



Realtime community "Leading the Conversation" **IT Compliance**

WE BLOG DIGITAL LIBRARY PODCAST *Resident Editor: Rebecca Herold*

NOW AVAILABLE:



« [6 Critical Factors for Effective Information Security & Privacy Policies | Main | CEs and BAs: Be HIPAA/HITECH Compliant Or Pay A Hefty Penalty](#) »

Smart Grid Privacy: Laws and Implications

I was recently asked several questions about my work with the NIST Smart Grid privacy group and associated issues. Here are a couple of those questions, and my answers to them...

Question: Are there any laws or regulations that would govern utilities' use of personally identifiable information?

Actually there are many laws and regulations that could apply. Our NIST Smart Grid privacy group is actively researching, through our connections with NARUC and other utilities organizations, all the types of state laws that may exist which govern how utilities, or any other entity with access to Smart Grid data, may use the associated PII.

A topic that is important and interesting to think about is how non-PII data items, when combined with certain other non-PII data items, can actually become PII. In other words, aggregating non-PII to form PII. A collection of data items that, when each individually is not considered, could become PII and reveal insights into personal lives and activities. For the sake of our discussion I'll call these "multi-part PII."

Because consideration of the concept of multi-part PII is so new, I'm not aware of any law that governs such "new" types of PII. Plus, there is no comprehensive data protection law or regulation within the US that will protect all types of PII in all ways.

Much also depends upon any privacy policies that the utilities, or the other smart grid entities, have published or posted. The entities involved certainly must follow their legally binding privacy policies under Section 5 of the Federal Trade Commission Act, which prohibits unfair and deceptive practices. If an organization makes a promise within their posted privacy policy and then does not follow through with implementing business practices and tools to support those promises, then they could be seen by the FTC as being deceptive and unfair under the FTC Act. The FTC has applied sanctions using the FTC Act many times against organizations who didn't keep their privacy policy promises. So this could govern certain activities involving smart grid PII, and perhaps even multi-part PII, depending upon how the policy is worded.

Because of the complexity of the smart grid, and the many different types of organizations/businesses/vendors that will be part of this vast energy management network, there are many other possibilities for U.S. laws, regulations and standards that could apply as well. A few of these include:

- The Computer Fraud and Abuse Act
- Electronic Communications Privacy Act
- Gramm Leach Bliley Act and supporting rules
- At least 48 state and territory breach notice laws
- Federal Rules of Civil Procedure (eDiscovery Rule)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standard
- Title XIII of the Energy Independence and Security Act of 2007

There is also the pending Cybersecurity Act of 2009 bill (S.773) that may be enacted and should be kept in mind.

And, since portions of the smart grid may go into Canada and Mexico, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and Mexico's Federal Freedom of Information Act (FOIA) may also apply.

And there are likely many others not listed here. We are still exploring those possibilities.

Question: Do you see this issue have broader implication beyond utilities and consumers?

Yes, there are going to be many entities initially involved with the smart grid who are neither a utility or consumer, such as the meter vendors. History shows that when opportunities arise, there are many types of businesses and organizations that will take advantage of those opportunities to gain market share for their products. to do

SEARCH

MOST ACTIVE POSTS

- » [CEs and BAs: Be HIPAA/HITECH Compliant Or Pay A Hefty Penalty](#) **comments (2)**
- » [Movies and TV Shows to Use for Infosec and Privacy Training and Awareness](#) **comments (1)**
- » [5 Common, Dumb and Dangerous Privacy Assumptions](#) **comments (2)**

LIBRARY RESOURCES

- » [Realtime Essentials Series](#)
- » [Realtime eBooks](#)
- » [Rebecca's Upcoming Speaking Dates](#)



Recommended Download

PC Magazine Editor's Choice - Best AntiVirus
Free Virus, Spyware, Adware, Trojan, & Rootkit Scan
Rated 5 Stars by Industry Experts



www.dctools.com

Ads by Google

RECENT POSTS

- » [CEs and BAs: Be HIPAA/HITECH Compliant Or Pay A Hefty Penalty](#)
- » [Smart Grid Privacy: Laws and Implications](#)
- » [6 Critical Factors for Effective Information Security & Privacy Policies](#)
- » [Who Are Your Business Associates?](#)
- » [HIPAA/HITECH Etc. Retention: Does Your Reality = Your Requirements?](#)
- » [Proposed HIPAA Privacy Rule Change Explicitly Makes Genetic Info PHI](#)
- » [Privacy For The Deceased](#)
- » [10 Smart Grid Consumer-to-Utility Privacy Concerns; Are There More?](#)
- » [Don't Throw Your Privacy Out The Window; Know How Your PII Is Used](#)
- » [How To Do Privacy Impact Assessments](#)

CATEGORIES

- » [Government](#)
- » [Identity theft](#)
- » [Information Security](#)
- » [Laws & Regulations](#)
- » [Lost & Stolen Laptops](#)

FEATURED RESOURCES:



REALTIME COMMUNITIES

- » [Messaging and Web Security](#)
- » [Unified Communications](#)
- » [Vista](#)
- » [Windows Server](#)

NEWSLETTER

Email Address:

MONTHLY ARCHIVES

- » [October 2009](#)
- » [September 2009](#)
- » [August 2009](#)
- » [July 2009](#)
- » [June 2009](#)
- » [May 2009](#)
- » [Complete Archive](#)

RSS

- » [FEEDBURNER](#)
- » [PODCAST](#)
- » [iTUNES](#)

ASK THE EXPERT

Have a question for our resident expert? Email your questions to Rebecca.

a wide range of research (such as for product development, consumer activities, and so on), to do criminal investigations, and so many other types of activities.

Just consider the Internet. It evolved from a very early type of small scientific research network for the U.S. Department of Defense network in the early 1960's. Their small closed network evolved into ARPANET in 1969. ARPANET quickly grew, and publicly available services appeared in 1979 when CompuServe offered personal computer users email and other types of communications paths. Once the public was able to get access, innovations and advances occurred at an even greater speed, and by 1992 ARPANET had evolved to the infant of the Internet we know today. Look at all the great benefits the Internet has provided. Look also at all the types of cybercrime and privacy breaches that have occurred because privacy protections were not built into the Internet as it evolved. Just think; the Internet grew as computer technologies were evolving.

Now consider the smart grid. It is another type of network which will be a huge interconnected network from the very start. It will basically skip infancy and adolescence and leap right into full functioning adulthood from the very start. It will have advanced technologies from the very start. It took the Internet a few decades to get to the point where entire online industries were formed, and entirely new types of privacy breaches, cybercrimes and frauds emerged. It will take a fraction of that time for new businesses, services and products to emerge to take advantage of this new network of energy use data.

It will also take a fraction of that time for new types of security exploits and privacy breaches to emerge, with no comprehensive laws currently existing that are specific to such new misdeeds. And then imagine the possibilities of merging the smart grid with the Internet. It will happen quickly, and perhaps at the get-go.

It is important that we consider all the possible and imaginable privacy issues now so we can foresee the problems before they happen, and then establish the standards and rules to help prevent them from happening. Such a task is, indeed, large and challenging. However, that is what makes the work that the NIST Smart Grid privacy group, along with the work of the NIST Smart Grid information security group, so important. My hope is that we can clearly identify and communicate the concerns, and then help to establish effective rules to ensure privacy protections are built in from the very beginning while the smart grid is still in the embryonic stage.

Tags: [awareness and training](#) [information security](#) [IT compliance](#) [IT training](#) [NIST NISTIR 7628](#) [personally identifiable information](#) [PIA](#) [PII](#) [policies and procedures](#) [privacy impact assessment](#) [privacy law](#) [privacy training](#) [security training](#) [Smart Grid](#)



Posted by Rebecca Herold on October 21, 2009 12:07 PM | [Permalink](#)

TrackBack

TrackBack URL for this entry:
<http://www.realtime-itcompliance.com/type/mt-tb.cgi/1048>

Post a comment

(All comments are approved by site leader before appearing here. Thanks for commenting!)

Name:

Email Address:

URL:

Remember personal info?

Comments: (you may use HTML tags for style)

- » [Miscellaneous](#)
- » [Non-compliance Sanctions Examples](#)
- » [Podcast](#)
- » [Privacy Incidents](#)
- » [Privacy and Compliance](#)
- » [Training & awareness](#)

REBECCA HEROLD'S BIO:

Rebecca Herold, CISSP, CIPP, CISM, CISA, FLMI, has been providing information security, privacy and regulatory assistance and services to organizations from a wide range of industries for the past two decades. Rebecca was instrumental in building the information security and privacy program while at Principal Financial Group, which was awarded the CSI Information Security Program of the Year Award in 1998. IT Security ranked Rebecca as one of the top 59 IT security influencers, and Computerworld put Rebecca their list of the world's best privacy experts and on their list of the best privacy consulting firms in both 2007 and 2008. Rebecca has been CPO for two consulting organizations, and has had her own information privacy, security and compliance business since 2004. Rebecca has written chapters for several books, dozens of articles, and has been writing a monthly privacy column for the CSI Alert newsletter since the beginning of 2001, and is working on her 13th book. Some of her other books include The Privacy Papers, Managing an Information Security and Privacy Awareness and Training Program, The Definitive Guide to Security Inside the Perimeter (Realtime Publishers), The Shortcut Guide to Improving IT Service Support through ITIL (Realtime Publishers), and The Practical Guide to HIPAA Privacy and Security Compliance. In addition, Rebecca is the leader of The Realtime IT Compliance Community where she posts to her IT Compliance weblog. You can contact Rebecca at: rebecca_herold@realtimepublishers.net.

[CONTACT US](#) | [PRIVACY POLICY](#) | [FAQ](#) | [ABOUT US](#) | [TERMS OF USE](#)