PCADV
Pennsylvania Coalition
Against Domestic Violence
Prevention • Intervention • Change

June 3, 2011

VIA e-FILE

Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
400 North Street, 2nd Floor
P.O. Box 3265
Harrisburg, PA 17105-3265

Re: Investigation of Pennsylvania's Retail Electricity Market
Docket No. 1-2011-2237952

Dear Secretary Chiavetta,

Enclosed please find the Comments of the Pennsylvania Coalition Against Domestic Violence in reply to the questions posed by the Commission in its first phase of its Investigation of Pennsylvania's Retail Electricity Market, referenced above.

Respectfully Submitted,

Laurie L. Baughman
Senior Attorney

Enclosure

Cc: Office of Competitive Market Oversight – ra-OCMO@state.pa.us

BEFORE THE PENNSYLVANIA PUBLIC UTILITY COMMISSION

Investigation of Pennsylvania's Retail Electricity Market	: : :	**Docket No. I-2011-2237952**

COMMENTS OF THE PENNSYLVANIA COALITION AGAINST DOMESTIC VIOLENCE IN REPLY TO THE PUC'S INVESTIGATION OF PENNSYLVANIA'S RETAIL ELECTRICITY MARKET

I. INTRODUCTION

The Pennsylvania Coalition Against Domestic Violence (PCADV) submits the following comments to express its concerns on behalf of the 61 domestic violence programs across the Commonwealth and the thousands of victims and families each program serves.

In reply to the Commission's official investigation into the state of the current retail electricity market, and the potential changes that may be necessary "to allow customers to best realize the benefits of competition,"[1] PCADV asserts that safety for all customers must be at the forefront of any alteration to the current electricity market. To that end, PCADV states the following:

(1) Eliminating or altering default service would have drastic unintended consequences for the safety of victims of domestic violence.

   a. The default system plays an integral role in assisting victims of domestic violence achieve safety during periods of transition by providing stable, flexible service at an affordable rate.

   b. The default system ensures continued safety and privacy for victims of domestic violence by protecting private customer data from compounded risks of exposure.

(2) To ensure the continued safety of victims of domestic violence and other vulnerable populations, the PUC should adopt and implement a comprehensive data protection mechanism – in the form of an affirmative opt-in program – before initiating any transition in the competitive market structure.

---

[1] Joint Motion of Chairman Robert F. Powelson and Chairman John F. Coleman, Jr., Public Meeting, No. 2237952-CMR (Apr. 28, 2011).

Customers cannot realize the benefits of a competitive market under conditions that do not adequately protect their broader interests in safety and, concomitantly, privacy. Therefore, PCADV urges the PUC to proceed cautiously in its assessment of the current markets with a critical eye toward protecting consumer safety.

II. Safety First: Assessing the Unintended Consequences of Eliminating or Changing Default Service

The PUC asks whether there are "unintended consequences associated with EDCs providing default service, and related products, such as time-of-use rates." PCADV believes the current default service system should be retained and that the focus of the inquiry must consider whether there are unintended consequences associated with eliminating the current EDC-provided default service. To that end, PCADV asserts that the consequences of eliminating default service are potentially far-reaching, affecting clear legal protections for victim safety and privacy.

A. Default service allows victims of domestic violence to achieve safety during periods of transition by providing low-risk, flexible electric service at a reasonable rate.

Default service provides consumers, particularly vulnerable consumer groups such as low-income or financially struggling customers, with a valuable choice to maintain their current service at a reasonable rate.[2] Victims of domestic violence are one of the groups that benefit from default service, particularly because it offers a stable, low-risk alternative to shopping for electricity and provides victims with the service flexibility necessary for a successful transition to safety.

Understanding the way batterers coerce and control their victims is an important part of understanding the attendant need for default service. Financial abuse is a common form of coercive control by a batterer. Preventing the victim from working, requiring the victim to turn over earnings, refusing to discuss household finances, collecting the victim's earnings and damaging or selling the victim's property are all examples of how a batterer exercises power and control over a victim.[3] Financial abuse is used in conjunction with other methods of control, including isolation from family and friends, intimidation, and force, to

---

[2] PCADV recognizes that default service is an integral service for many vulnerable populations and recognizes that many victims of domestic violence are also part of other marginalized population groups. Therefore, PCADV echoes the comments of the Pennsylvania Utility Law Project (PULP), the Office of Consumer Advocate (OCA), and the American Association of Retired Persons (AARP) to the extent they highlight the rights of marginalized populations and the government's responsibility to those populations.

[3] Duluth Model, Power and Control Wheel, http://www.theduluthmodel.org/wheelgallery.php; *see also, e.g.*, Jill Davies et al., Safety Planning with Battered Women: Complex Lives/Difficult Choices (Sage Series on Violence Against Women) (1998).

prevent the victim from escaping.[4] Thus, when victims are able to escape, they often are fearful, lack financial resources and are without the support of family or friends. Moreover, the transition period is typically very lengthy; a victim may need to relocate several times – often in the middle of the night – before they can successfully achieve safety.

It may appear that, on its face, shopping for electricity would help victims of domestic violence during periods of transition because it could alleviate some of the financial burden by offering competitive prices. But shopping for an electric supplier is a complicated and time-consuming process requiring cost comparisons and careful examination of varied terms and rates.[5] A customer must have the ability to commit time and energy to this examination, but victims of domestic violence have many more pressing and competing demands on their time and energy. Further, switching suppliers offers no guarantee of savings, particularly in the short term when fleeing victims are most financially vulnerable. Competitive suppliers often come with added costs, early termination fees, and uncertain privacy protections that may not be clear in the supplier's initial offer.[6] Additionally, low-income cost assistance programs are not necessarily available through a market competitor.[7] Victims in transition, whose priority is to achieve safety for themselves and their family, cannot be forced into a market where added fees, disconnection, and lack of public assistance are a possibility.

The only method proven to maintain the consumer protections necessary to continue providing essential electric service to vulnerable populations, such as victims of domestic violence, is to continue to provide default service in its current form. The process for transition to a competitive market may not be as fast as the Commission originally envisioned, but a slow yet purposeful approach to transition which preserves the default system is the only way to achieve a robust market capable of providing all customers with access to electric service without risking the safety of victims of domestic violence and other vulnerable populations.

B. Default service protects the privacy, and therefore provides safety, for victims of domestic violence by protecting private customer data from compounded risks of exposure.

If EDC-provided default service were eliminated, it is unclear what would happen to volumes of customer information. EDC-provided default service protects victims of

---

[4] *See id.*

[5] *See, e.g.*, PA. OFFICE OF CONSUMER ADVOCATE, PA OFFICE OF CONSUMER ADVOCATE'S ELECTRIC SHOPPING GUIDE (2011), http://www.oca.state.pa.us/Industry/Electric/elecomp/ElecGuide.pdf.

[6] *See id.*

[7] Pa. Power Switch, Help Paying Your Bill: Consumer Assistance Program (CAP), http://www.papowerswitch.com/help-paying-your-bill/ (explaining that "CAP customers are able to choose a competitive supplier, but the discount they receive in CAP may be greater than the discounted rate offered by the supplier.")

domestic violence because it ensures victims' data will remain in one place, thereby reducing unnecessary exposure of sensitive private data and eliminating the compounded risk of data breach. PCADV acknowledges that the PUC is in the process of issuing proposed regulations that will monitor electric generation supplier protocols and practices, but the proposed rules are insufficient to counterbalance the risk of data breach. EDCs are trusted entities that have been successfully regulated by the PUC for decades. As it stands, the efficacy of current data-related regulations has been called into question. Regulatory measures to oversee the creation of an eligible customer list – which is to contain only a portion of the information contained in a customer's file – were scrutinized by the Commonwealth Court just this past January when the Court issued a stay to prevent the further dissemination of private information pending conclusion of a suit.[8] Allowing full customer files to be transferred to an EGS, without the affirmative consent of the customer, would unnecessarily expose customers to a potential data breach.

The risk of data breach is not imagined or exaggerated. The Privacy Rights Clearinghouse (PRC), which houses the Chronology of Data Breaches database, reports that over a half-billion private, sensitive records were breached between 2005 and the present.[9] But millions of additional data breaches go unreported each year.[10] Recorded breaches range from health records to police records and everything in between, including utility records.[11] The information obtained by third parties in these data breaches has been used for identity theft; to set up false bank, utility, and credit accounts; and to stalk and/or harass victims of the data breaches.[12] Unfortunately, it is impossible to measure the extent of data breaches in utility companies in the United State: "an astounding 80% of utilities" do not disclose their privacy/data breach risk factors.[13] It would be negligent for the PUC to dismiss the very real threat that increased exposure of public data presents, especially when faced with data that demonstrates the clear threat.

i. Pennsylvania Law and Policy Support Robust Privacy Protections for Victims of Domestic Violence

Eliminating or altering default service without establishing a mechanism for affirmative, informed customer consent[14] would be contrary to various federal and state statutory protections. These statutory protections are grounded in strong public policy that

---

[8] PCADV v. PUC, No. 2712 C.D. 2010 (Jan. 27, 2010) (Order Granting Application for Supersedeas).
[9] PRIVACY RIGHTS CLEARINGHOUSE, CHRONOLOGY OF DATA BREACHES: SECURITY BREACHES 2005-PRESENT http://www.privacyrights.org/data-breach#CP (last updated May 16, 2011).
[10] *Id.*
[11] *Id.*
[12] *Id.*
[13] Jared Wade, *Hiscox Studies Privacy & Data Security*, RISK MGMT., Apr. 22, 2009.
[14] *See infra* section II (discussing the importance of implementing an affirmative, opt-in program for disclosure before sanctioning any transition in the current competitive market).

prioritizes privacy protection and confidentiality for victims of domestic violence and other crimes.

First and foremost, there are a large number of legislative provisions in Pennsylvania protecting the private data of victims of domestic violence and other victims of crime. The Pennsylvania Protection From Abuse (PFA) Act requires courts to prohibit law enforcement, human service agencies, and school districts from disclosing the location of a victim or from furnishing the address, phone number, or other demographic information about the victim or the victim's children.[15] The PFA Act also extends absolute privilege and confidentiality to communications between a victim and a domestic violence service provider.[16] Parallel protections are afforded to victims of sexual assault.[17] The victim holds this right, which can be waived only by the victim's explicit and informed consent.[18] Pennsylvania's Child Custody law also protects against the disclosure of confidential information, including the location of a domestic violence shelter or the address of a victim.[19] Similarly, the Domestic and Sexual Violence Victim Address Confidentiality Act protects a victim's personal information by allowing a program participant to create an alternative address for official and nonofficial purposes.[20] The Act prohibits the disclosure of a victim's actual address, except under certain limited exceptions.[21]

The federal Violence Against Women Act (VAWA), the Family Violence Prevention and Services Act (FVPSA), and the Victims of Crime Act (VOCA) also protect victims from the release of information. Pennsylvania programs, both private nonprofits and government-sponsored programs, receive millions of dollars in federal funds in exchange for their commitment to maintaining victim confidentiality.[22] In particular, VAWA offers a range of data protection for victims. In addition to conditioning grant awards on certifications of ensuring victim confidentiality, VAWA made changes to the rules of evidence, restricted the use of victim data on federal criminal databases, and provided for specific grants for privacy protection. The information subject to strict confidentiality provisions now includes a victim's name, address (home or other physical address), contact information, social security number, and any other information that would "serve to identify any individual."[23]

---

[15] 23 Pa. C.S. § 6112.
[16] 23 Pa. C.S. § 6116; VBT v. Family Servs. of W. Pa., 705 A.2d 1325 (Pa. Super. Ct. 1998), *affirmed* 728 A.2d 953 (Pa. 1999) (holding that the privilege protecting confidential communications between a domestic violence counselor/advocate and a victim of domestic violence "is absolute" and can be waived only by the victim).
[17] 42 Pa. C.S. § 5945.1.
[18] 23 Pa. C.S. § 6116; 42 Pa. C.S. §5945.1(b); VBT, 705 A.2d 1325.
[19] 23 Pa. C.S. § 5336 (formerly 23 Pa. C.S. § 5309(c)).
[20] 23 Pa. C.S. §§ 6701 *et seq.*
[21] 23 Pa. C.S. § 6708.
[22] Violence Against Women Act, 42 U.S.C. § 13925; Family Violence Prevention and Services Act, 42 U.S.C. § 10406; Victims of Crime Act, 42 U.S.C. § 10601 *et seq.*
[23] 42 U.S.C. § 11383(a)(18).

Exposing private data without a sufficiently protective mechanism is also inconsistent with the best practices of United States Department of Energy and the National Institute of Standards and Technology (overseen by the Department of Commerce), which provides that no information may be released unless the customer affirmatively opts to be included in the class of persons wishing to have their personal information released to ECL participants.[24]

ii. Privacy Equals Safety for Victims of Domestic Violence

The risk of exposing private data is a crucial concern for victims and their children. "For a domestic violence victim, the need for privacy is a need for physical safety."[25] Access to personal data of victims of domestic violence facilitates stalking and aids batterers in locating and further harassing their victim. Statistically, batterers who stalk their former partners are the most dangerous and present the highest risk of lethality. In fact, the National Institute of Justice reports that nearly 60% of female stalking victims are stalked by a current or former intimate partner and 75% of women killed by a batterer were stalked prior to their murder.[26] Victims who manage to escape abuse live in constant fear of being found. This fear is exacerbated by the potential for the batterer to easily uncover important information about the victim's location and activities. Eliminating or altering Pennsylvania's current default service, without implementing a comprehensive plan to protect customer information, would expose thousands of customer files to a potential breach and would expose victims of domestic violence to further stalking and harm by their batterer.

Alarmingly, customer files include smart meter data, which – if breached - would reveal real-time electricity usage data capable of predicting an individual's home activities.[27] This is particularly troubling for victims of domestic violence attempting to flee abuse.[28] If a batterer had access to this data, they would not only know the victim's home address, they

---

[24] *See* Dep't of Energy, *Data Access and Privacy Issues Related to Smart Grid Technologies* 9-10 (Oct. 2010) ("[C]onsumers should have rights to protect the privacy of their own [electronic usage data] and control access to it."); U.S. Dep't of Commerce, Nat'l Inst. of Standards & Tech., *Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid* 19-20 (Aug. 2010).

[25] Electronic Privacy Information Center (EPIC), *Domestic Violence and Privacy*, http://epic.org/privacy/dv.

[26] PATRICIA TJADEN & NANCY THOENNES, NAT'L INST. OF JUSTICE, STALKING IN AMERICA: FINDINGS FROM THE NATIONAL VIOLENCE AGAINST WOMEN SURVEY (1998); *see also* Judith M. McFarlane et al., *Stalking and Intimate Partner Femicide*, 3 HOMICIDE STUD. 300 (1999).

[27] *See* David Falchek, *Meter Reading a Dying Job as Companies Convert to Smart Meters*, TIMES TRIBUNE, May 31, 2011, http://thetimes-tribune.com/news/business/meter-reading-a-dying-job-as-companies-convert-to-smart-meters-1.1154918#axzz1NwpC4G00.

[28] *Comments of the Electronic Privacy Information Center (EPIC) on Proposed Policies and Findings Pertaining to EISA Standard Regarding Smart Grid and Customer Privacy, Before the California Public Utility Commission*, Rulemaking 08-12-2009 (Dec. 18, 2008).

would know when the victim was home and could track the victim's movements about the home.[29]

Victims often go to extreme lengths to hide from their batterer, including fleeing across state lines, using post office boxes and unlisted phone numbers, using pre-paid phones to avoid having a phone account linked to their home address, changing social security numbers, relocating to a shelter, and sealing court records.[30] Forgoing electricity service is not something that victims should be expected to do to avoid being located by a batterer.

iii. Federal and State Constitutions Protect the Right to Privacy for Victims of Domestic Violence

The PUC's stated goal for this investigation is to "ensure a properly functioning and workable competitive retail electricity market ... in the state." To achieve a "properly functioning and workable" market that properly balances consumer and commercial interests, the PUC must proceed cautiously to address potentially far-reaching constitutional ramifications. There are compelling privacy concerns attendant to maintaining default customer accounts. To eliminate this consumer option without first establishing a mechanism for affirmative, informed customer consent runs contrary to an individual's right to privacy as guaranteed in the Pennsylvania and United States Constitutions.

Federal Right to Privacy: Avoiding Disclosure of Personal Matters

The federal courts have definitively established a constitutional right to privacy in personal information, including an individual's address. In *Whalen v. Roe*,[31] the United States Supreme Court explained that the Fourteenth Amendment, which guarantees the right to liberty, includes a "constitutionally protected 'zone of privacy'" that protects both "the interest in avoiding disclosure of personal matters and ... the interest in independence in making certain kinds of important decisions."[32]

This federally recognized "zone of privacy" is triggered when an individual demonstrates a "reasonable expectation of *confidentiality*."[33] The Third Circuit Court elaborated on this standard, explaining that "the more intimate or personal the information, the more justified is the expectation that it will not be subject to public scrutiny."[34] The Court provided some additional guidance, finding that there is a "general understanding" that the interest in

---

[29] *See id.*

[30] Nat'l Network to End Domestic Violence, *SafetyNet Project: Comments on Safety Risks of RFID*, http://www.aclunc.org/issues/technology/asset_upload_file625_9490.pdf (last visited May 17, 2011).

[31] *Whalen v. Roe*, 429 U.S. 589, 598 (1977).

[32] *Id.* at 598.

[33] *Paul P. ex rel. Laura L. v. Verniero*, 170 F.3d 396, 401, 404 (3d Cir. 1999) (citing *Fraternal Order of Police v. City of Philadelphia*, 812 F.2d 105, 112-17 (3d Cir. 1987)).

[34] *Id.*

avoiding disclosure of personal matters encompasses an individual's name, address, and other personal identifying information, regardless of whether protection is required by statute.[35]

Pennsylvania's state courts have also addressed the federal right to privacy, as it extends to individuals under the Fourth Amendment. In *Commonwealth v. Duncan*, the Superior Court found that the applicable standard is a reasonable expectation of privacy, plus something more.[36] Applying this stricter Fourth Amendment privacy standard, the *Duncan* Court found that "a person's name and address, by themselves, do not constitute information about which a person can have a reasonable expectation of privacy that society is willing to recognize."[37] However, when coupled with something more, the expectation may be reasonable.[38] In this case, the "something more" is met by the compelling interests of victims of domestic violence and other crimes who must keep their personal information private in order to maintain their personal safety.

If the PUC were to eliminate or alter the current default system, it would have to first institute a system for individuals to give their informed, affirmative consent to the switch. Otherwise, the PUC risks violating the customer's constitutional right to avoid disclosure of personal matters. Individuals have a reasonable expectation that information – including their name, address, usage rates, smart meter data, and other sensitive personal information about their utility accounts will remain confidential. Customers can and do reasonably expect that the information will be used only for the limited purpose for which it was provided to the utility company. Because it is reasonable for a customer to have an expectation of confidentiality in their customer account information, the PUC must obtain explicit, opt-in consent from customers before it eliminates or alters the current default system in a manner that subjects personal customer information to broad disclosure.

Even if the somewhat more stringent standard established in *Duncan* were to apply, the PUC would still need affirmative, opt-in consent from customers before eliminating or altering the current default system. While the *Duncan* court explained that, alone, a personal address or name is not protected, the court recognized that – if coupled with something more – the right to privacy would apply under the Fourth Amendment. The "something more" required to meet his standard would be satisfied by the additional safety risks for battered individuals, others victims of crime, and the shelters or other programs that serve these individuals. Not only is it reasonable to expect that the PUC would not forcibly expose their personal confidential information without their affirmative consent, it is also the law. As discussed below, this information is protected – as a matter of course – for all victims of domestic violence and others (individuals and entities) who are similarly endangered in various aspects of our law.

---

[35] *Paul P. ex rel. Laura L. v. Verniero*, 170 F.3d 396, 401, 404 (3d Cir. 1999).
[36] *Commonwealth v. Duncan*, 752 A.2d 404 (2000).
[37] *Id.*
[38] *Id.*

Pennsylvania's Constitutional Right to Privacy
Pennsylvania's Constitution also prohibits the government from interfering with fundamentally private interests absent necessary and compelling countervailing interests of the government.[39]

It is arguable that the onus for protecting against potential data exposure would not be the responsibility of the PUC, but rather would fall to the distribution and supply companies because they have the ultimate authority over and access to the records. But the Third Circuit, as affirmed by the United States Supreme Court, has clearly held that the action of a private company is considered government action when a regulatory agency participates in, facilitates, or affirms the action.[40] Thus, any action of the Commission to eliminate or alter the existing default service program in Pennsylvania would be considered state action subject to the constitutional constraints discussed above. And, as a result, any record breach resulting from the Commission's instructions to eliminate or alter default service would be considered an action of the government.

III. OPT-IN: IMPLEMENTING RESPONSIBLE MECHANISMS TO BALANCE COMPETING INTERESTS

The PUC should implement an affirmative opt-in method for information disclosure to protect the rights of residential customers, including victims of domestic violence and other crimes, while fostering responsible growth in the electric market.

The PUC asks, in question six (6), "what mechanisms could be employed to transition the default service role..." PCADV opposes any shift in the current default service structure. But in the event that the elimination of the current default service is a foregone conclusion, it is important for the PUC to implement an opt-in method for disclosing any personal account information as part of the transition to this new status quo. Only an opt-in method for information disclosure can ensure privacy protection, safety, and confidentiality for victims of domestic violence. Practically speaking, default service can be altered only if customer files are transferred to another provider. Therefore, to assure an appropriate level of protection for sensitive customer data, default service should be changed only if customers are afforded the right to affirmatively opt-in to any alternative default plan.

First and foremost, switching an individual's default service without their express, affirmative, and informed consent runs contrary to the anti-slamming provisions of the Pennsylvania Utility Code.[41] Choosing to stay with a default service provider is, in and of itself, a choice of service. The purpose of the anti-slamming provisions of the code is to

---

[39] PA. CONST. art 1, §§ 1, 8; *see also Stenger v. Lehigh Valley Hospital Center*, 609 A.2d 796 (Pa. 1990)("Only a compelling state interest will override one's privacy rights"); *Denoncourt v. Commw. State Ethics Comm'n*, 470 A.2d 945 (1983); *Hartman v. Dep't of Conservation & Natural Res.*, 892 A.2d 897, 905 (Pa. Commw. Ct. 2006).
[40] *Jackson v. Metropolitan Edison Co.*, 483 F.2d 754, 757 (3d Cir. 1973), *aff'd* 419 U.S. 345, 357 (1974).
[41] *See* 52 Pa. Code § 64.23.

protect customer's choice for service. Therefore, switching default service providers or eliminating default service altogether, without obtaining the affirmative consent of the customer for the switch, violates the Pennsylvania Utility Code.

Moreover, the PUC is statutorily mandated to obtain customer consent before it can release a customer's smart meter data to a third party.[42] Shifting to an alternative default service provision would require sharing customer smart meter data and, thus, would require the PUC to obtain customer consent from each and every default customer before the service could be switched and the records released. For the sake of consistency, the PUC should require affirmative consent from customers before releasing any customer information.

Empirical data shows that taking a strong stance to protect private customer information, including the adoption of an opt-in policy for any information disclosure, boosts customer confidence and fosters a robust marketplace. Consumers are now – more than ever – concerned with the availability of their private data. A survey conducted by the First Amendment Center in August 2000 revealed that 81% of respondents felt that privacy was "essential" – an increase from 78% in 1997.[43] Consumers by and large expect that their privacy will be protected and support opt-in as a standard for sharing personal data. A Harris Poll conducted by Business Week revealed that 88% percent of respondents supported opt-in as the standard model for sharing personal data.[44] The Pew Research Center's American Life Project poll confirmed these findings: 86% of their respondents preferred opt-in privacy policies.[45]

Before making any move to alter or eliminate the current default structure in Pennsylvania, the PUC must address the current data privacy shortfalls. As discussed above, there is a range of statutory and constitutional protections as well as public policy priorities protecting victims' private information. When these legal and policy considerations are coupled with the regulatory history and consumer trends that clearly favor opt-in methods for data protection, it is clear that the PUC should adopt an affirmative, opt-in disclosure mechanism. An opt-in mechanism for disclosure is the only way to truly respect customer safety and privacy while fostering responsible competitive growth.

IV. Conclusion

PCADV asserts that safety must be the number one priority of any alteration to the current retail electricity market. To that end, it is imperative for the PUC to continue the current

---

[42] 66 Pa. C.S. § 2807(f)(3).

[43] Electronic Privacy Information Center (EPIC), Public Opinion on Privacy: Privacy Polls and Studies, http://epic.org/privacy/survey/ (last visited May 17, 2011) (citing First Amend. Ctr., *State of the First Amendment* (Aug. 2002), http://www.freedomforum.org/templates/document.asp?documentID=16840).

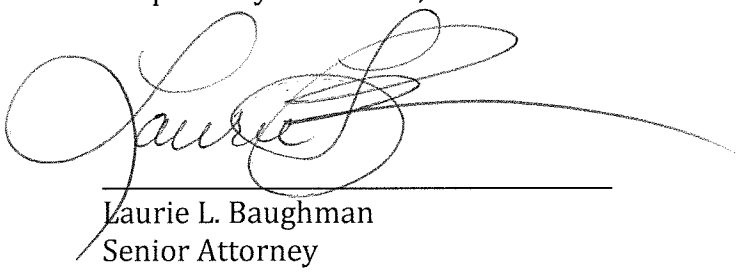
[44] *Business Week/Harris Poll: A Growing Threat,* BUSINESSWEEK (Mar. 20, 2000), *available at* http://www.businessweek.com/2000/00_12/b3673010.htm.

[45] Pew Internet & American Life Project, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules* (Aug. 20, 2000).

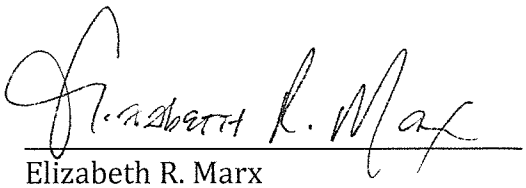
default service plan. Forcing all customers into the open market would have drastic unintended consequences for victims of domestic violence attempting to make the transition to safety. Changing or eliminating default service would add additional burdens on victims who are already resource-strapped, making it difficult for victims in transition between homes. Such a move also has the potential of exposing the personal identifying information of victims of domestic violence in contravention of federal and state laws, constitutional principles, and prevailing public policy across the Commonwealth and the nation.

We thank the Commission for carefully considering our concerns and welcome any additional opportunity to participate in this investigation.

Respectfully Submitted,



Laurie L. Baughman
Senior Attorney
Pa. Coalition Against Domestic Violence
3605 Vartan Way
Suite 101
Harrisburg, PA 17111
717.671.4767
llb@pcadv.org



Elizabeth R. Marx
Staff Attorney
Pa. Coalition Against Domestic Violence
3605 Vartan Way
Suite 101
Harrisburg, PA 17111
717.671.4767
erm@pcadv.org

Dated: June 3, 2011