMAN BARTON. Okay. Thank you, Mr. Chairman, for your courtesy in letting me go over.

MR. FERGUSON. You bet.

CHAIRMAN BARTON. Just don't get too comfortable in that chair.

MR. FERGUSON. The other gentleman from Texas, Mr. Gonzalez, is recognized for five minutes for questions.

MR. GONZALEZ. Thank you very much. You know, it is interesting what we are talking about here. Everybody agrees the pretexters should be criminalized and so on. I am not real sure that is really going to be the issue. We are all going to be there at the end of this whole process. The real question is its application in the real world. Opt-in, opt-out; I have never been a real opt-in person because it has been so difficult in the business world to actually--but in this instance, I think it may be the only thing to do. But what are we opting in or opting out of? My assumption is not the sharing of my information, of my phone record.

Now, I would believe, whether it is opt-in or opt-out, that whether it is Cingular or Sprint or whatever it is, they are still going to have my information and that particular company where I have that direct relationship with will still be able to analyze it and they are going to figure that Charlie Gonzalez makes most of his calls after 6:00 p.m. or 9:00 p.m. and on weekends and they may send something to me offering me something. I mean, there are certain business deductions that can be

made from that information. Opting in or opting out is not going to interfere or jeopardize the utilization of that information.

So I will ask each one of the witnesses if you agree with this assumption?

MR. LARGENT. Yes, I do.

MR. GONZALEZ. Okay.

MR. MERLIS. Provided that opting in and opting out doesn't interfere with the description. I mean, if we could look at your pattern and say you know, Mr. Gonzalez, you could save a lot of money based on when you call if you did something. I don't know if that falls in the opt-in or opt-out. As long as we can do that, I think it is in the consumer's interest.

MR. ROTENBERG. Congressman, I agree. I think it is a different type of activity, but even so, in fairness the point that I was making earlier was that there is still privacy risks associated with maintaining the information, even if it isn't disclosed under the more restrictive opt-in regime.

MR. DOUGLAS. I agree with Mr. Rotenberg's comments and just one quick point, going back to the foundation of your statement, which I share the concern about opt-in and opt-out and what the business community needs, but there have been examples around the country. In the financial services world, New Hampshire--excuse me--Vermont went with opt-in where the rest of the country went opt-out and it has worked fine there. So from a marketing perspective, often it tells the business community specifically who wants products marketed to them.

MR. GONZALEZ. Well, in the context of what we have here on phone records, I am not real sure that opt-in may work in so many other settings. I was never convinced regarding other particular products and services. But I guess what I am just getting at is we understand pretexters and all that, and the defrauders and all that, but that is--and we are going to pass some law that is going to be able to address that. To be real clear of what is the behavior that we are trying to rein in and control, and I still go back that we shouldn't ignore better standards and requirements and so on that will actually govern this particular industry.

So I am going to ask you--I still have almost two minutes--when would it be legitimate to share that information at the request of a non-customer? Forget about pretexters, I mean, forget about that. I mean, that is just fraud being perpetrated. We are going to hopefully safeguard and criminalize and do all sorts of things on the civil side, but is there an instance where my phone company legitimately would be able to share that information, upon request, and grant that access other than Charlie Gonzalez requesting it?

MR. ROTENBERG. Congressman, one obvious answer would be a law enforcement investigation.

MR. GONZALEZ. I don't know. I mean, there is a law enforcement exception to everything.

MR. ROTENBERG. Right.

MR. GONZALEZ. And if you read in the newspapers, there may even be a different reading about the Constitution and the statutes today.

MR. ROTENBERG. Yes.

MR. GONZALEZ. Forget about that. I acknowledge that. I'm talking about in the business world.

MR. ROTENBERG. Yes. I mean, there could be circumstances and we discuss this in our testimony. There may be a civil subpoena, for example, or some business matter, but the point that we try to make is that there are legal procedures for getting access to business records where court reviews are requested and a business says okay, go ahead. I think the sense that many of us have is you really can't imagine why it is outside of a legal process that your personal information should be sold or disclosed to a third party. It is really a hole that needs to be sealed, I think.

MR. DOUGLAS. And if I could, Congressman, pull on one thread of what Marc just said, and back to your comment about how do we rein it in. To rein it in, and I cover it extensively in my written statement, but didn't address it in my oral testimony. You do need to understand who is in the market. While it is identity theft, and I have talked about that, the sad reality, the number one buyers of this type of information are: attorneys, collections agencies, bail bondsmen, and private investigators. They are the number one market and they look to do this outside the judicial process.

They are doing it extra-judicially to avoid the subpoena process, to avoid the discovery process; in some cases, even to see if it is worth going forward in a case. One thing I would like to see come out of this committee and this Congress is a loud signal to the legal community, as well, that this won't be tolerated. The Federal Trade Commission is well aware, in Operation Detect Pretext and Touch Tone, who the majority buyers were and they have never gone after that market for whatever reasons. I will let them explain it to you, but that is who is driving, that is where the cash flow comes to drive this market.

MR. GONZALEZ. With the recent information and publicity, I guarantee you it is not just lawyers and investigators and everybody else out there. You have a large segment of the population out there that is very curious about a whole lot of activity and behavior by someone that they are very interested in or have relationships with. That is what we are really getting down to here. But I think we have identified the real

problem and I think let us all work together and get to that solution and thank you very much for you all's testimony today.

MR. FERGUSON. Thank you. The gentleman from Washington, Mr. Inslee, is recognized for five minutes.

MR. INSLEE. Thank you. I want to thank two folks who have helped Washington, Mr. Merlis with Senator Menendez's staff and Mr. Largent with the Seattle Seahawks staff and Mr. Largent, we will miss you on the field. We have a pretty good twelfth man program, but we wish you were going to be there. I wanted to ask you what you thought of the Pittsburgh Steelers, but Mike Doyle of Pittsburgh is not here and I don't think that would be appropriate, so we will be sportsmanlike. I want to ask you about the modus operandi of these operations. Do they tend to customize their search? In other words, if Mr. Smith calls this Internet outfit and asks to find Mr. Jones' records, do they then go find Mr. Jones' records by calling and doing a pretext call, or do they already built up some massive data bank they just draw on already?

MR. DOUGLAS. No, they do it on an individual basis.

MR. INSLEE. It is customized? So they are pretexting on a customized basis?

MR. DOUGLAS. Right. And one of the ways, when you look at these websites, there are a number of indicia that can tell you whether it is a pretext operation. The three most obvious are, cost, they will cost higher than other records that they are selling, which are from public record data bases. Turnaround time, you will see that if they are just buying a Social Security number and address that can come from a public record database, it might be hours; whereas for pretexted information, the turnaround time may be days or even a week. And the third is a term used in the industry, no hit, no fee, which means if they don't, and there is a percentage of times when they will not succeed in getting the information, maybe because of password protection, maybe because of a very sharp customer service representative, they will not charge the person who came through the site. Reason being, they don't want the Lisa Madigans of the world on their tail because if they know they are not going to succeed and they charge clientele coming through the site for not delivering the product, more likely that customer, if you will, is going to go to the Lisa Madigans of the world and file a consumer complaint in a very backwards handed way here. So it will say no hit, no fee because hey, if I don't get it for you, you don't have to pay. Go your sweet way.

MR. INSLEE. So do you have concerns that there are losses of massive amounts of data at once, that, you know, there is some big data bank that has already been disclosed? You talked about a bribery

situation that you believe is going on. Do you think that has happened or are we just looking at pretexters doing one shot at a time?

MR. DOUGLAS. One shot at a time, but going back to the chairman's initial questions to the first panel, which they all deferred on. As to how often, how many sites, the volume, and also the dollar factor; the number of sites is hundreds, but as I explained in my written statement, those hundreds, like a pebble in the pond, are networked out to thousands of illicit information brokers and illicit private investigators. So pretty much anybody in America, calling up the right person in their yellow pages in the investigative industry, asking the right questions, if that investigator is convinced they are not a reporter or a cop doing a sting operation, they will get it. So there are thousands of people selling this. It is happening thousands of times every day. The records, again, are there in Docusearch, Touch Tone, Operation Detect Pretext, for anybody to research in the Federal government.

And another place I split hairs with the FTC is when they said that these are bottom feeders. Well, I have some idea what a Congressional salary is and I know what my paltry salary is. Some of these bottom feeders, like Docusearch--two people, Touch Tone, a husband and wife were doing, grossing, a million dollars a year selling these types of information; more than just phone records, banking records, as well. But I don't call that bottom feeding. I call that a lot of money and there is a lot of these operations, so this is a big underground black market operation in information in this country.

MR. INSLEE. Got you. I don't know if you gentlemen have taken a look at the bill I have sponsored with Representative Blackburn, but I just wondered if any you have comments or any of you who would say other limits should be passed with great fanfare and unanimous--do you have any comments about it, suggestions, critiques? Yes.

MR. DOUGLAS. I support anything that will immediately take on phone records and address this issue, but I would ask the committee to also consider at an appropriate point broadening this and what I say is because these guys are sitting here and they are on the hot seat today. Eight years ago it was the bankers on the hot seat. Eight years from now it is going to be your cable and satellite television providers. Some of these very sites that we are looking at are already selling utility record information. They are selling what are called post office breaks, which is defrauding the U.S. Postal Service out of address information. So what I say in my written statement is an unintended consequence of Gramm-Leach-Bliley. We created a nightmare for the phone industry because we pushed them, to a certain degree, from the financial information industry. So I would just ask that at an appropriate time the committee considers something a little bit more expansive, but please move immediately on

phone records for the women that are being harassed. Every time I appear in the news and I am sure when I get back to my hotel room, I get e-mails from women who say thank you. I am in hiding from so and so. I had two more this morning. So move quickly on the phone records, but consider more.

MR. INSLEE. You bet. Good point. Thank you.

MR. FERGUSON. I want to thank all of our witnesses for being here. Thank you very much for your generosity of your time and your expertise. We appreciate it. This is, like many issues on this committee, this has a big impact on the lives of a lot of our constituents and we appreciate your help. We are adjourned.

[Whereupon, at 6:09 p.m., the committee was adjourned.]

○