**BEFORE THE**
**PENNSYLVANIA PUBLIC UTILITY COMMISSION**

Interim Guidelines for Eligible Customer Lists for Electric Distribution Companies

Docket No. M-2010-2183412

# COMMENTS OF THE PENNSYLVANIA COALITION AGAINST DOMESTIC VIOLENCE

Nicole A. Lindemyer, Esquire
Policy Manager
Pennsylvania Coalition Against Domestic Violence
6400 Flank Drive, Suite 1300
Harrisburg, PA 171112
717-545-6400
nal@pcadv.org

Dated: August 4, 2010

In response to the request for comments in the Tentative Order and draft interim guidelines for Eligible Customer Lists, the Pennsylvania Coalition Against Domestic Violence submits the following comments to express our concerns on behalf of domestic violence victims.

The Pennsylvania Coalition Against Domestic Violence is the statewide network of 61 community-based programs serving all 67 counties in the Commonwealth. Our programs provide emergency shelter, hotlines, counseling, legal advocacy, children's advocacy, and other services to nearly 100,000 domestic violence victims per year.

The Coalition commends Vice Chairman Christy for raising concerns on behalf of domestic violence victims, and Secretary Chiavetta for incorporating these concerns and call for comments. The Coalition has a long history of working with the Public Utility Commission to protect the interests of domestic violence victims with regard to utility related issues. We are grateful for this opportunity to once again provide our input and expertise.

The Coalition's position with regard to inclusion of personal data in the Eligible Customer Lists is that **an affirmative opt-in mechanism should be used prior to disclosure.** While we understand and respect the value of cultivating competition in the utilities markets, we believe that **the value of protecting domestic violence victims' customer information, so as to prevent abusers from tracking and further harming victims, outweighs any potential benefits of broad disclosure of customer information for the purpose of fostering competition within the electricity generation market.** Anything less than an affirmative opt-in measure jeopardizes data privacy and hence, in the case of domestic violence victims, customer safety.

**The Crucial Link Between Domestic Violence and Data Privacy**

Domestic violence, sexual assault, and stalking are the most personal of crimes, and the more personal information 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.[1] Here in Pennsylvania, according to a national survey, on a single day, domestic violence programs served 2,597 victims.[2]

Leaving the relationship 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, forced to relinquish ties to family and friends, to give up driving or voting to keep their names out of public rolls, and to

[1] 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).

[2] National Network to End Domestic Violence (NNEDV), *Domestic Violence Counts: The National Census of Domestic Violence Services, Executive Summary for Pennsylvania* (2009), *available at* http://www.nnedv.org/docs/Census/DVCounts2009/DVCounts09_StateSummary_PA_Color.pdf.

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

ceaselessly look over their shoulders. Batterers who stalk their former partners, determined to hunt them down, are the most dangerous and pose the highest lethality risk.[4] Victims live day to day with the mind-numbing, knee-buckling fear that somehow, someday, their whereabouts will be revealed and they will be hunted down and killed.

The ability to keep their address and other personal information confidential offers some degree of respite from that fear. While nothing is failsafe when it comes to domestic violence, we do know that every additional layer of safety and protection for victims can be enough to make the difference between life and death.

For domestic violence victims in particular, data privacy is not simply an abstract concept, but rather is inextricably linked to safety. Indeed, utility service information is part of a larger problem that victims of abuse face—the prevalence of information regarding their location and activities and the ease with which that information can be obtained by their abusers.

Victims are increasingly being tracked and killed through the abuse of data and technology, pretexting, and information brokers.[5] There is a staggering amount of data generated and maintained about individuals in our society every day—far beyond but including utility records. Personally identifying information like dates of birth, Social Security numbers, frequently visited websites, and even grocery shopping preferences, are now being tracked as never before. Data breaches resulting in disclosure of sensitive personal information are only increasing as more and more systems and sectors maintain electronic databases of such revealing information. In its running toll of reported security breaches revealing sensitive personal information, the Privacy Rights Clearinghouse reports a total of 494,692,655 records from 1,651 breaches made public since January 2005.[6]

Likewise, information broking is a growing industry. 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, Social Security numbers, and even photos and floor plans of people's homes.

Pretexters—those who claim to be someone else for the purpose of accessing private information—and information brokers are not just breaching someone's privacy, they may be endangering someone's life. Fifty-nine percent of female stalking victims are stalked by current or former intimate partners,[7] and 76% of women killed by their abusers had been stalked prior to

---

[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] The Federal Trade Commission has also recognized the dangers posed by data mining and information brokers, and is taking steps to curb the illegal trade of mining and selling personal data. See, for example, *FTC v. Accusearch, Inc., d/b/a Abikka.com, and Jay Patel*, Case No. 06-CV-105-D (U.S. Dist. Wyoming), involving the unauthorized acquisition and sale of confidential consumer phone records.

[6] See www.privacyrights.org.

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

their murder.[8] Stalkers are often in a prime position to obtain utility 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 private information about their victims (such as date of birth, mother's maiden name, or 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.

Utility records are a particularly rich source of information for the determined stalker. By obtaining this information, a stalker can locate his victim without the victim even knowing that she has been tracked until it is too late.

The theft and/or disclosure of 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 abuse of private information is not just financially or personally devastating – it can be fatal.

⇒ 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.[9]

⇒ 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. The perpetrator, Liam Youens, paid Docusearch, an information broker that collects personal information via an array of electronic databases, 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.[10]

⇒ In another 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 asked about other "records" such as where she got her car fixed, rented videos, etc. Several businesses she used, including the video store and the local auto repair shop, used her 7-digit cell phone number as her customer identifier. Her ex-husband asked someone he knew to look up her name in one system, which made tracking her movements simple. He discovered that

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

[9] 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.

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

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.

⇒ In yet another case, 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 elsewhere and rented a car to use. Since there are only a few rental places on the island, it was not long before the abuser found the car rental office she used, 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.

While these tragic instances are but a sampling of the known assaults stemming from privacy violations, they exemplify the very real safety risks at the heart of data privacy protections, and underscore the severity of our concerns about disclosing utility customer names and addresses.

Notably, it is not just the victims of domestic violence who are at risk if their personal information and location is revealed, but also the individuals and programs that help them. 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 do, by using post office boxes and unlisted phone numbers and addresses for both the shelter and for staff and volunteers. Whether the utility 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.

**The Interim Guidelines and Existing Law on Customer Privacy Are Insufficient to Protect Domestic Violence Victims' Privacy and Safety Concerns**

The current law governing the privacy of utility customer information, 52 Pa. Code Section 54.8, provides for an "opt-out" mechanism whereby a customer may restrict the release of either the customer's telephone number or historical billing data. Assuming customers are aware of their rights to opt out, **current law does not even allow for the restriction of names and addresses, which is precisely the data that most endangers domestic violence victims**. For this reason alone, the opt-in mechanism fails completely to protect domestic violence victims.

Assuming for argument's sake that the statute or implementing regulations were expanded to include names and addresses, the opt-in mechanism still fails for several reasons. First, customers may not receive it—particularly victims who are between and among addresses after fleeing abuse, who may go first to an emergency shelter, then to transitional housing, then to a permanent address and whose mail commonly and unsurprisingly fails to reach them. Next, customers may receive the opt-out notice yet simply not read it because they consider it "junk mail" or unimportant; domestic violence victims are just like all other customers in this regard.

Next, customers may not understand the import of the notice—more accurately, the import of not responding to the notice. A victim who has received and read an opt-out notice may have no idea that unless she acts accordingly, her personal, private information will be released to hundreds of third parties, making it exponentially easier to track her down. It is hard to predict the lengths to which an abuser will go to track them down; as illustrated in the examples above, the victims had already taken steps to protect themselves yet their abusers were able to track them nonetheless. What's more, few persons grasp how much information is collected on them, and just how easy it is to obtain anyone's personal information—from utility companies or any other aggregate source or database. Mailing an opt-out notice runs the foreseeable risk that victims do not have enough information about the widespread nature and harmful consequences of information disclosure and therefore do not respond.

It bears noting that the personal information to be included on the Eligible Customer Lists is information that utility companies *require* customers to provide as a condition of receiving utility service. Customers have no option but to provide it, and do so assuming that it will be kept confidential. Customers' presumption of privacy is at stark odds with the presumption that their information is fair game for dissemination among commercial interests. Given the lengths that domestic violence victims go to simply to protect their and their children's safety, it is not reasonable that they are compelled to take even further action to prevent such a breach of their reasonable expectation of privacy—of information they had no choice but to provide.

**The Presumption of Information Sharing Inherent in an Opt-Out System Is At Odds With the Growing Penumbra of Legal Measures to Protect Data Privacy**

In recent years, there have been concerted efforts at both state and federal levels 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.

- At least 17 states, including Pennsylvania, now offer Address Confidentiality Programs, which provide a secure system for receiving mail without revealing a victim's address[11];
- Twenty-two states 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 states, including Pennsylvania,[12] 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;

[11] 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). See also 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.

[12] 54 Pa. C.S. § 701.

- The Social Security Administration allows domestic violence victims to change their Social Security numbers to help them seek protection.[13]

These and other efforts to protect personal information about domestic violence victims are in stark contrast to the "notice and consent" opt-out model of the Interim Guidelines and of existing law (52 Pa. Code Section 54.8). As a matter of public policy, given not only the safety risks in domestic violence situation but also the growing prevalence of identity theft, information broking, and other criminal violations of privacy, it would be a startling contradiction to presume customers' private information is made broadly available for commercial purposes.

For the purpose of analysis, there is a rough analogy to be made between the "notice and consent" opt-out model and the general tenet of contract law that holds that silence is not consent. It is elementary within contract law that forming a contract requires an affirmative act of consent on the part of the contracting party. For example, if a retailer mails a letter to an individual stating that by opening the letter he has agreed to be delivered and charged for goods unless the individual tells them otherwise, that individual is not liable for the goods because he never consented to the purchase.

By analogy, a utility company requires certain information of a customer as a condition of providing utility service, and the customer provides such information with the assumption that it will be kept private and used only by that utility company. However, the Interim Guidelines for Eligible Customer Lists now turn that presumption on its head: the act of enrolling for utility service mandates disclosure of personal information, but at no time is a customer informed that such information will be broadly disseminated for commercial purposes. There is no affirmative consent to the dissemination unless and until the customer gives it. The only way to ensure true informed consent is an opt-in mechanism.

**Conclusion**

In sum, the more broadly victims' personal information is disseminated, the greater the ease with which their abusers can obtain that information and use it to hunt them down and harm them. Therefore, the Coalition urges the Commission to enact a universal opt-in mechanism rather than the insufficient opt-out provisions in the Interim Order and existing law and regulations. Customers should not have to overcome a presumption that their personal, private data can be disclosed and disseminated—particularly customers for whom data privacy too often means the ability to remain safe. At the very least, we request that the names, billing addresses, and service addresses of customers be added to the categories of information that customers can restrict release of.

We thank you for consideration of these concerns and welcome further opportunity to participate in the regulatory process.

[13] *See* SSA Publication 05-10093 (December 2005).

Dated: August 4, 2010

Sincerely,

/s/

Nicole A. Lindemyer, Esquire
Policy Manager
Pennsylvania Coalition Against
Domestic Violence
6400 Flank Drive, Suite 1300
Harrisburg, PA 17112
Tel. 717-545-6400
*nal@pcadv.org*