The Testimony of

Ms. Cindy Southworth, MSW

Director of Technology & Director of Safety Net:
the National Safe and Strategic Technology Project
at the National Network to End Domestic Violence

Before the Subcommittee on
Consumer Affairs, Product Safety, and Insurance

United States Senate

Protecting Consumers' Phone Records

February 8, 2006

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 relationship does not stop the violence. In fact, the most dangerous time

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

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

---

[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).

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% 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 email 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.

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

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

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.

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 Albuqueque 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.

[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.

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.

---

[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.

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 through relatives' phone records and other means, often obtaining their information by more 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

[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)

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.