S. HRG. 109–452

PROTECTING CONSUMERS' PHONE RECORDS

HEARING

BEFORE THE

SUBCOMMITTEE ON CONSUMER AFFAIRS, PRODUCT SAFETY, AND INSURANCE

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

FEBRUARY 8, 2006

Printed for the use of the Committee on Commerce, Science, and Transportation

U.S. GOVERNMENT PRINTING OFFICE

27–705 PDF 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

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

TED STEVENS, Alaska, *Chairman*

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

DANIEL K. INOUYE, Hawaii, *Co-Chairman*
JOHN D. ROCKEFELLER IV, West Virginia
JOHN F. KERRY, Massachusetts
BYRON L. DORGAN, North Dakota
BARBARA BOXER, California
BILL NELSON, Florida
MARIA CANTWELL, Washington
FRANK R. LAUTENBERG, New Jersey
E. BENJAMIN NELSON, Nebraska
MARK PRYOR, Arkansas

LISA J. SUTHERLAND, *Republican Staff Director*
CHRISTINE DRAGER KURTH, *Republican Deputy Staff Director*
KENNETH R. NAHIGIAN, *Republican Chief Counsel*
MARGARET L. CUMMISKY, *Democratic Staff Director and Chief Counsel*
SAMUEL E. WHITEHORN, *Democratic Deputy Staff Director and General Counsel*
LILA HARPER HELMS, *Democratic Policy Director*

SUBCOMMITTEE ON CONSUMER AFFAIRS, PRODUCT SAFETY, AND INSURANCE

GEORGE ALLEN, Virginia, *Chairman*

TED STEVENS, Alaska
CONRAD BURNS, Montana
JIM DEMINT, South Carolina
DAVID VITTER, Louisiana

MARK PRYOR, Arkansas, *Ranking*
DANIEL K. INOUYE, Hawaii
BARBARA BOXER, California

CONTENTS

WITNESSES

APPENDIX

PROTECTING CONSUMERS' PHONE RECORDS

WEDNESDAY, FEBRUARY 8, 2006

U.S. SENATE,
SUBCOMMITTEE ON CONSUMER AFFAIRS, PRODUCT SAFETY, AND INSURANCE,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m. in room SD–562, Dirksen Senate Office Building, Hon. George Allen, Chairman of the Subcommittee, presiding.

OPENING STATEMENT OF HON. GEORGE ALLEN, U.S. SENATOR FROM VIRGINIA

Senator ALLEN. Good afternoon. I call this hearing of the Senate Subcommittee on Consumer Affairs, Product Safety, and Insurance to order. This hearing is going to examine ways to protect consumers' phone records from being fraudulently obtained and sold into the public domain. I am pleased to see the Ranking Member of the Subcommittee, Senator Pryor, here with us, as well as the Chairman of the Full Committee, Senator Stevens, and the Ranking Member, Senator Inouye. Senator Vitter and Senator Burns and other Senators will be appearing.

This is a very serious topic that is disturbing to all of us, that people can fraudulently obtain someone's phone records surreptitiously, without their knowledge, and invade their privacy. We appreciate all the witnesses who will be here today. We are going to, instead of two panels, have all the witnesses in one panel, all six, after we hear from Senator Schumer. We appreciate all of you being here. We look forward to your testimony.

The impetus, of course, of this hearing today is the deceptive practice of obtaining and selling confidential phone records without an owner's consent. I know I probably speak for all Americans, and Members of the Subcommittee, when I say that it was important to take action as soon as we heard that these unscrupulous marketers were obtaining and selling confidential personal phone billing records. This is fraudulent and criminal activity that must be prosecuted and must be stopped to protect innocent people.

Especially of concern to me are the rights of some women, who have had their privacy violated by stalkers who use the information to get details of their personal lives—also harming law enforcement investigations. This fraudulent activity can be every bit as harmful, and in some cases even more disconcerting, than when a third party uses false pretenses to obtain an innocent person's confidential financial records.

In some cases, even physical harm can result from one's private phone records becoming a public record. We have a witness today who will explain how domestic violence can result if a woman's call records are divulged to an abusive spouse or an ex-boyfriend. We will also hear how law enforcement can be hindered if records of an undercover agent are suddenly made available to a criminal party.

We all feel that we cannot allow these unscrupulous, deceptive, and fraudulent practices to continue. That is why Chairman Stevens and I, along with the Ranking Member, Senator Pryor, decided that we should hold a hearing, listen, learn, and then craft legislation, effective legislation—do not just pass a bill, but let us make sure this is effective legislation—to protect innocent individuals from becoming prey to conniving people willing to make a quick buck by violating someone's privacy and security.

Senator Stevens and I and others are working on legislation to address this issue, but it is important that we listen. We will hear from our witnesses today regarding a prudent, balanced perspective on how to ensure that customer phone records are protected. We hope that our witnesses will offer to us possible solutions as well. We look forward to hearing from each of our witnesses on a commonsense and properly focused solution to avoid any unintended consequences. In fact, any Federal involvement in addressing deceptive business practices can harm, obviously, consumers; it does need to be reasonable; and, it needs to be effective.

With that, I would now like to turn it over to Senator Pryor if he would like to make an opening statement, and then opening statements from—while he was not the next one here, I will defer to the Chairman and Ranking Member, and then in the order in which Senators arrived. Senator Pryor.

STATEMENT OF HON. MARK PRYOR, U.S. SENATOR FROM ARKANSAS

Senator PRYOR. Thank you, Mr. Chairman.

The Internet has provided a whole new world of information services and a vigorous platform to conduct commerce. Unfortunately, the success of the Internet has also created problems regarding consumer privacy, which this Committee has wrestled with for the past several years. There has been spam, spyware, identity theft, and several other issues we have tackled with varying degrees of success.

Congress has been addressing issues of privacy in a piecemeal fashion and this approach, quite frankly, places us at a disadvantage. There is always a new threat to our privacy because of the very nature of changing technology and Congress has to address each threat separately.

Today we face the threat of data brokers selling cell phone records with $100 in their pocket. Phone records make the owner of that phone number especially vulnerable. These records show every incoming and outgoing number, the duration of the call, and even the location of the numbers called. GPS systems are on all cell phones now, making it possible for sophisticated parties to track the person holding the cell phone.

I reviewed the testimony and our witnesses note that some data brokers have been selling cell phone records for years and have likely been obtaining these records by legally questionable practices. There can be only a few ways to get a cell phone number and record for virtually anyone in the United States just within a few hours. The sellers either get the information by fraudulent misrepresentations, or pretexting, hacking into a phone company database, or bribing a phone company employee to steal this information.

However this information gets into the hands of data brokers, it has to stop. The consequences of this type of information being available to anyone are too severe. As the Chairman mentioned a moment ago, murderers have been aided by the information sold by these data brokers and countless others have been endangered.

The Federal Trade Commission and the Federal Communications Commission have regulatory responsibility in protecting the privacy of consumers. The FTC has jurisdiction over the data brokers and other sellers of this type of information via its authority from section 5 of the FTC Act. The FCC has jurisdiction over the telecommunications company via section 222 of the 1996 Telecommunications Act.

We need to make sure that both agencies have the statutory authority they need to quickly and effectively end this activity. Most importantly, we must make sure that both agencies use their authority aggressively and that they are working together to vigorously protect and prosecute these cases. I look forward to hearing from today's witnesses and moving quickly toward a solution that will protect all of America's consumers.

I would also like to welcome Senator Schumer, wherever he may be, because he has done some work on this issue and he has really shown some leadership here.

Mr. Chairman.

Senator ALLEN. Thank you, Senator.

Now we would like to hear from the Chairman of the Full Committee, Senator Stevens, who has been working and trying to address this matter. We thank you, Mr. Chairman, for allowing the Subcommittee to hold this hearing, and I think it will allow us to craft workable and effective legislation.

STATEMENT OF HON. TED STEVENS,
U.S. SENATOR FROM ALASKA

The CHAIRMAN. Thank you, Mr. Chairman. I would ask that you put my prepared remarks in the record.

Senator ALLEN. Without objection.

The CHAIRMAN. I am here despite another conflict because I want to listen to the FCC. I am particularly interested in knowing why the FCC regulation requires notice to a party before moving to an enforcement action. In effect, they give notice to the people that are doing wrong that they are about ready to look into whether they are doing wrong. So they just disappear and we never have a real enforcement. So I hope that FCC can address that.

But please put my statement in the record. Thank you.

Senator ALLEN. Without objection, the full statement will be put in the record. If opening statements could be limited to 5 minutes, and full statements will be made part of the record.

[The prepared statement of Senator Stevens follows:]

PREPARED STATEMENT OF HON. TED STEVENS, U.S. SENATOR FROM ALASKA

The recent reports detailing the ease with which third parties can access private phone records are alarming. These reports have shown us that it is important that Congress ensure that Americans' phone records are protected and that there will be severe penalties for invading phone record privacy.

I have been working on crafting a legislative solution to address this growing problem and assess the proper role of government. As we move forward, I look forward to continuing to work with the industry, the relevant Federal agencies, and other Members of Congress to ensure that all phone records are kept safe.

This hearing is an important step as this Committee addresses this issue. But we are not alone in this fight, and I look forward to hearing the thoughts of the Federal agencies with oversight, the industry, and concerned public interest groups.

Senator ALLEN. Now we would like to hear from the Ranking Member of the Full Committee, Senator Inouye.

STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

Senator INOUYE. Mr. Chairman, I thank you very much and commend you for convening this hearing. I wish to associate myself with your remarks, with that of the Chairman Stevens, and Mr. Pryor as I see what is pending before us, the horrendous possibility of invasion of privacy. I have got a cell phone and all of us have cell phones and just the thought that someone is passing information to others just horrifies me.

Thank you very much, sir. May I have my statement put in the record.

Senator ALLEN. Your full statement will be made part of the record.

[The prepared statement of Senator Inouye follows:]

PREPARED STATEMENT OF HON. DANIEL K. INOUYE, U.S. SENATOR FROM HAWAII

It was troubling to learn that unscrupulous data brokers have made a business of selling consumers' personal phone records. Equally disturbing is the fact that the Federal Trade Commission (FTC) received numerous complaints about these egregious practices and refused to act on them.

While many recent identity theft scams have employed tech-savvy tactics of hackers, the sale of consumer phone records is simply the work of swindlers. It is well within the FTC's current authority to address this problem. I understand the FTC found numerous instances of cell phone record sales in other investigations related to financial services and chose to turn a blind eye.

Unfortunately, the FTC's inaction resulted from a lack of attention, not a lack of authority. Nonetheless, if further clarity and additional authority are necessary, this Committee should not hesitate to provide it.

The Federal Communications Commission (FCC) has a key role to play as well. The FCC must ensure that telecommunications providers are doing all that is necessary to protect the confidentiality of consumers phone records, or what is also known as customer proprietary network information (CPNI). The FCC appears to be taking this matter seriously.

Next week, the FCC will consider ways to strengthen CPNI safeguards through rulemaking. In addition, FCC Chairman Kevin Martin has recommended specific Congressional action to address this problem, including enhancing the FCC's enforcement authority.

We also need to keep in mind emerging services, such as Voice over Internet Protocol (VoIP). They, too, must be subject to the same privacy requirements. Con-

sumers have every right to expect that their personal data will be protected regardless of the communications service they choose to utilize.

It is my hope that the recent press attention to this matter has served as a wake up call, and that, in the interest of consumer privacy and public safety, the FTC and FCC do everything they can to eliminate these egregious practices as quickly as possible. I can assure both agencies that this Committee will be a willing and cooperative partner in their efforts.

Senator ALLEN. Now we would like to hear from Senator Vitter of Louisiana. Welcome, Senator.

STATEMENT OF HON. DAVID VITTER,
U.S. SENATOR FROM LOUISIANA

Senator VITTER. Thank you, Mr. Chairman, and thank you for holding the hearing today. It is clearly a very important issue. I join everybody in expressing my concern and outrage about data broker companies with fraudulent websites selling these sorts of records. It is clearly a part of the growing family of issues like identity theft that we need to get ahead of the curve on in this Committee, and this Subcommittee is a big part of that.

I understand, as others have said, that there are many theories about how these data brokers get this information. It could come from inside the wireless companies by a corrupt employee, by hacking into the system, by pretexting. However it is obtained, we need to do what we can to protect consumers.

My first thought is that all of these practices appear to be criminal activities already, but because there are loopholes in the current law and probably even bigger loopholes in the enforcement, we need to do more. My hope is we will follow up on this hearing and move legislation that removes all doubt and, even more importantly, gives relevant agencies the powers they need to go after this fraud. I believe we should focus on fraudulent actors and make sure this is stopped.

Again, Mr. Chairman, I want to thank you for calling this hearing. I look forward to working with you and the rest of the Subcommittee.

Senator ALLEN. Thank you, Senator Vitter.

Now we would like Senator Burns, if you would have any opening remarks and wisdom.

STATEMENT OF HON. CONRAD BURNS,
U.S. SENATOR FROM MONTANA

Senator BURNS. Thank you, Mr. Chairman and Ranking Member Pryor. I appreciate that, and the Members of this Committee. I would ask unanimous consent that my statement be made part of the record today.

Senator ALLEN. Without objection.

But I just want to bring up—and I am glad to see Senator Schumer here. We are on a bill right now. We are crafting a bill. It is the Consumer Telephone Records Protection Act of 2006. We look forward to working with Members on this Committee, knowing that you are interested in this, and whenever you get your legislation put back together we can marry up with those two pieces and I think could come up with a pretty good bill.

I was appalled when I learned of this, that anybody could call up a telephone company and, especially with a stolen Social Security

number and your date of birth, you can obtain the records, and those records were being harvested. Then you have got people that put up a website that says, we will sell you that number for 100 bucks or so, whatever. I thought—I just could not believe it.

I want to applaud first Chairman Martin of the FCC for the action that he has taken pursuant to the statutory authority to protect consumers' personal telephone records. If you take right out of section 222 of the Communications Act and the Commission's rule will result, I think, in pretty strong enforcement by the FCC. The FTC also is involved in this.

But we have got to make this fine on those who would participate in such an action such as this a pretty hefty fine and with some little jail time behind it, because basically you are robbing a person's private records. It can be used for a multitude of things. We all have cell phones.

Now, I would say, today is the tenth anniversary of the telecom bill of 1996, and I can remember working on that bill a long time and it took a long time, I think anyways, from 1991 to 1996, to get that changed. We were trying to deal with 1990s' technology with a 1935 law. Now we have got to go back, because technology moves so fast, and look at that Act again. How much did we miss the number of prospective cell phone users by the year 2000? We only missed it 300 percent. I do not think you want me coming out and estimating what you can produce on your ranch under those kind of circumstances.

But this is appalling and we must take action. It has to be now and it has to be stringent. There can be no loopholes in it like that exist today in the law.

I thank the Chairman for having these hearings.

[The prepared statement of Senator Burns follows:]

PREPARED STATEMENT OF HON. CONRAD BURNS, U.S. SENATOR FROM MONTANA

Good afternoon Chairman Allen, Ranking Member Pryor, Members of the Committee, and distinguished panelists. Thank you for holding this important hearing on protecting consumers' phone records. First, I am very disturbed about the disclosure and sale of personal telephone records through data brokers pretexting or by data brokers obtaining access to consumers' accounts online by overcoming carriers' data security protocols.

As an original cosponsor of the Consumer Telephone Records Protection Act of 2006, I'm proud to say my bill will close existing loopholes and will make you pay a hefty price in both money and jail time if you access someone's private records without their permission. Importantly, this bill criminalizes the act of pretexting, adding a new violation for fraud and related activity connected with obtaining confidential phone records from a company that provides telephone service. Specifically, the Consumer Telephone Records Protection Act of 2006 proposes that for each occurrence the illegal actor can be fined up to $250,000 and/or imprisoned for up to 5 years. These penalties can be doubled for aggravated cases. The criminal violations in this bill, along with action taken by the FCC and further Congressional Action, if needed, will restore consumers' confidence that their personal information is safe when they sign up for phone service with a telecommunications company.

Next, I want to applaud Chairman Martin for the action that the FCC has undertaken pursuant to its statutory authority to protect consumers' personal telephone records. Chairman Martin recently appeared before the House of Representatives and testified that any noncompliance by telecommunications carriers with the customer proprietary network information (CPNI) obligations under section 222 of the Communications Act and the Commission's rules will result in strong enforcement action by the FCC. Section 222 of the Communications Act was written to protect consumers' privacy. Specifically, it provides that carriers must protect the confiden-

tiality of customer proprietary network information. CPNI includes, among other things, customers' calling activities and history, and billing records.

Under FTC Law, it is already considered an illegal deceptive business practice to use false pretenses to gather a consumer's financial information. The FTC has the power to pursue actions against phone record pretexters based on its authority to prevent deceptive and unfair business practices, but without this statutory authority spelled out in a statute, a question of statutory interpretation regarding FTC authority could be litigated. Furthermore, even if the FTC's authority to pursue actions against pretexters of phone records is assumed, the FTC is not authorized to immediately impose civil penalties against third party data brokers.

Unfortunately, in today's information age, there are those who are constantly seeking new ways to navigate the gray areas of our laws in hopes of finding something they can use to their advantage. My bill will shine a bright light on this particular gray area, wiping it out, and protect Americans from these rats who invade someone's privacy.

Thank you all for your time and concern and I look forward to working with the Members of this Committee, panel and other interested parties as this discussion moves forward.

Senator ALLEN. Thank you, Senator Burns.

Senator Boxer.

STATEMENT OF HON. BARBARA BOXER, U.S. SENATOR FROM CALIFORNIA

Senator BOXER. Thank you so much, Mr. Chairman. I really appreciate your having this hearing. The battle to keep confidential consumer information is never-ending. It seems like every month we hear of a new way that shady companies are exploiting the information of consumers for a profit.

The latest example is the sale of phone records by online data brokers. We have all read that sites like *datatraceusa.com* will sell a person's phone records to anyone willing to spend $100. The time, duration, and number of every call a person has made from their phone is being made available to the public. Such information is being purchased by the likes of abusive spouses, leading to more domestic violence, and stalkers, who are able to infiltrate the lives of their victims.

It has gotten to the point that the Chicago police and the FBI are warning their undercover agents that their phone records may be compromised, which could lead to their cover being blown. Most of the online data brokers take no steps to make sure that the information is being used for legitimate purposes. Moreover, the data brokers themselves are using fraudulent means to obtain the information from cell phone companies. In the pursuit of making a few dollars, these companies are helping criminals and undermining law enforcement. This must be stopped.

That is why I have cosponsored the Consumer Telephone Records Protection Act introduced by Senators Specter and Schumer, and I am so glad that Senator Schumer is here. This bill will criminalize the sale of phone records without the consent of the subscriber. Mr. Chairman, it is a very simple notion and it will work.

I also would urge my colleagues to support another privacy bill, introduced by Senator Specter and myself, the Wireless 411 Privacy Act, that prohibits the listing of a cell phone number in any wireless directory unless the subscriber elects to be included. Again, abused women should not have to worry that their cell phone number will be listed in a directory without them knowing

about it. More generally, consumers should be able to keep their numbers private if that is what they want.

So I would ask unanimous consent that the rest of my statement be placed in the record, Mr. Chairman. But I do feel we see this problem; we must act before people are really hurt. Also, we have a couple of bills out there that are so good, and they are bipartisan and they make sense. I hope we can move them quickly, and I think we will be doing something very good for our constituents.

Thank you.

Senator ALLEN. Thank you, Senator Boxer. Your full statement will be made part of the record.

[The prepared statement of Senator Boxer follows:]

PREPARED STATEMENT OF HON. BARBARA BOXER, U.S. SENATOR FROM CALIFORNIA

Mr. Chairman, thank you for holding this hearing on the privacy rights of cell phone subscribers.

The battle to keep confidential consumer information private is never ending. It seems like every month we hear of a new way that shady companies are exploiting the information of consumers for a profit.

The latest example is the sale of phone records by online data brokers. We have all read that sites like *datatraceusa.com* will sell a person's phone records to anyone willing to spend $100.

The time, duration, and number of every call a person has made from their phone is being made available to the public. Such information is being purchased by the like of abusive spouses leading to more domestic violence and stalkers who are able to infiltrate the lives of their victims.

It has gotten to the point that the Chicago police and FBI are warning their undercover agents that their phone records may be compromised, which could lead to their cover being blown.

Most of the online data brokers take no steps to make sure that the information being sold is used for legitimate purposes. Moreover, the data brokers themselves are using fraudulent means to obtain the information from cell phone companies.

In the pursuit of making a few dollars, these companies are helping criminals and undermining law enforcement.

This must be stopped and that is why I have cosponsored the Consumer Telephone Records Protection Act introduced by Senators Schumer and Specter, which criminalizes the sale of phone records without the consent of the subscriber.

I also would urge my colleagues to support another privacy bill I introduced last session and reintroduced last year with Senator Specter—the Wireless 411 Privacy Act. This bill prohibits the listing of a cell phone number in any wireless directory service unless the subscriber elects to be included.

Abused women should not have to worry that their cell phone number will be listed in a directory without them knowing about it. And more generally, consumers should be able to keep their number private if that is what they want.

This is especially important with respect to cell phone numbers, because consumers pay for each call they receive.

Last session, a number of wireless carriers objected to certain provisions of my bill, including the requirement that subscribers opt-in to being listed. It is my understanding that the major wireless companies no longer object to this provision.

This is a promising change. It is a sign that companies are beginning to recognize that it is our responsibility to protect the privacy of consumers.

In response to press reports, the wireless phone companies are improving their privacy practices and suing data brokers to prevent the release of their customers' phone records.

Reacting to revelations in the papers of privacy breaches, however, is not enough. All companies—not just the wireless operators—should be proactive in protecting the privacy of their customers. They know the weakness of their own systems and how to fix those problems.

If companies fail to act, Congress has a duty to step in and legislate the changes that are necessary to protect consumers.

I look forward to hearing from the witnesses about what is being done to protect consumers' confidential information and I plan to work with this Committee to get my Wireless 411 Privacy bill marked-up and brought to the floor.

Thank you, Mr. Chairman.

Senator ALLEN. Senator Smith.

STATEMENT OF HON. GORDON H. SMITH,
U.S. SENATOR FROM OREGON

Senator SMITH. Thank you, Senator Allen and Chairman Stevens, for this very important hearing. The deceptive practice of pretexting has gotten, rightfully, a lot of attention lately. It is nothing more than lying to get something you are not entitled to have, and it is currently illegal. The Federal Trade Commission has the authority to pursue companies or individuals that engage in pretexting or other deceptive practices under section 5 of the FTC Act, which prohibits unfair or deceptive acts or practices in or affecting commerce.

Using this authority, the FTC has brought civil actions against U.S. businesses that use false pretenses to gather information on consumers. Unfortunately, the FTC lacks authority to pursue bad actors operating overseas. We need to give the FTC these necessary tools. I sponsored the U.S. SAFE WEB Act with Senator Inouye, Senator McCain, Senator Nelson of Florida, Senator Burns, Senator Dorgan, and Senator Pryor. This is an important bill that will provide the FTC with the tools to protect consumers from cross-border fraud and deception, including pretexting. Our bill has already passed the Commerce Committee. It did so unanimously and I urge quick passage on the floor of the Senate. It will help solve this problem we are dealing with.

One last point. Like consumers, phone companies are victims of fraud perpetrated by pretexters. Additional regulation of phone companies may not change fraudulent behavior pretexters. I think it is important to emphasize that enforcement is the key. If we need more laws, let us get more laws. But let us enforce the laws that we have.

Thank you, Mr. Chairman.

Senator ALLEN. Thank you, Senator Smith.

I would like to hear from our first panelist, all by his lonesome, but not by his lonesome insofar as this issue and concern. Senator Chuck Schumer has joined us today to discuss this issue in terms of the law enforcement perspective proceeding from his viewpoint as a Member of the Judiciary Committee. Senator Schumer's involvement also extends to a bill that he has recently introduced.

Senator Schumer, you can go ahead with your testimony. Then we will hear from the rest of our witnesses. Senator Schumer.

STATEMENT OF HON. CHARLES SCHUMER,
U.S. SENATOR FROM NEW YORK

Senator SCHUMER. Thank you. Thank you, Mr. Chairman, and I want to thank you, Senator Pryor, Chairman Stevens, and all the rest of the Members, for the opportunity to speak to you today. I know this issue is of great concern to all of us, protecting the very privacy and personal information that is kept part of people's telephone records, because when a person talks on the phone, whether it is their cell phone or their home phone, they have an expectation of privacy. No one thinks that information about who they are calling and when they are calling them, as well as all of the personal

information kept by phone companies for billing purposes, are available for sale to anyone with $100. But, sadly, that is the case.

The activities of websites such as *locatecell.com* and other pretexters who pose as telephone customers to get people's personal phone record information from the phone companies have made some of our most personal and confidential information vulnerable to criminals who want that information for nefarious purposes.

Even worse, unauthorized access to this information can put law enforcement officers and victims of domestic abuse in danger. A former spouse, a stalker, can find out who their target is calling and intensely personal information, like who their doctor is, whether the person sees a psychologist. Targets of criminal investigations can find out if someone is talking to law enforcement authorities about them. And in a particularly frightening scenario, the FBI recently was able to obtain the cell phone records of one of its agents online in just 3 hours.

Business people too are subject to this. A list of who a salesperson is calling upon could be available to a business rival.

So this is a problem that we have to deal with. We already have a law that protects our financial information. Pretexting of financial information is illegal *per se*. That is in the Gramm-Leach-Bliley Act that many of us supported and worked on several years ago. But there is no Federal law that makes it a criminal offense to steal someone's cell phone records. Right now there are laws on the books, as has been mentioned, but they are general fraud statutes, far less specific, and not good tools according to law enforcement for what they need to go after these illegal acts.

So far the cell phone companies have to go after pretexters with civil lawsuits or prosecutors have to cobble together a case from a patchwork of laws. But if all that pretexters really face are civil fines, they are going to look at this as the cost of doing business. What these thieves do is a crime and ought to be treated like a crime.

That is why, along with Senator Specter and many others, eight Members of this Committee cosponsored legislation that will do that, make stealing a person's phone records a felony. It is called the Consumer Telephone Records Protection Act, and I am happy to report that we have a bipartisan group of cosponsors, mainly from the Commerce and Judiciary Committees, which are the two committees of relevant jurisdiction.

In addition, three of the major wireless carriers—Verizon Wireless, T-Mobile, and Sprint Nextel—as well as consumer groups like Consumers Union, support the bill.

It is a very simple bill. It makes it a crime to fraudulently buy someone's phone records. It prohibits the sale or transfer of those records and specifically prohibits employees of phone companies from selling this information.

We are also looking at enhanced penalties when the records are used to commit a crime of domestic violence or if they are used to harm law enforcement officers. The bill also contains an enhanced penalty for multiple offenses, aimed at the websites and companies that make a business out of stealing records, such as some of them that are on the screen over there.

All of the bipartisan support, support from industry and consumers groups, I think shows very clearly the need to do something now, and I look forward to working with all of you on the Commerce Committee, which you have jurisdiction, of course, over FTC and all of that (we have jurisdiction over the criminal law in Judiciary) to find a quick solution that will stop pretexters and protect the privacy of American citizens.

Thank you.

Senator ALLEN. Thank you, Senator Schumer.

We would now like to hear from the rest of the panel. We appreciate again, Senator Schumer, your willingness to work with us. We look forward to working on a team effort.

I would like all of the six witnesses to come forward. I will introduce all of the witnesses. The order that we will go through the witnesses' testimony will be: first, Ms. Kris Monteith and Ms. Lydia Parnes, then the Honorable Steve Largent, Mark Rotenberg, Robert Douglas, and Cindy Southworth. So if you could—it looks like we are not going to get them in that order.

As our witnesses are getting seated, let me begin with a brief introduction of each for those assembled here and for our Committee. To start, we have Ms. Kris Monteith, the Chief of the Enforcement Bureau at the Federal Communications Commission. Ms. Monteith's role at the FCC places her in a direct role in protecting consumers' phone records. We appreciate your willingness to discuss the role of the FCC and what it can play in the safety of consumer phone records. Thank you for testifying.

Next we will hear from Ms. Lydia Parnes, who is the Director—she is Director of the Bureau of Consumer Protection at the Federal Trade Commission. The FTC is at the center of protecting consumers from deceptive business practices. Ms. Parnes will be able to give us a better idea of how to deter this fraudulent behavior and put these bad actors out of business, and we want to do that for good. Thank you for being here.

Next we will hear from the Honorable Steve Largent, President and CEO of the Cellular, Telecommunications and Internet Association, otherwise known as "CTIA." He is a Hall of Famer, was there at the Superbowl. The Seattle Seahawks had a tough game. Still, they made it to the Superbowl. More importantly, as a Hall of Famer we hope you help bring this team here together for success in combatting these pretexters.

Next we will hear from Mr. Marc Rotenberg, Mr. Rotenberg, who has actually been here testifying on several occasions. He is Executive Director of the Electronic Privacy Information Center, otherwise known as "EPIC." He has testified on a variety of issues. We welcome you back. He is here to give us his suggestions on how to best prevent an individual's phone records from being compromised.

Then we will hear from Mr. Robert Douglas, Chief Executive Officer of *PrivacyToday.com.* Mr. Douglas is a former private investigator and has testified in front of Congress multiple times regarding information security. He can provide us with examples of real-life experiences with pretexting. Thank you, Mr. Douglas, for coming all the way from Steamboat Springs, Colorado. I know you once lived in Virginia, but now you have a farther trek.

Finally, we are going to hear from Cindy Southworth. Cindy Southworth is the Director of Technology and Director of the Safety Net Project at the National Network to End Domestic Violence. Ms. Southworth's testimony can shed light on the potential ramifications of a person's phone records being divulged to someone other than the customer. Domestic violence against women is her area of expertise and she can offer a perspective on how physical abuse can result if a woman's phone records are obtained from an abusive husband, ex-boyfriend, or stalker, and we appreciate, Ms. Southworth, your attendance today and we look forward to your insight.

Senator BURNS. Mr. Chairman, before we go to the witnesses, can I make an announcement here, because I have got to go to the floor in about 15 minutes.

Senator ALLEN. All right.

Senator BURNS. Just an announcement to remind everybody. The Internet Caucus—and what we are talking about is the Internet here and the Internet business—is tonight, 5 o'clock, over in Dirksen G–50. We have got a lot of vendors——

Senator INOUYE. It is for Members.

Senator BURNS. Well, no; for everybody. Everybody can go. We do not check anybody at the door.

Senator ALLEN. Open standards.

Senator BURNS. Open standards.

I just thought I would remind it to you if you are in the buildings and want to attend that.

Senator ALLEN. All right, thank you. Thank you, Senator Burns.

Now we would like to hear from Ms. Monteith.

STATEMENT OF KRIS ANNE MONTEITH, CHIEF, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Ms. MONTEITH. Good afternoon, Mr. Chairman.

Senator ALLEN. I am going to ask, in the event that you can, I know you all have written testimony. If you can present it in 5 minutes; if it is longer than 5 minutes you may summarize, and all of your testimony will be made part of the record. In the questioning of the witnesses, I would ask that the Senators also be limited to 5 minutes in their inquiries.

Ms. Monteith.

Ms. MONTEITH. Good afternoon, Mr. Chairman and Members of the Subcommittee and the Full 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. As Chairman Martin made clear in his testimony last week, the Commission is deeply concerned about the disclosure and sale of these records. Determining how this violation of consumers' privacy is happening and addressing it is a priority for the Commission.

In my testimony today, I will describe the Commission's current investigation into this serious issue and then touch on the legislative proposals Chairman Martin identified as possible measures Congress might take to prevent data brokers from selling consumers' phone records.

The Commission is taking numerous actions to combat this issue. First, we are investigating how data brokers are obtaining con-

sumers' personal telephone records. Second, we are investigating whether telecommunications carriers are adequately protecting 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 records from unauthorized disclosure.

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 filed a petition expressing concern over the sale of consumers' private telephone data by data brokers. The Commission's Enforcement Bureau began researching and investigating these practices. Its research culminated in the Commission issuing subpoenas to several of the most prominent data brokers. When these companies failed to adequately respond to the subpoenas, we issued letters of citation and referred to responses to the Department of Justice for enforcement.

Subsequently, we issued subpoenas to another 30 data brokers and are awaiting their responses. We also made undercover purchases of phone records from various data brokers to assist us in targeting additional subpoenas and to determine exactly how the consumer phone record data is being disclosed.

In conjunction with our investigation of data brokers, in December and January the Commission met with the major wireless and wireline providers to discuss efforts they have undertaken to protect their confidential consumer data. Formal letters of inquiry followed that required 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 brokers issue.

In late January we asked the five largest wireline and wireless carriers to send us their required annual compliance certificates. In addition, early last week the Enforcement Bureau issued notices of apparent liability in the amount of $100,000 against two companies for failure to comply with the certification requirement. We also issued a public notice requiring all telecommunications carriers to file their most recent certification with the Commission.

Throughout our investigation, we have coordinated closely with the FTC and will continue to share any evidence of fraudulent behavior that we detect in the course of our investigation.

Finally, several weeks ago Chairman Martin circulated an item to his fellow Commissioners granting EPIC's petition and inviting comment on whether additional Commission rules are necessary to strengthen the safeguards for customer records. The item will be acted on by February 10th.

In response to questions about what Congress might do to prevent data brokers from selling consumers' phone records, Chairman Martin identified three primary actions. First, Congress could specifically make illegal the commercial availability of consumers' phone records. Second, Congress could overturn the Tenth Circuit ruling that limited the Commission's ability to implement more stringent protection of consumer phone record information. This ruling has resulted in a much broader dissemination of consumer

phone records and may have contributed to the proliferation of the unlawful practices of data brokers that we are seeing today.

Third, the Commission's enforcement tools could be strengthened by, for example, eliminating the citation requirement in section 503(b) of the Act, raising the statutory maximum forfeiture penalties, and lengthening the applicable 1-year statute of limitations.

To conclude, the disclosure of private calling records represents a significant invasion of privacy. The Commission looks forward to working collaboratively with the Members of this Subcommittee, other Members of Congress, and our colleagues at the Federal Trade Commission to ensure that consumers' personal phone data remains confidential. Thank you for the opportunity to testify. I would be pleased to answer your questions.

[The prepared statement of Ms. Monteith follows:]

PREPARED STATEMENT OF KRIS ANNE MONTEITH, CHIEF, ENFORCEMENT BUREAU, FEDERAL COMMUNICATIONS COMMISSION

Introduction

Good afternoon, Chairman Allen, Ranking Member Pryor, and Members of the Subcommittee. I appreciate the opportunity to speak with you today about what appears to be an alarming breach of the privacy of consumers' telephone records. As Chairman Martin made clear in his testimony last week, 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 Subcommittee 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 Chairman Martin and 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, the Commission is 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 im-

[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 the purchaser intends to use the information in a legal proceeding.

personating 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 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, the Commission's Enforcement Bureau 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 late January, we asked the five largest wireline and wireless carriers to send us their CPNI certifications. Early last week, the Enforcement Bureau issued Notices of Apparent Liability in the amount of $100,000 against both AT&T and Alltel for failure to comply with the certification requirement. 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, Chairman Martin 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, Chairman Martin circulated an item to his fellow Commissioners granting EPIC's petition and inviting comment on whether additional Commission rules are necessary to strengthen the safeguards for customer records. Specifically, the item seeks 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, the item also seeks 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.

As Chairman Martin has indicated, the 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. Chairman Martin has identified three primary actions that Congress could take to prevent data broker companies from selling consumers' phone records. First, 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, Chairman Martin has recommended 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. We look forward to working collaboratively with the Members of this Subcommittee, other Members of Congress, as well as our 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.

Senator ALLEN. Ms. Monteith, thank you very much for your testimony and your very specific ideas of what we can do to strengthen the enforcement capabilities of the FCC. You will undoubtedly have some questions posed to you later, as will all the witnesses.

Now we would like to hear from Ms. Parnes with the Federal Trade Commission. Please proceed.

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

Ms. PARNES. Good afternoon, Mr. Chairman and Members of the Subcommittee. I too appreciate the invitation to appear today to discuss the important topic of the privacy and security of consumers' telephone records. My oral testimony and responses to questions reflect my own views and not necessarily those of the Commission or any individual commissioner.

Maintaining the privacy and security of consumers' sensitive personal information is one of the Commission's highest priorities. We have wrestled with spam, spyware, and identity theft and, in cooperation with the FCC, are now vigorously investigating companies that use subterfuge to gain access to consumers' telephone call logs. Today I will describe the FTC's efforts to protect consumers from pretexters generally and the specific practice of pretexting for telephone records. Then I will address the issue of whether new laws are needed to stop this troubling practice.

The Commission filed its first pretexting suit in 1999, against a company that offered to provide consumers' bank account numbers and balances to anybody for a fee. The FTC alleged that this decep-

tive conduct violated section 5 of the FTC Act. Later that year, Congress enacted the Gramm-Leach-Bliley (GLB) Act, which expressly prohibits pretexting for financial records.

Since GLB's passage, the FTC has sent warning letters to 200 firms that sold asset information to third parties and brought more than a dozen financial pretexting cases. But it is also important to control the supply side of sensitive consumer information. In that vein, the Commission recently announced a recordbreaking $15 million settlement against ChoicePoint, challenging business practices that we alleged unreasonably exposed consumer data to theft and misuse.

Now let me turn to the cottage industry of companies peddling cell phone and landline records. In preparation for this hearing, we did a quick review of the telephone record marketplace. The results are illuminating. First, we looked at 40 websites previously reported to be selling call records. As of this Monday, more than half were no longer advertising the sale of such records. One website told would-be customers, and I quote: "Due to controversy surrounding the availability of phone records via the Internet, we have decided to discontinue offering these searches."

Unfortunately, we also found that at least nine of the companies still make unabashed offers to obtain call records. The remaining companies are making more ambiguous offers that are still of concern. Thus, thanks to the attention this issue has received in the media and in hearings like this one, at least some in the pretexting industry have gotten the message. But there is still work to be done.

Yesterday we sent warning letters to 20 companies that are offering to obtain and sell telephone call records, and the Commission has a number of ongoing investigations as well.

I know the Committee is considering whether additional legislation is necessary to protect these records. One approach would be a specific prohibition on the pretexting of telephone call records, modeled on the Gramm-Leach-Bliley Act's protection of financial records. If Congress were to consider such legislation, I would recommend that it give the Commission authority to seek civil penalties against violators, a remedy that the FTC does not currently have in cases like this. I believe that in this area, penalties are the most effective civil remedy.

This is also a situation where criminal penalties may be warranted, but as a civil agency we would defer to the Department of Justice on the need for criminal legislation and particularly its structure.

In addition, our recent surf revealed that some sites offering these records were registered to foreign addresses. This finding underscores the importance of the Commission's previous recommendation that Congress enact cross-border fraud legislation. The proposal, called the U.S. SAFE WEB Act, will overcome many of the existing obstacles to information-sharing and cross-border investigations. I would like to thank the Committee for its leadership on this bill.

Finally, Congress may consider, as recommended by the FCC, whether a ban on the sale of call records in all cases is appropriate. Should it do so, I would recommend that Congress exercise caution

in determining the breadth of such a ban. Certainly law enforcers will continue to have legitimate reasons for obtaining phone records and it is possible that there may be other limited circumstances in which these records might be disclosed for appropriate and useful purposes. For example, the GLB pretexting prohibition provides an exception in cases involving the collection of court-ordered child support payments.

Again, thank you for the opportunity to testify today. We look forward to working with the Committee and its staff on this very important issue.

[The prepared statement of Ms. Parnes follows:]

PREPARED STATEMENT OF LYDIA B. PARNES, DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION

Introduction

Mr. Chairman, and Members of the Subcommittee, I am Lydia B. Parnes, Director of the Bureau of Consumer Protection at 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 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

---

[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.

[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).

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"). 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]

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, e-mail, 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]

---

[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.

[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.

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 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, two weeks ago 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 landline 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

---

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

[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.,* No. 106–CV–0198 (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 landline 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, *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.*

not prohibited 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.

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.

Senator ALLEN. Thank you, Ms. Parnes. We appreciate your comments and we will have questions of you also.

Now we would like to hear from the Honorable, a former Congressman and now Chairman, Steve Largent.

STATEMENT OF HON. STEVE LARGENT, PRESIDENT/CHIEF EXECUTIVE OFFICER, CELLULAR TELECOMMUNICATIONS AND INTERNET ASSOCIATION (CTIA)

Mr. LARGENT. Well, thank you, Mr. Chairman and Ranking Member and other Members of the Committee, for giving me a chance to testify here this afternoon on the theft and illegal sale

---

[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 CFR § § 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/2006/012006h.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/HiTech/view.php?StoryID=20060124-6403r; http://www.wired.com/news/technology/1,70027-0.html; http://news.zdnet.com/2100-1035__22-6031204.html.*

of phone records by data brokers. With your consent, I would like to have my full written statement made a part of the record.

Senator ALLEN. It will be.

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 very seriously. The theft of customer call records is unacceptable and CTIA and the wireless carriers believe that the current practice of pretexting is illegal.

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, and 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 down these data thieves.

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, 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, it 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 would note that no two carriers can or should employ the exact same security procedures and I would caution the 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. Moreover, 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 their procedures would provide a road map to criminals to avoid fraud detection measures. The industry fears that public disclosure potentially could lead to serious harm to consumers and carriers alike.

One security practice 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 to require personal identification numbers and passwords when obtaining call

record information and many carriers have instituted a ban on e-mail and faxing 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 inspection flaw. Wireless carriers collectively received hundreds of millions, if not billions, of customer inquiries in 2005 alone. Inside our member companies, customer service reps are striving to address the requests of customers as best they can with the very best interests of the customer at heart.

Bearing this statistic in mind, it would prove counterproductive 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 backward from the convenient and responsive customer service wireless carriers strive to achieve.

Clearly, the privacy of a small percentage of our customers and 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.

There is one component to this problem that really has not been discussed, but I believe plays a very large role in the sale of call records, and that is the use of credit cards to purchase these records. I think we all agree that pretexting should be made illegal, and if we make the underlying act of making the sale of records illegal, does it not make sense then to prohibit the use of credit cards to buy the records? I know my suggestion goes beyond the jurisdiction of this Committee, but I truly believe that if Congress dries up the funding source for these sites they will disappear.

The wireless industry wholeheartedly supports making it explicitly clear that the marketing, possession, and sale of call records is against the law. If we have learned anything from this experience, it is that combatting pretexting is a war where the unscrupulous continuously seek out vulnerabilities and the 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, thank you for this opportunity and I welcome any questions you may have, Mr. Chairman.

[The prepared statement of Mr. Largent follows:]

PREPARED STATEMENT OF HON. STEVE LARGENT, PRESIDENT/CHIEF EXECUTIVE OFFICER, CELLULAR TELECOMMUNICATIONS AND INTERNET ASSOCIATION (CTIA)

Chairman Allen, Ranking Member Pryor and Members of the Subcommittee, 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* 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 database 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 voice mail, 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 e-mail account identifier to another's ac-

count, 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 counterproductive 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.

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

Senator ALLEN. Thank you, Mr. Largent, for your comments.

Now we would like to hear from Mr. Rotenberg.

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

Mr. ROTENBERG. Thank you, Mr. Chairman and Members of the Committee, for the opportunity to be here today. I would like to ask that my full statement be entered into the record.

Senator ALLEN. It is so ordered.

Mr. ROTENBERG. Thank you.

I want to thank the Committee for holding this important hearing today, the sponsors of the legislation to safeguard the privacy of our cell phone records, and also the chairman of the FCC, who I think has taken important steps in the last few months to address this problem.

Last summer my organization, the Electronic Privacy Information Center, EPIC, wrote to the Federal Trade Commission and we expressed our concern about a new problem that many people were not aware of. That was the fact that their cell phone records, those monthly billing statements that are received by more than 190 million Americans, were available for sale on the Internet. We asked the Federal Trade Commission to investigate the matter. We followed up with a supplemental filing after we had identified 40 different companies that were selling our monthly billing statements.

We also filed a petition with the FCC and we expressed concern in that petition that the security standard simply seemed to be inadequate. Yes, we understood there were people engaging in fraud

or pretexting to obtain personal information, but the companies also were not doing enough to safeguard the information. So we asked the FCC to look at its authority under section 222 to see if it could take more steps to ensure that there would be stronger security measures to protect those important call billing information records.

Well, here we are today and it seems clear that it is time for Congress to do something about this problem. Even though it may be the case that fraud is illegal, there has just not been enough action on the enforcement front. In fact, last week, after the House hearing was held on the problem, the companies engaged in this practice had such an increase in activity that a couple of the websites actually had to go down because they could not take all the increased business resulting from the publicity surrounding their practices.

So I am going to make a few suggestions about the type of steps that Congress could take at this point and at the same time acknowledge that many of the proposals that EPIC and other privacy and consumer groups will put forward are similar to those that have been suggested by the chairman of the FCC.

First, it is clear that pretexting should be banned. If there is any question about this, it has to be answered that it is unfair, deceptive, unethical, illegal, and wrong. The ban should be broad, it should be emphatic, and the report should be no ambiguity about that practice.

The second key point is that the sale of these monthly billing statements should be made illegal. There is just no scenario under which it makes sense for a company to take the records of who we have called each month and make that data available for sale. If those records are needed, for example by a law enforcement agent in the course of a criminal investigation, then there is subpoena or warrant authority. If those records are needed in civil litigation, subpoena can also be used. If an individual wants to disclose billing information, for whatever purpose, it can be done by consent.

But there is no scenario, I believe, under which it makes sense to allow a market for the sale of personal phone records.

The third key recommendation is that stronger security standards are clearly needed in this industry. We were, frankly, disappointed by the decision of the wireless industry to oppose our recommendation to the FCC for stronger security standards.

Mr. Largent, I have a very simple recommendation for the companies in your industry: If they cannot protect the information, they should not collect the information. It is placing consumers at risk when their personal information can be obtained online over the Internet.

Mr. Chairman, this goes to the final recommendation. This Committee of course over the years has had to consider many new communications services and oftentimes we have held these hearings about privacy-related issues. I think one of the lessons that we are learning is that when personal information is collected in the context of a communication service, it creates a privacy risk.

We know that historically it was not always the case that this type of detailed call information was made available. Local call service traditionally in the United States was actually treated as

a utility. It was only the long distance calls that included the detailed billing information. We know that there are new telephone services on the horizon, such as VoIP services, that take advantage of the Internet.

So I would just like to suggest to you, sir, and other Members of the Committee that going ahead, if it is possible to develop communications services that do not require the collection of so much detailed personal information, at least the privacy problem will not be as serious as it is today for the American consumer.

Thank you so much for the opportunity to testify.

[The prepared statement of Mr. Rotenberg follows:]

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

Introduction

Chairman Allen, Ranking Member Pryor, 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, D.C. 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. We especially commend the sponsors of the Telephone Consumer Protection Act, S. 2178, and the Phone Record Protection Act, S. 2177, which would ban the sale of personal telephone records. These measures will help establish important safeguards for American consumers and keep call record details off the Internet, but more work remains to be done: Records other than telecommunications records must be protected from abuse for profit.

In this statement today, I will summarize EPIC's efforts to bring public attention to the problems of pretexting and communications record sales; suggest several approaches to the problem, including a ban on pretexting and the restriction of the sale of telephone records; and make specific recommendations concerning current and future legislation.

EPIC's Efforts to Address Pretexting and Phone Record Sales

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.

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 communication records online, EPIC also petitioned the Federal Communications Commission, urging the agency to require enhanced security precautions for phone companies' customer records.[1] Although telephone carriers unanimously opposed enhanced security requirements, proposing that lawsuits against pretexters would solve the problem, Chairman Martin of the FCC last week announced that he and his fellow Commissioners will be considering EPIC's petition and acting upon it within the next few days. The FCC has recognized that 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.

Phone Records Are the Tip of the Problem

While the sale of cell phone records has gained significant media attention, and telecommunications records are the focus of the two bills currently before the Senate, many other types of private records are being bought and sold in the public

[1] 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.*

market. 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 offered for sale as well, and we commend the authors of S. 2178, who have included this and other emerging technologies in their legislative efforts.

However, the problem of record sales is not limited to the many methods of voice communication that we can use. Sites commonly advertise the ability to obtain the home addresses of those using P.O. Boxes. 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."[2] The same page 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, or outside of existing legal process.

We therefore urge the Committee to follow up on Congress' excellent first steps by expanding pretexting bans, as well as restrictions on record sales, to cover other forms of communication, such as Internet services and other information services, as well as postal information.

In Addition to Pretexting, Sales of Communications Records Should be Banned

Just as initial attention on this issue needs to expand beyond cell phone records, discussion of solutions needs to look beyond merely banning one method of obtaining and abusing personal information. EPIC fully supports a ban on pretexting, as such action would make unmistakably clear the fact that such practices are unfair, deceptive, illegal, and wrong. However, *any* method used to obtain and sell a person's private records should be prohibited, whether that method involves pretexting, computer hacking, bribery, or other methods. In order to curb these invasions of privacy, consumers and law enforcement need to be able to pursue those who would offer private consumer information for sale, regardless of the methods used to steal it. We support the provisions in S. 2177 and S. 2178 that would ban the sale of consumers' telephone information.

Banning the commercial sale of private consumer information is a necessary complement to banning pretexting, as it would "dry up the market" for illegally obtained telephone records. Such a prohibition would also allow consumers and consumer protection agencies to go after those who advertise privacy-invasive services without having to prove the specific techniques that the data brokers have used.

EPIC has asked both the Federal Trade Commission and the Federal Communications Commission to take action on this issue. The FTC proposes a ban on pretexting; the FCC proposed a ban on commercial sale of records. EPIC believes that these efforts are necessary complements to the effort to protect consumers' communication records.

No Law Enforcement Exception

Both of the bills introduced in the Senate have included exceptions for law enforcement. We recognize the need for law enforcement to gain access to communications records, and that is why there are existing, routine procedures under the law for such access, such as warrants and subpoena powers. We note that Senator Schumer's bill notes that any law enforcement acquisition of records must be made "in accordance with applicable laws," and we agree that such a caveat is necessary. EPIC would go further, however, in urging that, since such procedures for law enforcement access exist, there is no need for law enforcement to engage in the fraud that these bills are trying to prevent.

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

The acquisition and sale of these records, however, is only a part 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 informa-

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

tion 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.

If legislation that is to fully address the problem of private information sales, Congress must look not only at the practices and tactics used by bad actors, but also at the loopholes and vulnerabilities they exploit. Laws that criminalize deceptive, unfair, and privacy-invasive sales must be complemented by laws and regulations that strengthen communications privacy and security.

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.

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 utility, 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 concept of data limitation—that data should only be collected and stored when necessary—can be applied not only in protecting call records, but other sensitive personal information. Senators Specter and Boxer's proposal, S. 1350, the Wireless 411 Privacy Act, to provide privacy for consumers' mobile phone numbers is a good example of this important privacy safeguard. If the number need not published in directories or in billing records, then it should not be provided, and opportunities for abuse are reduced by just that much.

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.[3] We support the provisions in Senator Durbin's bill that extend anti-pretexting provisions to next-generation wireless communications, as well as Senator Schumer's inclusion of Internet telephony and other communications services.

We hope that the Committee will act on the proposals from Senator Schumer and Senator Durbin to protect the privacy of customers' phone records. There is no good reason that our monthly call billing records should be available for sale on the Internet.

Senator ALLEN. Thank you, Mr. Rotenberg. We appreciate your comments and your testimony and your insight.

Now we would like to hear from Mr. Robert Douglas.

Mr. Douglas.

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

Mr. DOUGLAS. Thank you, Chairman Allen, Ranking Member Pryor, Senator Smith, and Members of the Committee. It is a pleasure to be here today. As you mentioned before, I was a private investigator in Washington, D.C., for the better part of 20 years. For the last 9 years, I worked as an information security consultant, specifically on the issue of theft of consumer records, and I

[3] Letter of EPIC to FCC Chairman Powell, Dec. 15, 2003, available at *http://www.epic.org/privacy/voip/fceltr12.15.03.html*.

served as a consultant to the FTC in Operation Detect Pretext, which has been mentioned, to the Florida statewide grand jury on identity theft, and specifically in a murder case in New Hampshire where a young woman named Amy Boyer was murdered when this type of information was stolen, and I will address that in just a moment.

I have submitted very extensive written testimony, but I would like to use pictures, if I could, instead of words in my 5 minutes to demonstrate what is happening, what is out there, and maybe bring a face to what we are discussing today, Mr. Chairman.

[Screen.]

The screen up right now is *CellularTrace.com.* This is one of the companies that was named in the EPIC complaint. I worked with EPIC's Chris Hoofnagle in putting together the 40 companies that were named in that complaint last July. And this company is continuing to sell specific cell phone records and, as Mr. Rotenberg noted, this is one that has a notice up about how inundated they are being with business. They are saying right now: "Notice. As a result of the recent newscast on cellular research, we have been completely inundated with orders. We are getting caught up as quickly as possible, but those placing the orders should expect delays." This may be one of the companies—I believe, Mr. Smith, you referenced this issue earlier—that is operating offshore, but we are taking a look at that right now.

I also want to address some of the tangential issues which address how they are getting some of this information.

[Screen.]

This is a website called *HackersHomePage.com,* where they are specifically selling a voice-changing device, telephone voice changer. I have noticed in one of the suits brought by Verizon they have publicly acknowledged that one of the methods being used to defeat their call center operators customer authentication procedures was to impersonate a nonexistent division of Verizon, claiming to be—I do not even really need the microphone, evidently—claiming to be a division that helps disabled customers who have problems using their voice. So when the call center operator says to the pretexter, well, I still need to speak to the customer, they just use this voice changer to change their voice and continue to be one and the same thief.

[Screen.]

This is a site called SpoofTel, Spoof Telephone, and these types of websites and actual devices that are for sale all over the Internet are used by private investigators and information brokers as part of pretext, allow you to make any caller ID system look like it is coming from a different number. So Kevin Mitnick, who is known in social engineering circles, hacking circles, once demonstrated how he could make a call look like it is coming from the White House.

More specifically for what we are talking about today, you could make the call look like it is coming from your telephone carrier, thereby duping the customer themself into turning over important information to then beat the customer authentication protocols that the phone companies have.

What I would like to close my testimony with is talking about where we were back in 1998. I testified at that time and my testimony with others resulted in the anti-pretext legislation contained in Gramm-Leach-Bliley, and I find myself having a little deja vu. I am here again on a similar issue, different type of record.

At that time, as there has been some mention about danger to police officers, there was a company, Touchtone, as mentioned by the FTC today. But in addition to stealing financial record information, they stole thousands and thousands of phone records of Americans. They were involved in stealing records in the Clinton–Lewinsky investigation, in the JonBenet Ramsey investigation, in the murder of Bill Cosby's son Enis Cosby.

But most relevant to what we are talking about today, they sold the phone records of undercover Los Angeles police officers to organized crime in an ongoing investigation—not a what-if with the FBI buying records, not a what-if with the Chicago Police Department. This has happened already. That is one we know about. I am sure it has happened many other times.

[Screen.]

This company, Docusearch, same timeframe, back in 1998–1999 when Gramm-Leach-Bliley was being signed into law, advertised and continues to advertise to this day—Mr. Chairman, when we spoke before the hearing this afternoon I told you I would talk about a company in your home State. That is Docusearch. That is Dan Cohen, who owns it, who moved from Florida after he was sued in the Boyer murder case and now operates right out of Northern Virginia.

To this day—this is today on his website—he is trumpeting that he was the featured cover story article in Forbes Magazine November 1999, as Gramm-Leach-Bliley was being signed into law, bragging about how he steals financial records and phone records, specifically phone records back at that time.

[Screen.]

Well, we should have paid attention, because this woman, Amy Boyer, who was 20 years old, had her whole life ahead of her, was murdered, and she was murdered by this man, Liam Youens, standing in the corner of his bedroom with an AK–47, shortly before he went out and gunned her down. He was telling the world on this website that I have got one captured page from here, documenting for the better part of a year how he obtained information on her. And while it was not specifically phone records, it was her employment address, obtained through pretext—part of what we are talking about today.

The sad and sick thing was they called her mother and impersonated an insurance company and said they had an insurance refund from her. So her mother today says: I was an accomplice to my own daughter's murder.

I will close with what he says at the end, which is that "It is actually obscene what you can find out about somebody on the Internet." He wrote those words right before he left on October 15, 1999, and murdered Amy. With that, I will avail myself to your questions, Mr. Chairman.

[The prepared statement of Mr. Douglas follows:]

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

Chairman Allen, Ranking Member Pryor, Members of the Committee, my name is Robert Douglas and I thank you for the opportunity to appear before this 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 seventh 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 and 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 website. 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 and 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 D.C. 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 records. 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 1990s, 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 e-mail and Internet service providers), cable and satellite television, utility (including electric, gas, water and 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 *all* 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.

IV. To Understand Why Records Are Sold, You Need To Know Who Buys Them

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 JonBenet 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 ob-

tain 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 Fed-

eral 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 websites 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 voice mail. 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 website, 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 website?

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 watchdog 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 watchdog is nothing more than a lapdog 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 Tone 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 JonBenet 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 and 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. and Mrs. Mervin Pugh.
5. Credit card tolls on the following:
   a. Mr. John Ramsey, AMX and VISA
   b. Mr. John Ramsey Jr., AMX.
6. Home location of ex-wife in Georgia, we have number, address and 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 and number of Mr. Sawyer and 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 JonBenet 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 and Deceptive Trade Practices Act, Mesis asked Winston about the use of pretext for phone records. The following Q and 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, D.C.
>
> *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 websites 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 your 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. In a subsequent case, the FTC made a criminal referral to the Department of Justice recommending prosecution of a broker selling financial information obtained through pretext. That broker received a $1,000 fine and a 2-year suspended prison sentence.

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 website, 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* website.

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, D.C.

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

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 firsthand 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.

VIII. The FTC's Attitude Towards Pretexting is Inexcusable

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 websites 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 FBI while simultaneously empowering state attorneys general 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.

Senator ALLEN. Thank you, Mr. Douglas, for your testimony. I am sure there will be follow-up questions.

Finally out of our witnesses, we would like to hear from you, Ms. Southworth.

STATEMENT OF CINDY SOUTHWORTH, DIRECTOR, TECHNOLOGY AND THE SAFETY NET PROJECT, NATIONAL NETWORK TO END DOMESTIC VIOLENCE

Ms. SOUTHWORTH. Thank you. Chairman Allen, Ranking Member Pryor, and distinguished Members of the Committee. My name is Cindy Southworth and I thank you for the opportunity to appear before this Committee. I am the Director of Technology at the National Network to End Domestic Violence, which represents 53 State domestic violence coalitions who in turn represent over 3,000 local domestic violence shelter and hotline programs across the country. I founded the Safety Net Project to educate victims and their advocates on the strategic use of technology and I have focused on the intersection of technology and domestic violence since 1998.

Our member State domestic violence coalitions from around the country, including the Arkansas Coalition and the Virginia Action Alliance, are extremely pleased that we are addressing this issue with you today because they have been expressing concerns about pretexting for many, many years.

Every day there is a staggering amount of data generated and maintained about all of us, far beyond cell phone records. Personally identifying information is now tracked as never before. The theft of such personal information can be extremely inconvenient for all of us here in this room, but may be fatal for a victim of domestic violence. As Mr. Douglas explained, Amy Boyer was one of my examples, but I think he covered it quite thoroughly.

Sadly, domestic violence is quite prevalent and many victims are stalked relentlessly for years after having escaped. The batterers that hunt them down are the most dangerous batterers and they pose the highest lethality risk. Because of this, victims often take extraordinary and desperate steps to hide their location. They use post office boxes, they change their Social Security numbers, and they hide in confidential shelter locations.

Pretexters and information brokers are not just stealing someone's data, they may be endangering someone's life. Seventy-six percent of women killed by their abusers had been stalked prior to the murder. Stalkers are often in a prime position to obtain cell phone and other records through pretexting or through information brokers who steal the data and then sell it to the abusers. Since abusers often know their victim's date of birth, their mother's maiden name and computer passwords, they can easily either pose as the victim or have someone pose as the victim for them. It is not uncommon for abusers to have a new girlfriend pose as the victim and call and get information.

In one case in rural Virginia, a woman was stalked by her ex-husband. She changed her e-mail address, she moved, she found a new job, she did everything. Several businesses that she frequented used her seven-digit cell phone number as her customer identifier. Her ex-husband simply asked someone at the video store to look up her cell number in the system, which made tracking her movements quite simple. He discovered that she had rented a video on Monday and it was due back on Wednesday. He was lying in wait for her when she showed up at the video store.

Phone records are a particularly rich source of information for the determined stalker. By illegally obtaining this information, a stalker can easily locate his victim.

In recent years there have been concerted efforts by Congress, various Federal agencies, and nearly every State to create privacy and confidentiality provisions that help shield victims of domestic violence. For example, at least 17 States now offer address confidentiality programs and 39 States provide for confidentiality of shelter records. All of these extraordinary steps that victims take to shield their location and identity and that shelters take on behalf of victims are futile if pretexting is allowed to continue.

In Hawaii, a victim on the run was found through a car rental agency. Her abuser walked into the agency, pretexted. He pretended and told the staff that his wife was diabetic and forgot her insulin—a common strategy—and he said he thought she might have rented a car. After a simple reverse look-up using her phone number, staff provided him the make, model, and license plate number of the rented car. The victim was found by the abuser later that day and badly beaten in a parking lot.

The theft of personal information is not only a violation of privacy, it is a crime. Stolen goods are addressed by various State and Federal laws and both the original thieves and those who trade in stolen goods are subject to prosecution. The theft of personal information should be handled in a similar fashion. However, because pretexting phone records is just one piece of a larger problem of stealing and selling personal information, a multi-faceted approach would protect all consumers.

Pending Federal legislation makes the stealing, selling, and fraudulent transfer of these records a criminal offense. Strengthening Federal law will help discourage data mining and protect consumers, including battered women. We encourage State and Federal entities to use all existing and emerging laws to hold individuals and organizations accountable for illegally obtaining, using, or selling phone records or other personal information.

All companies that collect and retain personal information about their customers should enhance the security and privacy options available to consumers and create levels of security that are not easily breached from within or outside of the company. Given the creative and persistent tactics of perpetrators, companies must work with consumers to identify the methods of security that will work best for general consumers as well as for consumers in higher risk situations, like victims of domestic violence.

Cell phones can be a lifeline for battered women and victims of sexual assault and stalking, but with illegitimate pretexting, a phone, and other personal records, those lifelines can forever connect the victim to her abuser without hope of escape.

Thank you for allowing us this opportunity to address the Committee on this critical and urgent issue, and I am happy to answer any questions. Thank you.

[The prepared statement of Ms. Southworth follows:]

CINDY SOUTHWORTH, DIRECTOR, TECHNOLOGY AND THE SAFETY NET PROJECT,
NATIONAL NETWORK TO END DOMESTIC VIOLENCE

Introduction

Chairman Allen, Ranking Member Pryor, and distinguished Members of the Committee, my name is Cindy Southworth 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. The Committee is taking remarkable leadership by seriously considering the issues of pretexting and the sale and acquisition of personal data by information brokers. It means so much to victims of domestic violence and stalking that you are carefully considering all aspects of these complex issues and are contemplating enhancing privacy protections for all citizens, including these vulnerable victims. Our members from around the country, including the Alaska Network on Domestic Violence and Sexual Assault, the Arkansas Coalition Against Domestic Violence, the California Partnership to End Domestic Violence, the Hawaii State Coalition Against Domestic Violence, the Louisiana Coalition Against Domestic Violence, the Montana Coalition Against Domestic and Sexual Violence, the South Carolina Coalition Against Domestic Violence and Sexual Assault, and the Virginia Sexual and Domestic Violence Action Alliance have been expressing concern about the dangers of pretexting and stealing phone records, and they are extremely pleased to see their Senators take such an active role in addressing this issue and protecting the privacy of victims.

I am the Director of Technology at the National Network to End Domestic Violence, a social change organization dedicated to creating a social, political, and economic environment in which violence against women no longer exists. Founded in 1995, the National Network to End Domestic Violence (NNEDV) represents 53 state domestic violence coalitions who in turn represent over 3,000 local domestic violence service providers across the country.

In 2002, I founded the Safety Net Project at NNEDV to educate victims of sexual and domestic violence, their advocates and the public on the strategic use of technology to increase personal safety and privacy. Safety Net is the only national initiative addressing the intersection of domestic violence and all forms of technology. Looking beyond the traditional "digital divide," our project is ardently working to increase the technology knowledge and skills of victims, advocates, law enforcement, and allied organizations in every state and each of the local shelter and hotline programs across the country. Safety Net also tracks emerging technology issues and their impact on victim safety, working with local, state and Federal agencies to amend or create policies that enhance victim safety and confidentiality.

I have been working to end violence against women for over 16 years and have focused on the intersection of technology and domestic violence since 1998. I thank you for the opportunity to submit testimony about the real dangers that victims of abuse and stalking face as a result of pretexting and selling stolen personal information.

Risks to Victims

There is a staggering amount of data generated and maintained about individuals in our society every day—far beyond cell phone records. Personally identifying information like date of birth, Social Security number, frequently visited websites, and grocery shopping preferences, are now being tracked as never before. The theft of such private information can be devastating for the average individual who may have her identity stolen and her credit destroyed. For a victim of domestic violence or stalking, however that theft of private information is not just financially or personally devastating—it can be fatal. In 1999, Amy Boyer, a young woman in New Hampshire, was tracked down and murdered by a former classmate who had been stalking her for years. Liam Youens paid Docusearch, an Information Broker, to obtain Amy's work address. Docusearch contracted with a pretexter to illegally obtain her work address by pretending to need it for insurance purposes. [1]

Domestic violence, sexual assault and stalking are the most personal of crimes, and the more personal information that the perpetrator has about his victim, the more dangerous and damaging the perpetrator can be. Sadly, domestic violence is quite prevalent, and women continue to be the vast majority of victims. The National Institute of Justice reported that 4.9 million intimate partner rapes and physical assaults are perpetrated against U.S. women annually. [2] Leaving the relation-

[1] Ramer, Holly. "Murdered woman's mother settles suit." *The Union Leader* (Manchester NH), March 11, 2004, State Edition: Pg. A1.

[2] Patricia Tjaden and Nancy Thoennes, National Institute of Justice and the Centers of Disease Control and Prevention, *Extent, Nature, and Consequences of Intimate Partner Violence*

ship does not stop the violence. In fact, the most dangerous time for a victim of domestic violence is when she takes steps to leave the relationship.[3] Many victims are stalked relentlessly for years after having escaped from their partners. These batterers who stalk their former partners, determined to hunt them down, are the most dangerous and pose the highest lethality risk.[4]

Because of this, victims often take extraordinary and desperate steps to hide their location, sometimes even changing their identities to avoid being found by their abusers. Those steps can include:

- Moving to new states;
- Using post office boxes;
- Getting unlisted phone numbers;
- Using only cell phones to avoid having utility records tied to a home phone and thus a particular address;
- Changing names through the court system;
- Changing Social Security numbers;
- Relocating to confidential shelters;
- Enrolling in state address and voter record confidentiality programs;
- Sealing location information in court filings; and
- Never using the Internet from a home computer.

Victims of domestic violence, acquaintance rape, and stalking are particularly vulnerable because perpetrators know so much about their victims that they can often predict where their victims may flee, and to whom they may turn for help. Notably, it is not just the victims of domestic violence who are at risk if her personal information and location is revealed, but also the individuals and programs that help them.

Pretexting and Information Brokers

Pretexters and information brokers are not just stealing someone's data, they may be endangering someone's life. Fifty-nine percent of female stalking victims are stalked by current or former intimate partners,[5] and 76 percent of women killed by their abusers had been stalked prior to their murder.[6] Stalkers are often in a prime position to obtain cell phone and other personal records through "pretexting" or through Information Brokers who have used this tactic and then sold the stolen data. Since abusers often know enough private information about their victims (such as date of birth, mother's maiden name, or her commonly chosen computer passwords), they can easily pose as their victims and illegally access their credit, utility, bank, phone, and other accounts as a means of getting information after their victims have fled.

In one case, a woman in rural Virginia was stalked by her ex-husband. She couldn't figure out how he kept showing up wherever she was. She had changed her e-mail address, moved, and found a new job. Eventually, a savvy advocate started asking about other "records" such as where she got the oil in her car changed, where she rented videos, etc. Several businesses she used, including the video store and the local autoshop, all used her 7-digit cell phone number as her customer identifier. Her ex-husband simply asked someone he knew to look up her name in one system, which made tracking her movements simple. Finally, he discovered that she had rented a video on Monday and that it was due back on Wednesday. He was lying in wait when she came to return the video.

Phone records are a particularly rich source of information for the determined stalker. Through pretexting, a stalker can access records that include who was called, when the call was made, how long the call took, and the location of the calls. By illegally obtaining this information, a stalker can locate his victim without his victim even knowing that she is being tracked. For example, a victim from rural Louisiana, whose cell phone records reveal to her batterer that she contacted a shelter program in South Carolina, is no longer safe going to that South Carolina shelter, though she may never realize that until it is too late.

(2000); Dr. Callie Marie Rennison, Department of Justice, Bureau of Justice Statistics, *Intimate Partner Violence*, 1993–2001 (February 2003).

[3] Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey* 1 (January 2000).

[4] Barbara J. Hart, *Assessing Whether Batterers Will Kill*. (This document may be found online at: *http://www.mincava.umn.edu/hart/lethali.htm*), Jacqueline Campbell, *Prediction of Homicide of and by Battered Women, reprinted in Assessing Dangerousness: Violence by Sexual Offender, Batterers, and Sexual Abusers* 96 (J. Campbell, ed., 1995).

[5] Tjaden &Thoennes. (1998) "Stalking in America," NIJ.

[6] McFarlane et al. (1999). "Stalking and Intimate Partner Femicide," *Homicide Studies*.

In January 2003, Peggy Klinke was brutally killed by a former boyfriend, Patrick Kennedy, after he hunted her down with the help of a private investigator. Peggy had worked closely with the Albuquerque Police Department, obtained a restraining order, and after Patrick burned down her home in New Mexico, she fled to California to try to remain safe until the pending criminal court hearing. Patrick hired a private investigator, located her, flew to San Jose, rented a car, drove to her neighborhood, posed as a private investigator to find her exact apartment location, and chased her around the apartment complex before shooting her and eventually shooting himself. [7]

Shelter programs and their employees and volunteers are also vulnerable to being located through pretexting. Shelters try to protect their location in the same way that individual victims of domestic violence do, by using post office boxes and unlisted phone numbers and addresses for both the shelter and for staff and volunteers. However, many shelters' emergency response teams use cell phones and pagers for on-call staff, which puts those individual staff and volunteers at risk from abusers who are trying to gain access to the shelter to find their partners.

Whether the phone records obtained are those of the domestic violence or sexual assault program or are those of an individual who contacted the program, the harm can be devastating.

Circumventing Laws That Protect Victim Privacy

In recent years, there have been concerted efforts by Congress, various Federal agencies, and nearly every state to create privacy and confidentiality protections that help shield victims of domestic violence from being found by their perpetrators and from having to reveal private information about their victimizations. For example, at least 17 states now offer Address Confidentiality Programs, which provide for a secure system for receiving mail, often through the Attorney General or Secretary of State's office, without having to reveal a victim's address. [8] A number of other states, including Hawaii, Virginia, Maryland, and Texas, are presently considering enacting similar address confidentiality programs. [9] Twenty-two states, including Virginia, California, Maine, and Arizona, provide that voter registration data, including address and other identifying data, can be kept confidential by victims of domestic violence. The great majority of states (39) provide for confidentiality of domestic violence or sexual assault program records and communication, including the time, location, and manner by which a victim may have consulted a program for help in escaping the abuse—some of the very information that is at risk through pretexting of records.

The recent reauthorization of the Violence Against Women Act, enacted by Congress and signed by President Bush just over a month ago, includes several confidentiality provisions that protect identifying data disclosed by a victim of domestic violence to a domestic violence program from being shared with databases. [10] Some states, including Nevada and New York, have provisions that allow an individual to change her name without publishing that name change in the newspaper, as a way of protecting the identity and location of victims of stalking and domestic violence. Nearly every state allows victims to ask to seal their address from the public (and the perpetrators) in protection order actions and in certain types of criminal cases.

The Social Security Administration allows domestic violence victims to change their Social Security numbers to help them seek protection. [11] But even taking the drastic step of obtaining a new social security number does not eliminate the problem caused by pretexting. Determined abusers continue to track their victims

---

[7] Holland, John. "Grim act of a man unable to let go." *The Modesto Bee* (Modesto California), January 25, 2003, Available online *http://www.modbee.com/local/story/5973772p-6932417c.html*.

[8] California, Cal. Gov Code § 6205, *et seq*. (2005); Connecticut, Conn. Stat. § 54–240, *et seq*. (2005); Florida, Fla. Stat. § 741.401, *et seq*. (2005); Illinois, 750 ILCS 61/1, *et seq*. (2005); Indiana, Burns Ind. Code Ann. § 5–26.5–1–1 (2005); Maine, 5 Maine Rev. Stat. 90–B(2005); Massachusetts, MGLA ch. 9A § 1 (2005); Nebraska, Neb. Rev. Stat. § 42–1206, Nevada, Nev. Rev. Stat. Ann. § 217.462 , *et seq*. (2005); New Hampshire, N.H. Rev. Stat. Ann.§ 7:41 *et seq*. (2005); New Jersey, N.J. Stat. § 47:4–2, *et. seq*. (2005); North Carolina, N.C. Gen. Stat. 15C–1 (2005); Oklahoma, 22 Oklahoma Stat. § 60.14 (2005); Pennsylvania, 23 Penn. C. S. § 6702 (2005);Rhode Island, R.I. Gen. Laws @ 17–28–1, *et seq*. (2006); Vermont, 15 V.S.A. Ch. 21, § 1101 to 1115 (2005); Washington, Rev. Code Wash. (ARCW) § 40.24.010, *et seq*. (2005).

[9] For example, Alaska, 2005 AK HB 118; Hawaii, 2005 HI HB 1492; Maryland, 2006 MD SB 25; New York, 2005 NY AB 5310; Texas, 2005 TX SB 160; Virginia, 2004 VA HB 2876.

[10] The Violence Against Women and Department of Justice Reauthorization Act of 2005, Public Law 109–162, Sections 3(b)(2) and 605.

[11] *See* SSA Publication 05–10093 (December 2005).

through relatives' phone records and other means, often obtaining their information by additional pretexting.

All of these extraordinary, difficult and sometimes costly steps that victims of domestic violence take to shield their location and identity, and that domestic violence programs take on behalf of victims, are completely futile if data mining through pretexting is allowed to continue.

Phone records and pretexting are the focus of this hearing. Those issues are part of a larger problem that victims of abuse face—the prevalence of information regarding their activities and location and the ease with which that information can be purchased by their perpetrators. A quick search of the Internet reveals hundreds of businesses that, for a relatively nominal cost, will provide information including the address of record associated with a post office box; AOL screen names and e-mail addresses; unlisted phone numbers; physical addresses and Social Security numbers; and even photos and floor plans of people's homes. Any one of these invasions of a victim's privacy could put her in grave danger.

A woman in Hawaii was getting ready to flee to a shelter and was nervous about her abuser recognizing her car in front of the shelter building. She parked her own car on a side street and rented a car to use. Since there are only a few rental places on the island it was not long before the abuser walked into the office, told the staff his "wife was diabetic and forgot her insulin" but thought she might have rented a car while hers was getting fixed. She had used her sister's identity and paid cash, but had given her own phone number because her sister did not have a phone and the rental agency had insisted on entering a number into the system. After a reverse lookup using the phone number, staff provided him with the make, model and license plate number of the rented car. The victim was found by the abuser later that day and badly beaten in a parking lot behind a store.

A Multi-Faceted Approach is Needed

The theft of personal information is not only a violation of privacy, it is a crime that particularly puts victims of domestic violence, stalking and sexual assault at risk. Stolen goods are addressed by various state and Federal laws, and both the original thieves and those who trade in stolen goods are subject to prosecution and punishment. The theft of personal information should be handled in a similar fashion. However, because pretexting phone records is just one piece of the larger problem of pretexting, stealing, mining, and selling personal information, a multi-faceted approach would offer the best protection to all consumers.

Pending Federal legislation, including the Consumer Telephone Records Protection Act of 2006 and the Phone Records Protection Act of 2006, make the stealing, selling, and fraudulent transfer of telephone records a criminal offense. A number of states also have or are considering specific laws to criminalize and punish pretexting and the use and sale of such stolen information, while other states like Florida, Missouri, and Illinois are addressing the issue through the court system. Strengthening Federal law enforcement options through the pending legislation, and subsequent prosecution, will hold offenders, information brokers, pretexters, and those who use illegally obtained information accountable, and will help discourage data mining and protect consumers, including battered women. We encourage State and Federal entities to use all existing and emerging laws to hold individuals and organizations accountable for illegitimately obtaining, using, or selling phone records or other personal information.

All companies that collect and retain personal information about their customers should enhance the security and privacy options available to consumers, and create levels of security that are not easily breached from within or from outside of the company. Given the creative and persistent tactics of perpetrators, companies must work with consumers to identify the methods of security that will work best for general consumers, as well as methods for consumers in higher-risk situations, including victims of domestic violence and law enforcement officers.

Conclusion

Cell phones can be a lifeline for battered women and victims of sexual assault and stalking. But with illegitimate pretexting of phone and other personal records, those lifelines can forever connect the victim to her abuser, without hope of escape. As the examples I have described demonstrate, we cannot underestimate the potential harm to victims of allowing pretexting to continue. I applaud Congress and the state Attorneys General for addressing the widespread problem of pretexting and selling of stolen personal data.

Thank you for allowing me this opportunity to address the Committee on this critical and urgent issue. I am happy to answer any questions.

Senator ALLEN. Thank you, Ms. Southworth, for your testimony, and all our witnesses. We will go through questions. There will be 5-minute rounds.

Let me begin asking you, Ms. Parnes. Clearly there is kind of a loophole, and most of this is under the FCC as far as Federal agencies. If Congress, in this legislation that we are crafting, amends the Communications Act, would the FCC have jurisdiction to enforce any pretexting provisions?

Ms. PARNES. Senator, the Commission would not have the authority to enforce an anti-pretexting provision that amends the Communications Act. There have been instances, however, where Congress has given both the FCC and the FTC jurisdiction in a particular area. 900 numbers is one area where that occurred.

Senator ALLEN. How about the Telephone Disclosure and Dispute Resolution Act?

Ms. PARNES. Yes, yes, that as well. There what Congress did is it amended the Communications Act and also included separate provisions that gave the FTC authority.

Senator ALLEN. That was on advertising and billing and collection of 900 number services.

Ms. PARNES. Yes, sir.

Senator ALLEN. Would the FCC—would anybody object if somehow we could craft language—and we need help from the FTC and I know, Mrs. Parnes, you are here representing yourself, not the FTC; we heard that caveat. Would anyone object—clearly, FCC is involved and should be involved. Would there be any objection to dual jurisdiction out of any of our witnesses?

[No response.]

Senator ALLEN. Seeing none, let me ask you this. Anybody, any of the witnesses: It seems to me that this should be a national standard. Everyone says this all ought to be made illegal, the acquisition, the pretexting, the fraud, and the sale. Everyone agrees that that should be made illegal, and the question is whether there should be a national standard for this so you don't have a different law, in Florida it might be different than Virginia. It seems to me that it does not matter what State you are in of the Union; we ought to have a uniformity of a national standard, which should be stronger than any particular State law. But regardless, is there any objection to a national standard?

Mr. ROTENBERG. Well, Senator, if I may say, if the national standard is stronger than any State law, then certainly there would be agreement. I think the concern always is that sometimes we may end up with a national standard that preempts a stronger State protection, and then of course the residents in those States find themselves with less protection than they might otherwise receive. If there is a strong national standard, then I think that would be supported.

Mr. DOUGLAS. Mr. Chairman, if I might, one other thing in case we do not get to it, and specifically because the FTC raised the issue of the exception in Gramm-Leach-Bliley which allowed private investigators, in theory allows private investigators to use pretext in a court-ordered situation for child support, that is an exception that has allowed those types of offerings of financial records to continue to appear on websites by the dozens. Yet when you call

them they do not use the exception; they will sell to anyone if they think you are not law enforcement.

I would challenge, not necessarily the FTC, but the investigative industry to demonstrate once that a judge has authorized the use of deception against a United States bank. It is an exception that swallows the whole. If you had the criteria necessary you could get a subpoena, which is the case in many of these. So I would ask that there not be that exception this go-around.

Thank you.

Senator ALLEN. Thank you. I am sure in the event we do this, Ms. Parnes, you have no problem?

Ms. PARNES. And we would certainly—the staff of the Commission would certainly be happy to work with the Committee in developing any legislation.

Senator ALLEN. All right. Other things that were said: make this specific—this is from Ms. Monteith and others, that we need to overturn a court decision, which we can get into; and greater enforcement tools, eliminate the citation issue, which is what Chairman Stevens talked about; raise fines, forfeiture, and so forth.

I am one who just wants to bring everything we can against these pretexters, whether it is through FCC enforcement or FTC enforcement—and in fact, if we have a national standard, that helps with enforcement. But also, like what we did in other legislation, State attorneys general could enforce the law against pretexters. They usually have offices themselves. Would there be any objection from any of you, any of our witnesses, to also allow States attorneys general to enforce this national standard within their states?

Ms. PARNES. Senator, at the FTC we have had a tremendous amount of success working with the State AGs under just that type of statutory system.

Senator ALLEN. Well, I am glad to hear that and that is an example and something I have advocated in the past. We again want to bring everyone and all resources because, listening to Mr. Douglas's testimony, which was very disturbing, as to what is going on right now, and who knows what the impact of this hearing will be. I saw when Mr. Rotenberg was talking about it earlier, I saw you raise your eyebrows in agreement. So I think our legislation should empower attorneys general across the country as well.

Senator PRYOR.

Senator PRYOR. Thank you, Mr. Chairman.

The first order of business is I have Senator Boxer's questions that she wanted submitted for the record. So I will make sure those get in the record, without objection.

Senator ALLEN. Her questions?

Senator PRYOR. Yes.

Senator ALLEN. Well, to the extent they are posed to any of our witnesses, if you would be willing to, you may get some written inquiries posed to you and if you can respond we would surely appreciate it.

Senator PRYOR. Thank you, Mr. Chairman. Thank you.

I want to direct my first few questions to the FCC. I want just a little clarification on a couple of items. First, is this limited to cell phones? Is this problem limited to cell phones?

Ms. MONTEITH. No. We are looking at wireline providers and their records as well, although most of the information that we have obtained and what we have heard obviously in the media has focused on cell phones. But no, not limited.

Senator PRYOR. I understand that. But you are looking at residential and business wireline?

Ms. MONTEITH. Yes, we are.

Senator PRYOR. Also, in your view is pretexting already illegal?

Ms. MONTEITH. Under the Communications Act—the Communications Act does not deal with the issue of pretexting by data brokers, what we have heard. The Communications Act section 222——

Senator PRYOR. Right.

Ms. MONTEITH.—deals with the safeguards and the kinds of procedures that the carriers have to put in place.

Senator PRYOR. Right. But in your view it is not illegal, at least from your jurisdiction's standpoint?

Ms. MONTEITH. Not from our jurisdictional standpoint, no.

Senator PRYOR. OK. Let me now ask—I know that the FCC recently made some requests of some of the wireless carriers and that was, when, within the last few weeks; is that right?

Ms. MONTEITH. Yes, in January.

Senator PRYOR. Had you made any before that time under the 1996 Act?

Ms. MONTEITH. We have at various points looked at CPNI issues and had a number of investigations. We have not taken formal enforcement action.

Senator PRYOR. So you had not made those requests of the wireless companies before?

Ms. MONTEITH. No, I do not believe so. I would like to verify that, though, with my staff.

Senator PRYOR. Do you feel like the FCC has been as aggressive and proactive as it should have been on this issue before recently?

Ms. MONTEITH. Yes, I think we have. Certainly when any information has come to our attention we have acted aggressively to determine what the issues are and go after those that are violating the Communications Act.

Senator PRYOR. You say that even though you had not sent these letters of inquiry to the wireless companies before January 2006?

Ms. MONTEITH. That is correct. We did not have any evidence before us that would suggest this was an issue.

Senator PRYOR. Let me, if I may, turn to the FTC now. That is, in your opening statement I picked up on three facts. First is that the FTC recognized that this has been a problem for some time now. Second is that the FTC believes it has legal authority to go after pretexters under section 5 of the FTC Act. Third is enforcement actions have not been brought against any company or individual involved in records pretexting. Why is that?

Ms. PARNES. Senator, we have not brought a public action against a company engaged in pretexting phone records. We do have a number of active investigations. As I mentioned in my statement, we have also done a surf and we have sent warning letters.

But pretexting, whether for financial records or for telephone records, is just one part of the FTC's privacy program and we have a very aggressive program in this area. We have brought more than 80 spam cases, 11 data security cases, 6 spyware cases, 18 do not call cases, 12 in the area of financial pretexting. I am certain as a former attorney general yourself you understand the hard choices we have to make in selecting the areas that we proceed in.

Senator PRYOR. So in other words, you have done in those areas, which are great—I am all for those areas. But in terms of cell phone or telephone pretexting, you have not been very active on that until recently; is that fair to say?

Ms. PARNES. That is fair to say.

Senator PRYOR. And apparently you sent out warning letters yesterday to 20 companies offering to obtain—for the companies who obtain and sell telephone records, is that right?

Ms. PARNES. Well, yes, we did a look at the 40 companies that EPIC identified, as I mentioned, and we saw that more than half of those companies are no longer making claims. We also looked at—we did a similar search to the search that EPIC did, using similar search criteria, to identify additional sites and we sent warning letters to those companies as well.

Senator PRYOR. Mr. Chairman, I have one last question for both of these two witnesses. That is, are you satisfied with the cooperation you are receiving from the other agency?

Ms. MONTEITH. Yes.

Ms. PARNES. Yes, we are. Yes, very much so.

Senator PRYOR. Thank you, Mr. Chairman.

Senator ALLEN. It sounds like EPIC is doing a very good job in helping you figure out which places to be looking. Congratulations, Mr. Rotenberg.

Mr. ROTENBERG. Thank you, Senator.

Senator ALLEN. For good citizen action.

Which of the two Senators here to my right were here—Senator Dorgan.

STATEMENT OF HON. BYRON L. DORGAN,
U.S. SENATOR FROM NORTH DAKOTA

Senator DORGAN. Mr. Chairman, thank you. I regret I was not here to hear the testimony. As you know, we have the attention span of gnats around here.

Senator ALLEN. And many things going on.

Senator DORGAN. We flit from hearing to hearing.

But at any rate, I have had a chance to review some of the testimony. I just wanted to ask a question. Chairman Martin of the FCC laid out several legislative steps he thought Congress should take. One, Congress could specifically make illegal the commercial availability of consumers' phone records. That would mean that if any entity is found to be selling this information for a fee, regardless of how it is obtained, it would face liability.

Let me ask whoever on the panel wishes to respond to that. Do you agree with Chairman Martin's recommendation? He is saying that is one of the things Congress could do. We have a couple of pieces of legislation, I think, that have already been introduced here in the Senate on that subject.

Mr. ROTENBERG. Senator, we think it is a very good proposal, and we were at the hearing last week when the chairman of the FCC made it. As I remarked earlier during my testimony, it is just very difficult to understand the circumstances under which cell phone records should be sold. They can be obtained by law enforcement under warrant or subpoena or civil litigation under subpoena. We just cannot understand why we would allow a market for that type of personal information.

Senator DORGAN. Mr. Largent, do you agree?

Mr. LARGENT. Senator, I would agree with that. We are for the swift enforcement of an act like that and stand ready to assist you any way we can.

Senator DORGAN. Let me ask. We have apparently data brokers online—there was a story I believe in the *Chicago Sun-Times* that I saw earlier in January. The FBI paid a fee of $160 and obtained the cell phone records of an FBI special agent within 3 hours. Apparently they were just testing the system. The Chicago Police Department was warning its officers their cell phone numbers were available to anyone for a small fee.

There apparently are data brokers online and you go online, access those data brokers, and then engage in a transaction to purchase cell phone call records. They also claim that they can provide calling records for landline and voice over Internet protocol, or VoIP calls, as well as nonpublished phone numbers.

Let me ask the two Federal agencies: Have you done a lot of work to go online, figure out who these companies are, trace back to these companies, and begin investigations? And if so, when did that begin?

Ms. MONTEITH. We first began looking into this issue late last summer, and the first phase of our enforcement actions was internal investigations to try and determine who these online data brokers were. We did, using the companies that EPIC had pointed out in its petition and our own research, identify a number of online data brokers. We then made undercover purchases ourselves to try and obtain the kind of evidence that we need in an enforcement action to really take action against these types of brokers.

Those activities were in the timeframe of October, November, December, and then on up to the present.

Senator DORGAN. Ms. Parnes, if Chairman Allen wanted to spend whatever was necessary this afternoon to find out all of your telephone calls for the last 3 or 4 months, do you think he could do that, just based on what you know?

Ms. PARNES. I imagine he could today, yes.

Senator ALLEN. I have no desire and will not do that.

Senator DORGAN. Let me quickly stipulate, I am not suggesting that.

Ms. PARNES. Thank you.

Senator DORGAN. But the fact that you believe that he probably can do that and the fact that most of us believe that is probably possible is pretty frightening, is it not, because anybody for a certain amount of money might be able to go find a broker someplace that can serve up a substantial amount of not just telephone records, a substantial amount of other problems out there with other financial and medical information. But now we are talking

about telephone records. It is pretty frightening when you think about it. Anybody can spend some money and go find out your complete telephone records, your history over the last couple of months.

I tend to think Chairman Martin has given us a recommendation that we ought to pursue immediately. There ought not be great debate on the question of whether you ought to be involved in commercial sale of these kinds of private records. Congress ought to move quickly and immediately to deal with that issue.

Chairman Martin mentioned a couple of other things. He recommends that enforcement tools be strengthened. He argues that the need to issue a citation to non-licensees before taking any other type of action can hinder the investigation. I agree with that as well. Apparently in many cases, because the Internet is a venue in which you do not see anyone—what you see are bytes or bits—by the time they get around to dealing with citations, that enterprise is long gone. So I think we probably should take Chairman Martin's recommendations pretty seriously here and move as quickly as we can. I know a number of my colleagues, including myself, are interested in doing that.

So again, I regret I did not hear all of your testimony, but I will have a chance to read it and I appreciate very much your willingness to testify and I appreciate the Chairman for holding this hearing. I think it is timely and really important.

Senator ALLEN. Thank you, Senator Dorgan. For your information, the sole issue on the citations and warning and so forth as we are crafting this legislation—this is a concern of mine and Senator Pryor's, including also Chairman Stevens, and that is one clear unanimous approach. You do not give warning to someone when you are going to get after them or shut them down, right.

Senator Nelson.

STATEMENT OF HON. BILL NELSON,
U.S. SENATOR FROM FLORIDA

Senator NELSON. When eight of us on this Committee filed a bill having to do with these telephone records about 2 weeks ago, the press wanted to test it. Senator Dorgan, it is exactly as you said. They paid—went online, found 40 sites, paid 100 bucks by credit card, and got the cell phone records of a number that someone had given to them to see if they could test the system, and they certainly had.

My goodness. What happens if this is—as the sheriff of one of my biggest counties in Florida says, what if this is the cell phone record of one of his undercover detectives, and all of a sudden all of his confidential informants are suddenly on that record?

We have got a problem here, and it is not just this. I think Senator Burns spoke about this earlier today, it is this whole question of privacy on the Internet, the whole question of shredding our credit statements is not good enough any more. Now all of this information is collected electronically and these data information brokers house all of this information virtually on every American and are buying and selling this information. If we do not do something, none of us are going to have any privacy any more.

Here again is another dramatic example. I think in your questioning you have already brought out why it is necessary that we

move on this legislation fast, because the regulatory agencies have been slow on the uptake, as we have heard testimony here today. For example, the FTC knew about these problems in 1999 in the Touch Tone case, but here we are talking about cracking down.

Let me ask all of the panel here: Do you think that in order to stop this dead in the tracks we need to make it a crime?

Mr. ROTENBERG. Yes, Senator, I think it has to be made absolutely clear that pretexting by any means in this country is clearly illegal and subject to criminal penalty, absolutely.

Senator NELSON. Congressman Largent?

Mr. LARGENT. Absolutely.

Senator NELSON. Congressman, you have testified that the vast majority of cell phone records are fraudulently obtained through pretexting. How did you decipher that information?

Mr. LARGENT. Well, we had a number of our companies that have actually gone back in when all this came to light, several months before it hit the press, and they have been in an earnest process of interviewing the employees that are on the phone with their customers, and they cannot find any instances that they know of that their employees have given information to somebody that was not the account holder. These pretexters, they represent that they are the account holder.

We are getting literally hundreds of millions, if not billions, of calls every year asking for information about their—various questions about their accounts. As I said in my testimony, what was good customer service is now becoming a liability in this case. So we just want to ensure that we have the ability to serve our customers, our legitimate customers, and at the same time take care of these pretexters that are using lies and schemes to gain access to this information.

Senator NELSON. Well, someone who is posing as someone that they are not, what about the requirement of the telephone company to use a password instead of the Social Security number, because of now the availability, unfortunately, of Social Security numbers on some of the government documents?

Mr. LARGENT. Yes, sir, and many of our companies are doing precisely that. They are developing passwords, pass codes. They are no longer sending information via e-mail or faxing information now. They are only sending them to the address that is on the account if it is requested. So those are some of the things that I can tell you about. Many other things our companies are involved in. It was requested by the FCC on Monday and that is available to all of you. I do not want to talk about that here in this open session, but it is available to you and it is recorded down at the FCC.

Senator NELSON. In your business, in order to protect consumer confidential information what kind of checks do you have on the employees that have access to that information?

Mr. LARGENT. Well, all the ones that you would expect us to have. We have the highest security you can imagine of employees that are dealing with that information. But as you know——

Senator NELSON. Do you do background checks?

Mr. LARGENT. Sure, background checks.

Senator NELSON. You do?

Mr. LARGENT. Absolutely. But as you know, a lot of these call centers, you are talking about people that are oftentimes working at entry level wages, and so we definitely have issues. But I can tell you that we have scrupulously been going over and interviewing those employees to ensure that the breakdowns are not there. But as was mentioned in testimony here today, there is no doubt that some of that has been taking place, and we are trying to weed it out as quickly as we can.

Senator NELSON. A final question: Did you not pay for the Seattle Seahawks?

Mr. LARGENT. I did.

Senator NELSON. Your team came a long way. Congratulations.

Senator ALLEN. Thank you, Senator Nelson.

Let me go through some other ideas here. I just want to elicit responses or ideas from you. I think it was in answer to Senator Dorgan's questions, we somehow got Mr. Rotenberg and Mr. Largent together, Congressman Largent, together. What would be any legitimate reason for anybody to ever want somebody's telephone records other than for law enforcement? Is there any other reasons other than a court order where someone would want to have someone's telephone records? This came up. I just wanted to get some clarification. Mr. Douglas, if you want to add to it you may.

Mr. DOUGLAS. Well, as the former private investigator in the room, I will make the——

Senator ALLEN. Congressman, I just want to make sure your reply in that one on one there was accurate.

But go ahead, Mr. Douglas.

Mr. DOUGLAS. I will make the argument that they are making. And by the way, this morning they were discussing how this is a very—the PI and investigative trade was discussing how this is a very unbalanced panel here today. They feel that there should be somebody here arguing for them to be able to get these records. The argument they will make—and this addresses one bigger point I would like to make if I could, Mr. Chairman. The argument they will make is that they fight fire with fire, that to track down deadbeats, to develop witnesses, to locate witnesses, that they need access to these records the way law enforcement has it. And they have developed this tactic of going out and—let us call it what it is—stealing these records.

But they have found there is a very lucrative market and, without the pretexting connotation, it is the elephant in the room here that nobody is talking about, and that the FCC and the FTC have never addressed. I think the FTC is very aware. It is attorneys that are driving the cash flow that puts these websites up so that stalkers can buy them. It is some of the most prestigious law firms in this country using these investigators and illicit information brokers to buy this.

Monday, the Pelicano indictment in Los Angeles, where he was wiretapping celebrities and Hollywood executives. If you read the indictment closely, it talks specifically about bribing and using SBC Global phone company employees to get customer proprietary information, toll records, and the information to conduct these wiretaps. Who did he sell it to? Attorneys in Los Angeles.

So I support—and, excuse me, I think it was Mr. Pryor who raised the question before. I support the outlawing of the sale and purchase of records because law enforcement authorities will tell you that you cannot go after the buyers if you are just using the pretext standard, because under Gramm-Leach-Bliley to make those cases against the attorneys you would have to demonstrate that they know the records were obtained by these brokers through deceit and that is a very difficult standard for the Federal agencies to meet.

So I just wanted to add that to the record.

Senator ALLEN. Thank you. In view of that, what would you think of the idea of allowing phone companies, whether it is SBC or others—and Congressman Largent, you might want to bring up; we are talking about attorneys general and the FTC, which gets after individuals; FCC gets after companies. But what about allowing SBC or whatever it may be to actually also have a private right of action against any of these third-party data brokers?

Mr. DOUGLAS. Absolutely——

Senator ALLEN. Would you like that, Congressman Largent?

Mr. LARGENT. We would, yes, sir.

Senator ALLEN. What about the idea—and we have kind of gotten around this. What about the idea—and you do not need to get into all the details of how there is security. What about the idea of telephone companies filing security procedures with the Federal Communications Commission, in other words proving to the FCC that you—and the FCC has to approve it—that you have approved security procedures?

I am not saying that that may still not get breached. But it seems to me that, while there may be some rare legitimate uses or need for these records to be compiled—and every company may do it differently, which in its own way may actually be good because if somebody breaks the code to one they will break it for all, and it is probably best—and obviously this has to be kept confidential.

What would you think of that, Congressman Largent? I am talking about pre-approved plans by the FCC. And I would like to hear from you, Ms. Monteith, as far as the FCC having the capabilities of pre-approving security guidelines from communications companies.

Mr. LARGENT. Well, based upon the experience that we have had, I will just speak very briefly. This is an ever-evolving problem, that just when you set up a system to prevent people from breaking in they figure out how to get around that one and we have to improvise and we have to change it and do something, we have to tweak the system in order to cut them off at the pass.

So I am afraid that if we try to implement a system, even if it is different systems for different companies, and we submit that plan to the FCC, it could mean in 3 months or 6 months or 9 months we have to change it because they have figured out how to get around the system at that point in time, even if it is a confidential disclosure to the FCC only.

Senator ALLEN. Ms. Monteith?

Ms. MONTEITH. Thank you. I think Chairman Martin has made clear that he thinks that the strongest proposal would be to specifically make illegal the commercial availability of consumers'

records, very clean and no loopholes. I would have to take back to the Chairman and the Commission the idea of filing best practices, I believe, with the Commission and our review of those. But I am happy to do that and follow up with you.

Senator ALLEN. Well, we need to come up—and I will turn it over to Senator Pryor for another round of questions. We need to—there is a responsibility on the part of many people. The communications companies clearly have this information and there should be—and I am sure that you find no desire in having to be here and explaining what some of your member companies have done. But it seems to me that this has to be hit at so many different angles, that every single approach that we can take to assure that this privacy will be protected needs to be put into legislation and enforced and everyone pitching in on it.

Senator Pryor.

Senator PRYOR. Thank you, Mr. Chairman.

Ms. Parnes, I have one—the last time I want to put you on the spot. That is, if you answer this question correctly.

[Laughter.]

Ms. PARNES. I will try.

Senator PRYOR. On the issue of civil penalties, if the Congress were to give the Federal Trade Commission the authority to impose civil penalties, what do you think the level of those penalties should be?

Ms. PARNES. Well, currently the general civil penalty authority for the Commission when we have it gives us the authority to seek $11,000 per violation. It is usually difficult for us to actually get that much money because there are many, many violations and we could be talking about millions and millions of dollars. But I would think that that is a reasonable place to start, certainly.

Is that the right answer?

Senator PRYOR. That is the right answer.

Ms. PARNES. Thank you.

Senator PRYOR. That is actually what I was thinking too, but I just did not know if you had a different take on it.

Let me ask you, Congressman Largent if I may. That is, you said something in your earlier testimony that I thought was interesting about credit cards. I would like to hear a little bit more detail on your idea there about what, in your view, what should the rule be on credit cards and if you could expand on that.

Mr. LARGENT. Well, that is actually a new twist. We testified over in the House last week and we started thinking about this and realized that some of the violations as it pertained to the Gramm-Leach-Bliley Act created penalties if you were to use a credit card in a transaction to gain access to information that were found in financial records.

Senator PRYOR. Penalties against the card user or against the company that is using a credit card in a transaction?

Mr. LARGENT. The law actually is constructed, it is my understanding it is constructed, that the credit card company—that they cannot utilize the credit card to engage in a transaction of this type that we are talking about.

Senator PRYOR. I would like to explore that further. Do you have in mind that if you have these data brokers, I guess you want to

call them, that in order for them to get information, say for example on the cell phone number, that the number on the—the information on the cell phone they are seeking would have to be the same name as on the credit card? Is that the kind of safeguard you are talking about, where the credit card would have to match up with the person requesting information?

Mr. LARGENT. Right. And I misspoke. I said it was the Gramm-Leach-Bliley Act. It was not. It was on the pornography legislation that passed in the House and the Senate.

Senator PRYOR. Well, what you said is intriguing and I would like to pursue that after the hearing and visit with you about that and talk to your folks about that.

Mr. Rotenberg, let me ask you about, last July you filed a complaint with the FTC about a website that offered phone records and PO Box information; is that right, for a fee through pretexting? What was the response from the FTC to that complaint?

Mr. ROTENBERG. Well, initially really nothing, Senator. In fact, we followed up the initial complaint with a more detailed letter, with the assistance, I should mention, of Mr. Douglas, who has been very helpful to us throughout this, where we were able to describe 40 different companies that were making this kind of call detail information available.

Now, it is true that the FTC has gone after pretexting in the financial services context. They did so back in 1999. But they really have not looked at pretexting in the phone records context until very recently.

Senator PRYOR. Is that also true for the FCC?

Mr. ROTENBERG. Well, the FCC we understand in the next couple of days is going to announce action on our petition. They have already taken enforcement action against two companies under section 222 and I believe that this week they will be announcing a broader rulemaking on stronger security standards, and that is in response to our petition.

Senator PRYOR. Mr. Douglas, if I can turn to you just for a moment. You mentioned the caller ID spoofing in your testimony and showed us a website. Is there any legitimate reason why you would do a caller ID spoof other than maybe law enforcement?

Mr. DOUGLAS. No, and many of the sites will advertise it as entertainment purposes. But it has become very well known in the fraud community as a way to deceive people, and particularly in stalking situations and others it is very dangerous.

Senator PRYOR. You also mentioned attorneys a few moments ago. I just was a little confused about that. How in your view, how are the attorneys using this information?

Mr. DOUGLAS. Well, for the short period of time in 1997 when I actually bought these and learned about what was going on, it was all attorneys, since that is all that I worked with as a private investigator, who were interested in them. They do it in collections cases, they do it in competitive intelligence cases.

In fact, there is a very good paragraph in the indictment, in the Pelicano indictment, at least Monday, where they describe it as being used for tactical advantage in litigation situations. So if I want to know what my competitor is doing in a business deal or

any type of litigation that you can think of, knowing who they are talking to is very important.

It has become the electronic equivalent in the private investigative trade of dumpster diving. In the old days before the Internet, if you wanted to know what a business was doing, pick up their trash at the end of the night, hopefully when it is put out at the curb—that makes it, unfortunately in my opinion, legal—and go through their records. Well, now just buy them online.

Senator PRYOR. It sounds like your solution to this problem would be to follow pretty much what we did with Gramm-Leach-Bliley, just make it clear that it applies to telephone information?

Mr. DOUGLAS. Yes, twofold. First and foremost, I would like to see a fast bill out of the Senate and action very quickly to outlaw specifically what we are talking about today. In my perfect world, down the road we need to address these tactics being used for all consumer records. They are already being used to get utility information, gas, electric, cable TV, satellite TV.

You have to understand how they work. It is not about the record itself. It is where can I find information. There is a five-step process: know what information I want, know who is the custodian of the information, know who the custodian will release it to, know under what circumstances they will release it, become that person with those circumstances.

So it is not just that it is about phone records, although the prevalence of that has brought it to a national crisis. It is about any consumer record.

Senator PRYOR. The last question I have for you, Mr. Douglas, is, just by way of background, have you been contacted or do you work for any telecom companies in order to try to help them fight against pretexting and identity theft? Have you been contacted by anyone in the telecom industry?

Mr. DOUGLAS. No, not so far.

Senator PRYOR. That is all I had, Mr. Chairman. Thank you.

Senator ALLEN. Thank you, Senator Pryor. Let me follow up on that question.

Since you have not, Mr. Douglas, been asked——

Mr. DOUGLAS. And my cell phone drops out just like everybody else's, too.

[Laughter.]

Senator ALLEN.—what do you believe that the phone companies and the telecommunications associations, like CTIA, could do to better protect their phone records and their customers? What recommendations would you have?

Mr. DOUGLAS. Sure, and I actually wrote down what Mr. Largent said because he hit the nail on the head when he said customer service as a security flaw. That is how this works in all industries, but specifically the phone industry. The pretexters, to use the shorthand, know that they can take advantage, that the phone company's priority is customer service.

In the customer call center, which are the employees with the least amount of time, the least paid and the highest turnover rate, and usually the least trained overall, they are graded on how fast they move the call, how successfully they move the call, and do they offer other services through marketing. Security, customer au-

thentication, is usually, unfortunately and historically, fairly low on that schematic, if you will.

So a number of things. One, they need to better educate their employees as to these tactics. The banking industry went through this very industry after the passage of Gramm-Leach-Bliley and was fairly successful in that regard.

Where I would disagree with Mr. Largent respectfully is that there do need to be some baseline standards in customer authentication protocol. You cannot use biographical identifiers like Social Security number, mother's maiden name, date of birth. In many cases, even when they use passwords or PINs they will default to that if the person says, I have forgotten my password or PIN. Excuse me, this is what they will say on the phone: Come on, you SOB; I am trying to catch a plane; I need my information right now. That is how the art of pretext works, either badgering, cajoling, whatever.

So there need to be some baseline standards. The banking industry is looking at two-tier authentication. There is a great template out there in the banking regulatory agencies and some of the regulations that they have promulgated in the wake of Gramm-Leach-Bliley. So education and baseline standards, Mr. Chairman.

Senator ALLEN. Congressman Largent, what is your initial response to Mr. Douglas's?

Mr. LARGENT. I agree with him. I think—and these are exactly the type of steps that our companies are engaged in right now.

Senator ALLEN. Thank you.

Let me finish finally with you, Ms. Southworth. You have been listening to all of this from the FTC and FCC, the communications industry, PIs, and the folks with EPIC. You testified on the inherent risks and the real live risks to women who have been victimized on account of it, as did Mr. Douglas in his very graphic, sad testimony of a woman who was killed by someone who received this information.

What would you suggest? Just give us one, two, three suggestions. What would you suggest that we do in this legislation that we are going to be working on? It is going to come up, I suspect, very soon after this hearing. Give me one, two, and three, what components would you suggest to your government leaders?

Ms. SOUTHWORTH. I cannot talk about this issue without thinking about stolen goods. We think of theft when you steal something from someone and it is a crime. If you steal my personal information it is theft, it is a crime. So I do not think there should be any less penalties because it is data versus property. So I would love to see that this be taken seriously.

I agree with all the other panel members with the issues. I have been nodding vigorously throughout the discussion. The piece that I think may or may not be something you can address in the legislation, but it is the critical element that has not been mentioned yet, it is the consumer education piece. Everybody can do everything to increase security standards and deal with the people misusing the data. However, if consumers do not know not to use their pet's name as their password, we still have a security problem. So it is critical to reach the consumers too so they understand that

this is a broader issue and please do not use your mother's maiden name as your password.

Senator ALLEN. Use your pet's name is your suggestion?

Ms. SOUTHWORTH. No, do not, do not use your pet's name, your mother's maiden name, or your anniversary date.

Senator ALLEN. Thank you, Ms. Southworth.

Do you have any further questions?

Senator PRYOR. I just have one quick follow-up.

Senator ALLEN. Go ahead.

Senator PRYOR. To you, Ms. Southworth. Again, thank you for what you do and your organization does in the realm of domestic violence. I used to work very closely with your folks in Arkansas and they are wonderful to work with.

Ms. SOUTHWORTH. They are great.

Senator PRYOR. I do have a question to you about the FCC and the FTC. Have you ever worked with them in any investigatory capacity?

Ms. SOUTHWORTH. Not an investigatory capacity. We will be working closely with the Federal Trade Commission tomorrow on the anti-spyware initiative issues.

Senator PRYOR. But not on this issue?

Ms. SOUTHWORTH. Not thus far, but we would be happy to work—we work closely with many Federal agencies.

Senator PRYOR. Right.

Ms. SOUTHWORTH. So we would be happy to work with them in any capacity.

Senator PRYOR. Either the FTC or the FCC.

Ms. SOUTHWORTH. Absolutely.

Senator PRYOR. Even after Amy Boyer was killed in 1999, you did not—as far as you know, you did not have any contact?

Ms. SOUTHWORTH. My project did not exist then. We were founded in 2002. So now we are sort of the go-to folks for anything around domestic violence victimization and technology.

Senator PRYOR. Thank you.

Ms. SOUTHWORTH. The one piece that I would add to that, though, is that you mentioned, is the private investigator piece. Peggy Klinky was killed in 2003 after her ex found her using a private investigator, and I do not know what information that private investigator got through pretexting.

Senator PRYOR. Thank you.

Mr. Chairman, thank you for the hearing.

Senator ALLEN. Thank you.

One final question, Ms. Southworth, just to make sure. You have worked with State attorneys general undoubtedly.

Ms. SOUTHWORTH. Absolutely.

Senator ALLEN. So I think that will be one component that is very important in this legislation, to have that additional enforcement from those that actually have such offices that are in the States, closer to the people, and probably—not that an attorney general's office is something you walk into, but nonetheless it is closer and responsive to the people.

So I want to thank all of you, all of our panelists, for your interest, for your insight, your testimony, your ideas. It is going to make it very, very helpful to us as we put together, working together on

a bipartisan basis—when I look at this list, you have folks from Virginia, Arkansas, Alaska, Hawaii, Louisiana, Montana, California, Oregon, North Dakota, and Florida. There is a great deal of concern.

I mentioned in the beginning when I first heard this I said we need to act. You have given us some good ideas. I also like the ideas that some of you mentioned, is that people need to be aware of this and come up with passwords, so to speak, that are not easily discernible and replicable. The phone companies or communications folks are going to need to make a better effort clearly of this. I am glad to hear, Congressman Largent, your leadership and willingness to do it. Mr. Douglas, you have brought up the tragedies that occur from this. Mr. Rotenberg, thank you for your great public citizenry. I think it helps certain Federal agencies get moving.

But we need to crack down. It is going to be made a crime. We are going to bring every aspect that is logical and reasonable toward this at the Federal level, State attorneys general, get rid of some of the loopholes and, what were they calling it, the certifications, giving the criminals a heads up. Absolutely absurd. We will have greater fines, longer statutes of limitations. There may be some aspects of this that you do have to certify a security approach with the communications companies.

But we are going to act. America expects us to. You help propel us and give us the information that we can put together legislation, not just legislation for the heck of it, but legislation that is effective.

I thank you all and this hearing is adjourned.

[Whereupon, at 4:23 p.m., the Subcommittee was adjourned.]

A P P E N D I X

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO KRIS ANNE MONTEITH

Question 1. In recent weeks, both the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) have initiated enforcement actions against pretexters. How do your two agencies coordinate your enforcement activities to ensure that we are not duplicating efforts?

Answer. FCC staff and FTC staff have communicated regularly to discuss our respective enforcement efforts and to avoid duplicative efforts. We will continue to engage in regular communications to share information with each other to facilitate our enforcement activity. The FCC is focused principally on the activities of telecommunications carriers in protecting their customers' sensitive personal information while the FTC is focused on the activities of the data brokers themselves in acquiring the data from carriers. Thus, our efforts are naturally complementary and the risk of duplication is low.

Question 2. What are the maximum penalties under both the Communications Act and the FTC Act, respectively, that can be imposed on pretexters?

Answer. The FCC's rules regarding the protection of Customer Proprietary Network Information (CPNI) apply to telecommunications carriers. Thus, the FCC would not be able to impose penalties against pretexters for their CPNI-related practices unless the pretexters were also licensed telecommunications carriers. If pretexters, as carriers, engage in violations of the Communications Act or Commission rules, the FCC may impose a maximum penalty of $130,000 per violation or per day of a continuing violation up to a maximum of $1.35 million.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO LYDIA B. PARNES

Question 1. In recent weeks, both the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC) have initiated enforcement actions against pretexters. How do your two agencies coordinate your enforcement activities to ensure that you are not duplicating efforts?

Answer. The FTC and FCC have both formal and informal cooperative arrangements for working on cases with overlapping jurisdiction. For example, the agencies have a formal memorandum of understanding relating to telemarketing enforcement, which includes an agreement to meet regularly in order to coordinate comprehensive, efficient, and non-redundant enforcement of our respective telemarketing statutes and rules. Under that agreement, the FTC provides the FCC access to Do Not Call Registry data, and each agency agrees to make its consumer complaints available to the other regarding possible violations of Federal telemarketing rules. That agreement has worked well.

On other projects and cases, the FTC has granted the FCC access to investigative files and both agencies share complaints with the other. The agencies are continuing this close coordination with respect to our current investigations of telephone pretexters. Staffs of the agencies have frequent and ongoing discussion about targets, and have shared information obtained in the investigations. Because the agencies have different enforcement tools and jurisdictional limits, the FTC's investigations are focused on the businesses that offer to obtain and sell consumer phone records, while the FCC has oversight of the telecommunications carriers. [1]

Question 2. What are the maximum penalties under both the Communications Act and the FTC Act, respectively, that can be imposed on pretexters?

[1] The FTC's governing statute, the FTC Act, specifically excludes FTC jurisdiction over common carrier activities that are subject to the Communications Act. 15 U.S.C. § 46(a).

Answer. With respect to the FTC, the Commission has the authority to seek equitable remedies in its Federal court actions. These remedies could include, in appropriate cases, consumer redress or disgorgement of ill gotten gains. It can also seek conduct prohibitions including injunctions against further violations of the law, or, in certain cases, an outright ban on engaging in certain types of conduct or business. Once entered, violations of Federal district court orders are punishable by civil or criminal contempt.

The Commission does not have authority to seek civil penalties for a law violation except in specified circumstances, i.e., for violation of a trade regulation rule or of an order in a prior enforcement action, or if specifically so provided in an applicable statute. I believe that civil, and possible criminal, penalties would provide a strong deterrent to telephone pretexting. In the telephone pretexting context—where the harm includes a privacy violation—it may often be difficult to calculate either consumers' economic injury or a violator's gains. Consequently, civil penalties may be a more appropriate remedy than some of the agency's existing tools like consumer redress.

Question 3. The FTC originally fined Touch Tone $200,000 for violation of the GLBA and unfair and deceptive practices under Section 5. Why was this amount later suspended, allowing Touch Tone to get away with no monetary punishment?

Answer. The Touch Tone case was filed prior to the passage of the Gramm-Leach-Bliley Act and therefore charged violations only of the FTC Act. The $200,000 judgment in Touch Tone represented the defendants' alleged unjust enrichment from the sale of consumers' financial information. However, according to sworn financial disclosures, the individual defendants were unable to pay this amount. The final order makes the judgment immediately payable to the FTC if either defendant is found to have materially misrepresented his or her financial condition.

Question 4. In Operation Detect Pretext, the FTC brought charges against three firms, two of which were fined $2,000 and the third wasn't fined at all. Why didn't the FTC exact larger fines for this activity and why weren't the original fines maintained?

Answer. The FTC's remedies in the three Operation Detect Pretext cases were based on the disgorgement of unjust enrichment and injunctive relief. In two of the cases, the defendants' gains from the sale of the alleged pretexting services were $2,000. In the third case, the defendant's financial gains were $15,000. However, as in Touch Tone, a sworn statement from the defendant in the third case established that he was financially unable to pay this amount. The final order in this case also makes this payment immediately payable to the FTC if the defendant is found to have materially misrepresented his financial condition. [2]

In addition to imposing monetary payments, the orders in each of the three cases also prohibit the defendants from engaging in the same unlawful conduct, require them to provide the Commission with reports on their compliance with the orders, and ultimately allow the Commission to bring contempt actions for failure to comply with material terms of the orders.

Question 5. Why hasn't there been any more legal action taken against pretexters by the FTC since 2001?

Answer. The Commission has brought seven additional pretexting cases since 2001, bringing the total to 11 such actions. [3] These cases are part of the larger Commission program aimed at protecting consumers' privacy. For example, since the Subcommittee hearing, the Commission announced a settlement with CardSystems Solutions, Inc., a credit card processor that allegedly failed to implement reasonable measures to protect consumer credit card information. The Commission's complaint alleges that the company's lack of appropriate security measures exposed the credit card information of tens of millions of consumers and resulted in millions of dollars of fraudulent charges. [4] The CardSystems settlement follows the FTC's record-breaking settlement with the data broker ChoicePoint, Inc. This agreement settles charges that ChoicePoint lacked reasonable security and customer verification procedures in violation of the Fair Credit Reporting Act and FTC Act. The settlement requires ChoicePoint to pay $10 million in civil penalties (as a remedy for the FCRA violations) and $5 million in consumer redress.

As mentioned in the Commission testimony and my oral remarks during the hearing, the Commission is also investigating a number of companies that appear to be engaging in telephone pretexting. Commission attorneys currently are evaluating the evidence to determine if law enforcement action is warranted.

---

[2] *See http://www.ftc.gov/opal2002/03/pretextingsettlements.htm*.
[3] *See http://www.ftc.gov/privacy/privacyinitiatives/pretexting_enf.html*.
[4] See *http://www.ftc.gov/opa/2006/02/cardsystems_r.htm*.

I also believe that in addition to law enforcement efforts, legislative changes could help address the problem of telephone pretexting. Although the Commission already can bring actions against pretexting for consumers' telephone records under the FTC Act, I believe Congress should consider whether additional legislation would be appropriate in this area. One approach would be a specific prohibition on the pretexting of telephone records. Legislation of this kind could help deter pretexting by making clear that this practice is illegal. If Congress were to consider such legislation, I would recommend that it give the Commission authority to seek civil penalties against violators, a remedy that the FTC does not currently have in cases like this. I believe that, in this area, penalties are the most effective civil remedy. This is also a situation where criminal penalties may be warranted, but I would defer to the Department of Justice on the need for criminal legislation and its structure. I and my staff would be happy to work with Commerce Committee Members and staff on any legislation that may be under consideration.

Finally, FTC staff recently conducted an Internet surf of telephone pretexters and found that some sites offering these records were registered to foreign addresses. This finding underscores the importance of the Commission's previous recommendation that Congress enact cross-border fraud legislation. The proposal, called the U.S. SAFE WEB Act, would overcome many of the existing obstacles to information sharing in cross-border investigations.

I hope that the foregoing information is helpful. Please let us know whenever we may be of service. If you have any questions or comments, please feel free to contact me, or you or your staff may contact Anna Davis, the Director of the FTC's Office of Congressional Relations, at (202) 326–2195.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO MARC ROTENBERG

Question 1. In a statement made by Jimmie Mesis, Editor-in-Chief of Private Investigator (PI) Magazine, on June 11, 2005, to his readers regarding pretexting complaints, "My immediate concern is not the FTC . . . [w]hen the complaint comes from EPIC, we have a problem."

Why do you believe you have been more successful in intimidating pretexters than the FTC has?

Answer. Since its founding in 1994, EPIC has made effective use of the Internet to draw public attention to new threats to personal privacy. While we lack the resources and enforcement authority of the Federal agencies, we believe that it is possible, in the short term, to curtail some of the worst business practices by publicizing the problem online.

However, our "watchdog" role is not an adequate substitute for the effective enforcement of privacy laws that help safeguard consumers and establish trust and confidence in the online business environment.

Consumer concerns about new threats to privacy are broad and growing. The Federal Trade Commission clearly needs more resources to bring enforcement actions against companies violating Section 5 of the FTC Act.

The statement from the Editor-in-Chief of Private Investigator Magazine points to another serious problem: he does not recommend curtailing pretexting or the sale of personal information, nor does he suggest that pretexting is inherently bad; rather he advocates that private investigators and others take the practice underground. Later in the message, he writes "PI's need to stop promoting the selling of toll records directly to the public as a commodity . . . I also suggest that PI's promote such services as 'telephone research' as compared to coming right out and mentioning tolls, non-pubs, etc." (emphasis added).[1]

We believe that the community will follow this advice, and simply move the trade underground, and further obfuscate the practice by calling it "telephone research" rather than "phone breaks" and the like. That is why it is critical to enact comprehensive legislation that will broadly prohibit pretexting.

Question 2. If legislation was passed to prevent pretexting, who would you recommend be the enforcement authority on matter?

Answer. Because widespread pretexting can easily occur without necessarily attracting the attention of the FTC, EPIC recommends that the Committee empower state attorneys general, individual consumers, and companies deceived by pretexting to seek damages from pretexters and the sellers of personal information. The limited action by the FTC indicates that additional law enforcement support is needed to

[1] E-mail of Jimmie Mesis, Editor-in-Chief of Private Investigator Magazine, to readers (July 11, 2005).

combat the problem and properly enforce any legislative solution to this problem. State attorneys general are in a better position to hear the complaints of individual consumers, and can supplement FTC action.

However, even state officials operate at some remove from those most directly affected by the sale of personal information—the individual victims. A private right of action for individuals will allow victims to defend themselves from those who would sell their privacy for a profit, without having to attract the attention of, then wait for Federal or state authorities to focus on their particular case. The Telephone Consumer Protection Act of 1991, which limits telemarketing and the transmissions of junk faxes, contains model enforcement language that allows the individual to sue in state court and get default damages.

We also support the right of the carriers to bring actions against pretexters. Carriers are in a position to detect patterns of intrusions into their systems, and should be able to bring enforcement actions against pretexters.

Question 3. Mr. Rotenberg, in your testimony, you noted EPIC's rulemaking petition filed at the FCC that calls for action by the FCC to enhance the security requirements that telecommunications carriers must follow under section 222 of the Act. Like you, I am pleased to know that the FCC will soon put this petition out for public notice, and hope that they will expedite the consideration of this item.

Answer. Senator, we very much appreciate your support for the decision of the FCC to undertake a rulemaking, in response to EPIC's petition, to enhance the security requirements that telecommunications carriers must follow under section 222 of the Act.[2] We hope that EPIC's recommendations for stronger security safeguards will be incorporated into a final rule from the Commission. While we understand industry concerns about maintaining flexibility in combating fraud, we believe that sensible regulations will discourage particularly bad security practices, such as using easily obtained biographical data (such as zip code or date of birth) for authentication. Other guidelines, such as the maintenance of audit trails that allow investigators to know who has accessed customer data and notifications of data breaches, are commonsense techniques that companies that collect and maintain customer information should implement.

Question 4. In your opinion, does section 222 confer sufficient authority on the FCC to ensure that those who handle phone record data in the normal course of business will protect such data? For example, are Voice over Internet Protocol (VoIP) providers covered under section 222?

Answer. Section 222 states that "telecommunications carrier[s]" have a duty to protect "customer proprietary network information." The FCC has the authority under this section to create rules to protect the confidentiality of CPNI for telecommunications carriers. Therefore, the FCC has sufficient authority to ensure that those handling traditional telephone and cellular records must protect that data.

However, as your question indicates, this power is limited to the entities that the FCC may regulate under Title II of the Communications Act. The FCC has held that computer-to-computer VoIP, is not regulated under Title II, and thus fall outside the FCC's regulatory scope.[3] The extent to which the FCC might regulate VoIP providers that connect to the telephone network is a more problematic question, in which EPIC, in at least one other context, is involved.[4] The FCC, however, has not yet made a final determination on this issue.[5]

While I do not believe that Section 222 currently gives the FCC the power to regulate interconnected VoIP, Congress and your Committee should act to ensure that, as the government extends its regulatory power into new areas, it should also build privacy protections into new laws and regulations. If the FCC finds that it has regulatory power over other aspects of interconnected VoIP via the Telecommunications

---

[2] Notice of Proposed Rulemaking, *In re Petition for Rulemaking to Enhance Security for Access to Customer Proprietary Network Information*, FCC Docket No. 96–115, RM–11277 (Feb. 10, 2006), available at *http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC–06–10A1.pdf*.

[3] *See In re Petition for Declaratory Ruling that pulver.com's Free World Dialup is Neither Telecommunications Nor a Telecommunications Service*, 19 F.C.C.R. 3307 (2004).

[4] EPIC is one of several petitioners in *Am. Council on Educ.* v. *FCC*, Docket No. 05–1404 (D.C. Cir. filed Oct. 24, 2005), challenging the FCC's application of the Communications Assistance for Law Enforcement Act to facilities-based broadband providers and interconnected VoIP providers.

[5] *See In re Petition for declaratory Ruling that AT&T's Phone-to-Phone IP Telephony Services are Exempt from Access Charges*, 19 F.C.C.R. 7457 (2004) (holding that phone-to-phone services that use Internet Protocol are subject to access charges levied against telecommunications carriers in certain situations); *but see, e.g., Southwestern Bell Tel.* v. *Global Crossing Ltd.*, 2006 U.S. Dist. LEXIS 4655 (Feb. 7, 2006) (staying ruling pending FCC determination of whether or not the VoIP telephony at issue is regulated as a telecommunications service). *See also Frontier Tel.* v. *USA Datanet Corp.*, 386 F. Supp.2d 144 (W.D.N.Y. 2005) (same).

Act, then the privacy-protective portions of the Act, including Section 222 should apply equally.

Question 5. Does VoIP call data information qualify as "CPNI" under the statute?

Answer. Since the statute specifically defines CPNI by referencing "telecommunications carrier[s]," VoIP call data information would not be considered CPNI, insofar as a VoIP provider would not be considered a telecommunications carrier.

Question 6. Do you have suggestions for how section 222 of the Communications Act might be changed to apply evenly and fairly?

Answer. Consumers have clearly been disturbed by the news that their phone records are for sale by pretexters. Many are similarly disturbed that their call records and subscriber information are also being sold by their carriers to other for marketing purposes, under the very auspices of Section 222. Under current FCC regulations interpreting Section 222,[6] telecommunications carriers may place the burden upon consumers to opt out of this sale of their CPNI to others. Frequently, the notices informing consumers of this right are hard to find, hard to read, and hard to understand. Chairman Martin of the FCC has expressed a desire to use a more privacy-protective opt-in standard for the disclosure of such sensitive information, and legislation specifying the standard within Section 222 would allow this to happen.

Meanwhile, consumers lack the ability to limit disclosure of their "subscriber information," which includes home addresses. Many individuals, such as victims of stalking or domestic violence, are made more vulnerable by the disclosure of this information. Such individuals frequently rely upon the increased privacy afforded by the use of a cell phone. Section 222 should also ideally prevent the sharing of subscriber information, absent the permission of the individual consumer.

As for protecting consumers' records held by VoIP providers and other businesses, a general ban on pretexting could be coupled with requirements that VoIP providers implement basic data security measures. This could be achieved by amending Section 222, although any amendments should limit their scope to that section, to prevent inadvertent application of the Telecommunications Act to VoIP, a technology not widely contemplated during the drafting of the Act.

Another solution would be to require VoIP providers to implement security measures for customer data in some other portion of the U.S. Code, to be enforced by the FTC, attorneys general, individual consumers, or other bodies. This would avoid the jurisdictional questions of regulating VoIP as either a telecommunications or an information service, instead focusing on the handling of customer data as a trade practice.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. DANIEL K. INOUYE TO CINDY SOUTHWORTH

Background: In July 1999, Liam Youens obtained information from an Internet-based investigation service called Docusearch on Amy Boyer, a woman Youens had been stalking since high school. He was able to obtain her Social Security number for a mere $45 and hired someone to pretext Boyer to get her employment information. Then in October 1999, Youens drove to Boyer's workplace, shot and killed her, then turned the gun onto himself.

Question 1. The Amy Boyer case brought to light another aspect where pretexting can have a direct effect on one's privacy and safety. Do you believe the safety of domestic violence victims has decreased significantly with the increase in popularity of pretexting?

Answer. We agree that the safety of victims has decreased with the increase in popularity of pretexting by both abusers and by information brokers who sell illegally obtained victim information to abusers.

The murder of Amy Boyer not only highlighted the ease of pretexting, but also the use of pretexting by information brokers, who then sell the sensitive data they obtain. Unfortunately, perpetrators of domestic violence have tried to obtain information about their victims under false pretenses, or "pretexted," for decades, but the growth of the information broker industry has provided an almost unlimited amount of sensitive data for anyone willing to pay.

Internet use has reached new levels and stalkers are also using this technological tool to track down victims. Research by Pew Internet and American Life Project shows that 69 percent of adult women and 75 percent of adult men use the Inter-

[6] The current FCC regulations followed the decision in *U.S. West, Inc.* v. *FCC*, 182 F.3d 1224 (10th Cir. 1999), *cert. denied*, 530 U.S. 1213, (2000).

net.[1] Eighty-four percent of those adult Internet users have used an online search engine to help them find information on the Web.[2] Information brokers abound on the Internet and many of these businesses engage in pretexting to illegally obtain sensitive information.

Question 2. Do you, and if so how, do you see pretexting affecting those choosing to leave an abusive situation?

Answer. Abusers use pretexting to stalk their victims before, during, and after a victim leaves a violent relationship. They also use information brokers to gain private data about their victims. The most dangerous time for a victim of domestic violence is when she takes steps to leave the abusive relationship.[3] Many victims are stalked relentlessly for years after having escaped from their partners. These batterers who stalk their former partners, determined to hunt them down, are the most dangerous and pose the highest lethality risk.[4]

On February 23, 2005, Luis Alberto Gomez-Rodriguez tracked his ex-girlfriend from Florida to Iowa with the aid of illegally obtained cell phone records and court records. He found her new home near Iowa City and murdered her.[5] The news reports did not reveal whether he purchased the cell phone records from an information broker who used pretexting or whether he personally pretexted to obtain them.

In another example of pretexting and stalking, an Arizona man placed a global positioning system on his ex-girlfriend's car and obtained her phone records to see who she was calling. He also threatened to kill her before she discovered the tracking device and contacted the police.[6]

By monitoring phone and other records before a victim attempts to leave an abuser, the perpetrator may be able to anticipate her plans to flee. Once a victim has fled and is trying to establish a new life, a stalker can learn of her new location by illegally obtaining her records by pretexting or purchasing her records from an information broker who has used this method.

The National Network to End Domestic Violence has received calls from countless victims and their advocates who have either been found by abusers who misuse records or who are terrified that their perpetrators will locate them through pretexting.

○

---

[1] Pew Internet and American Life Project, September 2005 Tracking Survey. Available online at: *http://www.pewinternet.org/trends/User_Demo_12.05.05.htm.*

[2] Pew Internet and American Life Project, "Usage Over Time" spreadsheet. Available online at: *http://www.pewinternet.org/trends/UsageOverTime.xls.*

[3] Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, "Violence Against Women: Estimates From the Redesigned Survey" 1 (January 2000).

[4] Barbara J. Hart, "Assessing Whether Batterers Will Kill". Available online at: *http://www.mincava.umn.edu/hart/lethali.htm*; Jacqueline Campbell, "Prediction of Homicide of and by Battered Women" reprinted in *Assessing Dangerousness: Violence by Sexual Offender, Batterers, and Sexual Abusers* 96 (J. Campbell, ed., 1995).

[5] Byrd, Stephen. "The hunt begins: Witnesses tell of suspect's methodical search for Muscatine couple." *The Muscatine Journal,* (Muscatine, Iowa) February 11, 2006. Available online at: *http://www.muscatinejournal.com/articles/2006/02/11 /news/doc43ed60933bfef871578540.txt*.

[6] Sakal, Mike and O'Brien, Charlie. "Records detail Belle's threats." *The East Valley Tribune* (Mesa, Arizona) February 18, 2006. Available online at: *http://www.eastvalleytribune.com/index.php?sty=59420*.