

4/13/2012 – NIST Smart Grid Privacy Subgroup Meeting

Attendance:

- Rebecca Herold – Lead – The Privacy Professor
- Amanda Stallings - PUCO
- Peter McGee - FTC
- Tanya Brewer – NIST
- Christine Hertzog – SG Library
- Krystina Schaefer – PUCO
- Ruth Yodaiken – FTC
- Maryann Ralls – NRACA
- Paul Zumo – EMBDA
- Aryeh Fishman – EEEI
- Ward Piles – Southern Company
- Dan Francis - AEP
- Lynette Horning Cobus - Northrup Grumman
- Brent Struthers - Neustar
- Chris Villarreal - CPUC
- Steve Daugherty – IBDE
- Ken Wacks – GridWise
- Tim Shekel – University of Colorado

- ✓ *Guest Speaker – Peter McGee – Asked to give some background on FTC Privacy Report.*
 - In the Fall of 2009-March 2010, Committee held a series of WS's to examine consumer privacy that covered new technologies. A growing recognition of gaps or limitations in the way the FTC's historic approach to consumer privacy coupled with new business models and new technology (cloud computing, mobile usage, social media, etc.) Wide public participation – over 200 participants in 3 round-tables. Consumer advocates, academics, governments (both US and European) all participated.

Topics Discussed:

- Benefits and risks
- Consumer expectations
- Adequacy of existing regulation
- Privacy existing technologies
- How to treat data

- New business models allow companies to see monetary value from collecting data. Workshop also touched on how to control data collection and usage. A real interest right now is that consumers are concerned about how their data is released. The workshop also discussed significant benefits that come out of data collection and use. Finally, the FTC noticed there was a decreasing relevance of a distinction between labeling information as personally identifiable or non-personally identifiable. Anonymous bits of information can be combined to show particularly detailed info about consumers.
- The FTC staff developed and published a prelim privacy framework out of RT discussions. Set up a number of questions about framework that solicited public comments.

Framework includes 3 components:

- Companies should develop privacy by design
 - A call for companies to simplify consumer choice mechanisms
 - Public Policy, law enforcement and internal ops
- Development of do-not-track mechanism – allows consumers to control what information is being collected while they are online.
- The framework calls on companies to offer meaningful choice mechanisms to consumers.
- A call for increased transparency in data collection. Consumers should know what information is being collected and how it is used.
- In response, FTC received 450 comments, of which half came from individual consumers. The majority of consumer comments supported a do-not-track mech.
- After getting the comments in, staff analyzed the comments, synthesized them and made changes to prelim framework. Final privacy framework is now Commission framework, not a Staff report.
- FTC calls on Congress to name a baseline privacy legislation that is not focused on any one industry. Should be based on FIPPs. If we have such a law that is going to provide a greater certainty for businesses and build consumer trust; trust that will benefit all parties involved.
- FTC also made changes to scope and created a carve-out for small business exception. Also discusses how to de-identify data. Also discussed practices that don't require consumer choice.
- There is some discussion in the report about the concept of companies of anonymizing data. FTC states that if company collects data either anonymously or anonymizes the data later and commits to re-identify data or IF they transfer data onto 3rd parties, require downstream 3rd parties to commit to the same, that data would be taken out of scope to FTC framework (i.e. not required to follow further guidelines).
- If co takes steps to de-identify data for SG, would not be committed to seek permission for collecting data.

- As analytics power changes, changes what's important. There are many more ways to discover identity and activities than ever before. FTC framework is helpful to provide guidelines for protecting consumer privacy.
- Cites AOL issue where folks could take anonymized data, add data to it, and track back to specific people. Also cites Netflix releasing anon data about consumer movie practices. Researchers were able to add a database and trace movie data back to specific customer. FTC is trying to prevent these scenarios from occurring again.
- For more information and to view the framework, please visit:
<http://www.ftc.gov/opa/2012/03/privacyframework.shtm>
- ✓ **Reminder:** We are having our f2f meeting at the Neustar facility on April 25-26. This is a 1.5 day workshop for **all** CSWG subgroups. This f2f will give us a chance to meet and discuss the upcoming NISTIR update. It will also give us a chance to see how our work in each of the subgroups is linked to, or aligns with, other CSWG subgroups. Currently we have eight active subgroups. If interested in attending or for more information, please contact [Tanya Brewer](#) to get more information or visit the CSWG Twiki.
 - **There will also be dial-in capabilities if you are unable to attend.** Information will be posted as it is received.

Team Updates:

PEV Team – No update. Need to flesh out the outline.

NSTIC Team – have begun meeting every other Wednesday to discuss NSTIC's progress thus far and what it means to the CSWG Privacy subgroup. Currently looking for guest speakers to come talk with us about NSTIC capabilities and possible concerns for smart grid functionality.

Training & Awareness – met Monday to do some final clean-up of Consumer slides. Will send those to Marianne for review. During our discussion on Monday, looking at consumer slides and talking about other groups involved in SG as identified on Privacy twiki, determined that institutional group would have the need for same information as consumers. Slide-set for consumers will also apply for institutions with some exceptions. With the contracted agents, those really need to be covered under utilities. The groups that were commercial and non-institutional (i.e. data centers, industrial sites, etc.) as we've determined over the years that while they do have confidential information, not a lot of privacy issues involved. Hence, we probably won't need to create slides specific to them. If they want to look at consumer slides for information, more than welcome. Points out difference between confidentiality and privacy – not the same. 3rd parties – going to wait to create slide sets until 3rd party teams release their recommendations so we can reference them in the training slides. Some time later today, there will be a message with the consumer slide set contained.

Third Party – Hope to be done with 3rd party recommended practices next week. Running through areas that Tanya thought needed to be fixed. Will hopefully hand off to full privacy group next week.

REQ 22 – going to have a meeting today at 2:00pm. We haven't made any progress since last privacy meeting. Still trying to get organized on REQ 22. May need an extension on availability of NAESB standards to complete the project.

Privacy Use Cases Team – received more feedback – thank-you. Are in the process of mapping the feedback against the existing content. Starting the process of incorporating comments into the documentation. Process of going through comments – chunking out project into manageable tasks for volunteer team to accomplish. We received interesting feedback from Canada Commissioner nothing that this look like a great effort to help supplement activities and overall arching guidance on how to develop utility use cases. Some other things focused on- how to create final document. Create an appendix that incorporates all raw feedback. Plotting out the mapping of how responded to feedback. Need to make task manageable. After all feedback is incorporated, bring it back to the group for one more round of final comments.

ANYTHING NEW:

A few articles referring to concerns of hackability of smart meters. This has obvious implications for privacy protections. Are these re-emergents of older news? A lot of reports seen is related to a de-classified FBI report and discussed with news outlets. Dealing with information that is about three years old. Especially with the magnet issue – dates back to stuff utilities have been dealing with for 10-20 years. “Hacking” – it was an issue that was dealt with and investigated by FBI about 3 years ago. This issue does not occur on newer technology – occurs on older meters that had optical port that was not secure. The article in question was more related to defrauding the meter readings rather than a critical infrastructure takedown.

Our next full group meeting will be Friday, April 27th.