

August 5, 2010 NIST Smart Grid Privacy Subgroup Meeting Notes

Minutes by Rebecca Herold

Please send this distribution list any necessary corrections or additions.

Next full group teleconference meeting:

Thursday, August 12, 2010 at 11:00am est

Erika McCallister, acting CPO for the Department of Commerce, and Scott Mathews, also from the Department of Commerce, attended our meeting to represent their views of, and concerns with, our privacy chapter draft.

Here are my summary notes from Thursday's meeting:

1) **Rebecca provided overview of the privacy subgroup's work to date, our work on the current draft of the privacy chapter, and the reasons why we included the information and topics within the current draft.**

- See our current privacy chapter draft at

http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/NISTIR7628v1July2010/draft-nistir-7628_vol1_final.pdf

- *NOTE: Some of our group members contacted me directly following our meeting, asking if I could send them notes for the overview I provided, so I'm including them here for the benefit of all who may be interested.*
- Creating this chapter has been a truly collaborative process based upon establishing as much of a consensus among our very diverse group members as possible after thoughtful discussion and consideration of all perspectives for the very wide range of privacy issues involved.
- Because of time restraints associated with the nature of having an all-volunteer group project, we focused on the privacy issues related to residential use. We recognize that there are also privacy issues that must be considered for business locations. This is on our list of topics to tackle for the next version of the NISTIR, if there is another version.
- We do not view the privacy chapter as it exists now to be a stopping point. It is a beginning point to continuing the work to improve upon security and privacy practices as the Smart Grid continues to evolve. NIST has indicated in the past that they would like for us to continue our work and provide updates for future versions; so this was also taken into consideration.
- We've included a 2-page Chapter Abstract to summarize the main points within the privacy chapter. This was first created as an Executive Summary, requested by several of our privacy group members from the utilities and third party vendors to use to be able to give to their executive management to more easily and quickly read than the full chapter.
- We included a discussion of privacy and what this nebulous concept means. Over the past year it is clear that the members of our group, like the public in general, have very different opinions about what privacy really means. We are writing this chapter for a very wide range

of readers, including not only consumers, but very importantly the utilities and Smart Grid vendors who will be creating various components of the Smart Grid. Some think that privacy is just about protecting the confidentiality of a very limited set of personal information items. Others believe that it is just about complying with existing privacy laws. Yet others believe it is about using personal information in a very wide range of circumstances, and so on. With all these readers in mind, and based upon feedback and discussions with many different people in a wide range of venues, it became clear that it was important to include a discussion of privacy in general, and then describe how we are addressing it within our chapter. This is important to establish the basis for the information in the rest of the chapter.

- We have also included an appendix, which we refer to at the beginning of the chapter, with definitions of the privacy terms we are using within the chapter so that we can level set, for all our readers, the ways in which we are using privacy terms within the chapter. By defining privacy-related terms, such as "personal information" and "personally identifiable information," we can clarify, compared to the past drafts, what we mean by these terms within our chapter discussions and information.
- We've included a "Legal Frameworks and Considerations" section. This is an extremely important section to address the many ongoing questions and comments by diverse groups regarding the current legal protections that exist, or don't exist, with regard to the information that will be within the Smart Grid. It does not represent, nor claim to be, formal legal opinion. However, it is a carefully written and thoughtful discussion that addresses some of the many legal issues related to privacy that, not only group members, but others we talked to over the course of the past year, many that have been talked about and have been reported in the news over the past year. We've spent much more time on writing the section this time to help ensure it can be in the published version. We had a subgroup meeting separately and working on this portion of the chapter for several months. This group included lawyers, folks who have participated in creating state level (e.g., Massachusetts) privacy laws, folks from the utilities, and representatives from privacy groups.
- We've kept the PIA description and results that was the starting point for our work last year. However, we've clarified some of the ways in which the information, findings and recommendations are worded to make it more meaningful to utilities and Smart Grid vendors, in addition to helping to provide an example of the type of PIA that utilities and vendors are recommended to do.
- We've drastically rewritten the section describing the wide range of privacy concerns within the Smart Grid, including adding discussion for such things as personal electric vehicles, wireless issues, issues with public Internet sites just to name a few, as they apply to residential use. We also had another subgroup that met separately over many months, working on this section to communicate these issues in understandable ways, and provide information in some great informational tables that I anticipate many different types of players involved in the Smart Grid will be using. As with the group working on the legal issues, this group had representatives from the utilities, privacy groups, universities, and so on.
- We've added a section about how to address as many privacy concerns as possible by building privacy controls into the processes and architecture that makes up the Smart Grid. One of the tools we've provided a description for, and also provided a couple of examples for how to use within an appendix, is the privacy use case. Another subgroup met separately for this and spent a large amount of time trying to figure out the best way to approach these use cases. We finally based our privacy use case scenarios upon the OECD privacy principles for multiple reasons, but generally because we used the OECD principles for the PIA, they are long-established and widely recognized, they are freely available, they form the basis of most data protection laws throughout the world, and they are straight-forward concepts that will be more easily and consistently utilized when the architects and engineers, who will be a significant portion of those using our chapter, are building privacy controls into processes.

I've found that most business leaders want to know if their information security and privacy investments are required for compliance, and since most world-wide data protection laws and regulations, including those in the U.S., use the OECD privacy principles as a basis of the requirements, it made sense to use the OECD privacy principles to also be able to demonstrate due diligence with most regulatory compliance requirements in the process.

- We've provided a chapter summary that includes our group's recommendations to date. This wraps up the details earlier in the chapter that are important to include for those readers who will actually be implementing the privacy protections, into one area for quick reference, as well as communication to the business leaders benefit from such summaries.
- One of the recurring statements heard over the past year from utilities is that existing laws, particularly those specific to energy regulations, probably already address privacy. Besides going through this topic within the legal frameworks discussion we've also provided an appendix to serve as a reference of a large number of the current Smart Grid and electricity delivery regulations.
- Implementing the right controls depends upon thoughtful consideration of all the issues involved. This makes using good, representative privacy use cases, and performing PIAs, so important.
- We created this chapter to provide guidance and recommendations in a way, not previously available, that will help the wide spectrum of entities, at all levels of organizations, involved with implementing the Smart Grid. And addressing the issues we've identified.
- We wrote the chapter to not only look at the past and present, but also look at the future for potential privacy concerns. The Smart Grid is a new type of network, so we cannot limit ourselves to looking backwards. Indeed, one of the goals was to look forward, based upon current Smart Grid activities and plans, to the possible types of privacy problems that could occur if protections were not established up front.
- We are not a political group, and we did not perform our activities with politics in mind. We remained focused on the Smart Grid and did not look to the other types of political activities that were occurring, such as proposed bills, when we were doing our work. In fact, NIST advised us not to take such outside political activities into consideration or refer to them within our report.
- It is important for the NIST internal reviewers to also keep in mind that our group members volunteered their own time, several literally hundreds of hours each, working on this chapter. This in addition to all their other paying job responsibilities. We are all doing this because we all strongly believe in the importance of protecting privacy within the Smart Grid from the very inception of the Smart Grid and going forward. And we want to do all we can to make sure privacy is addressed appropriately from a practical manner, not a political manner.

2) **Open Forum Discussion of Concerns About Current Privacy Chapter: Internal NIST Reviewers & Group Members**

- Scott Mathews described some of his opinions and concerns with the current draft of the privacy chapter. Some points made include:
 - It is a long chapter.
 - There are some areas that don't need to be in the chapter. E.g., discussion of PEVs.
 - The effect of covering these extraneous areas and topics is that it confuses the issues. Gives the chapter a lack of focus.
 - Several areas where information is repeated.
 - Would have liked to have seen a discussion of consent and choice, as well as opt-in and opt-out.
 - Many areas need more direct discussion of how they are unique.

- Definitions and terms are not that accurate. E.g., discusses how PII is defined within the MA breach notice law.
- Does not see this document being read by the general public. More in the professional consulting business realm to start with.
- Large concern about this document not being consistent with other government initiatives.
- Erika McCallister described some of her concerns with the current draft of the privacy chapter. Some points made include:
 - Written quite differently from anything that NIST would publish.
 - Some material is repetitive. For example, that the Smart Grid data is granular; this was stated 14 times.
 - The legal issues section should just be a listing of laws with no discussion provided.
 - There are many factual errors and inaccuracies throughout, such as the information about the Massachusetts law.
- Bill Hunteman from DoE provided some input:
 - Indicated that the document would be very useful as a Department of Energy document.
 - Would it make more sense to take the privacy chapter into a DoE document and leave the summary materials in the NIST document?
 - Fix factual inconsistencies. Will that work for getting it into the publication?

3) To-Do's / Assignments

- Marianne must have the final version of the NISTIR published by August 31st that contains a Privacy Chapter or Volume.
- Erika and Scott will get redlines of the factual inaccuracies and errors (as opposed to high level comments, and nothing about restructuring) in the current draft of the privacy chapter to the group by next Wednesday (if at all possible).
- The privacy group will provide an upfront preface/paragraph, that states our privacy chapter is a starting point, consensus document, etc. *NOTE: On Friday Rebecca and Christine Hertzog drafted a couple of preface paragraphs for the group to consider putting at the front of the privacy chapter per Marianne's direction.*
- The current plan will be to complete the easy fixes, for errors and on tone and intent; and provide assurance to Erika through the new Preface paragraph that this will not be the only final version.

Thanks,

Rebecca