Pennsylvania Coalition
Against Domestic Violence
Prevention • Intervention • Change

March 22, 2013

VIA e-File

Rosemary Chiavetta, Secretary
Pennsylvania Public Utility Commission
Commonwealth Keystone Building
P.O. Box 3265
Harrisburg, PA 17105-3265

Re: Petition of PECO Energy Company for Approval of Its Smart Meter Universal Deployment Plan, Docket No. M-2009-2123944

Dear Secretary Chiavetta,

Please find the attached comments submitted on behalf of the Pennsylvania Coalition Against Domestic Violence (PCADV) in the above captioned proceeding. PCADV's comments are submitted pursuant to the Commission's Notice to be Published, which indicated that comments to this proceeding would be accepted until close of business today, March 22, 2013.

Thank you for the opportunity to comment in this proceeding. Please do not hesitate to contact me with any questions.

Respectfully Submitted,

Elizabeth R. Marx
Staff Attorney
emarx@pcadv.org
717-671-4767 x. 132

Enclosure

Before the Pennsylvania Public Utilities Commission

Petition of PECO Energy Company for Approval of Its Smart Meter Universal Deployment Plan	: : : :	Docket No. M-2009-2123944

Comments of the Pennsylvania Coalition Against Domestic Violence Regarding PECO Energy Company's Smart Meter Universal Deployment Plan

---

The Pennsylvania Coalition Against Domestic Violence (PCADV) submits the following comments to PECO Energy Company's Smart Meter Universal Deployment Plan (Plan) in accordance with the Commission's Notice To Be Published, which indicated that Comments would be accepted in this proceeding until March 22, 2013. PCADV is very concerned that consumer privacy and data security is not sufficiently addressed in PECO's Plan, which may place consumers at risk of financial or physical harm. PCADV agrees with PECO that the issue is best reviewed as a statewide concern, and not addressed piecemeal as part of individual smart meter deployment plans. However, PCADV cautions that failure to address the issue of data security on a statewide basis prior to approving PECO's Plan would be harmful to public safety.

Inadvertent disclosure of data available through smart meters is particularly dangerous for victims of domestic violence, dating violence, and stalking who may be placed at risk of further financial or physical harm should their real-time or near real-time energy usage become available to third parties without proper security. Domestic violence, dating violence, and stalking are the most personal of crimes, and the more personal information the perpetrator has about the victim, the more dangerous the perpetrator can be. Victims of these crimes face the greatest risk of physical harm and/or lethality after separation, when batterers regularly go to great lengths to re-establish power and control over their victim.[1] In addition to physical assaults and stalking, batterers regularly empty bank accounts, shut off utility services, and cut off joint

[1] PATRICIA TJADEN & NANCY THOENNES, NAT'L INST. OF JUST. & CTRS. FOR DISEASE CONTROL & PREVENTION, EXTENT, NATURE, AND CONSEQUENCES OF INTIMATE PARTNER VIOLENCE (2000); *see also* CALLIE MARIE RENNISON, DEP'T OF JUSTICE, INTIMATE PARTNER VIOLENCE, 1993-2001 (2003).

lines of credit after the relationship ends.[2] When a batterer has access to real or near-real time electric usage data of their victim, such access can facilitate further harassment, stalking, and potentially lethal physical violence because the data can reveal a picture of the victim's daily schedule: when they are home, when they shower, when they do their laundry, etc. As smart meter technology advances, the level of available data will only increase.

PCADV urges the Commission to look closely at both front and back-end data securities to ensure that sensitive smart meter data is adequately protected as smart meters are universally deployed across the state. In PECO Statement No. 1, Michael Innocenzo discussed PECO's cyber and data security plan with respect to back-end data transfer. (PECO Statement 1 at 17-19.) However, he does not explain PECO's plan for user-end data security. This serious omission leaves the question of consumer access to real-time or near real-time smart meter data unanswered, raising significant concern about public safety.

Mr. Innocenzo noted in his testimony that PECO "will continue to meet with interested stakeholders to discuss the safeguarding of smart meter data" and identified that "protecting victims of domestic violence and other related crimes" is a priority for PECO. PCADV has been working with PECO, and looks forward to a continuing dialogue on the issue of data security.

That said, stakeholder discussions - while crucial - may not be best suited to resolve complex privacy and data security issues that impact Pennsylvanians across the state. PCADV strongly recommends that the Commission launch a separate statewide proceeding to establish universal data security standards for both front and back-end data transfer. This recommendation is consistent with Mr. Innocenzo's testimony:

> If the Commission were to decide that a more formal process might be called for, the Company suggests that the Commission consider initiating a statewide proceeding to examine these and other issues surrounding smart meter data security and privacy.

PCADV has been involved in similar stakeholder discussions with each EDC about the need for comprehensive data security plans in conjunction with smart meter deployment. While each EDC has indicated that they recognize the need for security, no consensus has been reached about how to approach the issue. Guidance from the Commission is necessary to resolve the

---

[2] *See* Jill Davies, *Safety Planning with Battered Women: Complex Lives/Difficult Choices* (1998).

issue of smart meter data security in a manner that protects individuals equally in all areas of the state.

Guidelines from the National Institute of Standards and Technology (NISTIR) and the United States Department of Commerce on smart meter data security provide the following conclusions based on a comprehensive study of smart meter data and privacy:

1. The evolving Smart Grid technologies and associated new types of information related to individuals, groups of individuals, and premises may create ***privacy risks and challenges that are not fully addressed or mitigated by existing laws and regulations*** with regard to energy consumption, energy generation, billing, third-party Smart Grid applications data, and other related Smart Grid data.
2. New Smart Grid technologies, particularly smart meters, smart appliances, and similar types of endpoints, may create new privacy risks and concerns that may not be addressed adequately by the existing business policies and practices of utilities and third-party Smart Grid providers.
3. ***Utilities and third-party Smart Grid providers need to follow recognized privacy practices in a consistent and comprehensive fashion to effectively safeguard Smart Grid personal information and consumer privacy.*** Existing policies should be evaluated and revised, as required.[3]

NISTIR's conclusions are instructive, and strongly support the need to have the issue of smart meter data security addressed on a statewide level.

PCADV is grateful for the opportunity to comment on this important issue, and urges the Commission to take action on smart meter data security to protect consumers from the financial and physical harm.

Respectfully Submitted,

Elizabeth R. Marx, Esq.
Pa. Atty. ID: 309014
emarx@pcadv.org
717-671-4767, x.132
On behalf of:
The Pennsylvania Coalition Against Domestic Violence
3605 Vartan Way, Suite 101
Harrisburg, PA 17110

Dated: March 22, 2013

[3] NAT'L INST. OF STD. & TECH., GUIDELINES FOR SMART GRID CYBER SECURITY: VOL. 2, PRIVACY AND THE SMART GRID, at 39-40 (Aug. 2010), *available at* http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf.